The Datafication of education: Lessons learned from the USA

Data intensive technologies and education series
May 2018

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*".

Author: Lorenzo Olivieri.

The Datafication of Education

Executive summary

Digital devices and platforms have become a fundamental part of educational environments. The adoption of ICT technologies and solutions for administrative or pedagogic purposes pose however serious challenges concerning the privacy and data protection of the students who engage with them. In fact, even though the collection of personal data have always been part of schools' activities, the quantity and intensity of data that can be gathered and treated by new technologies is unprecedented, leading to new possible harms and dangers. Regulations and laws to effectively guarantee students' right and privacy play then a fundamental role in these new educational contexts, but, as shown by many US cases, these measures are often insufficient and partial. The USA are an interesting case as several problems emerged in relation to educational platforms and systems such as Edmodo or inBloom. Despite the demand and development of normatives aimed to protect students and minors' privacy, the US legal framework appears nonetheless unable to deal with the potentialities of the new informatics systems. Informed also by a field research conducted in Barcelona schools, this reports suggests that, beyond adequate protocols and regulations, the active engagement of teachers and parents, school directors and students is essential for an actual protection of privacy and personal data as well as for the emergence of awareness about these issues.

Introduction

Contemporary life in the Western world is increasingly characterised by the use and presence of technologies (Dogde and Kitchin, 2011). One of the contexts in which technology has been massively introduced is the educational environment, where students, parents and teachers deploy multiple ICT solutions for educational, administrative and communication purposes (Rosen y Santesso, 2014; Taylor, 2013). However, the use of these technologies, while increasingly common, evoke a number of concerns and risks involving the protection of students' privacy. This is particularly relevant because the majority of those affected are minors. Moreover, the variety of the technologies used and found in educational contexts makes it difficult to provide a single, unified framework through which to assess and deal with the possible hazards tied to the misuse of data.

The technologies used in educational environments can be divided into four main categories. The first are managing technologies, which include software for handling data and e-mail services used by schools and public administration. The second are physical institutional technologies, namely those systems used for security and control such as CCTV or biometric identification systems. A third category concerns educational technologies used as new pedagogic tools, like personalized apps or learning management systems. Finally, there are also students' personal devices: smartphones, personal computer or tablets.

Despite being used for many different purposes, what is common among all these technologies is the amount of personal data they collect and generate. Numerous authors have noted that the collection, storage and distribution of students' personal data is practiced by schools all over the world. Educational environments, in other words, are increasingly "datafied" (Taylor, 2013; Richards & Stebbins, 2014; Tierney and Koch, 2016). Information about processes that previously were not registered or remained invisible are now stored and available for use. What is important to highlight is that, even though the collection of data has always been a common practice in schools, the quantity and intensity of data collected with new technologies open up not only new possibilities, but also new risks. The potential benefits of data have been widely assessed, but their massive use can also seriously challenge the fundamental human right to privacy, one of the main tools through which humans can develop an autonomous and complete self. As a result, the misuse of personal data can affect fundamental right at short, medium or long term.

In recent years, a growing number of empirical studies has started to analyse the relation between educational environment and the use of technology, as well as the possible risks of ICT technologies in schools. For instance, one study on Australian schools (Selwyn et. al. 2015) identified three main topics related to data and schools. First, a distinction between useful data and compulsory data; second, the nature of data in and outside schools; third, digital data as a way to engage with knowledge and alternative solutions. The main finding of the study was that many actors involved in the collection of data do not know who controls, blocks or protects that data once it is sold to other institutions.

Meanwhile, McCahill and Fill (2010) explored how gender and social class can determine differences in the perception of surveillance technologies (CCTV). Their study showed that while working class students perceive them as tools for controlling or punishing their leisure activities, more privileged students believed those technologies were installed to monitor the activities of others, not themselves.

Generally, these studies have shown an extended lack of protocols for the protection of students' data. Moreover, though multidisciplinary studies have treated the potential advantages of educational technologies, much less attention has been paid to the social consequences and ethical implications of the use of data and technology in educational contexts. With that in mind, this report discusses the relation between students' privacy and data protection and the proliferation of technological systems in educational environments. More specifically, it looks at protocols, policies and regulations intended to guarantee and manage sensitive data. In order to frame the main issues around data intensive technologies in schools and the limitations of regulatory measures to tackle them, we focus specifically on the USA.

USA case studies

As educational methods change and evolve, new technologies, learning models and evaluation systems are introduced, transforming the lives of students. However, the extensive use of information and communications technology also leads to processes of *datafication* which raise concerns regarding the protection of students' privacy.

In USA, where EDtechs are widely diffused, several problematic issues have already emerged. A paradigmatic example was the case of Edmodo, a learning network which allowed teachers to establish virtual classes, where students can create individual profiles and upload photos or other content from classes. By examining the security practices deployed by this online platform, an engineer found that data was not encrypted, making it available to anyone with access to the information. The company thus decided to implement a system of automatic encryption, but it had to recognize that its database had been hacked, exposing teachers and students' information.

A similar case is that of PowerSchoolSystem, which was deployed by many schools around the world to store students' pedagogical and administrative information. In 2014 the system faced many technical problems involving limited or excessive access to students' data, making it impossible to regularly perform the administrative tasks it was designed to handle. Despite complaints by administrations and schools, the platform is still being used in many countries.

Another well-known example is inBloom, a data analysis company that aimed to collect an enormous amount of information from students, from grades to the right to free lunches. The centralised information would then be used to adjust teacher and educational software to students' needs and requirements. However, the quantity and quality of personal data that was gathered in this way led to the failure of the project because of its privacy implications. According to Daniel Solove, this case exemplifies the problem of education and privacy by showing how, compared to other institutions, educational domains are quite behind in the realm of data protection, with a notable lack of the necessary infrastructure for protecting data privacy and security.

A second set of problems has to do with the extensive presence of big tech companies, like Google, Apple or Microsoft in educational institutions. By lobbying and pressuring administrations, these companies steer policymakers towards modifying educational programs in order to introduce new technological supports. To cite a well-known example, Google apps for Education have become extremely common in schools, with roughly 40 million in February 2015 and 100 million expected by 2020 if the company maintains its current pace. Another example is DreamBox Learning, an educational start-up for studying maths developed by the CEO of Netflix. The platform records students' activities as well as the precision of his or her results, time needed to answer questions, whether suggestions were needed before answering, etc. These examples suggest that tech firms are strong social actors with the power to influence the transformation of class activities.

"Tech firms are strong social actors with the power to influence the transformation of class activities."

Policy and regulatory actions

The above review of online platforms and applications demonstrates the pervasive, increasing presence of technologies in educational domains. As a result, governmental regulations and initiatives are being developed to deal with the privacy and data protection issues they entail.

Though dated, the main legislative framework for dealing with privacy in schools is the Family Education Rights and Privacy Act (FERPA), which since 1974 forbids the unauthorized sharing of educational records in all schools funded by the Educational Department. The law has recently been criticised for allowing exceptions, especially due to the externalisation of schools' functions to private companies. Today, FERPA is broadly considered insufficient to face the increasingly sophisticated practices of data collection, which were not contemplated when the law was passed. It contains several ambiguities, both in terms of concepts and application, and it is only compulsory for schools, meaning that private companies are not required to follow it. Another important legal framework is the Children's Online Privacy Protection Act (COPPA), which was put in effect in 1998 to regulate the collection of online information on people under 13 years of age. It establishes that online service providers are responsible for the privacy and security of these minors and must include a privacy policy guaranteeing parents' consent. However, this law also had several blind spots. For instance, COPPA does not cover all of the possible modalities through which information on minors is gathered, for instance when that information is provided directly by adults (i.e., parents or teachers).

To address persistent social demands for privacy regulations in schools and fill the gaps in FERPA and other legal frameworks, the US federal government began to approve a number laws, as well as endorse various data protection initiatives. The majority of these new laws attempted to guarantee restricted access to minors' information and define the

purpose for which this data can be used by private companies. Most of these norms also involve the use of written protocols for notifying and obtaining consent from parents.

In 2012 the Educational Department established a Privacy Technical Assistance Center (PTAC), with the aim of generating and diffusing support materials about privacy, confidentiality and security tools for teachers. Additionally, in light of the existing gaps in the legislative framework, state governments also developed norms to protect students' privacy. For instance, in 2014 California promoted a law, The Student Online Personal Protection Act ("SOPIPA") to regulate students' data-cycles. According to SOPIPA, online educational services providers cannot use the information obtained by students to create commercial profiles, address advertisements to students and families, sell students' information, or divulge students' personal information, with few exceptions.

SOPIPA was important for the development other legislative frameworks and governmental measures. In 2015 the Student Digital Privacy and Parental Rights Act (SDPPRA) forbade the use of students' personal identification information for marketing or advertisement purposes and attempted to minimise the amount of information transferred from schools to private companies. This law was in part a response by the Obama administration to increasing demands from parents, teachers and school administrators regarding the proliferation of classroom technology.

Meanwhile, in 2014 the industrial sector voluntarily launched the "Students Privacy Pledge", which committed to protecting students' privacy. In that document, the companies agreed to develop and support products for learning or administrative activities that ensured effective protection of students' privacy and transparent communication with families about the protection and use of the information collected. The document is a public and legally enforceable statement signed by companies such as Apple or AT&T and endorsed by the White House in 2015. It includes the following commitments:

- Not to collect, maintain, use or share personal information beyond that needed for authorized educational or school purposes, or as authorised by the parent or student.
- Not to sell students' personal information.
- Not to use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioural targeting of advertisements to students.
- Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.

Despite these advances in regulations and private sector initiatives, many social and academic actors believe that these laws do not consider many cases or scenarios that are especially relevant for students' security. More broadly, regulatory frameworks in the technological field seem unable to keep up with the capacities and functionalities of new information systems and their impact on privacy. Indeed, many analysts claimed SDPPRA did not fulfil the administration's commitment to limit function creep in the educational context, yet still gave educational tech companies a wide scope of action when handling students' data.

Conclusions

The USA is one of the world's most advanced countries in the development and integration of ICT for use in the field of education. Beyond the social and political reasons for this extended use of data-intensive technologies in schools, it is a helpful example of how this process requires policies and regulations which can anticipate and mitigate potential risks for students' privacy. For this reason, it is troubling that initiatives such as the Student Digital Privacy and Parental Rights Act (SDPPRA) have always been in response to data breaches or hacking events that endangered the freedom and integrity of minors. However, despite these limitations, the measures described in this report do represent an advance in the protection of students' privacy in particular domains, such as online exchanges.

Nevertheless, the integration of data protection and human rights requirements into any regulatory framework can only be effective if concrete protocols for data management

are established. Administrative authorities in charge of data protection should complement legal requirements with specific protocols for data collection, sharing and deletion, with particular emphasis on informed consent and the development of mechanisms for raising awareness about data protection. The digital literacy of all stakeholders, including the private sector, is key for this process.

Drawing on the lessons learned from Eticas R&C's study on privacy and data in Barcelona' high schools (the *Entorns segurs* or *Safe environments* project), the following two aspects can be underlined. First, it is useful to dispel some myths and prejudices regarding privacy and data protection. To begin with, there is a tendency to underestimate the value of data protection. Privacy must be considered a necessity and a fundamental right. Discussions and reflections on privacy should not focus only on the technological and legal domain, but also consider the many ethical and social implications caused by the use of technologies. Similarly, it would be misleading to think that concern for privacy means there is something to hide, that otherwise our personal data has no value and is thus unlikely to be analysed. On the contrary, the more access people have to data, the more likely it is that private data will become public. Seemingly inoffensive or useless data can indeed be used in illegitimate or unforeseen ways, leading to uncomfortable or dangerous situations, such as access to bank or social networks accounts, personal emails or confidential information. In this sense, anonymised data, despite being considered a 'good practice', do not guarantee total privacy, since any dataset can be cross-tabulated and the number of variables increased such that a person's anonymity is considerably reduced.

Secondly, in light of these consideration, it is important to be aware of the measures for data protection implemented by schools. Asking high schools, parents' associations, staff and faculty questions about these issues is one of the most effective ways of finding out what kind of information is being collected and processed, and for what purposes. The different actors involved in the use of data-intensive technology in schools should have concerns shaped by their own roles and interactions with that technology. For instance, professors should ask themselves whether they are aware of privacy policies, who is going to eliminate the data being collected or generated or whether they have been offered specific training about any of these issues. Similarly, students should be asked if

they know what kind of personal information they are sharing, who will protect their personal information and destroy it when necessary, or whether they have been informed about the dangers and consequences of improper use of educational technologies. Finally, the role of parents in asking and gathering information about the protection of their children's data is especially relevant. Fathers, mothers or legal guardians must read and eventually question the consent forms they or their children sign, and they should be aware of the tools and applications used by schools and whether their children had the opportunity to opt-out.

These are just a few examples of the possible concerns that might emerge regarding data protection in the educational field. Open and informed debates about these issues are inescapable steps for developing safe and good practices through which to ensure students' privacy and wellbeing.

References

Kitchin, R.; Dogde, M. (2011). Code/Space. Software and Everyday Life. London: Massachusetts Institute of Technology.

McCahill, Michael and Rachel Finn (2010). The Social impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums'. *Surveillance & Society,* 7(3/4): 273-289.

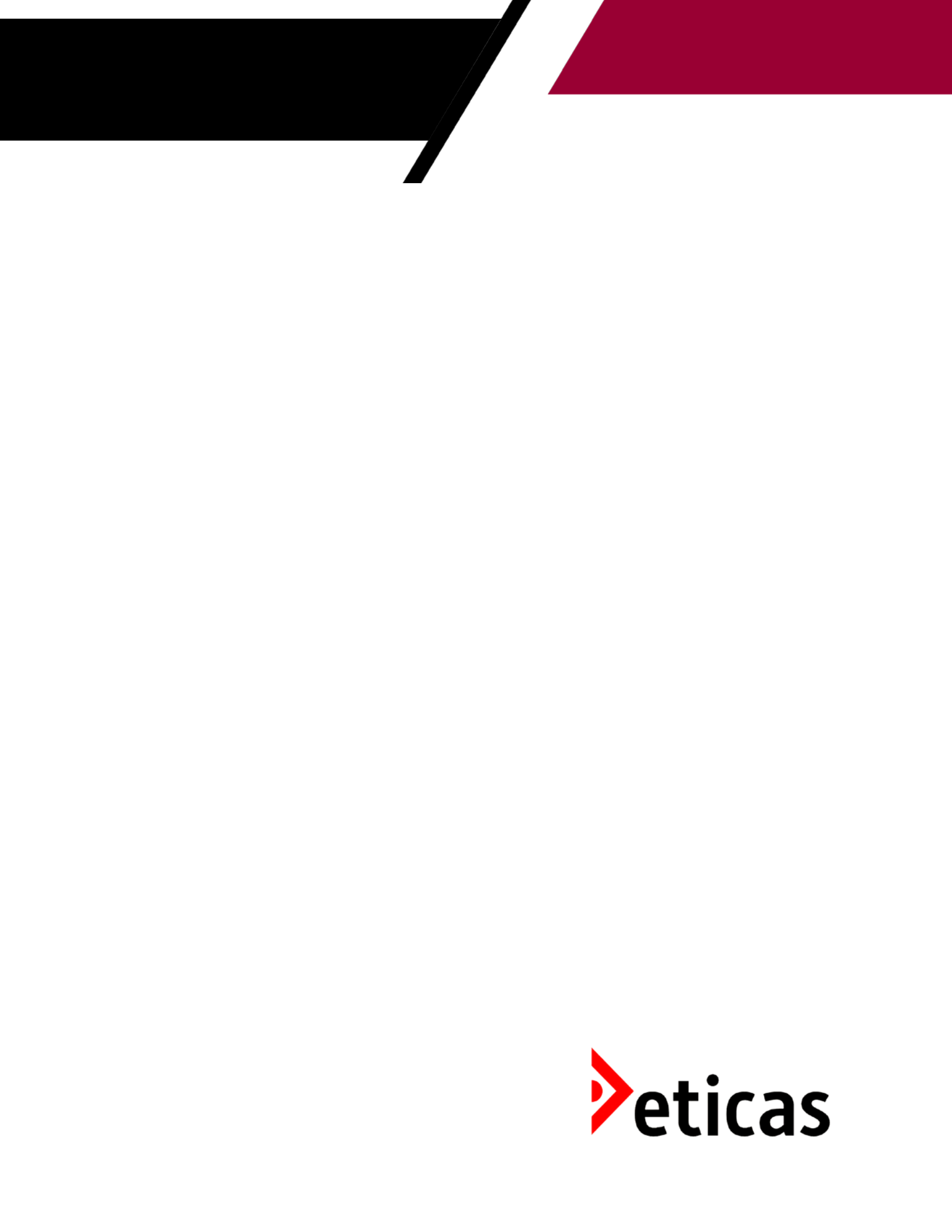
Richards, J. & Stebbins, L. (2014). Behind the data: Testing and assessment, a Pre K–12 US education technology market report. Washington, DC: Software & Information Industry Association.

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

Selwyn, Neil, Michael Henderson and Shu-Hua Chao (2015), Exploring the role of digital data in contemporary schools and schooling—'200,000 lines in an Excel spreadsheet', Vol. 41, No. 5, October 2015, pp. 767–781.

Taylor, E. (2013). *Surveillance Schools Security, Discipline and Control in Contemporary Education.* Springer. ISBN 978-1-137-30886-3.

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


eticas