Safe environments? Data intensive technologies in BCN high schools

eticas

Eticas R&C
This document is based on project work conducted by Gemma Galdón Clavell, Mariano Martín Zamorano and Olalla Losada for the project “Entorns Segurs”, funded by the Barcelona City Council.
Author: Lorenzo Olivieri. Editor: Emma Ahlert

Abstract

Digital technologies are more and more present in schools in the form of databases, educational platforms, social networks. While these tools are said to improve students' life and learning processes, the amount of data they collect and share might also lead to harm the privacy of the students as well as other fundamental rights. To uncover some of these issues, Eticas conducted a fieldwork project which involved the educational communities of four different Barcelona schools. The aim was to reveal whether the practices associated to the use of these systems comply to the legal framework established by the European Union and by the Catalan governments. Through interviews with professors and students, parents and school staff, our research has thus shown a general lack of knowledge and awareness about issues concerning the life-cycle of data, consent forms or digital identity. Heterogeneous protocols and requirements among the schools, legislative vacuums and the absence of specific information for professors and parents contribute to make the use and presence of technologies a critical and problematic dimension in educational environments.

Acknowledgments

Eticas team wish to thank the Ayuntamiento de Barcelona for the support received for the realization of this project as well as all experts from university departments, from the Departament d'Ensentament, the Consorci d'Educación de Barcelona and the Agencia Catalana de Protección de Datos, who accepted to be interviewed for this research. We also wish to thanks school authorities, teaching staff, mothers, fathers and students from the Institute Milá i Fontals (Raval), the Escola Vedruna (Raval), the Institut Menéndez i Pelayo (Sarrià) and the Institut Voramar (Poble Nou), who took part in the field research.

Introduction

Information and communication technologies are shaping more and more aspects of everyday life, and educational environments are no exception. Different types of technology that vary in purpose contribute to the daily practices of students, teachers and school staff. Databases, educational technologies and platforms, social networks and online searches are widely and increasingly used in schools. However, while rather extensive literature exists that illustrate positive effects of such systems on student life and school management (Rosen & Santesso, 2014; Taylor, 2013; Richards & Stebbins, 2014; Tierney and Koch, 2016), less attention has been paid to the risks of their use. A common thread throughout this technology is the amount of personal data they can gather and process, raising questions and concerns in respect to privacy and data protection of students. These issues are even more relevant in educational settings. Not only privacy is a fundamental human right, but minors are also significantly more vulnerable. It must not be forgotten that the school age is, essentially, a period for experimentation. Children and adolescents make mistakes, learn crucial lessons and develop their personalities. Recording and storing personal information during this delicate period can thus have negative consequences in the long-term. This threatens the right to be forgotten and the might affect the ability to develop a sense of self.

To unpack these questions and inquire about the relation between educational environments and data protection, Eticas Foundation designed field research to explore how teachers, parents, and students perceive and deal with the privacy issues posed by educational and administrative technologies. With this concept in mind, the project *Entorns segurs* analysed the use of data intensive technologies in four high schools of Barcelona, corresponding to three neighborhoods with varying socio-demographic situations. The aim of our research was to assess whether the proliferation of technologies in educational environments has been developed and implemented following practices, norms, or protocols that effectively ensure the protection of students' data.

Methodological approach

Our qualitative study was conducted in four different Barcelona high schools and was articulated upon four main variables:

1) the type of technology used to collect data
2) the life-cycle of the data collected and processed by institutes
3) the relative compliance with the set of laws, norms, recommendations and policies that orientate and regulate data protection in school environments
4) the multidimensional concept of *acceptability*.

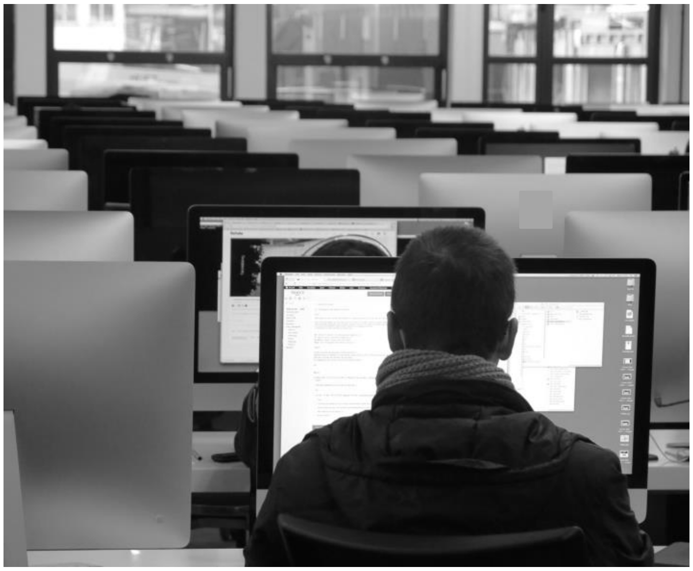
With the notion of acceptability, we refer not only to the functionality and efficacy of the technology but, more broadly, to the social construction of the use of technologies, which includes dimensions as awareness, consent, confidence.

For the actual collection of data, three main strategies were adopted. First, a desk researcher reviewed the relevant literature in the fields of privacy and education, including the legal and normative frameworks enforced in Catalonia, Spain and in the European Union. Second, a series of seventeen (17) interviews were conducted to map the views and opinions of the relevant actors involved in educational contexts. To provide a more comprehensive perspective, our interviews addressed both the socio-institutional domain (public administration, including the *Consorcio d'Educació de Barcelona* and the *Departament d'Ensenyament*, as well as experts from different universities in Barcelona) and the schools' communities (students, teachers and authorities within the studied schools). The seventeen semi-structured interviews involved four professors, four school directors, one parent, one administrative employer, five Government representatives, and two academic experts.

Finally, we conducted four focus groups with students between 14-16 years old (one group for every educational centre) and one group of discussion with parents and representatives from AMPA. The four schools (Mila i Fontales, Menendez y Pelayo, Vedruna and Voramar) were selected according to socio-economic criteria, taking into account the family's cultural diversity and average income.

Finally, the transcriptions of documents and interviews were analysed for content, context and an analysis of discourse through an interactive methodology in which the topics and thematic frameworks are determined by the collected data.

Data protection legal framework: delimiting education system requirements



The use of technologies in schools as well as related issues of privacy and data protection are, in fact, regulated by specific legal frameworks. Spain and The European Union and have developed sets of laws and norms that aim to guarantee students' rights to privacy, and to incentivize the diffusion of digital technologies for pedagogic purposes. From a broader European perspective, in 1995 the European Parliament created Directive No. 95/46/EC, which fought for the protection of physical persons, safe treatment of personal data, and the circulation of data. Article 28 of this norm states the need for a licit and loyal treatment of personal data, which needs to be adequate, pertinent, and not excessive.

However, it was just in 2016 that the European Parliament revised and strengthened the norms for data protection by promoting the GDPR (General Data Protection Regulation), which deeply changed how companies, organizations, and individuals have to manage personal data. This new regulation was enacted in May 2018. It is useful to look closely at the definitions of "personal data" and "data processing" found in this text. Personal data is defined as:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". (Art. 4).

Data processing refers to:

> "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". (Art. 4).

As Wright, De Hert, and Kloza (2011, 13) point out, the treatment of personal data does not deal merely with privacy concerns. It covers a wide spectrum of rights including freedom of expression, property rights, right to non-discrimination, children's rights, and the right to health. To ensure that these rights are respected, the GDPR applies and reinforces ethical principles while processing personal data. First, data must be processed lawfully, fairly, and transparently. Second, data shall be collected for specified, explicit, and legitimate purposes (principle of purpose limitation). Similarly, according to the principle of data minimisation, the personal data shall be adequate, pertinent, and limited to the purposes for which it was collected. In addition to this, the GDPR establishes more precise and restricted criteria and requirements to ensure data protection. It extends the categories of the protected data including biometric, genetic, and health data as well as personal data from which racial and ethnic origin, political opinion, religious or ideological conviction, or union membership can be attributed.

The GDPR also strengthens the rights of data subjects by stating not only that consent should be given by a "clear affirmative act", but that people have the right to obtain confirmation from the controller as to whether or not their personal data is being processed. Where that is the case, people have the right to access the personal data being stored (art. 15). Finally, the GDPR clarifies the right to erasure of personal data from the controller without undue delay. ("right to be forgotten", Art. 19).

While the requirements stated by the GDPR apply to all the socio-economic domains, more specific measures concerning minors and educational environments were also introduced. As we can read:

> "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. [2]Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." (GDPR, Recital 38).

However, to place our research within the specific context of Barcelona institutes, the legal framework which regulates the use of technologies in educational environments in Catalunya needs to be delineated as well. Looking at the legal dimensions allows us to individuate subjects who have the capacity to implement, promote and decide the kind of technologies that are deployed in schools and also who is responsible for ensuring the protection of students' data. This is important because Catalan schools, according to the Catalan Law of Education (2009), are autonomous in defining the use of technologies and in promoting tools for digital education. The single institutes are thus appointed to plan the managerial, pedagogic and technological aspects and have the duty to distribute the responsibilities among the members of the institute. Besides the autonomy of the institutes, the *Ley de Educacion 12/2009* emphasizes the relevance of acquiring competences with ITC tools and assign to professors the responsibility in this field. All these requirements have been further actualized by the PlanTAC, a project developed by the *Department d'Educació*, with the goals of: 1) planning the development and introduction of ICT in schools, 2) guaranteeing and promoting digital inclusion and competence among students and professors, 3) establishing measures for protecting students from inadequate online content, 4) assigning responsibilities for the management of technologies within the institutes, and 5) monitoring the compliance to the normatives about the use of technology, especially the *Ley Organica 15/1999* about the protection of personal data, and the *Ley de Propiedad intelectual*.

In Catalunya the protection of personal data in public institutions is a competence of the Generalitat, which established the Autoridad Catalana de Protección de Datos (APDCat). A number of documents promulgated by the APDCat delineate which must be the treatment of data owned by public institutions. One of these documents, *Recomendación 1/2010*, says that data with personal character needed for the functioning of a public service or of a public activity falls under the responsibility of the institution owner of the service or activity involved. This implies that the data collected for students' education will be under the responsibility of the students' school or institute. However, this norm also considers the possibility of externalization of certain services from public institute to private companies, and thus it suggests, in order to avoid poor data treatment, to designate a person in charge of the data. Beside this, the APDCat has developed a *Basic guide for the protection of data in educational* *institutes (Guía básica de protección de datos para los centros educativos)* which explicitly addresses issues of data protection in educational contexts. The document stresses the requirements for consent, that must be unequivocal, free, specific and informed and for the quality of data, which needs to be collected following the principles of proportionality, loyalty, finality and accuracy. The Guide also states the duties that have to be followed during the treatment of data, including the transfer of data to third party, and after the treatment, such as the possibilities of conservation and elimination of data.

Both the European Union and the catalan institutions have thus generated legal frameworks which established the rules, limits and obligations that have to be observed in order to guarantee students' rights to privacy and data protection.

Fieldwork results: four Barcelona high schools

In this section we discuss the main findings of the project fieldwork. The consequences and impact on privacy and data protection of the technologies used in educational environments can be separated into four main categories of technological systems and devices present in schools. Administrative technologies offer software for the management of data or e-mail services administered by school councils and public administration. Second, physical institutional technologies are systems used for security and control, such as CCTV or biometric identification systems. The third category is edtech, which is technology used for education and pedagogy, like personalized apps or learning management systems. Finally, students' personal devices: smartphones, personal computer or tablets. The use and implications of these systems for privacy are organized following an analytical scheme that goes from the description of the scenario of Barcelona high schools in terms of data management and data protection, to the definitions and opinions expressed by the surveyed stakeholders about both issues. This last dimension of the analysis is crucial for the study. Allow us to frame how the identified data intensive technologies are perceived by each of the actors who interact with them and, in the end, how they can work “in practice”.

A. Knowledge on the examined technologies and processes

a.1) Administrative technologies: extension and externalization

In the last decade, the majority of the schools have adopted automatized and digitized services for obtaining and managing data. Clickedu, for instance, is a cloud platform created explicitly for schools which allows users to manage academic records, and observe information about students and families such as economic status. It is also used for attendance and to communicate information about homework and exams to parents. However, one of the professors we interviewed told us that students also maintain a paper diary, so that they can learn to manage and organize their homework without their parents being able to control everything through the web. However, he recognizes that Clickedu is a great improvement compared to previous modalities for the managing of data, such as rigid disks or USB keys. It allows access to grades and records and, compared to previous methods, reduces the risk of viruses. Similarly, Esemtia is a system used for administrative and pedagogic functions that enables teachers to share student work or make comments on their homework. It also allows for daily communication between schools and families.

Data management externalization is relevant to privacy and data protection, since schools entrust external private companies to perform part of their activities. As a consequence, these platforms receive and manage a great amount of sensitive data, including academic records (grades, penalties for delay of improper behavior) but also more personal data collected during the enrolment process (home and e-mail address, telephone number). It must be noted, however, that next to these platforms, some schools still employ informal tools to manage data or communicate with the families. For instance, Excel documents are used to organize student data and then are shared among parents and school staff, while phone calls or SMS messages are used to notify families of an incident.

a.2) *Edtech* and their impact on privacy

As previously mentioned, *edtechs* refer to software, apps, or devices that are specifically used in educational settings, for pedagogic purposes. Three main types of technologies can be identified. First, there are systems and applications that make it possible to organize, monitor, and evaluate students' homework. Second, students can own computers or cell-phones provided by the schools. Finally, other hardware used for educational purposes include cameras and blackboards.

Among these systems, Moodle is one of the most used tools. Through Moodle, professors can administer and organize educational activities, and students can collaborate in online groups. Google Apps for Education is another increasingly popular tool that offers a set of applications including Google classroom, Google docs, Gmail for students' and staff's personal emails, and Google calendar. Google Drive is also offered. This is a cloud drive through which professors and students can share bibliographies and other documents. Gmail accounts, above all, are fundamental communication tools for students and teachers and according to the norms of many institutes, it should be used only for academic purposes. As one school Director reported, students are informed that the use of Gmail accounts should be restricted to school-related activities and that the institute is authorized to have access to it.

Beyond these more institutional and integrated tools, other technologies are used in class for pedagogic finalities. For instance, at the Voramar school students bring their own computers. As the Director of the Institute specifies:

> "students are free to bring the computer they have at home. Until few years ago they needed to have a specific model of computer but now not anymore, anything that has Wi-Fi connection and has some space on a rigid disk is useful for us"

Moreover, professors report that the use of digital devices for searching content online and then comparing the information found in this way is increasingly common among students.

In regard to this, it is worth noting that the use of mobile phones is not regulated at the State or Regional level, so their use depends, ultimately, on the discretion of each institute. For instance, the use of smartphone was prohibited in the Vedruna Angels institute, while other schools have adopted less restricting practices. In Milá y Fontanals, pictures taken by students are sometimes posted by professors. In another institute, the use of mobile phone is allowed in the courtyard between 13.30 and 15.00. However, a common denominator among the different schools is professors' acceptance of mobile technologies for pedagogic use, a situation reinforced by their relative independence when it comes to give permission and take responsibility for the use of phones. As one professor told us:

> "sometimes, due to problem with connectivity or Wi-Fi, we allow students to use their phone to look for information. Other times it is true that there are activities thought exclusively for using mobile phones, like video for example. Increasingly, when it is needed to make videos, we allow them to use their mobiles, but permission always needs to be asked. The mobile phone can be an additional tool".

A two-faced picture thus emerges from our investigation. On one hand, each school establishes, according to its own possibilities, norms and educational programs, as well as specific frameworks for the use of digital education systems. On the other hand, due to the relative freedom accorded to professors, the use of these technologies ultimately depend on the methods and requirements established by individuals.

Beyond this more general considerations about norms and practices, it is important to note that, like administrative technologies, also educational platforms often exert a form of control that goes beyond their pure educational functions. Platforms like Moodle or Google in fact record the time deployed to complete and submit homework. One student declares:

> “but professors know. They know how much time you are connected on Google platform. Sometimes they tell you - it has been many days you have not logged in, and you had to do it -. They are checking what I do. If I do not log in because I cannot or I do not want, well, they don’t have to tell me anything”.

The topic of control over students’ life also applies to systems of surveillance, that in schools are above all devices for video-surveillance. Beyond the lack of common and shared practices among the schools, our focus groups also revealed that, in most cases, students have not been informed about the presence of CCTV and become aware of them only when they see them. But, as anticipated, there are also less obvious modes of surveillance perceived by students. For instance, a student from Menendez y Pelayo declared that educational platforms such as Esemtia and Virtus are “more for control than for communication, as there is no dialogue between teachers and families”. Students from the Voramar Institute have reported that some webpages are blocked, and pointed out that professors exercise a control over them by monitoring their access to educational platforms.

a.3) Social networks: intersecting multiple practices and raising privacy concerns

The impact of ICT on educational environments is not limited to the implementation of educational systems, managing systems, or subtle forms of control. Popular social networks such as Twitter, Instagram, Facebook and Youtube are used in school more and more to communicate activities, trips, news, projects or other school-related information. Their use, however, pose privacy concerns as it is well known that social networks collect user information for commercial purposes. Policies for the use of these social networks are not homogenous across the schools. Various policies have generated different solutions. For instance, the Institute Vedruna Angels delegated the management of their Facebook and Instagram profiles to a private company, while maintaining control of their Twitter account. In conjunction with to the use of social networks, other informal practices shape the daily life of students. In particular, WhatsApp groups for classes, group-work, and projects were reported as highly common practices.

a.4) Data life cycle and data management

So far, we have provided a general overview of the numerous types of technologies found in educational environments. Next, we will discuss the life-cycle of data that is collected. First of all, data can be directly or indirectly collected. The first case applies to administrative platforms, where there is the precise will and intention of collecting specific kind of data. On the other hand, data can be produced and gathered indirectly, as a consequence of using digital technologies, but without the collection of personal data being the end goal. Pedagogic platforms or social networks fall within this latter category. The distinction is important because there is a quite extensive knowledge about the legal framework that regulates the management of the data gathered by administrative technologies, but much less is known for other types of technologies, which often produce more heterogeneous and unpredictable data. Moreover, while it is a common and well-established practice that school Secretary and Director are those responsible for the data generated by administrative platforms, our study identified different cases and solutions in relation to non-administrative technologies. In the Institute Mila i Fontals, for instance, the Director and the informatics Coordinator have access to all the material going through the school network and are those who take the responsibility to select which images will be published.

While norms and protocols for the collection of data appear to be more or less established, the processes of storage and elimination are quite unclear. Doubts, in particular, concern who has to delete the data and after what period of time. The issue is delicate, as schools also are obligated to keep some data in order to be able to contact students in the future when needed. Overall, the idea promoted by the *Department d'Ensenyament* is that data should be kept as long as they are used for their initial purpose, which means that once their function is accomplished, data should be eliminated. But what is clear to schools' staff is that each technology or platform has its specific logic of elimination, a condition that results in a general lack of systematization. According to the responsible of APDCAt, the problem mostly concerns the management of the student information tied to pedagogic fields that are outside the scholastic boundaries. This might occur, for instance, when professors use social networks to communicate and interact with students, eventually releasing personal data.

Respondents from the *Department d'Ensenyament* have thus recognized that they were not able to establish homogenous criteria for the elimination of data, so they tend to to keep them indefinitely. This state of things was testified also by our study, as in almost all the institutes analysed there were students' data which were not properly eliminated and institutes themselves declared that the elimination of data is one of the aspect that needs to be improved. This perception is shared by a professor as well:

> "Yes, yes, I am worried. There is a lot of technology but we lack information about how to delete in the end, whether we have to do this or something else. It would be good to learn not only about the use but also about the risks".

Nonetheless, some more systematic practices for data elimination were also found. For instance, one school director declared:

> "when we deregister a student who leaves, we end up destroying all the information we requested when the enrolment was done. This is done by a company for paper destruction which certificate us that they destroy them".

Another important issue was brought to light by the Institute Menendez y Pelayo. In the contracts with private companies to which educational services are externalized, it is in fact the responsibility of the companies to destroy data, but there is no specification about the timeframe and modalities of elimination.

a.5) Informed consent

To conclude this overview of how schools utilize data management, we can now turn to the cornerstone of data protection: consent and communication. The main tool for guaranteeing informed consent are consent forms, but the mechanisms for obtaining it are different in every school, and generate different reactions in persons responsible for students. In the Institute Mila i Fontanals the consent forms filled during the enrollment procedure only ask parents for image rights, while at Vedruna school the form is signed by students themselves to give consent for showing their image in the school webpage. At the Menendez y Pelayo Institute student and parent consent is asked for every platform separately and they are informed about whether, how and when data will be destroyed, about their right to access and rectificacion. This consent form applies to every application, from Google Apps to the digital version of a biology book. Moreover, the students from Menendez y Pelayo are the only ones who sign, together with their parents, the consent forms. Nonetheless, it is interesting to note that the development of these improvements and new practices at the Menendez y Pelayo did not depend on internal institutional needs or the auditing of legal compliance, but rather from the initiative of a father who identified a series of irregularities in the consent forms. He found that the consent forms provided were incomplete, as they did not cover the totality of the technologies and data generated by those platforms. In summation, , these case show that data protection laws are not strictly followed, leading to unsafe practices for the privacy of the students.

B) Opinions and awareness of the actors involved

b.1) Authorities trust in technology

As this report shows, topics of privacy and data protection are increasingly relevant in schools and, due to the prominent role acquired by technology in those contexts, they are expected to become more and more important. The views and opinions of the educational community are thus fundamental to assess the level of acceptability associated with the use of new educational tools. As anticipated, the concept of acceptability refers at how the members of the educational community know, accept and have been informed about the technologies they use, the information they generate and how their data are used. Unsurprisingly, the level of acceptability change depending on the actors involved.

School staff, such as directors or administrators, are generally quite confident and agree that things are being done well and without major problems. Nonetheless, they recognize that social networks present more risks than institutional platforms, and more generally, that there is not an exhaustive knowledge about the legal framework for data protection. As a school director states: “there are a lot of written norms, but they are not always known”. Interestingly, when asked whether the current legal framework is sufficient to protect students, and if it covers the combination of technologies and platforms that manage data in schools, contrasting opinions were collected. On the one hand, a *Jefe de Estudios* said:

> “I believe we are not yet where we should be. I believe that the legal framework is not controlling what is called the Big Data, the fact that when we make a click we share what we do and see and we end up giving information that is very valuable for companies. In the case of adolescents, even though perhaps they are always more conscious, it is thought that it is like a videogame and that virtual reality is not reality, it is something else. The problem is that digital identity exists and companies look at it when it is time to select employees. It is scary because our students have an age, specific of adolescence, where there is little self-control…”.

On the other hand, the staff of Vedruna school feels safe with the data they manage and do not perceive any particular risk. Similarly, a member from the Mila y Fontanals Institute stated:

> “For the moment it is not something I am worried about. What we introduced a lot is not the prohibition of new technologies, but rather education aimed to its adequate use. For instance, I, as a teacher allow the use of mobile phones, but I control that when they are using the phone, they are not using it for different things that are not educational. I am not afraid, and neither I perceive fear among teachers”.

b.2) Awareness about legal framework and data management related risks

There is a shared agreement among directors and school staff that students are not fully aware or conscious of the risks tied to the use of new technologies in terms of privacy and data protection. According to school authorities, the same is true for parents who are not worried about these issues and, in general, sign consent forms without further questions. At the same time, they appear to show more concerns for the possible risks caused by the use of social networks. However, it is not clear to what extent parents understand what they are signing and why. As we were told at the Menendez y Pelayo Institute:

> "all [the families] signed the consents. Whether they signed out of conviction and persuaded, or whether they perceive it more as a nuisance, I do not know. In the meeting we had in July the feeling was that many families understood the necessity to sign it, but actually we don't know exactly if they lived it as an annoyance or as something that needed to be done to protect their identity and that one of their sons".

The difficulty in engaging parents with these issues was observed at the Voromar Institute as well. They told us that parents were invited to participate to a meeting offered by Mossos d'Esquadra (Catalan Police) about the risks of the web, but the meeting had modest success and only parents who were already informed of the issues attended.

The lack of knowledge about the legal framework for data protection is a perception shared not only by school staff and directors, but by professors as well. They stress, first of all, the importance of formal (within the school) and informal (outside school) education about the management of personal data. Formation and sensitization about privacy, and the risks caused by not protecting it, are presented as very important topics. But professors, as seen before, also complain that there is a lot of technology in schools, but not many instructions about how to use it correctly.

Our assessment of the level of acceptability shown by students is the result of the focus groups we conducted with them, in which they were asked about the technologies used in class, their opinions in relation to security, advantages and disadvantages for educational activities and possible risks for privacy. Overall, students tend to identify the pedagogic technologies with which they interact daily in the class. On the other hand, they are less conscious of the administrative platforms used for managing their data, or they do not immediately perceive them as technological tools through which managing personal data occurs. In general, students believe that the purpose of such technologies are, above all, education and communication: they serve to facilitate study, and to share work and materials with mates and professors. But, as we have seen, there are also students who associate these technologies with a function of control. This is not only the case of CCTV, but also of educational platforms like Moodle.

In regard to this, despite recognizing that technologies are increasingly part of their educational and daily environment, students also note a lack of alternatives, a condition perceived to limit their freedom of choice and also as an additional control mechanism. The situation is well expressed by a student:

> "yesterday, for instance, the person who organizes the Moodle came and said – I don't have your documents for giving you the Moodle. You give me them signed and I will give you the Moodle -. He is asking for the permission for giving me the Moodle, but if I don't subscribe to the Moodle and tomorrow I have an exam, if I don't sign it, I will not have access to half of the information. Thus, you give your consent, but if you don't feel like, then there is not a second option, and this make things complicated".

Another student adds:

> "you give consent that they make/give you the Moodle with your data because it is something that you are going to need because, sooner or later, the professor will upload there something required".

For the most part, considerations do not undermine students' trust and confidence in those platforms. When interrogated about the reasons of this trust, students answered by pointing to the fact that they are technologies provided by professors, and, besides this, schools tend to be considered as safe environments. One of the pupils interviewed stated: "I am not worried either because it is something that goes through the school", while another commented "I believe that school supposedly gives you security". Some doubts and uncertainties were however reported. A student told us:

> "They sell us technology as the future but then, at school, in class, they do not show it, it is a contradiction. And then they don't teach us anything, all the programs we end up using, they assume we know them. I am the first who thinks that not everything can be replaced by technology. Because it frees us from publishing everything we do, but sometimes I need somebody which explain me because half of the programs I am going to use in the future, I don't know where to start from".

For what concerns social networks as Instagram or Facebook, students feel that they have been informed quite well about privacy issues and risks, even though they recognize that it is not easy to imagine and explain the many problems generated through the Internet. Students appear to have, however, a rather concrete perception of the information and data generated and released by them. As one student told us:

> "I am giving my opinion on Whatsapp about what you tell me, I am giving my grades to the world and my homework and what I think at a certain age. Within 20 years I am going to see what I thought and what I said about the presentation on abortion, for example. I am giving everything that I do to the school, I am putting it in Internet".

b.3) Informed consent and effectiveness of data protection law

A minor degree of knowledge and awareness was detected in relation to consent form and the life-cycle of data. In some cases, students remember having signed a consent form for image rights, without having received further information about it. Similarly, they are not aware of the processes followed for the elimination of their data.

The lack of homogeneous knowledge and awareness about privacy and data protection in Barcelona high schools was confirmed by our interviews with experts. Few schools, according to them, designed formative paths to provide information about the healthy use and habits of social networks,but no programs of prevention were developed as well. One of the expert comments:

> "We work about tutoring, about cyberbullying or digital identity, but it does not exist any space or course/class/lectures addressing the importance that data, privacy and digital identity have. In the schools in which we have worked these issues about identity replacement/stealing, the Mossos d'esquadra have to come to make the talks. Families have no idea of what their children are consuming. There is a significant ignorance among students, professors and families. Total lack of knowledge about the legal framework and how to protect, for example, your Facebook. Or your identity on Twitter. These topics are not dealt with, due to ignorance, and also because it has to do with the fact that are underplayed, in the sense that they are not considered important".

Moreover, as suggested by the *Autoridad Catalana de Protección de Datos*, even though the legal regulatory framework is comprehensive, sufficient and able to cover all the scenarios, it still can be compromised by the actual level of compliance and knowledge, or it might not be well explained or sufficiently clear. Thus, experts have made proposals for improvement, the majority of them related to the application of the legal framework in each scholastic institute. One of the experts interviewed declared:

> "This is an emerging problem. Not all the institute developed their education plans as they should have. Some have projects that have not changed in 10 years and will not do it and it is difficult to believe that in more than 10 years the things that happen in schools have remained the same. I would not appreciate a program in general, but it is important that the institutes have a policy for the use of technologies. It is important the they have a policy which establishes the final objective of the introduction of these technologies and how it is going to be carried on is also a very important question"

Another expert points out that "administration cannot be everywhere, and therefore it would be better to delegate tools so that institutes can take the necessary measures for facing these conflicts". For instance, discussion surrounding data protection realized by the *Mossos d'Esquadra* in all Catalan institutes are seen as a positive step but they are also met with skepticism. It is questionable that the formation and diffusion of information should be offered by the police rather than through programs able to offer more autonomy to the schools, so that all the members of the educational community will be aware and prepared on the relevant topics.

Conclusions

Our research revealed that educational institutes in Barcelona have been increasing the presence of digital technologies for education and administration, a process promoted by European, Spanish and Catalan policies. The management of personal information and the massive use of students' data enabled by the digital systems and platform usage in schools has thus led to a progressive datification of educational environments. As we have seen, the introduction and supervision of these technologies depend on public administrations, school directors, professors, but also private and external companies, so that the impact on students' privacy result from the dynamics and practices established among those actors. Due to the difference in institutional situations (for instance public vs. private schools) and in the application of legal frameworks, to the complex relations generated by the relations between the stakeholders involved and finally to the lack of transversal knowledge about issues of data protection, our research has shown the scarce awareness about the process of control, protection and elimination of data.

As school staffs, directors and professors reported, a number of reasons contributed to this state of things: public administration policies and regulations are often ignored, as well as those of online services providers; the technical and legal aspects of data protection are unknown; there is no knowledge about the measures that can be applied to guarantee the security of these systems. This general lack of knowledge about requirements and protocols that need to be done by the member of the school community has led to heterogenous and often unsafe practices.

Consent forms, which constitute the fundamental mean for ensuring data protection, are often incomplete or present many mistakes. It is important that consent forms inform about the particularities of each system of data collection and explain their finality. As we have seen, this is not yet a well-established practice and, as for the Menendez i Pelayo Institute, it occured merely as a reaction to one father's complaints. It must be also noted that informed consent is a fundamental mechanism for correctly, safely and functioning technological systems in schools, as they contribute to increased knowledge and awareness about privacy and data protection issues.

Our analysis of the life-cycle of data has shown other critical aspects for an adequate treatment of data. First, the unsafe access to students' and professors' personal data which might occur when they use educational platforms during scholastic hours and then leave their account open, unknowingly allowing other people to have access. Second, there is a general lack of awareness about the protocols for eliminating data, both in regard to the kind of data that need to be destroyed and the mechanisms and timeframe of such elimination. Third, the use of Excel documents as a means for

collecting and sharing parents' and students' data is problematic, as in this way all the parents, and potentially other people, can have access to the information concerning other subjects. Along similar lines, the massive dispatch of emails is problematic as it reveals the e-mail addresses of other parents and students. A final critical situation is the collection of data that is unnecessary for the institute's purposes. But students' data protection goes beyond the scholastic boundaries as well: according to experts from the APDCat the greater dangers come from the management of students' information released through services and platforms that are outside the administration of the educational centres.

A significant difference was observed between administrative and pedagogic technologies. The latter, and in particular emails, educational apps and social networks, present a wider legislative vacuum concerning all the information generated by them. The information collected by such technologies goes beyond personal information such as name or birth date, as it can also include research history, research terms/inputs, geolocalized data, contact list, or information about student's behavior. This is problematic because there is no direct consent about all this data, so that students, professors and parents are no aware of the information generated through those systems.

Another common dynamic revealed by our field research is the externalization of services to private companies. Generally, such companies are considered, from a security perspective, an added value that brings greater efficiency in data management, as testified by the words of one professor:

> "We hire Clickedu because those more sensitive data, about families, bank accounts, telephone numbers, stay there, we count on the fact that they are managed, those data are in the cloud and the cloud is in some servers that are protected with all the appropriated security measures, and thus there is security, a guarantee from the external company that it is safe".

Nonetheless, many of these private systems and platforms use students' sensitive information for purposes unrelated to education, eventually threatening data security and integrity.

What emerges is thus a quite restricted conception of privacy, one focused on the criminal use of data by third parties, rather than a more integral approach that considers more fundamental questions like digital identity and discrimination, right to be forgotten, consent, or the compliance to the purposes for which data were collected. Many of these aspects have actually been implemented in the new European legal framework, the GDPR. But our study has also shown that professors and students have a scarce knowledge of the legal framework for data protection and its peculiarities in school environments. Such a partial knowledge seriously undermine the compliance to the norms and, on the contrary, generates a chain of confidence going from students to professors, from professors to schools and from schools to administration. This may limit the attention to mechanisms of control for data protection. On the other hand, experts from the academic sector and education administrations have argued that the new legal regulations effectively provide an answer to the current scenario, but this does not necessarily guarantee that they will be applied. Some elements for the correct application of the legal framework were thus individuated. First, the GDPR requires a governance effort for the development of a common policy among the different actors. Second, the active participation and interest of parents about these issues should be promoted, as it was pointed out that in many cases, parents allocate their attention elsewhere.Finally, in order to comply to the law, there is the need for greater transparency and, more specifically, for a better understanding of the concrete conflicts generated by data management. All these things considered, a solid and up to date knowledge appears to be the most effective way for guaranteeing the proper application of the legal frameworks and the creation of best-practices.

Awareness is an imprescindible element for students as well. It was in fact observed that the concept of digital identity is not easily understood or recognized by students who are not completely conscious of the information released through educational platforms, of the preventive measures they need to take, or of their rights. It is also worth noting that while students initially tend to express confidence about educational environments, they change their opinion when asked more in depth. Even though they recognize the constantly growing presence of technological support for their scholastic activities, they feel like they do not have enough power over decisions about those systems and platforms, or feel fully comfortable in using them. As we have seen, they do not know which precautions need to be taken before giving up their personal information, do not know how to guarantee anonymity online and are not aware of the consequences provoked by a lack of protection. In addition to this, students have also pointed out the function of control exerted by educational technologies, which increase the level of surveillance of parents and professors, and thus deeply threaten students' autonomy.

As a final reflection, in light of the results of this study, we consider the problems associated to informed consent, the limitations in the protocols and practices of security and data protection, the progressive externalization of educational services to private technological companies and the scarce awareness among the actors of the educational community all to be particularly relevant. The exploratory nature of this study, combined with the existing and growing relevance of these topics, reveal the necessity of further research and, for this reason, Eticas has planned a second phase of this study which will aim to expand the focus of the research.

References

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.

Glossary

Data: a symbolic representation (numerical, alphabetic, algorithmic, spatial, etc..) of a feature or of a quantitative or qualitative variable. It is generated or collected by a computer and it constitutes the information manipulated by the programmer in the construction and development of algorithms and models.

Data life-cycle: the sequence of stages that data go through from its initial generation until its archival and/or deletion. It consists of the following main stages: creation and capture, transmission, maintenance and security, management and access, analysis and exploitation,

Digital identity: the body of online information associated to an individual, but also to an organization or electronic device. Digital identity emerges from individual online activity and might include: usernames and passwords, purchasing behavior or history, date of birth, social security number, online search activities, such as electronic transactions, medical history.

Informed consent: The act and result of allowing something (the use of personal data, or participation in a study) after being informed on what the consent is given and for which purposes. From a legal perspective, informed consent forms work as contracts, as they are understood as “manifest will” stated in a written form.

Privacy: There is not a clear-cut definition of the concept of privacy. It generally applies to multiple dimension of personal behavior and information, as it can refer to privacy of information, of communication, of personal conduct and actions, of personal intimity, of family life. The notion thus covers a wider spectrum than data protection, as it does not focus merely on data processing, but also on intrusions more strictly connected to the physical person.

Data protection: process of safeguarding personal information in order to avoid illegitimate and illegal practices which might affect fundamental rights and freedom. Data protection has a broader scope than privacy as it deals with any processing of personal data, regardless whether or not such processing interferes with the privacy of an individual.

Data intensive technologies: Technologies which treat a massive amount of data for their operations

Right to erasure (“right to be forgotten”): right to obtain the elimination of data when 1) data is not necessary for the purpose they were collected, 2) consent is revoked, 3) the interested subject opposed to data treatment, 4) data is treated in illicit ways or must be eliminated according to legal obligations.

eticas