Autoritat Catalana de Protecció de Dades

Dictamen en relació amb la consulta formulada en relació amb els riscos que per als drets i llibertats de l'alumnat, professorat i resta de persones presents als centres educatius pot comportar l'ús lectiu i no lectiu dels telèfons mòbils.

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta en què es demana un dictamen a aquesta Autoritat sobre els riscos que per als drets i llibertats de l'alumnat, professorat i resta de persones presents als centres educatius pot comportar l'ús lectiu i no lectiu dels telèfons mòbils des del punt de vista del compliment de la normativa de protecció de dades personals.

Segons la consulta, aquesta s'emmarca en el procés consultiu sobre l'ús del mòbil als centres educatius que ha endegat el Departament d'Educació, i s'acompanya de còpia de Document 4/2023, *"La regulació de l'ús dels mòbils als centres educatius"*, aprovat pel Consell Escolar de Catalunya en sessió plenària del 12 de desembre de 2023 (en endavant, document 4/2023).

Analitzada la consulta, vista la normativa vigent aplicable, i d'acord amb l'informe de l'Assessoria Jurídica es dictamina el següent:

I

(...)

II

Segons explica la consulta, el Departament d'Educació ha endegat un procés consultiu sobre l'ús del telèfon mòbil als centre educatius. S'exposa que, durant el dit procés s'han suscitat diversos debats amb participació de les famílies, docents, directors i alumnat i que, finalment, el Consell Escolar de Catalunya, com a òrgan consultiu, hauria adreçat al Departament la proposta de prohibir l'ús del telèfon mòbil a les escoles i restringir-lo als instituts.

La consulta explica que s'hauria ordenat crear un marc regulador general que estableixi els criteris d'ús del mòbil que totes les escoles i instituts de Catalunya hauran de complir a partir del curs vinent. Segons la consulta, tot plegat ha de servir perquè, seguint les directrius generals del Departament, el curs 2024-2025 tots les centres hagin regulat l'ús d'aquests aparells segons el seu projecte educatiu i els acords presos per la comunitat educativa corresponent.

En aquest context, es sol·licita un Dictamen sobre ***"els riscos que per als drets i llibertats de l'alumnat, professorat i resta de persones presents als centres educatius pot comportar l'ús lectiu i no lectiu dels mòbils des del punt de vista del compliment de la normativa de protecció de dades personals."***

III

Situada la consulta en aquests termes, cal partir de la base que, segons l'article 4.1) del Reglament (UE) 2016/679, de 27 d'abril, general de protecció de dades (RGPD), són dades de caràcter personal *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".*

Per tant, d'entrada, qualsevol informació que identifiqui directa o indirectament a persones físiques, com ara les que formen part dels col·lectius a què es refereix la consulta, en concret, la que es pugui tractar arran de la utilització de telèfons mòbils a l'escola, és dada personal, i queda protegida pels principis i garanties de la normativa de protecció de dades (RGPD i Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades personals i garantia dels drets digitals (LOPDGDD)).

Com es desprèn no només de la consulta, sinó també del Document 4/2023, del Consell Escolar de Catalunya, és clar que en el moment actual existeix una creixent preocupació a l'entorn de la utilització en l'àmbit escolar -principalment per part de l'alumnat, però també per part dels propis centres i del professorat-, de les diferents tecnologies digitals, smartphones, dispositius diversos, Internet, apps, xarxes socials, etc, que el mercat posa a disposició de la ciutadania.

Apuntem que al llarg del dictamen, sovint ens referirem no només al "telèfon mòbil" sinó a xarxes socials, eines digitals emprades en l'àmbit educatiu, continguts d'Internet, etc). Això és així perquè, d'entrada, la utilització d'un telèfon mòbil, en sí mateix, no ens permet valorar els riscos associats, si no tenim en compte que, sovint, és la utilització del mòbil com a eina d'accés a Internet, com a vehicle per instal·lar i utilitzar apps -algunes d'elles, inadequades per a menors-, etc, el que en determinarà el risc.

No s'entendria, doncs, una anàlisi de "riscos d'utilitzar el telèfon mòbil", si no fem una aproximació més àmplia en aquest sentit.

En qualsevol cas, als efectes d'aquest dictamen, el concepte de "xarxa social" que utilitzem en aquest dictamen és ampli, és a dir, qualsevol servei que mitjançant un dispositiu tipus ordinador, telèfon intel·ligent o tauleta que es connecti a Internet, permet comunicar-se amb tercers, compartir informació (textos, fotografies, sons, vídeos...) i crear grups de persones amb interessos comuns (grups de Whatsapp d'alumnes, etc).

Com es desprèn de la consulta, existeix en la societat una clara preocupació pel fet que la utilització del telèfon mòbil dins l'escola pot comportar un tractament de la imatge, de la veu, i d'altres dades personals, de diferents col·lectius (no només els alumnes, sinó també dels professionals que formen part de la comunitat educativa), i pel fet que això pugui suposarà un risc per a determinats drets fonamentals.

Així, no només la protecció de dades personals (art. 18.4 CE i art. 156 EAC), sinó altres drets igualment mereixedors d'una protecció reforçada, en la seva qualitat de drets

fonamentals, com ara els drets a l'honor, la intimitat personal i la pròpia imatge (Llei orgànica 1/1982, de 5 de maig), o la normativa de protecció de drets de la infància i l'adolescència.

En aquest punt, i vistos els termes generals de la consulta, també hem de fer una acotació, respecte els col·lectius afectats als que es refereix la consulta:

La consulta pregunta pels riscos de la utilització del mòbil "per l'alumnat, professorat, i altres col.lectius"). Òbviament, com a exemple, quan en aquest dictamen ens referim als riscos de difondre dades personals de terceres persones sense habilitació (imatge, dades identificatives, dades de categories especialment protegides *ex. art.* 9 RGPD, dades socio econòmiques, etc), des del punt de vista de la protecció de dades és clar que el risc és el mateix, ja es tracti de difondre dades d'un professor, o d'un altre professional amb presència habitual al centre, o d'un alumne.

Dit d'una altra manera, en principi, el risc que deriva d'un mal ús de les xarxes socials, és equiparable independentment de quina sigui la persona afectada, al menys, des de la perspectiva de la protecció de dades, que és el que correspon analitzar en aquest dictamen.

Això, sens perjudici que, com veurem a continuació, l'ordenament jurídic estableix una especial cura entorn dels menors d'edat, i que les conseqüències o responsabilitats jurídiques d'una mala gestió del risc o d'un mal ús de la informació personal d'un afectat, pugui ser diferent en funció de les persones implicades.

Com ha fet avinent aquesta Autoritat abastament, els menors d'edat són un col·lectiu especialment protegit per l'ordenament jurídic, i això es tradueix, en matèria de protecció de dades, també en una protecció reforçada. Tot i que les dades de persones menors d'edat no constitueixen, com a tals, una categoria especial de dades (ex. art. 9.1 RGPD), el RGPD té en compte aquesta especial vulnerabilitat que, com a col·lectiu, pot atribuir-se als menors, als efectes de protegir la seva informació personal.

No oblidem, en aquest sentit, que l'ordenament jurídic estableix el principi bàsic de l'interès superior del menor, que ha de regir totes les actuacions dels poders públics en relació amb aquest (article 11.2.a) Llei orgànica 1/1996, de 15 de gener, de protecció jurídica del menor, de modificació parcial del Codi civil i de la Llei d'enjudiciament civil, i article 5.1 de la Llei 14/2010, de 27 de maig, dels drets i les oportunitats en la infància i l'adolescència (LDOIA), com ha recordat aquesta Autoritat en els Dictàmens CNS 4/2020, CNS 37/2022, CNS 58/2017, o CNS 48/2014, entre d'altres.

En definitiva, la utilització d'aquestes eines en l'entorn educatiu, per part dels diferents col·lectius que integren la comunitat educativa i, singularment, pels menors d'edat, genera dubtes i preocupació per l'impacte que això pot comportar en diversos àmbits, com ara l'àmbit pedagògic (a nivell cognitiu, d'afectació per a la concentració i aprenentatge de l'alumnat en atenció a l'edat i grau de maduresa), curricular (en relació amb la conveniència o no d'introduir l'ús de tecnologies i dispositius digitals segons les etapes de desenvolupament de l'alumnat), de salut (relació amb la salut mental dels alumnes, detecció de patologies relacionades amb els riscos que poden comportar la utilització d'aquests dispositius per l'accés a contingut pornogràfic, violent, inadequat, continguts relacionats amb trastorns alimentaris), o conductes d'assetjament o *mobbing* en l'entorn escolar que, si bé no és provocat pròpiament ni exclusivament per l'ús dels mòbils (aquesta problemàtica respondria a qüestions socials, relacionals, ambientals, educatives i familiars), sembla

innegable que la difusió de determinats continguts nocius a través dels telèfons mòbils, com a través d'altres eines, s'incrementa exponencialment i, per tant, també els seus efectes.

Tal i com recorda el Document 4/2023, que acompanya la consulta, el currículum actual en l'àmbit educatiu té en compte *"la competència digital com a competència transversal que desenvolupa la competència específica a tot al llarg de l'educació bàsica: Conèixer els riscos i adoptar, amb l'orientació del o de la docent, mesures preventives en l'ús de les tecnologies digitals per protegir els dispositius, les dades personals, la salut i el medi ambient, i iniciar-se en l'adopció d'hàbits d'ús crític, segur, saludable i sostenible d'aquestes tecnologies."*

Des de la perspectiva de la protecció de dades, el Dictamen 2/2009 del Grup de Treball de l'Article 29, sobre la protecció de dades personals dels menors (11 de febrer de 2009), fa esment a la vulnerabilitat específica dels menors d'edat, i posa atenció a l'ús de la telefonia a l'escola:

"Las escuelas pueden desempeñar un papel crucial en la adopción de precauciones para la utilización del servicio de mensajes multimedia (MMS), y de las grabaciones sonoras y de vídeo, en los casos en que existan datos personales de terceros y los interesados no tengan conocimiento de ello. Las escuelas deben advertir a sus alumnos que la circulación sin restricciones de grabaciones de vídeo y sonoras, así como de imágenes digitales, puede vulnerar gravemente el derecho de los interesados a la intimidad y la protección de datos personales."

Aquesta Autoritat, conscient de la problemàtica que ens ocupa, ha elaborat en els darrers anys diversos informes i documents (com ara la Guia *"Pautes de protecció de dades per als centres educatius"* 2018, disponible al web de l'Autoritat), i ha impartit i promogut tallers de formació i activitats en l'àmbit educatiu (com ara els tallers sobre *"Menors, Internet i Tecnologies. Créixer i conviure en un món digital"*, duts a terme per la pròpia Autoritat a centres escolars de Catalunya, adreçats als propis menors, a les famílies i al professorat), posant de manifest la importància d'introduir la perspectiva de la protecció de dades en aquest àmbit, així com els riscos i problemàtiques que comporta l'ús de les eines tecnològiques, xarxes socials, apps, etc, per part dels menors d'edat, no només en el context educatiu.

Com ha considerat aquesta Autoritat, no s'ha d'oblidar però que l'ús d'aquests dispositius i l'accés a la xarxa també aporten beneficis evidents: fomenta la comunicació interpersonal i de grup, es generen dinàmiques positives de treball en grup i de col·laboració, permeten aproximar-se a d'altres realitats salvant les distàncies i el temps, s'afavoreix el respecte a la diversitat, es pot accedir a més informació per decidir, potencien la llibertat d'expressió, etc. Tant per combatre'n el vessant negatiu com per potenciar-ne els aspectes positius, cal disposar d'unes pautes clares de com fer les coses en un context de societat altament tecnificada i exhaustivament connectada.

En termes generals i pel que fa a l'ús de la xarxa en la nostra societat, ha de ser positiu i constructiu, i les pautes a implementar no haurien de passar necessàriament per la prohibició o per la limitació d'accés a la xarxa en tots ens casos. Els menors han de prendre consciència dels riscos i les amenaces a què s'exposen ells i els qui els envolten, i han d'assumir la seva part de responsabilitat. Hem d'assegurar un nivell adequat de "ciberconvivència", alhora que garantim el lliure desenvolupament de la personalitat en la societat digital.

A efectes de valoració del risc, també cal tenir en compte que les pautes que es puguin anar elaborant per a minimitzar-los o evitar-los, han de ser dinàmiques i s'han d'adaptar a aquest procés de canvi continu i evolució de les pròpies eines digitals; no serveixen regles fixes, ni amb expectativa de perdurabilitat en el temps.

També fem esment de *"L'Auditoria sobre la publicació d'imatges i altres dades personals dels alumnes a internet. Informe de conclusions sobre l'auditoria per verificar l'adequació al Reglament (UE) 2016/679 i a l'LOPDGGD, en la publicació d'informació personal dels alumnes"* (també disponible al web de l'Autoritat), i a la que es refereix el document que acompanya a la consulta.

L'Auditoria citada, es va dur a terme atès que: *"Des de fa ja temps, l'APDCAT ha registrat un increment de les consultes i denúncies sobre l'exposició d'imatges de menors a internet, com a conseqüència de l'evident profusió de publicacions d'infants i adolescents tant en webs com a les xarxes socials. Aquesta circumstància ha motivat que l'Autoritat hagi decidit dedicar una actuació preventiva a verificar de quina manera els centres docents publiquen les imatges, la veu i els materials elaborats pels alumnes, i si aquestes publicacions s'ajusten a la normativa de protecció de dades personals. (...)."*

La dita Auditoria no analitza específicament la utilització del telèfon mòbil per part de l'alumnat en l'entorn escolar i les seves conseqüències, sinó la difusió d'imatges que duen a terme els propis centres escolars. En qualsevol cas, és un element més a tenir en compte en el sentit que, efectivament, el tractament de les dades dels menors han de ser mereixedores d'una especial cura pel que fa a l'aplicació dels principis i garanties de la protecció de dades.

Per referir-nos, en síntesi, a l'actuació de l'Autoritat en el context que ens ocupa, ens remetem a la informació disponible al web de l'Autoritat: https://apdcat.gencat.cat/ca/menors_i_joves/ .

IV

- La utilització dels mòbils, xarxes socials, etc, per part dels menors, i el factor de l'edat

És clar que, fora de l'àmbit estrictament educatiu (fora dels centres escolars), la utilització de les eines digitals, xarxes socials, l'accés a continguts inadequats a Internet, i en definitiva la gestió inadequada de les dades personals pròpies i d'altres persones, especialment per part dels menors, és una problemàtica que, en síntesi, pot presentar els mateixos riscos que identifiquem en aquest dictamen, més centrat el l'àmbit educatiu.

Ara bé, és important partir de la premissa que la decisió i consegüent responsabilitat que pugui derivar-se del tractament de dades personals que es produeixi arran de la utilització de telèfons mòbils (com d'altres eines o tecnologies digitals, de determinades aplicacions, de xarxes socials, etc), per part de menors d'edat, fora de l'àmbit escolar al que es refereix la consulta, correspondria als pares, tutors, titulars de la potestat parental del menor i, si escau, als propis menors, en atenció al que disposa la normativa aplicable.

Com ha tingut ocasió d'assenyalar aquesta Autoritat en nombroses ocasions, els pares o tutors del menor d'edat no només tenen el dret, sinó que tenen l'obligació imposada per l'ordenament jurídic, de tenir cura i exercir la representació legal dels menors d'edat.

Així, l'article 236-17.1 del CCC, que regula les relacions entre pares i fills, estableix que: *"Els progenitors, en virtut de llurs responsabilitats parentals, han de tenir cura dels fills, prestar-los aliments en el sentit més ampli, conviure-hi, educar-los i proporcionar-los una formació integral. Els progenitors també tenen el deure d'administrar el patrimoni dels fills i de representar-los."*

Segons l'article 236-1 del llibre segon del Codi civil de Catalunya, relatiu a la persona i la família aprovat per Llei 25/2010, del 29 de juliol (CCC), els progenitors són els titulars de la potestat parental respecte els fills menors no emancipats. L'article 236-2 CCC estableix que la potestat parental és una funció inexcusable que, en el marc de l'interès general de la família, s'exerceix personalment en interès dels fills, d'acord amb llur personalitat i per a facilitar-ne el ple desenvolupament. Segons l'article 236-18.1 CCC, l'exercici de la potestat sobre els fills comporta la representació legal d'aquests. L'apartat 2 de l'article 236-18 CCC, exclou de la representació legal dels fills els actes relatius als drets de la personalitat, llevat que les lleis que els regulin estableixin una altra cosa. L'ordenament jurídic també estableix i regula determinats supòsits (ens remetem a la normativa aplicable) que poden suposar la pèrdua de la capacitat dels progenitors per a exercir la representació legal dels fills menors.

Vinculat amb això, des de la perspectiva de la protecció de dades, hem de tenir en compte que l'RGPD estableix determinades previsions respecte els propis menors en la matèria que ens ocupa i sobre la seva capacitat d'actuació per ells mateixos, si escau, en matèria de protecció de dades.

Com ha fet avinent abastament aquesta Autoritat (entre d'altres, en el Dictamen CNS 17/2021), cal referir-se a l'article 8.1 RGPD (tenint en compte els considerants 38, 65, entre d'altres), segons el qual:

"1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años."

L'article 7 de l'LOPDGDD, preveu el següent:

"1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela."

Si la normativa de protecció de dades reconeix als menors d'edat que siguin majors de 14 anys la possibilitat de consentir el tractament de les seves dades, en lògica conseqüència la mateixa normativa reconeix a aquests menors majors de 14 anys la capacitat d'exercir els drets d'autodeterminació informativa. Entre d'altres, l'RGPD preveu el dret d'accés (art. 15), el dret de rectificació (art. 16), el dret de supressió o "dret a l'oblit" (art. 17), i el dret d'oposició (art. 21), l'exercici dels quals correspon a la persona interessada, titular de la informació (art. 4.1 RGPD).

L'article 12.6 de l'LOPDGDD preveu que "en qualsevol cas" els titulars de la potestat parental podran exercir els drets en relació amb menors de 14 anys. Ara bé, aquesta previsió normativa no exclou la possibilitat que aquests mateixos titulars puguin exercir els drets en relació amb menors d'edat majors de 14 anys, tenint en compte les previsions de la normativa sectorial aplicable.

En definitiva, és important tenir en compte que els menors d'edat, a partir dels 14 anys, poden tenir el marge de decisió que els atorga la normativa en matèria de protecció de dades, en els termes apuntats, pel que fa al tractament de les seves dades personals. I també cal aclarir que això no exclou ni és incompatible amb l'exercici d'aquests drets per part dels titulars de la potestat parental.

Per tant, en relació amb els riscos que pot comportar l'ús dels telèfons mòbils per part dels menors en l'àmbit escolar, cal tenir en compte que aquests menors poden tenir un cert marge de control i disponibilitat respecte del tractament de les seves pròpies dades personals, al menys, a partir dels 14 anys.

És rellevant tenir en compte això, perquè com s'apunta en la documentació que acompanya a la consulta, des de diferents àmbits puguin concórrer elements -psicopedagògics, ambientals, de salut o benestar dels menors, de vulnerabilitat i maduresa, d'aprenentatge...etc-, que puguin ser rellevants a l'hora de determinar, per exemple, la conveniència o no de que els menors puguin disposar d'accés a aquestes -o d'altres- eines de comunicació en funció de diferents rangs d'edat (i dels riscos que aquest accés representa), des de la perspectiva estricta de la protecció de dades, l'edat que podria determinar o condicionar la capacitat d'actuació dels menors envers la seva pròpia informació personal, és l'assenyalada (majors o menors de 14 anys).

Des d'altres perspectives -que s'infereixen de la documentació disponible sobre la problemàtica plantejada-, es puguin establir distincions segons l'etapa educativa dels alumnes. Així, sembla innegable que el grau de maduresa dels menors, condiciona no només els continguts a què pot ser convenient que accedeixin, la informació i mesures de protecció que poden interioritzar, etc.

Ara bé, en relació amb el factor edat i la capacitat d'exercir els propis drets de protecció de dades, la distinció que pot ser rellevant a efectes d'avaluar riscos, als efectes de la normativa de la protecció de dades, seria la distinció entre menors d'edat, majors o menors de 14 anys.

Finalment, respecte la possible responsabilitat de pares o tutors, ens remetem a les previsions de l'article 82 RGPD, d'una banda, i dels articles 1101, 1902 i 1903 de Codi Civil, pel que fa a responsabilitat civil, de l'altra).

Així mateix, pel que fa a la responsabilitat penal que podria derivar-se de la comissió de delictes o faltes per part de menors d'edat, ens remetem a les previsions de la Llei orgànica 5/2000, de 12 de gener, de responsabilitat penal dels menors (LORPM).

V

- Especial rellevància de la finalitat ("ús lectiu" vs. "ús no lectiu") de la utilització de tecnologies digitals dins l'entorn escolar

La consulta es planteja a partir d'una certa dicotomia, en el sentit que hi podria haver diferents riscos generats per l'ús del mòbil a l'escola, en funció de que sigui per a finalitats lectives ("ús lectiu", és a dir, utilitzar recursos que els alumnes tenen a disposició en el telèfon mòbil per a realitzar un treball en equip, per a cercar informació, per a generar continguts, etc), o per a finalitats no lectives ("ús no lectiu").

Tenint en compte aquest plantejament, des de la perspectiva de la protecció de dades és important subratllar que la utilització de tecnologies o eines digitals dins l'entorn escolar implica tractament de dades personals, i pot comportar uns riscos per als drets dels afectats (entenent per tals els titulars de la informació, ja sigui un alumne, un professor, o qualsevol treballador del centre). Per tant, aquesta utilització haurà de ser objecte d'una valoració acurada, en quant als pros i contres de la seva utilització als centres, per part dels responsables del tractament. Això, en funció de la finalitat que es vulgui donar a aquesta utilització.

Segons l'article 4.7 RGPD, el responsable del tractament és *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;"*

Sens perjudici de les responsabilitats que puguin correspondre als pares responsables legals o tutors dels menors -qüestió a la que ja ens hem referit-, quan es planteja l'ús d'eines digitals a l'escola, és la pròpia Administració competent i, si escau, les escoles, com a responsables (*ex. art.* 4.7 RGPD), a les que els correspon fer l'anàlisi de riscos pertinent (art. 24 RGPD), per tal de valorar la pertinença d'emprar determinades eines audiovisuals amb finalitats educatives (no només els telèfons mòbils, sinó també d'altres eines audiovisuals sens perjudici que la consulta es centra en el telèfon mòbil).

Atès que, com veurem més endavant, certament es poden identificar determinats riscos en relació a un ús inadequat dels telèfons mòbils a l'escola, el primer que cal tenir en compte (a efectes de valorar o minimitzar aquests riscos), és analitzar per a quina finalitat es pretén utilitzar aquesta eina digital en el marc de l'escola, ja que això pot condicionar, com veurem, els riscos afegits i la seva minimització.

Sobre això, fem avinent que aquesta Autoritat ha tingut ocasió d'analitzar diverses qüestions relacionades amb **l'ús de tecnologies digitals en l'àmbit escolar i de l'ensenyament** (entre d'altres, els Dictàmens CNS 11/2021, CNS 3/2021), als que ens remetem pel seu interès en aquest punt.

Pel que fa al principi de licitud del tractament de dades personals (art. 5.1.a) RGPD), recordem que l'article 6 de l'RGPD disposa el següent:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

*a) **el interesado dio su consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;*
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
(…).
*e) el tratamiento es necesario para el **cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento;*

*f) el tratamiento es necesario para la satisfacción de **intereses legítimo**s perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, **en particular cuando el interesado sea un niño.***

(...)."

D'entrada, la introducció de determinades eines digitals a l'escola, en la mesura que això comporti un tractament de dades personals, ha de disposar d'una base jurídica adequada.

Així, en l'àmbit educatiu, podria plantejar-se la utilització del consentiment (art. 4.11 RGPD) dels pares o responsables dels alumnes menors d'edat o, si escau, dels propis alumnes en cas que tinguin més de 14 anys (art. 7 LOPDGDD), com a base jurídica per al tractament de dades dels alumnes (per exemple, imatges recollides per aquests per a realitzar determinat contingut lectiu).

L'article 6.1.e) de l'RGPD disposa que la licitud del tractament pot fonamentar-se en la necessitat per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics del responsable del tractament.

Afegir que, segons disposa l'article 6.3 RGPD, la base del tractament indicat en l'apartat 1, lletres c) i e), ha d'estar establerta pel dret de la Unió o dels Estats membres que s'apliqui al responsable del tractament.

Aquest mateix article 6.3 afegeix que: *"La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento."*

En relació amb això, ens remetem a la previsió de l'article 8 de l'LOPDGDD, segons la qual la norma que habiliti el tractament haurà de ser una norma amb rang de llei.

La legislació educativa habilita el tractament de les dades de caràcter personal necessàries en el context de la funció educativa que duen a terme els centres escolars.

En concret, la disposició addicional vint-i-tresena de la Llei orgànica 2/2006, de 3 de maig, de Educació (LOE), modificada per la Llei orgànica 8/2013, de 9 de desembre, estableix el següent:

"1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.
2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.
3. ***En el tratamiento de los datos del alumnado se aplicarán normas técnicas que garanticen su seguridad y confidencialidad****. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.*
(…)."

Per tant, d'entrada, el tractament de dades personals, també a través de la utilització d'eines digitals a l'àmbit escolar, haurà de disposar d'una base jurídica suficient que, sense descartar-ne d'altre, en el marc de la funció educativa podria ser principalment la base jurídica de l'article 6.1.e) RGPD.

En aquest context, en l'àmbit educatiu s'ha anat introduint la utilització d'eines digitals amb finalitats educatives en els darrers anys, per a aquest "ús lectiu". I als efectes que ara interessen, la utilització d'una determinada eina digital com a "eina educativa" als centres escolars, ha de respondre a una prèvia valoració per part del responsable respecte la seva pertinença o utilitat per a finalitats lectives i, en cas de comportar tractament de dades personals, de la base jurídica que legitima el tractament i de la correcta aplicació dels principis i garanties de la protecció de dades.

En aquest sentit, com ha fet avinent aquesta Autoritat, que un tractament de dades disposi de base jurídica (art. 6.1 RGPD), no exclou la necessitat d'aplicar la resta de principis i garanties de la protecció de dades.

A títol d'exemple, la introducció en l'àmbit escolar d'eines digitals, qüestió sobre la que aquesta Autoritat s'ha pronunciat anteriorment, ha de tenir en compte diversos factors, com ara l'edat o franja educativa en què s'introdueixen, la finalitat per a la que es faran servir les dades, o les mesures de seguretat que ofereix una determinada eina, entre d'altres.

De la mateixa manera, pel que fa a la utilització dels telèfons mòbils per a ús lectiu, el responsable del tractament de les dades personals que se'n pugui derivar (l'Administració educativa o, si escau, l'escola), haurà hagut de valorar prèviament, no només la concurrència de base jurídica suficient per a dur a terme el tractament, sinó també el correcte compliment de la resta de principis i garanties que com a tal responsable li imposa la normativa de protecció de dades.

Quan l'Administració educativa o els centres escolars, introdueixen una determinada eina digital (el mòbil, en aquest cas), per a una finalitat estrictament "lectiva" i, per tant, vinculada al desenvolupament de determinats continguts pedagògics, que pugui implicar el tractament de dades personals (dels propis alumnes, dels companys, dels professors si escau...), s'haurà tingut en compte prèviament quina és la informació que és pertinent utilitzar per a una determinada activitat lectiva, quines dades personals pot ser que es recullin i es tractin, quines es podran o no difondre, o quina aplicació pot ser necessari utilitzar per a un determinat treball de recerca que han de fer els alumnes, etc.

És a dir, la utilització del telèfon mòbil en l'àmbit educatiu per a una activitat lectiva concreta, comportarà, en major mesura, que aquesta es faci respectant, també, el principi de minimització, segons el qual només s'han de tractar les dades adequades, pertinents i limitades a allò necessari per a la finalitat (art. 5.1.c) RGPD).

A més, com hem dit, és obligació del responsable, segons l'article 24 RGPD, fer una anàlisi de riscos abans de dur a terme un determinat tractament:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2.Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

(...).

Així mateix, quan des de l'àmbit educatiu es valora la possibilitat d'emprar eines digitals, des de la perspectiva de la privacitat des del disseny i per defecte (art. 25 RGPD), cal valorar quin tractament pot ser el més adequat.

A tall d'exemple, si es planifica una activitat lectiva en què s'hagin d'utilitzar els telèfons mòbils i determinada informació personal (per exemple, dels propis alumnes, de les famílies, etc), la planificació d'aquesta activitat haurà hagut de tenir en compte aquests principis i, per tant, el risc que es pugui produir un tractament inadequat d'aquestes dades hauria de ser, en principi, menor. També com a exemple, com hem dit, la introducció d'eines digitals a l'escola no és una novetat. Així, si l'Administració educativa implementa l'ús d'ordinadors a l'escola per a activitats lectives, és obvi que prèviament s'haurà tingut en compte que aquests ordinadors, si tenen connexió a Internet, aquesta connexió no ha de permetre accés per part dels alumnes a pàgines web amb continguts inadequats. Mesura que, als efectes que

interessen, seria igualment aplicable a l'ús lectiu dels mòbils a l'escola, amb la minimització del risc que això comportaria.

Afegim que la normativa de protecció de dades també preveu que els afectats -titulars de la informació personal tractada- poden exercir els seus drets d'accés, rectificació, supressió o d'oposició, entre d'altres, en relació amb el tractament de les seves dades personals, en els termes que preveu la normativa, en el cas dels menors, directament o a través si escau dels seus pares o tutors (arts. 15 i ss RGPD).

En la mateixa línia que apuntem, la decisió de la utilització d'eines digitals (a tall d'exemple, una determinada aplicació que puguin tenir els menors instal·lada en el telèfon mòbil) per a una finalitat lectiva, hauria de permetre en principi un major control i coneixement de la informació tractada (art. 12 RGPD) i, en conseqüència, el risc que derivaria de no poder exercir els drets esmentats, pel simple desconeixement que s'ha produït el tractament, seria major.

Per tot l'exposat, podem concloure que, a priori, i atesos els principis i garanties de la normativa de protecció de dades, l'ús del telèfon mòbil per a finalitats estrictament lectives, pot oferir una major identificació, control i minimització o eliminació dels riscos, als que farem esment més endavant.

VI

La consulta també es refereix a **l'ús "no lectiu" del mòbil a les escoles**, i dels riscos que això podria comportar.

Com hem apuntat, el tractament de dades personals que es pot derivar de l'ús d'eines digitals i, singularment, del telèfon mòbil per a finalitats educatives o lectives (qüestió a la que ens hem referit abastament), hauria de comportar una aplicació dels principis i garanties de la protecció de dades per part dels responsables i, en conseqüència, en principi, un major control d'aquest tractament des de la mateixa comunitat educativa. Això, a priori, hauria de permetre identificar, controlar i minimitzar els riscos que es puguin presentar.

En contraposició amb això, la consulta no fa més concreció sobre l'ús "no lectiu" del telèfon mòbil en els centres educatius. Podem entendre que es refereix a l'ús del mòbil en espais no estrictament lectius (durant les classes i per a finalitats lectives), sinó en espais d'esbarjo, durant l'estada al menjador, patis, entrades i sortides de l'escola, etc.

És a dir, sembla que la consulta s'estaria referint, en aquest punt, a un ús del telèfon mòbil (i per tant, de les aplicacions, accés a Internet, càmera per enregistrar imatges i sons, etc, que a priori podria comportar la utilització, sense més concreció, del mòbil en l'àmbit escolar), sense connexió amb finalitats educatives o per a un ús lectiu, sinó com a simple eina d'entreteniment, de comunicació (ja sigui entre els propis alumnes, mestres, etc, o dels alumnes amb les seves famílies, etc).

Aquest context planteja, d'entrada, des de la perspectiva de la normativa de protecció de dades i de l'impacte dels riscos que es poden presentar, la necessitat de fer una consideració prèvia.

Sembla clar que alguns dels riscos que poden produir-se a conseqüència de l'ús d'eines digitals (singularment el telèfon mòbil) a l'àmbit educatiu, es poden evitar o al menys minimitzar en major mesura en el context d'un ús lectiu, atès que el responsable del tractament haurà dut a terme, en principi, una anàlisi de riscos prèvia, i en definitiva una valoració des de la perspectiva de la protecció de dades i de la privacitat, per tal de determinar de quina manera la utilització dels mòbils pot resultar adequat per als drets i interessos dels afectats (quines apps utilitzem, si enregistrem imatges i quin tractament en fem, com hem de gestionar, si escau, el consentiment dels propis menors o pares, o professors, la imatge dels quals s'hagi d'utilitzar, etc....).

Ara bé, aquest esquema que, a priori, permetria el dit control de riscos, no sembla aplicable, al menys, amb la mateixa intensitat, a un ús indefinit, general i inconcret dels telèfons mòbils a l'escola, amb finalitats diferents (però no concretades) a la finalitat lectiva.

Així, el fet que el responsable (Departament o escoles) no pugui establir quin ús es fa del telèfon mòbil en funció d'una activitat determinada lectiva, a priori pot dificultar el control dels riscos arran d'un possible mal ús d'aquestes eines.

Així, si bé els riscos per als drets i interessos dels afectats poden ser equiparables al supòsit anterior (ús lectiu dels mòbils), no sembla que es pugui fer un control de riscos amb la mateixa eficàcia. A tall d'exemple, si en una activitat lectiva els professors, l'escola, o l'administració educativa poden establir quin ús es fa del mòbil en funció de l'activitat curricular, un ús "no lectiu" -sense més concreció-, no facilita l'establiment d'aquestes condicions d'ús i, per tant, una prèvia anàlisi dels riscos concurrents.

Per tot això, i atesos els termes de la consulta en aquest punt, es recomana especialment dur a terme una concreció de quins serien aquests usos, i de la proporcionalitat dels possibles tractaments, per tal de minimitzar els riscos concurrents. Així, simplement a tall d'exemple, si la finalitat de l'ús no lectiu dels telèfons mòbils pot ser la possibilitat de comunicació dels alumnes amb les seves famílies o d'altres companys en espais de lleure durant la jornada lectiva, no semblaria imprescindible aquest ús o, com a mínim, es podrien tenir en compte altres vies de comunicació alternatives.

D'altra banda, no existeix un dret de l'alumne a l'ús del mòbil en els serveis educatius, ni en l'àmbit lectiu ni, menys encara, en l'àmbit no lectiu. En aquest sentit, no afectaria als drets dels infants i adolescents la introducció de mesures de limitació dels mateixos en l'entorn educatiu, sempre que es fes per part de l'autoritat competent, i de manera motivada.

La limitació pel que fa als usos lectius probablement hauria d'integrar-se en el projecte educatiu del centre i, de la mateixa manera, la seva prohibició o limitació per a usos no lectius hauria d'adoptar-se per part de l'òrgan competent i, tal com s'ha comentat anteriorment, hauria de garantir l'existència de vies de comunicació o eines alternatives que permetin atendre les necessitats de comunicació que eventualment requereixi l'alumnat.

En aquest punt, no correspon a aquesta Autoritat determinar quin seria l'òrgan competent, d'acord amb la normativa educativa, per establir una limitació en l'ús dels mòbils a les escoles, tot i que, d'acord amb l'exposat, la normativa de protecció de dades no impedeix l'establiment de la mesura.

Val a dir que l'RGPD no s'aplica al tractament de dades personals efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques (art. 2.2.c) RGPD) i, per tant, "sense connexió alguna amb una activitat professional o comercial" (considerant 18 RGPD), com ha fet avinent aquesta Autoritat en ocasions anteriors (entre d'altres, en els Dictàmens CNS 58/2015, CNS 2/2016, o CNS 58/2016).
Als efectes que ara interessen, l'aplicabilitat de l'excepció relativa al tractament domèstic no depèn només del context en el qual es captin les imatges, sinó també de la finalitat. I si ens referim a una finalitat "no lectiva", simplement social o relacional, de comunicació a través dels mòbils (amb les famílies, amb altres alumnes, etc), no podem descartar que es pugui considerar un ús domèstic i, per tant, exclòs del marc de protecció de la normativa de protecció de dades.

Ara bé, no s'ha de confondre això amb el fet que l'ús "no lectiu" del mòbil a l'escola pot generar riscos, no només per al dret fonamental a la protecció de dades (si no estem estrictament en aquest ús domèstic) i per altres drets fonamentals als que ens referim en aquest dictamen.

En qualsevol cas, una anàlisi més acurada des de la perspectiva de la protecció de dades en aquest punt, passaria per una prèvia concreció respecte la naturalesa i finalitats dels usos "no lectius" als que es refereix la consulta i, de la mateixa manera, justificar les raons per les quals s'imposa una limitació al seu ús.

VII

Aproximació general als riscos associats a l'ús de telèfons mòbils, xarxes socials i aplicacions per part dels menors d'edat

Com ha quedat apuntat, els riscos associats a l'ús de les noves tecnologies, xarxes socials, i mòbils per part dels menors d'edat, és una problemàtica que impacta en moltes àrees, no només en la protecció de dades personals. En qualsevol cas, això no ha de desmerèixer els beneficis i oportunitats que les xarxes socials ofereixen als diferents col·lectius socials, singularment, al col·lectiu educatiu, inclosos formadors, centres educatius, i els propis alumnes, beneficis que aquesta Autoritat no posa en qüestió.

En línia amb el que ja s'ha exposat, no és superflu recordar que, ja sigui en l'àmbit estrictament educatiu com des de l'àmbit social i familiar, cal acompanyar i compartir amb els menors una informació clara, rigorosa, i ajustada a les seves necessitats, ajudar-los a crear la seva *"identitat digital"* i a saber conservar la seva reputació digital ja que, en un futur no gaire llunyà, les persones serem valorades de manera significativa per allò que la xarxa pugui saber de nosaltres. En bona mesura, podem arribar a ser considerats allò que digui la xarxa que som i, per tant, hem d'ensenyar-los a protegir el seu futur.

Des del moment que, a través del telèfon mòbil, els menors accedeixen a Internet o utilitzen aplicacions mòbils, això pot generar una sèrie de riscos generals, que aquesta Autoritat ja ha tingut ocasió d'assenyalar a través dels diferents continguts i activitats que ha dut a terme al llarg dels anys, i a què hem fet esment anteriorment (FJ II).

Aquest Autoritat ha posat de manifest, a través de la seva feina de divulgació de la problemàtica que ens ocupa, una sèrie de riscos associats en general a l'ús de les xarxes

socials, accés a Internet, d'aplicacions i eines digitals diverses com ara els telèfons intel·ligents, per part dels menors, i que podem resumir en els següents punts:

- Navegació per Internet -si escau, a través del telèfon mòbil- sense supervisió de pares o tutors o, si escau, sense supervisió dels responsables en l'àmbit educatiu (mestres o responsables del centre escolar).

- Manca de coneixement previ i d'informació adequada sobre les condicions d'ús, o sobre les polítiques de privacitat, i de les mesures de seguretat de les eines, apps, etc, que utilitzen.

- Manca de coneixement i de valoració del risc que suposa difondre informació personal pròpia i de terceres persones (particularment, facilitar dades que ubiqui els menors en temps i espai).

- Riscos a conseqüència d'establir comunicació amb persones desconegudes (xatejar amb estranys, desconèixer mecanismes d'autoprotecció per confirmar identitat de persones amb les que connecten), etc.

- Captació i difusió inadequada d'imatges pròpies i de terceres persones, sense el seu consentiment. Afectació pels drets a l'honor i a la intimitat personal i familiar i a la pròpia imatge de terceres persones.

Sobre aquests riscos inicials, aquesta Autoritat ha posat de manifest una sèrie de mesures de protecció generals (i, per tant, aplicables no només als menors coma a usuaris de xarxes socials, sinó també a qualsevol altre col·lectiu de la comunitat educativa), com ara:

- Necessitat que els menors limitin els seus contactes en xarxes socials, a persones que coneixen directament i que formen part del seu cercle familiar i d'amics.

- Conveniència de limitar al mínim la informació personal que els menors publiquen a les xarxes socials, no només la informació pròpia (de la que els menors són titulars, ex. art. 4.1 RGPD), sinó, amb igual o major motiu, la informació de terceres persones. En aquest punt, l'Autoritat ha posat de manifest que cal preservar la informació d'altres persones com si fos la pròpia.

- Protegir especialment la fotografies i vídeos que es capten, i valorar la pertinença de la seva difusió, i evitar-la si no es disposa del consentiment dels afectats. Especialment, evitar difusió de continguts afectadors dels drets de la personalitat d'altri (honor, intimitat i pròpia imatge), continguts vexatoris, estigmatitzadors, discriminatoris, etc.

- En darrera instància, i especialment en l'àmbit educatiu, cal evitar el risc que un mal ús de la informació personal pròpia i d'altri, pugui generar conflictes i, si fos el cas, minimitzar el risc establint sistemes de mediació, que els pròpies centres escolars poden articular.

Fem aquest aproximació general a la qüestió plantejada, perquè és evident que la problemàtica que poden generar aquestes situacions impacta en molts aspectes de la vida dels menors, del seu entorn familiar i relacional, i de la dinàmica dels propis centres escolars.

Així, la documentació científica que ha estudiat aquest impacte des de diferents disciplines (qüestions relacionades amb la manca de concentració dels menors, afectació psicològica, qüestions relacionades amb la seguretat personal dels menors, increment de situacions de *mobbing* o assetjament, salut emocional...), té un paper molt rellevant en aquesta aproximació general a la problemàtica que emmarca la consulta. Certament, són molts els riscos vinculats a l'ús d'Internet (si escau, a través dels telèfons mòbils): ciberassetjament escolar, tecnoaddicció, nomofòbia -por a no tenir mòbil-, aïllament socials, distorsió de la realitat, pornografia infantil i sextorsió..., entre d'altres.

Aquesta Autoritat ha considerat, especialment pel que fa a l'ús dels telèfons mòbils per part dels joves i adolescents, que els menors veuen i assimilen els comportaments que, també els adults, hem assimilat com a "normals" (la incorporació dels dispositius mòbils a les rutines personals, familiars i laborals), qüestió que tota comunitat educativa (famílies, educadors i menors), hauria de tenir en compte.

Sobre això, apuntar que els riscos per a la seguretat del menor a conseqüència del l'ús inadequat de les xarxes socials, han de tenir una resposta adequada des de tot l'entorn del menor (administració pública educativa, família, comunitat educativa, administració competent en matèria de protecció dels menors), ateses les exigències que es deriven del principi de l'interès superior del menor, a què hem fet referència.

En aquest context, i partint d'aquesta identificació o enumeració inicial de riscos, aquest dictamen s'ha de centrar, pròpiament, en la identificació i valoració de riscos des de la perspectiva de la normativa de protecció de dades, i dels drets de la personalitat de les persones afectades, principalment, els menors d'edat i, per extensió, la resta de col·lectius de la comunitat educativa.

VIII

- Manca de coneixement i de valoració del risc que suposa difondre informació personal pròpia i de terceres persones (particularment, facilitar dades que ubiqui els menors en temps i espai).

Una de les qüestions que es posa de manifest de forma recurrent, com a risc per als menors, i que caldria tenir en compte en el cas que ens ocupa, és el relatiu a la difusió d'informació personal (tant pròpia com d'altres persones, com ara l'entorn familiar dels menors, etc), que es pot produir a partir de l'ús d'eines digitals (no només del telèfon mòbil).

Aquest risc pot venir derivat de la revelació de massa dades personals a través de les xarxes socials (fer difusió sense control, en obert, i a través de xarxes socials, sobre les pròpies relacions, sobre les activitats personals i familiars, activitats d'oci, etc), pot generar un risc en el cas que hi accedeixin persones de fora de l'entorn proper i de confiança del menor.

Ara bé, cal assenyalar que aquest no és un risc que s'hagi de produir especialment (ni exclusivament) en l'àmbit merament educatiu.

Ara bé, dins l'àmbit educatiu, la captació i difusió indiscriminada d'aquests continguts (ja siguin imatges, dades identificatives o de contacte, adreces, etc....), suposa un risc per a les

persones afectades, que podrien ser no només els propis alumnes, sinó també qualsevol altra persona de la comunitat educativa, la informació personal de la qual pugui ser objecte d'un mal ús o d'una difusió no coneguda o consentida.

Pel que fa a les responsabilitats que es puguin produir a conseqüència d'aquest mal ús d'informació pròpia o d'altri en l'entorn escolar, caldria remetre's a la normativa esmentada en aquest dictamen (civil o penal), en atenció a les circumstàncies concurrents en cada cas.

- Utilització indeguda d'aplicacions de telèfons mòbils, accés a continguts inadequats i la limitació d'accés per edat

D'entrada, un dels riscos principals que pot comportar la utilització del telèfon mòbil en l'àmbit educatiu, és el risc d'accés a continguts inadequats per part dels menors.

Si bé no correspon en aquest dictamen detallar quins són aquests continguts, o analitzar el seu impacte en els menors més enllà de l'àmbit estricte de la protecció de dades, ens estaríem referint a continguts qualificats per a majors d'edat (contingut pornogràfic o violent), continguts perjudicials, additius, publicitat prohibida per a persones menors d'edat, o continguts només disponibles en llocs d'internet que tenen l'accés limitat a menors de determinada edat (per exemple, a menors de 14 anys).

És obvi que determinats continguts a Internet als quals es pot accedir mitjançant la utilització de telefonia mòbil, no resulten adequats per a menors, com s'apunta abastament en la documentació que acompanya a la consulta, i sobre la que no cal fer més esment.

Ara bé, sobre això, caldria apuntar a un primer risc o, més exactament, el que podríem qualificar com a "malentès", això és, partir de la premissa errònia que utilitzar un telèfon mòbil implica necessàriament -o inevitablement- utilitzar qualsevol aplicació l'ús de la qual és viable a través dels telèfons amb connexió a Internet.

Dit d'una altra manera, i amb la finalitat de minimitzar el risc al que es refereix la consulta, cal partir de la base que la utilització d'un telèfon mòbil no porta aparellada necessàriament la utilització de determinades aplicacions o canals d'accés a informació molt diversa.

Partint d'aquesta premissa, i a efectes d'identificar i minimitzar riscos, caldrà analitzar quines són les aplicacions que es fan servir (o que per a finalitats educatives es considera que pot ser pertinent utilitzar), en l'àmbit educatiu, o quines pot ser aconsellable no utilitzar.

Com es desprèn de la consulta i de la documentació que l'acompanya, és obvi que la utilització dels telèfons mòbils (en l'àmbit que sigui), habitualment comporta la utilització d'aplicacions de missatgeria instantània, connexió a Internet, accés a continguts adequats o no als menors, etc.

Per tant, d'entrada, cal tenir en compte que l'anàlisi dels riscos que pot comportar cadascuna d'aquestes aplicacions dins l'àmbit escolar (independentment de que sigui per a ús lectiu o no lectiu), obligaria a l'administració competent i, si escau, a les escoles responsables, a analitzar les condicions d'ús, les polítiques de privacitat, i, sobre tot, atès que ens referim principalment a l'ús per part de menors d'edat, a les previsions que

cadascuna d'aquestes eines pugui tenir respecte la limitació d'accés per motiu d'edat, qüestió a la que farem referència més endavant.

Dit això, als efectes de la consulta formulada, cal recordar que la mera utilització d'un telèfon mòbil (o més concretament, dels anomenats "smartphones"), no porta aparellada necessàriament ni automàticament la utilització de determinades aplicacions (apps), l'ús de les quals pot no ser recomanable o fins i tot, pot estar prohibit pel propi fabricant o responsable (art. 4.7 RGPD), en relació amb els menors de determinada edat.

Tal i com es recull en el Document 4/2023, que acompanya a la consulta, i com ha subratllat també aquesta Autoritat, en relació amb les empreses tecnològiques responsables d'aplicacions d'utilització habitual a través de telèfons mòbils, cal advertir del risc que suposa la no supervisió de l'edat mínima d'accés a aquestes aplicacions i continguts. Això, amb el risc aparellat d'accés a continguts nocius o inadequats per als menors.

Cal dir que la consulta no es refereix específicament a cap aplicació en concret, però a títol il·lustratiu podem citar algunes aplicacions d'ús habitual, com ara l'aplicatiu de Whatsapp, Telegram, o d'altres de missatgeria instantània, o aplicacions gratuïtes d'utilització habitual, algunes adreçades a menors, com ClassDojo, Duolingo, Hooked Inc, Roblox, Kahoot!, Copa Toon 2018, Lingokids, Youtube Kids, etc), o d'altres que poden tenir una limitació d'accés que exclouria, d'entrada, determinades franges de menors.

A títol d'exemple, i si ens referim a aplicacions d'ús habitual (Whatsapp, Instagram,, Facebook, Gmail, o Twitter, entre moltes d'altres), les edats mínimes per accedir-hi i utilitzar-les oscil·len entre els 13 i els 16 anys. En determinats casos, els proveïdors del servei estableixen que per utilitzar determinat aplicatiu és necessària una edat mínima i donar-se d'alta amb el consentiment dels pares o tutors.

Evidentment, un gruix important dels usuaris d'aquests serveis no arriben a aquests mínims d'edat i, encara menys, tenen l'autorització dels seus pares o tutors.

Per tant, és obvi que el risc que suposa l'accés i utilització d'aplicacions per part de persones menors d'edat, no és un risc necessàriament aparellat al mer ús d'un telèfon mòbil, sinó que deriva de la utilització de la dita aplicació, si es fa en uns termes que no resultin adequats, com pot ser si s'utilitzen abans de l'edat que el propi proveïdor ha establert com a mínima per a l'accés.

Aquesta Autoritat ha tingut ocasió d'analitzar en diverses ocasions la problemàtica que presenten determinades aplicacions des de la perspectiva de la protecció de dades, entre d'altres, en els Dictàmens CNS 54/2017, i CNS 55/2016, respecte l'ús dels sistemes de missatgeria instantània; CNS 13/2018, sobre riscos i responsabilitats per l'ús de l'aplicatiu del Whatsapp; o la CNS 24/2013, sobre la utilització de dues aplicacions en particular, en les comunicacions advocat-client. Així mateix, aquesta Autoritat ha analitzat la problemàtica que, des de la perspectiva de la protecció de dades, pot presentar la utilització de serveis de cloud-storage (CNS 57/2013) i dels serveis de "Google Analytics" (CNS 1/2008).

Als efectes que ara interessen, cal apuntar que per valorar el grau de protecció que cadascuna de les dites aplicacions (d'ús habitual, tot i que no necessari, quan s'utilitzen telèfons mòbils) i, en conseqüència, per valorar el risc que la seva utilització pot suposar per als menors i per a la resta de col·lectius de l'àmbit escolar, caldrà analitzar les polítiques de

privacitat, les condicions d'ús de cada aplicació, i la protecció que ofereixen, si escau, en relació amb els menors d'edat.

Així, el risc que comportarà l'ús de cada aplicació per part de menors d'edat (més enllà del risc objectiu d'utilitzar-les per sota de l'edat mínima corresponent), no es pot determinar a priori, sinó que dependrà de les condicions d'ús del servei, de la transparència amb què es facilita la informació (polítiques de privacitat), fluxos informatius que es puguin produir (recordem, en aquest sentit, que molts proveïdors de xarxes socials i aplicacions poden tenir la seu ubicada fora de l'àmbit normatiu de l'RGPD, amb les dificultats aparellades que això pot comportar, i a les que s'ha referit aquesta Autoritat), entre d'altres qüestions.

Aquesta Autoritat s'ha referit, en alguns dels Dictàmens esmentats en aquest dictamen, a la problemàtica que genera no conèixer si l'entitat responsable d'una aplicació de què disposem al telèfon mòbil, tramet informació a terceres entitats, quines són aquestes entitats i quin règim de protecció de dades apliquen, si es recullen dades inadequades o innecessàries dels usuaris, si es produeixen TID -transferències internacionals de dades-, etc.

Així, en relació amb aquestes aplicacions, cal atendre especialment al compliment del deure d'informació que ofereixen aquestes aplicacions (art. 12 i ss RGPD, fent especial esment a que la informació facilitada a menors d'edat ha de ser clara i entenedora), o respecte la recollida del consentiment per a utilitzar-les.

Com és sabut, l'RGPD requereix que els responsables i desenvolupadors d'aquests tipus d'aplicacions informin els menors i els seus responsables sobre el tractament que es produeix de les dades personals, s'expressi en un llenguatge clar, senzill, i fàcil d'entendre per a la seva edat. L'exigència del RGPD en quant a que la informació adreçada als menors ha de ser adequada i entenedora no hauria de ser minimitzada en l'àmbit que ens ocupa, atesos els riscos que una falta de transparència en aquest sentit pot provocar en els drets i interessos dels menors.

Per tant, el risc s'incrementa quan la informació disponible, o bé no és entenedora, o bé no es troba en uns termes admissibles als efectes de l'RGPD, quan els usuaris són menors d'edat.

Lògicament, el risc d'accés a continguts inadequats per part de persones menors i, no només això, sinó també el risc que suposaria la pèrdua de control sobre la pròpia informació arran de la utilització d'aplicacions que no garanteixin suficientment aquest control, són elements que cal tenir especialment en compte en el cas que ens ocupa, a l'hora de valorar la pertinença o no d'utilitzar determinades aplicacions.

En definitiva, si les aplicacions que utilitzen els menors en l'àmbit escolar no ofereixen una informació adequada pel que fa als seus continguts, a la gestió de la privacitat, a la comunicació de dades a tercers que es pot produir, a la gestió del consentiment (i, si escau, als sistemes de verificació d'accés), entre d'altres, això dificulta la identificació i, si escau, minimització del risc pels drets i interessos dels propis menors.

I és en aquest punt on cal referir-se a una de les principals problemàtiques que presenta la utilització de telèfons mòbils per part de menors, també en l'àmbit escolar, com és la problemàtica de la verificació d'edat per a l'accés i utilització d'aplicacions. És evident que

no tenir certesa -i control- de si els menors accedeixen i utilitzen xarxes socials sense tenir l'edat mínima adequada (i degudament verificada) o, al menys, sense coneixement i control per part dels seus pares o tutors, suposa un risc en sí mateix.

En concret, en aquest àmbit es detecten riscos per la gestió ineficient dels proveïdors de serveis en relació amb la comprovació de l'edat adequada dels usuaris, o la gestió inadequada de la recollida del consentiment, si escau, dels pares o tutors -com a base jurídica que hauria d'habilitar el tractament.

Com ha apuntat l'Agència Espanyola de Protecció de Dades (AEPD) en el document *"Decálogo de principios. Verificación de edad y protección de persones menores de edad ante contenidos inadecuados"* (desembre de 2023), al que ens remetem pel seu interès en la qüestió plantejada:

"(...).Los sistemas de protección de personas menores de edad ante contenidos inadecuados implican tratamientos de alto riesgo para los derechos de las personas individualmente, pero también pueden tener un gran impacto para la sociedad en su conjunto. El alto riesgo de estos sistemas implica que las estrategias más adecuadas para gestionarlo son aquellas que preservan el anonimato de la persona usuaria de cara a los proveedores de servicios de Internet y terceras entidades ***en el marco de la verificación de edad****. Además, han de proporcionar herramientas transparentes, auditables, bajo el control de la persona usuaria para acreditar la autorización para el acceso a contenidos inadecuados y que generen confianza. Todo ello sin perjuicio de la obligación de implementar todas las medidas de privacidad necesarias que resulten de la realización de una evaluación de impacto para la protección de datos y superar un análisis de idoneidad, necesidad y proporcionalidad."*

Ens remetem també, sobre aquesta qüestió, a *la "Nota técnica. Descripción de las pruebas de concepto sobre sistemas de verificación de edad y protección de persones menores ante contenidos adecuados"* (AEPD, desembre de 2023).

IX

- Riscos derivats de la captació i difusió de dades pròpies i de terceres persones

Com hem apuntat, arran de l'ús de les eines digitals per part dels menors, es pot produir una afectació no només per al dret a la protecció de dades personals, sinó també per altres drets fonamentals, singularment, els drets a l'honor, a la intimitat personal i familiar i a la pròpia imatge.

Convé recordar que l'RGPD protegeix qualsevol dada personal (art. 4.1 RGPD), entesa com aquella que permet identificar una persona física, independentment que aquesta informació sigui en major o menor grau afectadora de la intimitat dels afectats, o d'altres drets fonamentals també diferents, si bé estretament vinculats amb el dret a la protecció de dades personals (art. 18.4 CE).

Cal precisar que l'RGPD no s'aplica al tractament de dades personals efectuat per una persona física en l'exercici d'activitats exclusivament personals o domèstiques (art. 2.2.c) RGPD) i, per tant, "sense connexió alguna amb una activitat professional o comercial"

(considerant 18 RGPD), com ha fet avinent aquesta Autoritat en ocasions anteriors (entre d'altres, en els Dictàmens CNS 58/2015, CNS 2/2016, o CNS 58/2016).

Sobre això, segons la jurisprudència (SAN de 15 de juny de 2006, FJ Tercer), cal tenir en compte que l'aplicabilitat de l'excepció relativa al tractament domèstic no depèn només del context en el qual es captin les imatges, sinó també de la finalitat. Així, si la finalitat de la captació d'imatges que es pugui produir en l'àmbit educatiu no desplega els seus efectes fora de l'àmbit privat, la captació restaria exclosa de l'àmbit d'aplicació de la normativa de protecció de dades (RGPD).

En relació amb imatges de persones físiques (tant d'alumnes, com de professorat, com d'altres membres de la comunitat educativa), que es capten habitualment per part de les escoles, i que tenen a veure amb el desenvolupament de la seva tasca educativa i de les activitats pròpies, sembla clar que el tractament aniria més enllà del mer àmbit domèstic i es trobaria subjecte a l'RGPD.

Això sens perjudici de l'aplicabilitat de la normativa reguladora del dret fonamental a la pròpia imatge (article 18.1 CE), que es pot definir com el dret que té "cada individu a que els demés no reprodueixin els caràcters essencials de la seva figura sense el consentiment del subjecte, de tal manera que tot acte de captació, reproducció o publicació per fotografia, film o un altre procediment de la imatge d'una persona en moments de la seva vida privada o fora d'ella suposa una vulneració o atac al dret fonamental a la imatge, com també ho és la utilització per a fins publicitaris, comercials o de naturalesa anàloga" (STS de 27 de març de 1999).

En concret, caldrà tenir en compte les previsions de la Llei orgànica 1/1982, de 5 de maig, de protecció del dret a l'honor, la intimitat personal i familiar, i la pròpia imatge (en endavant, LO 1/1982), que esmenta la consulta, i a la que farem esment més endavant.

A banda de la protecció de l'RGPD per a les dades personals, la imatge gràfica de les persones, la seva privacitat i el seu honor (cadascun d'aquests drets amb la seva corresponent configuració constitucional, *ex. art.* 18.1 CE, i tenint en compte el desenvolupament jurisprudencial d'aquests drets).

Pel que fa als drets esmentats, ens hem de remetre a les previsions de la normativa aplicable, singularment, la Llei orgànica 1/1982, de 5 de maig, de protecció jurídica dels drets a l'honor, la intimitat personal i familiar i la pròpia imatge.

En qualsevol cas, la captació i difusió d'imatges que resultin especialment afectadores per a la intimitat de les persones, en els termes de la normativa indicada (de caire sexual, fotos íntimes, etc), sense consentiment, podrien no només contravenir la normativa de protecció de dades, sinó també la LO 1/1982, esmentada, i fins i tot podria ser constitutiva de responsabilitats penals (en relació amb la comissió de delictes de descobriment i revelació de secrets, *ex. art.* 197 i ss. CP).

Més enllà de les previsions aplicables en protecció dels drets a l'honor, la intimitat personal i la pròpia imatge, cal recordar que la utilització i difusió d'imatges i informació personals de menors a xarxes socials que puguin implicar una intromissió il·legítima determinarà la intervenció del ministeri fiscal que podria instar les mesures cautelars i de protecció que determini la llei.

Finalment, apuntar que aquesta Autoritat també ha posat de manifest el risc que pot comportar per a la seguretat dels propis menors, la manca de coneixement i de valoració del risc que suposa difondre informació personal pròpia i de terceres persones. Particularment, apuntem que, facilitar informació personal i familiar que permeti ubicar els menors -aplicacions amb geolocalització, etc-,o simplement difondre informació personal i familiar a través de xarxes socials, pot suposar un risc per als menors.

Això, amb independència de la utilització del telèfon mòbil dins o fora de l'àmbit educatiu.

- Risc que suposa la impossibilitat o dificultat d'exercici de drets ARSOPOL

Aquesta Autoritat ha posat de manifest abastament una qüestió que, si bé pot resultar òbvia, no per això s'ha de deixar d'assenyalar, i és el fet que el dret fonamental a la protecció de dades personals, que es tradueix a efectes pràctics en la possibilitat d'exercir els drets d'habeas data (actualment, i atesa la denominació de l'RGPD, drets ARSOPOL), difícilment es pot dur a la pràctica si no es té coneixement de que les nostres dades personals han estat tractades.

Ja hem fet esment en aquest dictamen de la importància del compliment adequat del deure d'informació als afectats (usuaris, de xarxes socials, aplicacions, etc, en el cas que ens interessa (arts. 12 i ss RGPD).

Doncs bé, si la informació rebuda pels usuaris és inadequada (xarxes o proveïdors que no són transparents en la informació exigible, etc), això pot generar un risc atesa la impossibilitat de conèixer que s'ha produir un tractament i quines són les característiques d'aquest tractament i, en conseqüència, es dificulta l'exercici dels drets ARSOPOL, amb la consegüent indefensió que això suposa. Més, si ens referim a un col·lectiu especialment vulnerable, com són els menors d'edat.

En aquest punt, insistim en una consideració que aquesta Autoritat també ha manifestat abastament. Quan ens referim als drets dels menors, i als riscos que suposa una exposició continuada de les seves dades personals, singularment la imatge, a través de xarxes socials, cal tenir en compte la rellevància -i, sovint, la dificultat de la seva correcta aplicació- que a efectes de protecció de dades té el dret a l'oblit (art. 17 RGPD, i arts. 93 i 94 LOPDGDD, als que ens remetem).

La correcta aplicació d'aquest dret a l'oblit resulta clau per determinar de quina manera es pot arribar a protegir la identitat i la reputació digital dels menors (i no només d'aquests, sinó d'altres col·lectius afectats, als que també es refereix la consulta). El risc que pot portar aparellat en alguns casos un mal ús de la informació personal a través de la utilització d'eines digitals, aconsella, en qualsevol cas, que els mateixos menors prenguin consciència que molta part del que fan avui, si es publica a la xarxa, es podria recordar en el futur, quan ja siguin adults, per sorpresa i en moments o situacions inoportunes.

Conclusió

1.- Utilització del mòbil per a ús lectiu:

La utilització d'una determinada eina digital com a "eina educativa" als centres escolars, ha de respondre a una prèvia valoració per part del responsable respecte la seva pertinença o utilitat per a finalitats lectives i, en cas de comportar tractament de dades personals, de la base jurídica que legitima el tractament i de la correcta aplicació dels principis i garanties de la protecció de dades. A priori, i atesos els principis i garanties de la normativa de protecció de dades, l'ús del telèfon mòbil per a finalitats estrictament lectives, pot oferir una major identificació, control i minimització o eliminació dels riscos.

El tractament de dades personals que es pot derivar de l'ús d'eines digitals i, singularment, del telèfon mòbil per a finalitats educatives o lectives -el qual pot tenir base jurídica als efectes de la normativa de protecció de dades-, hauria de permetre, en principi, un major control dels termes d'aquest tractament des de la mateixa comunitat educativa (Administració pública i, si escau, les pròpies escoles).

Això, a priori, pot permetre acotar els termes d'ús del mòbil dins l'escola, identificar més fàcilment els riscos que es puguin presentar i minimitzar-los.

2.- Utilització del mòbil per a ús no lectiu:

L'esquema apuntat en relació amb la utilització del mòbil per a ús lectiu que, a priori, permetria el dit control de riscos, no sembla aplicable, al menys, amb la mateixa intensitat, a un ús indefinit, general i inconcret dels telèfons mòbils a l'escola, amb finalitats diferents (però no concretades) a la finalitat lectiva.

Si bé els riscos per als drets i interessos dels afectats poden ser equiparables al supòsit anterior (ús lectiu dels mòbils), no sembla que es pugui fer un control de riscos amb la mateixa eficàcia. En aquest cas, es recomana especialment dur a terme una valoració de proporcionalitat i analitzar possibilitats alternatives que, a priori, permetin minimitzar els riscos concurrents.

Caldria concretar els possibles usos no lectius, a efectes de valorar la concurrència d'un ús domèstic a efectes de l'aplicació de la normativa de protecció de dades.

En qualsevol cas, la normativa de protecció de dades no impedeix l'establiment de mesures de prohibició o limitació de l'ús dels mòbils a l'entorn educatiu, en els termes exposats al dictamen.

3.- Principals riscos que s'associen a la utilització dels telèfons mòbils en l'àmbit escolar (tenint en compte les consideracions fetes en els FJ VII a IX d'aquest dictamen):

- Navegació per Internet -a través del telèfon mòbil- sense supervisió de pares o tutors o, si escau, sense supervisió dels responsables en l'àmbit educatiu (mestres o responsables del centre escolar).

- Manca de coneixement previ i d'informació adequada sobre les condicions d'ús, o sobre les polítiques de privacitat, i de les mesures de seguretat de les eines, apps, etc, que utilitzen.

- Manca de coneixement i de valoració del risc que suposa difondre informació personal pròpia i de terceres persones (particularment, facilitar dades que els ubiqui en temps i espai).

- Riscos a conseqüència d'establir comunicació amb persones desconegudes (xatejar amb estranys, desconèixer mecanismes d'autoprotecció per confirmar identitat de persones amb les que connecten), etc.

- Captació i difusió inadequada d'imatges pròpies i de terceres persones, sense el seu consentiment. Afectació pels drets a l'honor i a la intimitat personal i familiar i a la pròpia imatge de terceres persones.

- En relació amb el factor edat i la capacitat d'exercir els propis drets de protecció de dades, la distinció que pot ser rellevant a efectes d'avaluar riscos, als efectes de la normativa de la protecció de dades, seria la distinció entre menors d'edat, majors o menors de 14 anys.

Barcelona, 13 de febrer de 2023