¿Entornos seguros? Las tecnologías intensivas en datos en los institutos de Barcelona

eticas

Eticas R&C

Este documento es un resumen del informe realizado con el soporte del Ayuntamiento de Barcelona para el proyecto “Entorns Segurs”. El proyecto fue llevado a cabo por Gemma Galdon Clavell, Mariano Martín Zamorano y Olalla Losada.

Autor: Lorenzo Olivieri. Editores: Emma Ahlert y Miguel Á. Valbuena León.

Resumen

Las tecnologías digitales están cada vez más presentes en las escuelas, en forma de bases de datos, plataformas educativas o redes sociales. Si bien estas herramientas pueden mejorar los procesos de aprendizaje y la vida de los estudiantes, la cantidad de datos que recogen y comparten también podría dañar su privacidad, así como otros derechos fundamentales. Para analizar algunas de estas cuestiones, Eticas llevó a cabo un proyecto que involucró a las comunidades educativas de cuatro escuelas de Barcelona. El objetivo de este trabajo era poner de manifiesto si las prácticas asociadas a la utilización de estos sistemas cumplen con el marco legal establecido por la Unión Europea y por el gobierno catalán. A través de entrevistas con profesorado, estudiantes, madres, padres y personal de las escuelas, nuestra investigación ha demostrado una falta general de conocimiento y conciencia sobre cuestiones relativas al ciclo de vida de los datos, formularios de consentimiento o la identidad digital. Los heterogéneos protocolos y requisitos desplegados por las escuelas, las lagunas legislativas y la ausencia de información específica para profesorado, madres y padres sobre la protección de los datos de los estudiantes, son algunos de los factores que contribuyen a hacer del uso y la presencia de las tecnologías en ambientes educativos un fenómeno problemático.

Agradecimientos

El equipo Eticas desea dar las gracias al Ayuntamiento de Barcelona por el apoyo recibido para la realización de este estudio, así como a las autoridades del Departament d'Ensenyament, el Consorcio de Educación de Barcelona y la Autoridad Catalana de Protección de Datos, que aceptaron ser entrevistados para esta investigación. También queremos agradecer a las autoridades escolares, profesorado, madres, padres y estudiantes del Instituto Milà i Fontals (Raval), la Escola Vedruna (Raval), el Instituto Menéndez y Pelayo (Sarrià) y el Institut Voramar (Poble Nou), que participaron en el trabajo de campo.

Introducción

Las tecnologías de la información y la comunicación (TIC) están transformando cada vez más aspectos de la vida cotidiana, y los entornos educativos no son una excepción. Diferentes tipos de tecnología, que varían en su propósito, intervienen en las actividades de estudiantes, profesorado y personal en las escuelas. Bases de datos, tecnologías y plataformas educativas, redes sociales y búsquedas online se utilizan cada vez más en este contexto. Sin embargo, aunque la literatura ha destacado los efectos positivos de tales sistemas en la vida de los estudiantes y en la gestión escolar, se ha prestado menos atención a los riesgos asociados a su uso (Rosen y Santesso, 2014; Taylor, 2013; Richards y Stebbins, 2014; Tierney y Koch, 2016). Un hilo conductor entre estas tecnologías es la gran cantidad de datos personales que pueden reunir y procesar, planteando preguntas y preocupaciones con respecto a la privacidad y la protección de datos de los estudiantes. Estos problemas son aún más relevantes en el ámbito educativo. No sólo porque la privacidad es un derecho humano fundamental, sino porque los menores de edad son especialmente vulnerables. No hay que olvidar que la edad escolar es, en esencia, un período de experimentación. Los niños y adolescentes cometen errores, aprenden lecciones cruciales y desarrollan sus personalidades. Registrar y almacenar información personal durante este período delicado puede pues tener consecuencias negativas a largo plazo, dado que en muchos casos condiciona el derecho de los menores a ser olvidados.

Para abordar estas cuestiones y analizar la relación entre los entornos educativos y la protección de datos, Eticas condujo una investigación de campo diseñada para explorar cómo profesorado, alumnado y familias perciben y hacen frente a los problemas de privacidad que plantean las tecnologías educativas y administrativas. Con este concepto en mente, el proyecto *Entorns segurs* analizó el uso de las tecnologías intensivas en datos en cuatro escuelas secundarias de Barcelona, correspondiente a tres barrios con diferentes situaciones sociodemográficas. El objetivo de nuestra investigación fue evaluar si la

proliferación de las mencionadas tecnologías en entornos educativos se ha desarrollado e implementado siguiendo prácticas, normas o protocolos que garanticen de forma eficaz la protección de los datos de los estudiantes.

Enfoque metodológico

Nuestro estudio cualitativo se llevó a cabo en cuatro escuelas secundarias de Barcelona y se articuló en torno a cuatro variables principales:

1) el tipo de tecnología utilizada para recopilar datos,
2) el ciclo de vida de los datos recogidos y tratados por los institutos,
3) el cumplimiento con el conjunto de leyes, normas, recomendaciones y políticas que orientan y regulan la protección de datos en el entorno escolar, y
4) el concepto de aceptabilidad. Con la noción de aceptabilidad nos referimos no sólo a la funcionalidad y eficacia de la tecnología, sino, más en general, a las representaciones sociales sobre su utilización, que incluye dimensiones como el conocimiento, consentimiento y confianza.

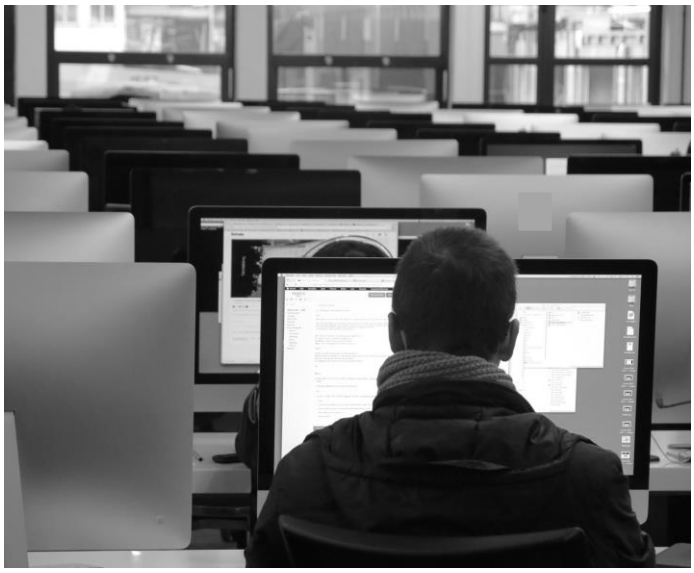
Para la recolección de los datos se adoptaron tres estrategias principales. En primer lugar, mediante una investigación de escritorio se revisó la literatura relevante en los campos de la privacidad y la educación, incluyendo los marcos legales y normativas vigentes en Catalunya, España y en la Unión Europea. En segundo lugar, se llevaron a cabo diecisiete (17) entrevistas para conocer los puntos de vista y opiniones de los agentes que actúan en los contextos educativos. Para proporcionar una perspectiva amplia, el proyecto incluyó una muestra de investigación que incluyó el dominio socio-institucional (incluyendo el Consorcio de Educación de Barcelona y el Departament d'Ensenyament, así como expertos de diferentes universidades de Barcelona) y las comunidades de las escuelas (alumnado, profesorado y autoridades de las escuelas estudiadas). Las diecisiete entrevistas semiestructuradas fueron realizadas a cuatro docentes, cuatro

personas correspondientes al personal directivo, un padre, una secretaria, cinco representantes gubernamentales, y dos expertos académicos.

Por último, se realizaron cuatro grupos focales con estudiantes de entre 14 y 16 años de edad (un grupo por cada centro educativo) y un grupo de discusión con los padres y madres y representantes de la AMPA de un colegio. Las cuatro escuelas (Milà i Fontals, Menéndez y Pelayo, Vedruna y Voramar) fueron seleccionadas de acuerdo a criterios socioeconómicos, teniendo en cuenta los ingresos medios de cada barrio[1] (Raval, Poble Nou y Sarriá) y su diversidad cultural.

Los documentos y las transcripciones de las entrevistas se analizaron mediante análisis de contenido básico y análisis del discurso, a través de un proceso iterativo en el que las categorías se determinan a partir de los datos reunidos.

Marco legal e institucional de la protección de datos en la educación de Barcelona



España y la Unión Europea han desarrollado políticas que, en muchos casos, incentivan la difusión de las tecnologías digitales para el trabajo escolar y un conjunto de leyes que tienen por objeto garantizar los derechos de los estudiantes a la privacidad. En 1995, el Parlamento Europeo estableció la Directiva Nº 95/46 / CE, que aboga por la protección de las personas físicas, el tratamiento seguro de los datos personales y de la circulación de datos. El Artículo 28 de la presente norma

[1] Véase: https://www.idescat.cat/pub/?id=aec&n=414&lang=es

indica la necesidad de un tratamiento lícito y leal de los datos personales, los cuales deben ser adecuados, pertinentes y no excesivos.

Sin embargo, no fue hasta 2016 que el Parlamento Europeo revisó y reforzó las normas de protección de datos mediante la promoción del Reglamento General de Protección de Datos (GDPR), que ha cambiado marcadamente la forma en que empresas, organizaciones e individuos deben gestionar los datos personales. Al analizar esta nueva regulación, que entró en vigor en mayo de 2018, es útil considerar sus definiciones de "datos personales" y "procesamiento de datos". La información personal es definida como:

> "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;" (Art. 4).

El mismo Artículo (4) define como actividades de tratamiento de datos a:

> "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

Como señalan Wright, De Hert, y Kloza (2011, 13), este conjunto de actividades realizadas durante el tratamiento de datos personales no concierne simplemente a cuestiones de privacidad. Estos procesos tienen impacto en una amplia gama de derechos como la libertad de expresión, los derechos de propiedad, el derecho a

la no discriminación, los derechos del niño y el derecho a la salud. Para garantizar el respeto de estos derechos, el GDPR aplica y refuerza distintos principios éticos al procesamiento de los datos personales. En primer lugar, los datos deben ser procesados de forma legítima, justa y transparente. En segundo lugar, los datos deben recogerse para y con fines legítimos y explícitamente especificados (principio de limitación de la finalidad). Del mismo modo, de acuerdo con el principio de anonimización de los datos, los datos personales deberán ser adecuados, pertinentes y limitados a los fines para los que son recopilados.

Además, el GDPR establece criterios y requisitos más precisos y restringidos que la normativa previa a la hora de asegurar la protección de datos. Por un lado, se extienden las categorías de los datos especialmente protegidos, incluyendo datos biométricos, genéticos y de salud. Por otro lado, el GDPR también fortalece los derechos ciudadanos indicando que el consentimiento debe ser otorgado mediante un "acto afirmativo claro", y establece que las personas tienen derecho a obtener información del controlador (responsable último de los datos) sobre sus datos personales y a acceder a los mismos (Art. 15). Por último, el GDPR delimita el derecho a la supresión de los datos personales, que debe ser concretado por el controlador sin demora indebida ("Derecho a ser olvidado", Art. 19).

Si bien los requisitos establecidos por el GDPR se aplican a todos los dominios socioeconómicos, el reglamento también introduce requerimientos y consideraciones específicos relativas a los menores y a los ambientes educativos. Como podemos leer:

> "Los niños merecen una protección específica con respecto a sus datos personales, ya que pueden ser menos conscientes de los riesgos, las consecuencias y las garantías en cuestión y de sus derechos en relación con el tratamiento de datos personales. Dicha protección específica debe, en particular, aplicarse a la utilización de los datos personales de los niños para fines de venta o la creación de la identidades o perfiles de usuario (...)" (GDPR, Considerando 38).

Para situar nuestra investigación en el contexto específico de los institutos de Barcelona, se debe analizar el marco legal catalán e individualizar las instituciones y agentes responsables de promover e implementar el tipo de tecnologías que se utilizan en los centros escolares. Esto es importante porque los centros de Catalunya, de acuerdo con la Ley de Educación catalana (2009), son autónomos en la definición del uso de las tecnologías y en el desarrollo de herramientas para la educación digital. Los institutos son así designados como responsables de planificar la gestión pedagógica y sus aspectos tecnológicos, así como de distribuir las responsabilidades entre los miembros del instituto. Además de establecer dicha autonomía para los institutos, la Ley de Educación 12/2009 hace hincapié en la importancia de la adquisición de competencias en el campo TIC y en la necesidad de asignar responsabilidades al profesorado en este ámbito.

Todos estos requisitos han sido especificados en el Plan TAC, un proyecto desarrollado por el Departament d'Ensenyament, con los objetivos de: 1) planificar el desarrollo y la introducción de las TIC en las escuelas, 2) garantizar y promover la inclusión digital y las competencias tecnológicas entre el alumnado y el personal docente, 3) establecer medidas para proteger al alumnado de los contenidos inadecuados online, 4) asignar responsabilidades para la gestión de las tecnologías dentro de los institutos, 5) supervisar el cumplimiento de las normativas sobre el uso de la tecnología, en especial la Ley Orgánica 15/1999 sobre la protección de los datos personales, y la Ley de Propiedad Intelectual.

En Catalunya la protección de datos personales en las instituciones públicas es una competencia de la Generalitat y de la Autoridad Catalana de Protección de Datos (APDCat). Una serie de documentos han sido promulgados por la APDCat con el fin de delinear cual debe ser el tratamiento de los datos en las instituciones públicas. Uno de estos documentos, la Recomendación 1/2010, especifica que los

datos de carácter personal necesarios para el funcionamiento de un servicio o de una actividad pública, se encuentran bajo la responsabilidad del propietario del mismo. Esto implica que los datos recogidos sobre el alumnado estarán bajo la responsabilidad de la escuela o instituto. Sin embargo, esta recomendación también considera la posible externalización de determinados servicios de los institutos públicos a empresas privadas. Del mismo modo, sugiere, con el fin de evitar el mal tratamiento de datos, designar a una persona encargada de los datos. En esta línea, la APDCat ha desarrollado una "Guía básica para la protección de los datos en los institutos educativos". El documento hace hincapié en la exigencia del consentimiento, que debe ser inequívoco, libre, específico e informado, y en la calidad de los datos, que deben ser recogidos siguiendo los principios de proporcionalidad, lealtad, firmeza y precisión. La guía también establece los deberes a ser considerados durante el tratamiento de los datos, incluyendo la transferencia de datos a terceros, y otras acciones como la conservación y eliminación de datos.

De este modo, tanto la Unión Europea como las instituciones catalanas han establecido marcos legales y mecanismos institucionales que definen las reglas, límites y obligaciones a ser observados con el fin de garantizar los derechos de los estudiantes a la privacidad y a la protección de datos.

Los resultados del trabajo de campo: cuatro institutos de Barcelona

Es posible distinguir entre cuatro categorías principales de tecnologías utilizadas en los entornos educativos estudiados. Las tecnologías administrativas, como por ejemplo el software para la gestión de datos o los servicios de correo electrónico administrados por los consejos escolares y la administración pública. En segundo lugar, las tecnologías institucionales físicas, que son los sistemas utilizados para la seguridad y control en las escuelas, tales como sistemas de identificación biométrica o CCTV (circuito cerrado de televisión). La tercera categoría está formada por las denominadas *EdTech,* es decir aquellas tecnologías dedicadas a

la educación y a la pedagogía, como, por ejemplo, aplicaciones personalizadas o sistemas de gestión del aprendizaje. Finalmente, los dispositivos personales de los alumnos, como los teléfonos inteligentes, ordenadores personales o tabletas.

Teniendo en cuenta estas categorías, en esta sección se analizan los principales resultados del trabajo de campo realizado para el proyecto. La examinación sobre el uso de estos distintos sistemas y sus implicaciones para la privacidad, derivados del trabajo de campo, se organizan siguiendo un esquema analítico que va desde la descripción del escenario de los institutos de Barcelona en términos de gestión y protección de datos, a las definiciones y opiniones expresadas por las partes interesadas. Esta última dimensión del análisis es fundamental para el estudio, ya que nos permite situar cómo las tecnologías intensivas en datos identificadas son percibidas por cada uno de los actores que interactúan con ellas, y considerar de mejor modo cómo operan y pueden operar "en la práctica".

A. Las tecnologías y los procesos examinados

a.1) La extensión y externalización de las tecnologías de administración

En la última década, numerosas escuelas de Barcelona han adoptado servicios automatizados y digitalizados para la obtención y gestión de datos. Clickedu, por ejemplo, es una plataforma en la nube creada expresamente para las escuelas, que permite a los usuarios gestionar los expedientes académicos y acceder a información sobre el alumnado y las familias. También se utiliza por parte del personal directivo, del profesorado y de padres y madres para controlar la asistencia del alumnado y para comunicar información acerca de las tareas y los exámenes a las familias. Cabe mencionar que uno de los docentes entrevistados señaló que los estudiantes también mantienen un diario de papel, para que puedan aprender a gestionar y organizar sus tareas, sin que sus padres sean capaces de controlar todo a través de la web. Sin embargo, dicho profesor reconoce que Clickedu es una gran mejora con respecto a las modalidades utilizadas

anteriormente en los institutos, tales como discos rígidos o dispositivos USB. Considera que estos nuevos sistemas permiten registrar los accesos a la información y, en comparación con métodos anteriores, reducen el riesgo de virus. Igualmente, Esemtia es un sistema utilizado para funciones administrativas y pedagógicas, que permite a los profesores poder compartir los trabajos del alumnado o hacer comentarios sobre su tarea. También permite la comunicación diaria entre la escuela y las familias.

Estas plataformas reciben y gestionan una gran cantidad de datos sensibles, incluyendo los registros académicos (calificaciones, penalizaciones por retraso o conducta impropias, etc.), así como datos personales recogidos durante el proceso de inscripción (direcciones postales y de correo electrónico, números de teléfono, etc.). En este sentido, es importante tener en cuenta que la creciente externalización de la gestión de datos con fines administrativos afecta la privacidad del alumnado, ya que las escuelas confían en empresas privadas externas a la hora de brindar parte de estos servicios.

Se debe señalar que, junto a estas plataformas, algunas escuelas siguen empleando herramientas informales para gestionar los datos o comunicarse con las familias. Por ejemplo, se ha detectado que los documentos de Excel se utilizan para organizar los datos del estudiante y luego se comparten entre los padres y el personal escolar, mientras que las llamadas telefónicas o los mensajes SMS se utilizan para informar a las familias sobre distintos tipos de incidentes.

a.2) Las *EdTech* y su impacto sobre la privacidad

Como se mencionó anteriormente, se entiende como *edtech* a software, aplicaciones o dispositivos que se utilizan en los centros educativos específicamente con fines pedagógicos. En este marco es posible identificar tres tipos principales de tecnologías. En primer lugar, se encuentran los sistemas y aplicaciones que permiten organizar, supervisar y evaluar las tareas de los

estudiantes. En segundo lugar, los ordenadores o teléfonos celulares del alumnado o proporcionados por las escuelas. Por último, encontramos otro tipo de hardware utilizado con fines educativos, como cámaras o pizarras.

Entre estos sistemas, Moodle es una de las herramientas más utilizadas. A través de Moodle, los profesores pueden administrar y organizar actividades educativas, y los estudiantes pueden colaborar en grupos online. Por otra parte, Google Apps for Education es una herramienta cada vez más popular, que ofrece un conjunto de aplicaciones, incluyendo Google aula, Google Docs, Gmail para estudiantes y correos electrónicos del personal, y el calendario de Google. Google Drive también se utiliza por parte del profesorado y el alumnado con el fin de compartir bibliografías u otros documentos. Las cuentas de Gmail, por encima de todo, son las herramientas de comunicación fundamentales para los estudiantes y profesores. Las mismas, de acuerdo con las normas de muchos institutos, deben ser usadas sólo con fines académicos. Según el director de una escuela, los estudiantes son debidamente informados tanto de que la utilización de dichas cuentas de Gmail debería limitarse a actividades relacionadas con la escuela, como de que el instituto se encuentra autorizado a tener acceso a las mismas.

Además de estas herramientas, también se utilizan en clase otras tecnologías con finalidades pedagógicas. Por ejemplo, la escuela Voramar permite a sus estudiantes traer sus propios ordenadores. Como el director del Instituto especifica:

> "Los estudiantes son libres de llevar el equipo que tienen en casa. Hasta hace pocos años tenían que tener un modelo específico de computadora, pero ahora ya no, todo lo que tiene conexión Wi-Fi y tiene un poco de espacio en un disco rígido es útil para nosotros".

En esta línea, el personal docente entrevistado confirmó que el uso de dispositivos digitales para la búsqueda de contenido online y para su comparación es cada vez más común entre el alumnado.

Por otro lado, vale la pena señalar que el uso de teléfonos móviles no está regulado a nivel estatal o regional, por lo que su uso depende, en última instancia, de cada instituto. Por ejemplo, el uso de teléfonos inteligentes se prohibió en el instituto Vedruna Àngels, mientras que otras escuelas han adoptado prácticas menos restrictivas. En el instituto Milà i Fontanals, las imágenes tomadas por el alumnado con sus teléfonos móviles a veces son posteadas por los profesores en las redes sociales del centro. En otro instituto, el uso del teléfono móvil está permitido en el patio entre 13.30 y 15.00 horas. Sin embargo, un denominador común entre las diferentes escuelas es la aceptación, por parte del profesorado, de las tecnologías móviles para su uso pedagógico, una situación reforzada por su relativa independencia a la hora de brindar permisos y asumir la responsabilidad sobre el uso de estos dispositivos. Como señala un profesor:

> "A veces, debido a problemas con la conectividad o la conexión Wi-Fi, permitimos a los estudiantes utilizar sus teléfonos para buscar información. Otras veces es cierto que hay actividades pensadas exclusivamente para el uso de teléfonos móviles, como el vídeo, por ejemplo. Cada vez más, cuando se necesita para hacer videos, permitimos que utilicen sus teléfonos móviles, pero el permiso siempre debe ser solicitado. El teléfono móvil puede ser una herramienta adicional".

De este modo, nuestra investigación ha revelado una heterogeneidad de prácticas en el uso de tecnología con fines didácticos en las aulas. Esta diversidad se deriva, en parte, de la autonomía institucional y de la relativa capacidad de decisión de cada profesor o profesora en este marco. Por un lado, cada escuela establece, de acuerdo con sus propias posibilidades, normas y programas educativos, los límites para el uso de los sistemas educativos digitales. Por otro lado, debido a la relativa libertad que posee el profesorado en este sentido, el uso de estas tecnologías depende, en última instancia, de los métodos y requisitos establecidos por cada uno de los responsables docentes.

Más allá de estas consideraciones generales sobre las normas y prácticas, es importante tener en cuenta que, al igual que las tecnologías administrativas, también las plataformas educativas a menudo ejercen una forma de control que va más allá de su función puramente educativa. Plataformas como Moodle o Google, de hecho, registran el tiempo desplegado para completar y enviar tareas por parte del alumnado. Así una estudiante indicaba:

> "…pero los profesores saben. Saben cuánto tiempo estás conectado en la plataforma de Google. A veces te dicen que ha habido muchos días sin haber iniciado la sesión, y que había que hacerlo. Ellos están comprobando lo que hago. Si no me conecto porque no puedo o no quiero, bueno, ellos no tienen que decirme nada".

Otra forma de control sobre los estudiantes también se establece mediante los sistemas de vigilancia, particularmente en el caso de los dispositivos de video vigilancia. Más allá de la falta de prácticas comunes entre las escuelas en este sentido, nuestros *focus groups* revelaron que, en la mayoría de los casos, los estudiantes no han sido informados sobre la presencia de circuitos cerrados de televisión, y sólo toman conciencia sobre los mismos cuando los ven. Pero, como era de esperar, también existen mecanismos de vigilancia menos evidentes que son advertidos por el alumnado. Por ejemplo, una estudiante del instituto Menéndez y Pelayo declaró que las plataformas educativas, como Esemtia y Virtus, son "más para el control que para la comunicación, ya que no hay diálogo entre los maestros y las familias". En esta línea, algunos estudiantes del Instituto Voramar señalaron que su acceso a algunas páginas web es frecuentemente bloqueado por el instituto, y agregaron que los profesores los vigilan mediante la administración de su acceso a las plataformas educativas.

a.3) Las redes sociales

El impacto de las TIC en entornos educativos no se limita a la aplicación de los sistemas educativos, sistemas de control administrativo, o formas sutiles de control institucional. Las redes sociales como Twitter, Instagram, Facebook y

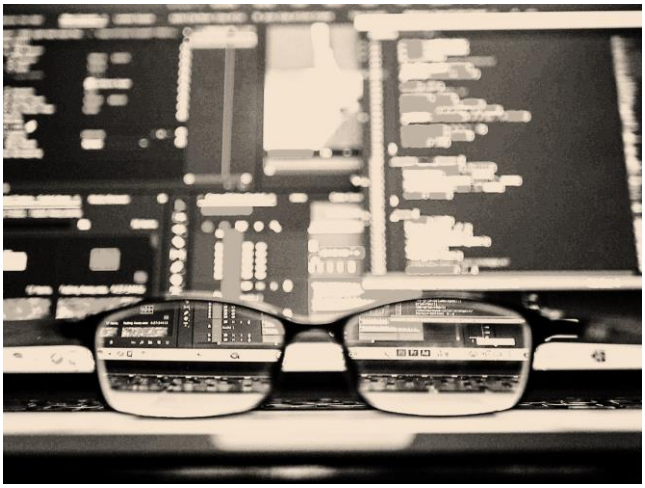
YouTube se utilizan cada vez más en la escuela para comunicar actividades, viajes, noticias, proyectos u otra información relacionada con la escuela. Su uso, sin embargo, plantea problemas de privacidad, ya que es bien sabido que las redes sociales recogen la información del usuario con fines comerciales. Por otra parte, se ha detectado que las políticas para el uso de estas redes sociales no son homogéneas en todas las escuelas. Por ejemplo, el Instituto Vedruna Àngels delegó la gestión de sus perfiles de Facebook e Instagram a una empresa privada, mientras mantiene el control de su cuenta de Twitter. Finalmente, cabe mencionar que, en conjunción con el uso de las redes sociales, otras prácticas informales dan forma a la vida cotidiana del alumnado. En particular, el uso de aplicaciones de mensajería como WhatsApp se ha documentado como una práctica muy común en el día a día de la escuela.

a.4) Ciclo de vida y gestión de los datos

Por el momento hemos proporcionado una visión general de los numerosos tipos de tecnologías que se encuentran en entornos educativos. A continuación, vamos a analizar el ciclo de vida de los datos que se recaban.

En primer lugar, los datos pueden ser recogidos directamente o indirectamente. El primer caso se aplica a las plataformas administrativas, donde existe la voluntad precisa y la intención de recoger unos tipos específicos de datos. Por otro lado, los datos pueden ser producidos y recogidos indirectamente, como consecuencia del uso de las tecnologías digitales. Distintas plataformas pedagógicas o redes sociales caen dentro de esta última categoría. La distinción es importante dado que nuestro estudio ha revelado un mayor conocimiento sobre el marco legal que regula la gestión de los datos recogidos por las tecnologías administrativas que sobre los requerimientos y condiciones aplicados a otras tecnologías, que a menudo producen datos más heterogéneos e impredecibles.

Por otra parte, si bien es una práctica común y bien establecida que la secretaría y la dirección de la escuela sean responsables de los datos generados por las plataformas administrativas, nuestro estudio identificó diferentes casos y protocolos en relación a tecnologías no administrativas. En el Instituto Milà i Fontanals, por ejemplo, el director y el coordinador de informática tienen acceso a todo el material que pasa por la red de la escuela y son los que asumen la responsabilidad de seleccionar las imágenes que se publicarán en las redes sociales.



Mientras que las normas y protocolos en torno a la recopilación de datos parecen estar relativamente establecidos, los procesos de almacenamiento y eliminación son menos claros. Las dudas tienen que ver fundamentalmente con quién tiene que borrar los datos y después de qué período de tiempo. La cuestión es delicada, ya que las escuelas también están obligadas a mantener algunos datos, con el fin de ser capaces de comunicarse con el alumnado en el futuro, cuando sea necesario. En general, la idea promovida por el Departament d'Ensenyament es que los datos deben mantenerse siempre y cuando se utilicen para su propósito inicial, lo que significa que una vez que su función se ha llevado a cabo, los datos deben ser eliminados. En cambio, según nuestro trabajo de campo, cada tecnología o plataforma tiene su lógica específica de eliminación, una condición que deriva en una falta general de sistematización de esta tarea. De acuerdo con el responsable de la APDCat, el problema del borrado de la información se vincula principalmente a la gestión de aquellos datos del alumnado vinculados a tareas pedagógicas mediadas por sistemas "informales". Esto podría ocurrir, por ejemplo, cuando del personal

docente utiliza las redes sociales para comunicarse e interactuar con los estudiantes.

Los responsables del Departament d'Ensenyament han reconocido que no se han establecido criterios homogéneos para la eliminación de los datos, por lo que predomina una tendencia a mantenerlos indefinidamente. Este estado de cosas fue comprobado también por nuestro estudio, ya que en casi todos los institutos analizados encontramos que no existe un protocolo para la eliminación de los datos del alumnado, y el personal a cargo de los institutos explicitó frecuentemente que la eliminación de datos es uno de los aspectos a mejorar. Esta percepción es compartida por un profesor, que se expresa de la siguiente forma:

> "Sí, sí, estoy preocupado. Hay una gran cantidad de tecnología, pero carecemos de información acerca de cómo eliminar al final, si tenemos que hacer esto o alguna otra cosa. Sería bueno para aprender no sólo sobre el uso, sino también acerca de los riesgos".

No obstante, también se encontraron algunas de las prácticas más sistemáticas para la eliminación de datos. Por ejemplo, un director indicó:

> "cuando eliminamos un estudiante que se va, terminamos destruyendo toda la información que solicitamos cuando se realizó la inscripción. Esto se hace por una empresa de destrucción de papel que nos certifica que los destruyen".

Una cuestión fundamental fue revelada por el Instituto Menéndez y Pelayo. En los contratos con empresas privadas a través de los que se externalizan los servicios educativos, la destrucción de los datos suele ser responsabilidad de la empresa, pero sin ninguna especificación sobre los tiempos y las modalidades de eliminación.

a.5) Consentimiento informado:
Para concluir esta revisión general sobre la gestión de los datos en las escuelas analizaremos la piedra angular de la protección de datos: el consentimiento y la comunicación.

La principal herramienta para garantizar el consentimiento informado son los formularios de consentimiento, pero los mecanismos para su obtención son diferentes en cada escuela. En el Instituto Milà i Fontanals los formularios de consentimiento proporcionados durante el procedimiento de inscripción del alumnado, únicamente consultan a los padres acerca de los derechos de imagen. En esta línea, en la escuela Vedruna el formulario se entrega a los propios estudiantes con el fin de que presten su consentimiento para mostrar su imagen en la página web de la escuela.

En cambio, en el Instituto Menéndez y Pelayo tanto el estudiante como los padres son consultados acerca del consentimiento para cada una de las plataformas que van a ser utilizadas en el centro. También se les informa acerca de cómo y cuándo se destruirán los datos, y sobre su derecho de acceso y rectificación. Este formulario de consentimiento se aplica a todas las aplicaciones, desde Google hasta la versión digital de un libro de biología. Por otra parte, de entre todas las escuelas analizadas, los estudiantes de este centro son los únicos que firman, junto con sus padres, los formularios de consentimiento. No obstante, es interesante observar que el desarrollo de estas mejoras y nuevas prácticas no provienen de las necesidades institucionales internas, o de la necesidad de cumplir con la legislación, sino de la iniciativa de un padre que identificó una serie de irregularidades en los formularios de consentimiento. Encontró que los formularios previos eran incompletos, ya que no cubrían la totalidad de las tecnologías y los datos generados por esas plataformas.

Así, estos casos revelan que las leyes de protección de datos no se siguen estrictamente, lo que lleva a prácticas poco seguras para la privacidad del alumnado.

B. B) Opiniones y sensibilización de los actores involucrados

b.1) Confianza en la tecnología por parte de las autoridades

La privacidad y la protección de datos son cuestiones cada vez más relevantes para las escuelas, en parte debido al creciente uso de los sistemas tecnológicos antes descriptos. Los puntos de vista y opiniones de la comunidad educativa son, pues, fundamentales para evaluar el nivel de aceptación y conocimiento asociados con el uso de estas nuevas herramientas educativas.

Como primer punto a destacar en este sentido, los responsables de los centros analizados generalmente tienen mucha confianza en las nuevas tecnologías y asumen que las mismas no acarrean mayores problemas. Así, los empleados de la escuela Vedruna se sienten seguros con los datos que controlan y no perciben ningún riesgo en particular. De manera similar, un miembro del Instituto Mila i Fontanals señaló:

> "Por el momento, no es algo que me preocupe. Lo que introdujimos mucho no es la prohibición de las nuevas tecnologías, sino la educación para su uso adecuado. Por ejemplo, yo como profesor permito el uso de teléfonos, pero controlo que, si se está usando el teléfono, no se está destinando a otros usos que no son educativos. No tengo miedo, y tampoco percibo miedo entre los profesores".

No obstante, las autoridades reconocen que las redes sociales presentan más riesgos que las plataformas institucionales y que, en términos más generales, no existe un conocimiento exhaustivo sobre la regulación de protección de datos. Como dice un director de instituto: "hay muchas normas escritas, pero no siempre se conocen".

Asimismo, cuando los responsables educativos fueron consultados sobre si el marco legal actual es suficiente para proteger a los estudiantes, y si abarca la combinación de tecnologías y plataformas que gestionan los datos en las escuelas, las opiniones fueron disímiles. Por un lado, un jefe de estudios expresó:

> "Creo que aún no estamos donde deberíamos estar. Creo que el marco legal no controla lo que se llama Big Data ni el hecho de que cuando hacemos un clic compartimos lo que hacemos y vemos, y terminamos dando información que es muy valiosa para las empresas. En el caso de los adolescentes, aunque tal vez siempre sean más conscientes, se piensa que es como un videojuego y que la realidad virtual no es realidad, es otra cosa. El problema es que la identidad digital existe y las empresas la ven cuando es momento de seleccionar empleadores. Es inquietante porque nuestros alumnos se encuentran en plena adolescencia, donde hay poco auto control".

b.2) Conciencia sobre el marco legal y los riesgos asociados a la gestión de datos

Tanto personal directivo como docente concuerdan que los estudiantes no son plenamente conscientes sobre los riesgos vinculados al uso de las nuevas tecnologías en términos de privacidad y protección de datos. Según las autoridades escolares, lo mismo es cierto para los padres y las madres, que, a su entender, no están preocupados por estos problemas y, en general, firman formularios de consentimiento sin hacer preguntas. Por lo tanto, no está claro en qué medida los progenitores entienden lo que están firmando y porqué. Como se dijo en el Instituto Menéndez y Pelayo:

> "todas las familias firmaron los consentimientos. Ya sea que hayan firmado más con gusto y persuadidos, o si lo perciben más como una molestia, no lo sé. En la reunión que tuvimos en julio el sentimiento fue que muchas familias entendieron la necesidad de firmarlo, pero en realidad no sabemos exactamente si lo vivieron como una molestia o como algo que se necesitaba hacer para proteger su identidad y la de sus hijos".

No obstante, cabe señalar que tanto padres como madres expresan cierta preocupación por los posibles riesgos derivados del uso de las redes sociales.

La dificultad de involucrar a los padres y madres con estos problemas también se observó en el Instituto Voramar. Por ejemplo, las familias fueron invitadas a participar en una reunión ofrecida por los Mossos d'Esquadra[2] sobre los riesgos de la web, pero la reunión tuvo poco éxito y solo aquellos padres o madres que ya estaban informados sobre estos temas asistieron.

Por otra parte, la mencionada falta de conocimiento sobre el marco legal para la protección de datos es una percepción compartida no solo por el personal de la escuela y los directivos, sino también por el profesorado. Profesores y profesoras enfatizan, en primer lugar, la importancia de la educación formal (dentro de la escuela) e informal (fuera de la escuela) sobre la gestión de los datos personales y los riesgos para la privacidad. En esta línea, como vimos antes, también consideran que hay mucha tecnología en las escuelas, pero no muchas instrucciones sobre cómo usarla correctamente.

Nuestra evaluación del nivel de aceptabilidad mostrado por los estudiantes es el resultado de los grupos focales que dirigimos con ellos, en los que se les preguntó sobre las tecnologías utilizadas en clase, sus opiniones en relación con la seguridad, las ventajas y desventajas de las actividades educativas y sus posibles riesgos para la privacidad. Inicialmente, los estudiantes tienden a identificar las tecnologías pedagógicas con las que interactúan a diario en la clase. Pero, son menos conscientes de las plataformas administrativas utilizadas para gestionar sus datos, o no las perciben de inmediato como herramientas tecnológicas a través de las cuales se gestionan los datos personales. En general, los estudiantes creen que el propósito de tales tecnologías es, sobre todo, la educación y la comunicación: sirven para facilitar el estudio y para compartir el

[2] Policía catalana.

trabajo y los materiales con compañeros y profesorado. Pero, como hemos visto, también hay estudiantes que asocian estas tecnologías con una función de control[3].

Con respecto a esto, a pesar de reconocer que las tecnologías se hallan cada vez más integradas en su entorno educativo, algunos estudiantes también notan la falta de alternativas. Se asume que esto podría limitar su libertad de elección y operar como un mecanismo de control adicional. La situación es bien expresada por un estudiante:

> "Ayer, por ejemplo, la persona que organiza Moodle vino y me dijo: <No tengo los documentos necesarios para darle el Moodle. Me los das firmados y te haré el Moodle >. Él está pidiendo permiso para darme el Moodle, pero si no me suscribo y mañana tengo un examen, si no firmo el consentimiento no tendré acceso a la mitad de la información. Por lo tanto, das tu consentimiento, pero si no te apetece no hay una segunda opción, y esto complica las cosas".

Otro estudiante añade:

> "das tu consentimiento para que te hagan /te den Moodle con tus datos porque es algo que vas a necesitar, porque tarde o temprano el profesor subirá allí algo que es requerido".

No obstante, generalmente, estas consideraciones no socavan la confianza de los estudiantes en estas plataformas. Cuando se les preguntó acerca de las razones de esta confianza, los estudiantes respondieron señalando el hecho de que son tecnologías proporcionadas por el profesorado y, también, asumen a las escuelas como entornos seguros. Uno de los alumnos entrevistados declaró: "Tampoco estoy preocupado porque es algo que pasa por la escuela", mientras que otro comentó "Creo que la escuela supuestamente te da seguridad". Sin embargo, se advirtieron algunas dudas e incertidumbres. Un estudiante indicó:

[3] Este no es solo el caso de los CCTV, sino también de plataformas educativas como Moodle.

> "Nos venden la tecnología como el futuro, pero luego en la escuela, en clase, no lo muestran. Es una contradicción. Y luego no nos enseñan nada, todos los programas que terminamos usando, ellos asumen que los conocemos. Soy el primero que piensa que no todo puede ser reemplazado por la tecnología. Porque nos libera de publicar todo lo que hacemos, pero a veces necesito a alguien que me explique porque la mitad de los programas que voy a usar en el futuro. No sé por dónde empezar.".

En relación con las redes sociales como Instagram o Facebook, los estudiantes sienten que han sido informados bastante bien sobre los problemas y riesgos de privacidad que conllevan, aunque reconocen que no es fácil imaginar los posibles problemas concretos derivados de su uso. Tanto alumnos como alumnas parecen tener, sin embargo, una percepción bastante concreta de la información y los datos generados y publicados por ellos. Un alumno nos manifestó:

> "Estoy dando mi opinión en WhatsApp sobre lo que me dices, le doy mis calificaciones al mundo y mi tarea y lo que pienso a cierta edad. En 20 años voy a ver lo que pienso y lo que dije sobre la presentación sobre el aborto, por ejemplo. Le doy todo lo que hago a la escuela, lo estoy poniendo en Internet".

b.3) Consentimiento informado y efectividad de la protección de datos

Como se ha detallado anteriormente, los distintos actores articulan un cierto conocimiento sobre los riesgos para la privacidad relacionados con el uso de redes sociales. No obstante, se detectó un menor grado de conocimiento y conciencia en relación con el consentimiento y el ciclo de vida de los datos. En algunos casos, los estudiantes recuerdan haber firmado un formulario de consentimiento para derechos de imagen, sin haber recibido más información al respecto. Del mismo modo, no conocen los procesos seguidos para la eliminación de sus datos.

La falta de conocimiento y conciencia sobre los mecanismos de protección de datos en las escuelas fue confirmada por nuestras entrevistas con expertos. Pocas escuelas, según ellos, diseñaron mecanismos formativos para proporcionar información sobre el uso y los hábitos saludables en el uso de las redes sociales. Tampoco se han desarrollado programas de prevención. Uno de los expertos comentó lo siguiente:

> "Trabajamos sobre tutorías, sobre acoso cibernético o identidad digital, pero no existe ningún espacio o curso que aborde la importancia que tienen los datos, la privacidad y la identidad digital. En las escuelas en las que hemos trabajado estos temas, sobre el reemplazo / robo de identidad, los Mossos d'Esquadra van a hacer las charlas. Las familias no tienen ni idea de lo que sus hijos están consumiendo. Existe una gran ignorancia entre los estudiantes, profesores y familias, una falta total de conocimiento sobre el marco legal y sobre cómo proteger, por ejemplo, su Facebook o tu identidad en Twitter. Estos temas no se tratan debido a la ignorancia, y también por el hecho de que se minimizan, en el sentido de que no se consideran importantes.".

Además, según lo sugerido por la APDCat, si bien el marco regulatorio actual es integral, suficiente y capaz de abarcar múltiples escenarios, aún puede verse comprometido debido al nivel de conocimiento y de divulgación, que no parece realizarse de forma suficientemente clara. En consecuencia, los expertos han hecho propuestas de mejora, la mayoría de ellas relacionadas con la aplicación del marco legal en cada instituto escolar. Uno de los expertos entrevistados declaró:

> "Este es un problema emergente. No todos los institutos desarrollaron sus planes de educación como deberían. Algunos tienen proyectos que no han cambiado en 10 años y no lo harán, y es difícil creer que en más de 10 años las cosas que suceden en las escuelas se hayan mantenido igual. Es importante que los institutos tengan una política para el uso de las tecnologías. Es importante que tengan una política que establezca el objetivo final de la introducción de estas tecnologías y cómo se llevará a cabo también es una pregunta muy importante."

Otro experto señala que "la administración no puede estar en todas partes y, por lo tanto, sería mejor delegar herramientas para que los institutos puedan tomar las medidas necesarias para hacer frente a estos conflictos". Por ejemplo, las presentaciones sobre la protección de datos realizadas por los Mossos d'Esquadra en todos los institutos catalanes se consideran un paso positivo, pero también diversos actores manifiestan un cierto grado de escepticismo sobre las mismas. Se ha cuestionado que la formación y difusión de la información deba ser ofrecida únicamente por la policía y no a través de programas capaces de dar una mayor autonomía a las escuelas, para que todos los miembros de la comunidad educativa estén al tanto y preparados sobre los temas relevantes.

Conclusiones

Nuestra investigación reveló que los institutos de Barcelona han aumentado la presencia de tecnologías digitales para la educación y la administración, un proceso promovido por las políticas europea, española y catalana. La gestión de la información personal y el uso masivo de los datos de los estudiantes habilitados por los sistemas digitales y el uso de plataformas en las escuelas ha llevado a una progresiva “datafication” de los entornos educativos. Como hemos visto, la introducción y supervisión de estas tecnologías depende de las administraciones públicas, del personal directivo de las escuelas y del profesorado, pero también de las empresas privadas y externas, de modo que el impacto en la privacidad de los estudiantes se deriva de las complejas dinámicas y prácticas establecidas entre esos actores. Nuestra investigación ha demostrado que la escasa conciencia sobre el proceso de control, protección y eliminación de datos, se relaciona con:

- La autonomía y diversidad institucional (por ejemplo, escuelas públicas vs. privadas) -reflejada en la desigual aplicación del marco legal-,
- Las complejas relaciones entre los actores involucrados, y
- La falta de conocimiento transversal sobre cuestionas relativas a la protección de datos.

Así, una serie de razones habrían dado lugar a este escenario según los expertos las autoridades entrevistados:

- A menudo se ignoran las políticas y normas de la administración pública, así como las de los proveedores de servicios en la red;
- Los aspectos técnicos y legales de la protección de datos son desconocidos;
- No se conocen las medidas que se pueden aplicar para garantizar la seguridad de estos sistemas.

Esta falta general de conocimiento sobre los requisitos y protocolos que deben llevar a cabo los miembros de la comunidad escolar ha derivado en prácticas heterogéneas y, a menudo, inseguras.

En segunda instancia, se debe tener en cuenta que el consentimiento informado es un mecanismo fundamental para que los sistemas tecnológicos funcionen de manera correcta, segura y operativa, ya que contribuyen a aumentar el conocimiento y la conciencia sobre la privacidad y los problemas de protección de datos. No obstante, los formularios de consentimiento, los cuales constituyen el medio fundamental para garantizar la protección de datos, a menudo están incompletos o presentan muchos errores. Es importante que los formularios de consentimiento informen sobre las particularidades de cada sistema de recopilación de datos. Como hemos visto, esta no es todavía una práctica bien establecida y, en el caso particular del Instituto Menéndez y Pelayo, ocurrió en parte como una reacción a las quejas de un padre.

En tercera instancia, nuestro análisis del ciclo de vida de los datos ha mostrado otros aspectos críticos para un tratamiento adecuado de los datos. Entre los principales asuntos detectados se incluyen:

- El acceso a los datos personales de alumnado y profesorado no se haya debidamente controlado. Por ejemplo, se utilizan plataformas educativas durante las horas escolares cuyas cuentas suelen quedar abiertas, permitiendo que otras personas tengan acceso sin saberlo.
- Hay una falta general de conocimiento sobre los protocolos de eliminación de datos, tanto en lo que respecta al tipo de datos que deben destruirse, como a los mecanismos y plazos de dicha eliminación.
- El uso de documentos de Excel como medio para recopilar y compartir datos personales de familias y alumnado es problemático, ya que de esta manera todos los padres y madres, y potencialmente otras personas, pueden tener acceso a la información personal. En la misma línea se encuentra el envío masivo de correos electrónicos, ya que revela las direcciones de correo electrónico de familias, alumnas y alumnos.
- Finalmente, se ha advertido la recopilación de datos innecesarios para los propósitos de los institutos.

En cuarto lugar, la protección de datos de los estudiantes va más allá de los límites académicos: según los expertos de la APDCat, los mayores peligros provienen de la gestión de la información de los estudiantes lanzada a través de los servicios y plataformas que están fuera de la administración de los centros educativos.

En esta línea, se observó una diferencia significativa entre las tecnologías administrativas y pedagógicas. Las últimas, y en particular los correos electrónicos, las aplicaciones educativas y las redes sociales presentan un vacío legislativo más amplio en relación a la información que generan. La información recopilada por dichas tecnologías va más allá de los datos personales, como el nombre o la fecha de nacimiento, ya que también puede incluir el historial de investigación, términos de investigación, datos geolocalizados, listas de contactos o todo tipo de información relativa al comportamiento del estudiante. La falta de consentimiento directo sobre todos estos datos plantea un problema, dado que alumnado, profesorado y familias usualmente no conocen la información generada a través de esos sistemas.

En quinto lugar, otra dinámica común revelada por nuestra investigación de campo es la externalización de servicios a empresas privadas. Frecuentemente, estas empresas son consideradas como un valor agregado en términos de seguridad, dado que aportarían una mayor eficiencia en la gestión de datos. En esta línea un profesor indicaba:

> "Contratamos Clickedu porque esos datos más confidenciales sobre familias, como cuentas bancarias o números de teléfono permanecen allí. Contamos con el hecho de que están administrados. Esos datos están en la nube y la nube está en algunos servidores que están protegidos con medidas de seguridad apropiadas, y por lo tanto hay seguridad, una garantía de la compañía externa de que es seguro".

Se debe tener en cuenta que muchos de estos sistemas privados y plataformas utilizan información sensible para propósitos no relacionados con la educación, lo cual puede amenazar la seguridad de los datos y su integridad.

De este modo, lo que emerge es una concepción restringida de la privacidad, enfocada en el uso criminal de datos por parte de terceros, en lugar de un enfoque más integral que considera cuestiones más fundamentales como la identidad digital y la discriminación, el derecho a ser olvidado, el consentimiento informado o la minimización de datos; aspectos contemplados en el nuevo GDPR.

En esta línea, tanto alumnado como profesorado tienen un conocimiento escaso del marco legal de protección de datos y sus peculiaridades en el entorno escolar. Tal conocimiento parcial socava seriamente el cumplimiento de las normas y, por el contrario, favorece una cadena de confianza que va de los estudiantes a los profesores, de los profesores a las escuelas y de las escuelas a la administración. Esto puede limitar la efectividad de los mecanismos de protección de datos. Por otro lado, los expertos del sector académico y de las administraciones educativas han argumentado que la nueva regulación efectivamente brinda una respuesta al escenario actual, pero esto no necesariamente garantiza su aplicación. Algunos elementos para la correcta aplicación del marco legal fueron individualizados:

1. El GDPR requiere un esfuerzo de gobierno para el desarrollo de una política común entre los diferentes actores.
2. Se debe promover la participación activa y el interés de los padres y madres sobre estos temas.
3. Se requiere una mayor transparencia. Más concretamente, para una mejor comprensión de los conflictos concretos generados por la gestión de datos.

La concienciación es un elemento indispensable para los estudiantes también. De hecho, se observó que el concepto de identidad digital no es fácil de entender o

reconocer por los estudiantes, que no son completamente conscientes de la información divulgada a través de plataformas educativas, de las medidas preventivas que deben tomar o de sus derechos vinculados a sus datos personales. También vale la pena señalar que, aunque inicialmente las alumnas y los alumnos tienden a expresar confianza en los entornos educativos, cambian de opinión cuando son consultados en mayor profundidad. A pesar de que reconocen la presencia cada vez mayor de soportes tecnológicos para sus actividades escolares, sienten que no tienen suficiente poder sobre las decisiones de esos sistemas y plataformas, o no se sienten totalmente cómodos al usarlos. En esta línea, los estudiantes también han señalado la función de control ejercida por las tecnologías educativas, que aumentan el nivel de vigilancia de familia y profesorado y, por lo tanto, amenazan la autonomía de las y los estudiantes.

A la luz de los resultados de este estudio, consideramos como hallazgos centrales a ser tenidos en cuenta: los problemas asociados al consentimiento informado, las limitaciones en los protocolos y prácticas de seguridad y protección de datos, la externalización progresiva de servicios educativos a empresas tecnológicas privadas y la escasa conciencia entre los actores de la comunidad educativa. La naturaleza exploratoria de este estudio, combinada con la creciente relevancia de estos temas, señalan la necesidad de más investigación en este campo y, por esta razón, Eticas ha planificado una segunda fase de este estudio.

Referencias

Generalitat de Catalunya (2010). Protecció de dades de caràcter personal per a centres i serveis educatius, Departament d'Ensenyament.

Generalitat de Catalunya (2016). Documents per a l'organització i la gestió dels centres Protecció de dades personals, ús d'imatges, propietat intellectual i Internet. Departament d'Ensenyament

Generalitat de Catalunya. (2015). Mobile technologies in schools. Consell Escolar de Catalunya.

European Commissión (1993). Green Paper on the European Dimension of Education.Luxembourg: Office for Official Publications of the European Communities.

European Commission (2014). The NMC Horizon Report Europe: 2014 Schools Edition, European Commission's Directorate General for Education and Culture; European Commission's Joint Research Centre – Institute for Prospective Technological Studies; and the New Media Consortium.

EU General Data Protection Regulation (GDPR), retrieved from https://gdpr-info.eu/

Rosen, David and Santesso, Aaron (2014). Surveillance and Education. Birkbeck Law Review Volume 2(2), 229-244

Richards, J. & Stebbins, L. (2014). Behind the data: Testing and assessment, a Pre K–12 US education technology market report. Washington, DC: Software & Information Industry Association.

Taylor, E. (2013). Surveillance Schools Security, Discipline and Control in Contemporary Education. Springer.

Tierney, Robin D. and Martha J. Koch (2016). "Privacy in classroom assessment", en Handbook of Human and Social Conditions in Assessment, London: Routledge

Wright, De Hert and Kloza (2011) Recommendations, for a privacy impact assessment framework for the European Union Prepared for European. Commission – Directorate General!Justice, Brussels – London.

Glosario:
Datos: una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de una característica o de una variable cuantitativa o cualitativa. Es generada o recogida por un ordenador y constituye la información manipulada por el programador en la construcción y el desarrollo de algoritmos y modelos.

Ciclo de vida de los datos: la secuencia de etapas que los datos atraviesan desde su generación hasta su archivamiento y borrado. Consiste de las siguientes etapas: creación y captura, transmisión, mantenimiento, gestión y acceso, análisis, explotación y eliminación.

Identidad digital: el conjunto de información disponible en la red asociada a un individuo, pero también a organizaciones o dispositivos electrónicos. La identidad digital se forma a través de la actividad en la red de un individuo y puede incluir: nombres de usuario, contraseñas, historial de consumo, fecha de nacimiento, número de la seguridad social, actividad de búsqueda en línea (transacciones electrónicas) o el historial médico.

Consentimiento informado: la acción y el resultado de permitir algo (el uso de datos personales o la participación en un estudio) después de haber sido informado acerca de los propósitos por los que se da el consentimiento. Desde una perspectiva legal, el consentimiento informado funciona de forma similar a los contratos, dado que son entendidos como la "voluntad manifiesta" expresada en forma escrita.

Privacidad: no existe una definición clara del concepto de privacidad. Por lo general, se aplica a múltiples dimensiones del comportamiento e información personal, ya que puede referirse a la privacidad de la información, de la comunicación, de la conducta y las acciones personales, de la intimidad personal o de la vida familiar. Por lo tanto, la noción abarca un espectro más amplio que la protección de datos, ya que no se centra únicamente en el procesamiento de datos, sino también en intrusiones más estrictamente conectadas a la persona física.

Protección de datos: proceso de salvaguarda de la información personal para evitar prácticas ilegítimas e ilegales que puedan afectar los derechos fundamentales y a la

libertad. La protección de datos tiene un alcance más amplio que la privacidad, ya que se ocupa de cualquier procesamiento de datos personales, independientemente de si dicho procesamiento interfiere con la privacidad de un individuo.

Tecnologías intensivas en datos: tecnologías que tratan una enorme cantidad de datos para sus operaciones.

Derecho a ser olvidado: derecho a obtener la eliminación de los datos cuando 1) los datos ya no son necesarios para los propósitos con los que se obtuvieron, 2) el consentimiento es retirado, 3) el sujeto interesado se opone al procesamiento de datos, 4) los datos son tratados de forma ilícita o deberán ser eliminados de acuerdo con obligaciones legales.

eticas