1. A PRIVACIDADE NAS REDES SOCIAIS

É importante ter claro o concepto de privacidade nas redes sociais porque, como xa quedou sinalado, é a principal fonte de problemas derivados do seu uso.

Á hora de elixir unha rede social para usar na escola é fundamental asegurar esta privacidade, e é por iso polo que non é aconsellable o uso de redes xeralistas do tipo de Facebook ou Twitter, agás para alumnado maior de 14 anos. Aínda así, nese caso convén dedicar un tempo a explicar e deixar claras as recomendacións de privacidade.

Pensemos que as redes sociais son espazos que aparentemente se usan de balde. Remarcamos o de "aparente" porque inda que non se paga en metálico polo seu uso, si que se paga cos datos persoais. As redes sociais son espazos creados para intercambiar información, algo esencial na sociedade de hoxe que se move por e para a información, e onde posuíla implica control e poder. Alguén comparaba a información persoal que deixamos nas redes sociais con graos de area. Dispoñer dun puñado de graos de area está ao alcance de calquera e non supón nada importante. Pero o que teña a posibilidade de manexar, manipular, toneladas de graos de area, si que dispón dun importante capital. Iso é o que ocorre coas redes sociais. Dispoñen da facultade de manexar e cruzar millóns de datos de todo tipo dos seus usuarios, desde imaxes a afeccións pasando por tendencias políticas, hábitos de consumo ou relacións persoais.

Por todo isto, o que os membros das redes sociais proporcionen información persoal e privada de forma gratuíta, fai das redes sociais un fenómeno xenuíno e que necesita ser comprendido.

2.1. Que entendemos por privacidade nas redes sociais

Enténdese por privacidade o nivel de protección de que dispoñen todos os datos e informacións que unha persoa introduce nunha rede social, en canto ao grao de accesibilidade a eles que outros usuarios ou internautas poden ter.

A configuración da privacidade depende en gran medida do usuario, pero non exclusivamente. Ao depositar os nosos datos na rede social podemos configurar o que e a quen queremos que se mostren, pero non debemos esquecer que eses datos están depositados no servidor da rede e –como xa vemos de cando en vez– pode ser que haxa ataques a ese servidor e que os datos acaben circulando por onde non desexamos.

Por outra parte, aínda no caso de restrinxir a nosa información só para os nosos contactos, non temos o control do que eses contactos poden facer con ela. Xa vimos casos de imaxes e vídeos íntimos, compartidos inicialmente só con contactos moi determinados, circulando de forma viral por toda a Rede.

No caso dos adolescentes, ademais, dáse a situación moitas veces de que aceptan como contactos a persoas descoñecidas, o que equivale a darlle a chave da súa información persoal. Nestas situacións non vale de nada a configuración de privacidade, porque se abre unha porta a persoas estrañas.

A privacidade tamén se pode ver comprometida cando usamos os perfís das redes sociais para rexistrarse noutros servizos de Internet. Seguramente máis dunha vez vistes estes servizos nos que, para supostamente facilitarnos o proceso de rexistro, nos dá a

posibilidade de loguearnos co noso perfil de Facebook. Desta maneira estamos dando a oportunidade a ese servizo de acceder a determinados datos da nosa conta de Facebook, algo non moi seguro.

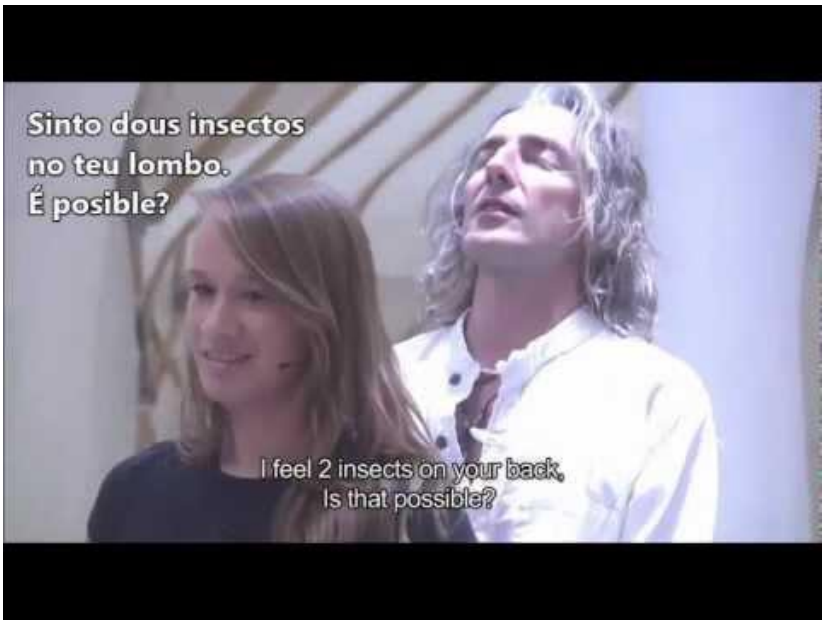
Ante todo isto é posible que moitas persoas pensen que o mellor é prescindir totalmente das redes sociais, xa que non existe a privacidade total. Non hai que caer tampouco na paranoia, senón utilizar sobre todo o sentido común. Hai tempo circulaba o dito de que non subas a Internet esa foto da que túa avoa se avergonzaría. Algo de certo hai diso. Por moito que se configure a privacidade nas redes, en vista do que xa vimos que pode ocorrer, o máis aconsellable é non subir informacións, fotos ou vídeos que non deberían saír do ámbito familiar o de amizade.

As redes sociais son ferramentas que se poden usar ben ou usar mal. Está en mans do usuario a responsabilidade de coñecer e saber usar as súas opcións de privacidade. Non é algo sinxelo porque hai intereses contrapostos entre usuarios e redes. Normalmente o usuario quere controlar a súa privacidade, mentres que as redes prefiren o contrario. A menor control de privacidade, máis datos se moven na rede, aumentando o tráfico dentro dela e, en consecuencia, a publicidade, que é do que viven realmente. Así os usuarios atopan varios problemas:

- Moitas persoas non son conscientes das consecuencias que certas publicacións poden ter no presente e no futuro. E os adolescentes son especialmente susceptibles.
- As redes no facilitan especialmente a xestión da privacidade. Son condicionados longos, pouco transparentes e ás veces pouco entendibles.
- Para complicalo máis, as redes cambian os seus condicionados e moitas veces sen sequera notificar ao usuario.
- Os usuarios non teñen claro o destino dos seus datos e para que se empregan.

Por todo isto, e para minimizar os riscos, sobre todo cos menores, é polo que recomendamos o uso de redes sociais estritamente educativas, nun contorno pechado. Aínda así é importante coñecer o funcionamento da privacidade nas redes xeralistas porque pode darse o caso de que en determinadas circunstancias, e con alumnado maior de 14 anos, desexemos aproveitar algunhas das súas potencialidades.

A modo de introdución á privacidade nas redes sociais, recomendamos o visionado destes dous vídeos que, dirixidos a distintas idades, pode dar pé a comentar a importancia da privacidade co noso alumnado.



2.2. Cláusulas de privacidade nas redes sociais. Lexislación de terceiros países.

Á hora de falar de privacidade e saber que é o que regulan as cláusulas das redes sociais, convén deixar claro o que entendemos por datos de carácter persoal.

Un dato de carácter persoal é calquera información referente a persoas físicas que nos pode identificar ou facer identificable.

No estado español estes datos están protexidos pola Lei Orgánica 15/1999 de Protección de Datos Persoais (LOPD) e o Real Decreto 1720/2007 que regula o seu desenvolvemento.

Os riscos que presentan as redes sociais respecto á protección de datos persoais son:

- Os datos poden ser comunicados, cedidos ou postos a disposición de terceiros por diversas razóns, entre a que destaca a comunicación a terceiros para realizar accións de márketing directo.
- Os textos legais referidos á protección de datos persoais que se poñen a disposición dos usuarios frecuentemente non son comprensibles polos usuarios, ou estes non dispoñen de experiencia ou formación xurídica. Ademais estas cláusulas de privacidade están en moitos casos publicados en lugares de difícil acceso e localización.

Por todo isto, o Observatorio da Seguridade da Información di que *"todo iso levounos á non lectura na gran maioría dos casos dos avisos legais e políticas de privacidade, e naqueles casos nos que son revisados polos usuarios, non son realmente comprendidos, polo que non cumpren o seu obxectivo principal, que é que o usuario coñeza absolutamente toda a información relativa á finalidade do tratamento dos seus datos persoais e a gran cantidade de implicacións que comporta o seu tratamento"*.

Proba de que a maioría das persoas non se molestan en ler as cláusulas de condicións á hora de rexistrarse nunha rede social é o caso de GameStation. Este servizo, para chamar a atención sobre este feito de que a xente non le a "letra pequena", permitiuse gastar unha broma que serviu de experimento social. Nas súas cláusulas incluía como condición: "Ao enviar unha orde de compra pola web o primeiro día do cuarto mes do ano 2010, Anno Domini, estás de acordo en concedernos a opción non transferible de reclamar, por agora e para sempre, a túa alma inmortal. Se desexamos exercer esta opción, permitirás rendir a túa alma inmortal e calquera reclamación que podas ter sobre ela nun prazo de cinco días laborables tras recibir a notificación escrita de Gamestation ou un dos seus secuaces debidamente autorizados". O resultado: máis de 7500 persoas aceptaron os seus termos, incluída esta cláusula.

Tamén é certo que ler todas as cláusulas é unha tarefa ardua e que leva tempo. Un estudo feito hai algún tempo indicaba que se tiveramos que ler todas as políticas de privacidade que aceptamos durante un ano, necesitaríamos dedicar uns 40 minutos ao día.

A idade legal.

En relación ao consentimento outorgado por menores, no estado español non existe ningunha regulación ao respecto. Só a Lei de Protección de Datos (LOPD) referida á idade á que un menor pode prestar o seu consentimento para transferir datos de carácter persoal e aceptar, por exemplo, unhas condicións de uso dun servizo en Internet.

O Real Decreto 1720/2007, ao que xa nos referimos antes, no seu artigo 13, que fala do consentimento para o tratamento de datos de menores de idade, di:

> *Poderase proceder ao tratamento dos datos dos maiores de catorce anos co seu consentimento, salvo naqueles casos en que a lei esixa para a súa prestación a asistencia dos titulares da patria potestade ou tutela. No caso dos menores de catorce anos, requirirase o consentimento dos pais ou titores.*

Así pois os datos persoais do alumnado de 14 ou máis anos poden ser xestionados por eles mesmos e polo tanto dispoñen de potestade para obter as súas propias contas e servizos de Internet. Esta modulación da idade esténdese tamén para a autorización da propia imaxe. Para os menores de 14 anos sempre será necesario o consentimento dos

pais ou titores legais. De non cumprirse este requisito, o seu consentimento non é válido.

Para o uso de redes sociais privadas, onde só teñen acceso os alumnos e os seus profesores en principio só sería necesaria a autorización paterna para os menores de 14 anos en canto á alta na rede se refire e o uso dos seus datos na mesma, xa que as publicacións que realice permanecerán no mesmo ámbito escolar. É algo equiparable a expoñer os traballos realizados polo alumnado no taboleiro de anuncios da clase. No entanto, como medida aplicable a outros ámbitos diferentes ás redes sociais, como blogs, wikis, páxina do centro educativo, etc., é moi aconsellable pedir a autorización do pai ou da nai tamén para os alumnos de idades comprendidas entre 14 e 18 anos.

Deste xeito ,tendo en conta o contexto máis amplo do centro educativo, sexa cal for a idade do alumno menor de idade, débense pedir dúas autorizacións: unha para o uso da propia imaxe e datos do alumno (fotografías, vídeos, alta en servizos, etc.) e outra para a publicación de traballos escolares. Nestas autorizacións debe intentar detallarse, na medida do posible, os servizos que serán utilizados.

A regulamentación de protección de datos tamén impón ás redes sociais á obriga de realizar as indagacións oportunas para establecer a idade real do usuario que pretenda acceder aos seus servizos. De detectar que un usuario non posúe a idade legal permitida, resérvanse o dereito de revocar dito consentimento e suspender, cancelar ou expulsar a conta.

Por suposto que todos e todas, como ensinantes que sodes, coñecedes moitos casos de menores de 14 anos que teñen contas en redes sociais. Desde logo, están incumprindo as normas. Segundo datos do Ministerio de Interior, o 19% dos menores de 11 anos teñen creado un perfil nunha rede social. Hai quen di tamén que este comportamento laxo das redes sociais á hora de verificar a idade vai cambiar porque pronto lles interesará saber a idade dos seus usuarios por intereses particulares. O recoñecemento biométrico (voz e facial sobre todo), son os métodos implementados máis viables polo momento.

Sendo realistas hai que recoñecer que as comprobacións de identidade realizadas durante o rexistro a calquera servizo na Rede accesible desde o estado español que non realice transferencias comerciais, e máis se é de balde, brillan pola súa ausencia. As únicas excepcións atopámolas nas páxinas de xogo online baixo o dominio *.es*, que están reguladas polo Ministerio de Facenda. O motivo real non é protexer ao menor, senón que se un xogador gaña cartos, ten que tributar os beneficios e polo tanto ao Ministerio interésalle saber quen está detrás do perfil gañador.

Se tedes experiencia rexistrándovos nunha rede social saberedes que o único requisito de verificación da idade é encher unha caixa coa data de nacemento, sen ningunha outra comprobación. Evidentemente, se unha rede social que, lembremos, vive dos datos proporcionados polos seus usuarios, dificultara o proceso de rexistro e esixira excesivas comprobacións de identidade, probablemente non tería moito futuro.

Ademais, supoñendo que as redes sociais estiveran dispostas a realizar comprobacións de identidade, só poderían levarse a cabo cos usuarios do estado onde operan, debido ás implicacións xurídicas y de seguridade nas transferencias de datos persoais entre estados.

Actualmente a idade legal para rexistrarse nun servizo de Internet é de 14 anos inda que é posible que cambie a partir do 25 de maio de 2018, cando entre en vigor o Regulamento Europeo de Protección de Datos, que establece unha franxa entre os 13 e os 16 anos, a criterio de cada país. É dicir, que podería darse o caso de que no estado español se estableza como nova idade os 16 en lugar dos 14 actuais. Ou pode ser que opte polos 13.

Acceso aos nosos datos

Todas as redes ofrecen, inda que de forma non sempre moi clara, opcións para restrinxir o acceso aos nosos datos e información por parte de terceiros, hai condicións que, se queremos rexistrarnos, temos que aceptar si ou si, e que en certo modo comprometen os nosos datos. Trátase dos datos nosos que comparten con outras empresas. Non é, como moitos pensan, unha cesión de datos, algo castigado polo noso ordenamento xurídico. O que fan é compartir datos persoais disociados da identidade. Un dato disociado non serve para identificar a ninguén.

Algo que moitas persoas descoñecen é que moitas redes sociais, nesas cláusulas que aceptamos ao rexistrarnos, son libres de facer uso dos contidos que publiquemos na rede. O caso máis coñecido é o de Facebook. Inda que a propiedade intelectual segue pertencéndonos, desde o momento en que publiquemos algo (fotos, vídeos, textos...) estamos autorizando a Facebook a facer o uso que crea más conveniente, sen dereito a recibir nós ningunha remuneración ou contrapartida. O mesmo, de forma similar, ocorre con outras redes como Twitter, Instagram ou Google+.

Un dos principais problemas que se atopa á hora de regular a privacidade nas redes sociais é o feito de que a gran maioría delas ten como sede un país alleo á Unión Europea, normalmente Estados Unidos. E no caso de ter que resolver algún conflito o demanda hai que facelo en tribunais doutros países. Por exemplo, o apartado 15.1 dos termos legais de Facebook establece di claramente: “Resolverás calquera demanda, causa de acción ou conflito (colectivamente, "demanda") que teñas connosco xurdida de ou relacionada coa presente Declaración ou con Facebook unicamente no tribunal do Distrito Norte de California ou nun tribunal estatal do Condado de San Mateo, e aceptas que sexan devanditos tribunais os competentes á hora de resolver os litixios de devanditos conflitos. As leis do estado de California rexen esta Declaración, así como calquera demanda que puidese xurdir entre ti e nós, independentemente das disposicións sobre conflitos de leis”. En parte esta cláusula é consecuencia do pouco interese dos gobernantes españois por esixir a aplicación da lexislación local ao xigante de Facebook. Non sucedeu así con Alemaña, e no apartado 16.3 dos mesmos termos de Facebook di: “As condicións aplicables especificamente aos usuarios de Facebook en Alemaña están dispoñibles aquí” (e inclúe un enlace ás condicións en alemán). De todos modos, isto é algo que vai cambiar coa entrada en vigor o vindeiro ano do Regulamento Europeo de Protección de Datos, do que xa falamos. Como ben di Víctor Salgado, socio director do bufete especializado en dereito informático *Pintos & Salgado*, “a entrada en vigor no 2018 do próximo Regulamento Europeo de Protección de Datos será unha dura proba de lume para as redes sociais. Obrigaralles máis a protexer, informar, solicitar consentimento que como no caso da cesión de datos deberá ser expreso. Non se poderá, como fixeron agora, marcar unha caixa senón que será o usuario quen o faga”.

Por se desexades ampliar a información polo miúdo sobre as cláusulas de privacidade dos principais servizos e redes sociais xeralistas, indicámosvos os enlaces directos ás páxinas onde as detallan.

Facebook	Instagram	Flickr (Yahoo)
Twitter	Snapchat	WhatsApp
Google+	LinkedIn	Youtube

E por se queredes saber máis sobre as cláusulas e condicións das distintas redes sociais e principais servizos de Internet, é moi recomendable o proxecto de Jorge Morell Ramos, Términos y Condiciones, onde se centra na análise e revisión das condicións legais de milleiros de servizos existentes en Internet. Ten unha sección dedicada enteiramente á análise e seguimento das cláusulas de condicións, rexistrando todos os cambios.

2.3. O que as redes saben de nós.

É habitual que leamos críticas nos medios de comunicación sobre o que as redes sociais chegan a saber de nós, toda a información que posúen sobre a nosa vida e os nosos hábitos. E lido así parece que os "malos" da película son precisamente as redes sociais. Non é de todo correcto.

As redes sociais non son omniscientes, pero si que son boas alumnas. Teñen equipos moi ben formados, con métodos eficaces, para aproveitar toda a información que os seus usuarios entregan voluntariamente. Ninguén ten a obriga de rexistrarse nunha rede social. Cando alguén o fai, como xa vimos, acepta unha serie de cláusulas –inda que non as lea– e nesas cláusulas consente achegar unha información básica determinada. Pero é que despois, co uso cotiá dos servizos da rede, segue regalando información. Información que se transforma en datos que, combinados sabiamente, constitúen a fonte de ingresos da rede social.

Para que nos fagamos unha idea: o 84% dos ingresos de Facebook proveñen dos anuncios en dispositivos móbiles. Hai catro anos apenas supoñían o 23%, mentres que hai dous apenas tiña un peso do 69%. Por poñelo en números, os anuncios en móbiles levaron 6.850 millóns de euros ás arcas de Facebook no último trimestre de 2016.

As redes sociais normalmente teñen catro vías para coñecer información sobre os seus usuarios: a actividade da conta, os *clicks* nos enlaces, os *likes* e o dispositivo e localización desde o que se accede.

Para facernos unha idea, estes son os datos que pode chegar a manexar unha rede social de tipo xeralista, como Facebook:

- O teu enderezo persoal e o lugar de traballo, todo isto sen necesidade de que llo digamos. Son os datos proporcionados pola xeolocalización.
- Os teus estudos. Sabendo isto tamén pode chegar a saber os teus intereses.
- A composición do teu fogar. Non serán os mesmos gustos se tes fillos, por exemplo, que se non os tes.
- Se estás cerca de familiares ou non. Detecta, por exemplo, se fas viaxes con frecuencia a un lugar determinado.

- Se algún dos teus contactos vai casar, comprometeuse, tivo descendencia, cumpre ou vai cumprir anos...
- O teu traballo e o sector laboral ao que pertences. E tamén en que traballan as persoas coas que te relacionas.
- O sistema operativo do teu equipo, o navegador co que accedes, a resolución de pantalla, mesmo o teu operador de Internet ou telefonía, a marca do teu dispositivo móbil, o idioma que tes configurado...
- O tipo de tendas nas que compras, os restaurantes que che gustan, as viaxes que fas, as aeroliñas que usas...
- Se fas compras online.
- Os programas de televisión que ves.

Recoméndovos, se tedes interese neste tema, que visitedes este artigo de The Washington Post titulado 98 datos persoais que Facebook utiliza para orientar a súa publicidade (en inglés)

2.4. Riscos referentes á privacidade nas redes sociais.

Poderiamos dicir que practicamente todos os riscos relacionados coas redes sociais teñen a súa orixe na perda da privacidade, ben sexa porque a persoa usuaria non é celosa dos seus datos, ben por un ataque á conta ou a rede social con roubo de datos, ou ben por uso indebido por parte de terceiras persoas. Pasamos a sinalar algúns dos problemas que se poden presentar.

- Xeolocalización. O uso maioritario dos dispositivos móbiles para o acceso a Internet, e en consecuencia ás redes sociais, agudiza este problema. É moi habitual que se leve activada a xeolocalización nos móbiles, ben para usar mapas, aplicacións de recomendacións de lugares próximos, etiquetado de ubicacións de fotos ou, simplemente, porque a persoa usuaria nin sabe que a ten activada ou non coñece como quitala. Isto comporta que estamos divulgando datos dos nosos hábitos cotiáns, porque grazas a isto se pode coñecer onde vivimos, onde traballamos ou estudamos, que lugares frecuentamos ou a onde viaxamos. Datos que, cruzados con outros tamén extraídos do uso das redes sociais, dan unha completísima información que pode ser utilizada de moitas maneiras.
- Difusión de imaxes propias e de terceiros. Inda que se usan habitualmente para compartir imaxes, as redes sociais non son os instrumentos máis axeitados para usar como repositorio ou almacenaxe das fotos persoais. Que aleguemos que só son visibles para os contactos non achega ningunha seguridade, porque eses contactos poden replicar a imaxe noutros lugares da rede fóra do noso control. O problema agrávase cando ademais colgamos fotos de terceiras persoas, pudendo comprometer tamén a súa privacidade polas mesmas razóns. Hai servizos en Internet moito máis axeitados para almacenar fotos e compartilas de modo máis seguro, como é o caso de Flickr ou otros lugares similares. De calquera xeito, hai que ter sempre presente que, ao contrario do que sucedía na era analóxica, na que as fotos se ensinaban en papel e logo se volvían a gardar, na era dixital xa non se ensinan: regálanse. Derivado do uso indebido das imaxes vén o fenómeno do sexting.
- Etiquetado. Os hashtags ou etiquetas, algo consubstancial ás redes sociais, facilitan moitas tarefas na busca de información, pero tamén poden comportar riscos para a

nosa privacidade. Que unha terceira persoa poda vincular un determinado comentario ou imaxe ao noso perfil, pode vincular o noso nome a unha publicación que non teremos porque compartir precisamente.

- Contactos. As redes sociais funcionan en base a relacións entre persoas. Pero cada rede ten unhas características propias. Así mentres en Facebook estas relacións deben ser mutuas, Twitter admite que sexan nunha soa dirección, e outras poden chegar a ser totalmente abertas por defecto. Polo tanto, os graos de privacidade son diferentes e a forma de configurar esa privacidade tamén. Pero por moi axustada que poda ser a configuración de visibilidade dos nosos datos, reducíndoa mesmo só ás nosas amizades e nin sequera ás "amizades das nosas amizades", nunca estaremos a salvo de indiscrecións e malas prácticas dos nosos propios contactos. Non digamos xa se se adopta un criterio laxo á hora de admitir persoas na nosa rede de contactos.
- Roubo o perda do dispositivo. Algo impensable hai uns anos, cando a conexión era a través dun equipo fixo na nosa casa. Perder o que che rouben o móbil non é algo tan estraño e dentro dese dispositivo portamos moita información persoal propia e de terceiros. Non adoptar medidas como o bloqueo mediante contrasinal, patrón de movemento ou pegada dixital o noso equipo, establecer contrasinais para acceso ás apps que almacenan información sensible ou que permiten o acceso aos nosos datos na nube ou usar servizos de localización e borrado remoto do noso móbil, poñen en bandexa todos os nosos datos persoais.
- Virus. Hai moitos anos, nos seus inicios, os virus informáticos facíanse notar decontado, porque facían que o ordenador funcionase de forma anómala. O comportamento dos virus hoxe en día mudou totalmente, porque o seu obxectivo é o roubo de datos persoais, principalmente contrasinais, polo que son en ocasións moi silenciosos e non nos decatamos de que están actuando ata que é demasiado tarde. Os métodos para que eses virus entren nos nosos dispositivos son normalmente do tipo de enxeñería social.

2.5. Identidade e reputación dixital.

Estivemos vendo as consecuencias da perda de privacidade nas redes sociais e en Internet en xeral. Son moitos os riscos que poden derivar da falta de privacidade. Pero tamén é importante contemplar este aspecto desde o punto de vista da identidade dixital.

Entendemos por identidade dixital toda aquela información publicada sobre un individuo en Internet e que se xera e comparte usando medios dixitais e tecnolóxicos. É unha información dinámica que evoluciona en función das interaccións do usuario e da información que se publique sobre un mesmo. Ademais, non desaparece polo paso do tempo e é accesible para calquera.

Desta definición parte a de reputación, online ou non. É a opinión que outras persoas teñen sobre nós. Trátase dunha consideración social subxectiva, construída colectivamente e que ten unha connotación da que se derivan tanto efectos positivos como negativos.

Cando os menores –e os adultos– interactúan nunha rede social, están compartindo e facendo públicos, con máis ou menos expansión, as súas imaxes, os seus gustos, as súas

afeccións, comportamentos... Trazan, con todo isto a súa identidade dixital. E pode darse o caso de que esta identidade supoña un condicionamento negativo cando sexan adultos, é dicir, unha reputación online negativa.

Ás veces son os propios menores os que non teñen en conta as consecuencias futuras do que comparten na Rede, pero outras veces son os pais e nais os que tampouco paran a pensar nisto. Nos primeiros anos do menor, son os responsables da súa imaxe dixital. Usar Facebook como álbum de recordos do fillo ou filla pode supoñer un verdadeiro problema. O director da Aula de Infancia e Adolescencia da Universitat Politècnica de València, Vicente Cabedo Mallol, explícao cun exemplo concreto: “Imaxinemos que non coñecemos a identidade dos fillos do ciclista Lance Armstrong, sancionado para sempre por dopaxe. Que ocorrería se o ciclista etiquetara en Facebook aos seus fillos? Transvasaríase a mala reputación aos seus fillos? Serían sinalados publicamente (audiencia planetaria) como 'os fillos do ciclista dopado'? Por que expoñelos dese modo e con que utilidade?”.

Polo tanto é fundamental dar a coñecer estes conceptos e as súas consecuencias ao alumnado. E deixar claro que a súa identidade dixital se constrúe non só nas redes xeralistas como Instagram ou Facebook, senón tamén nas redes sociais cerradas que podamos crear no centro educativo. Están interactuando con compañeiros e con profesores e polo tanto, igual que na vida offline, están dando unha imaxe de si mesmos. Por iso son tan importantes as normas de netiqueta, é dicir, as normas de comportamento na Rede.

É interesante que polo menos botedes unha ollada ao documento que tedes no curso, "Monográfico gestión de la privacidad e identidad digital" publicado por Red.es porque vos pode ampliar moito toda a información sobre este tema da privacidade e a imaxe dixital.