Local Technology to Enhance Data Privacy and Security in Educational Technology

Daniel Amo[1]*, Paul Prinsloo[2], Marc Alier[3], David Fonseca[1], Ricardo Torres Kompen[1], Xavier Canaleta[1], Javier Herrero-Martín[4]

[1] La Salle, Ramon Llull University, Barcelona (Spain)
[2] University of South Africa, Pretoria (South Africa)
[3] Polytechnical University of Catalonia, Barcelona (Spain)
[4] La Salle University Center, Autonomous University of Madrid, Madrid (Spain)

unir
LA UNIVERSIDAD
EN INTERNET

Abstract

In educational environments, technological adoption in the last 10 years has enabled a data-driven and decision-making paradigm in organizations. The integration of cloud services in schools and universities is a positive shift in the field of learning, but it also presents threats to all academic roles that need to be discussed in terms of protection, privacy, and confidentiality. Cloud storage brings the ubiquity of data to this technical transition and a delusive opportunity for cost savings. In many cases, this suggests that certain actors, beyond the control of schools and colleges, collect, handle and treat educational data on private servers and data centers. This privatization enables the manipulation of stored records, leaks, and unauthorized access. In this article, we expose the possibilities that open from the viewpoint of local technology adoption. We seek to reduce or even totally solve the detrimental effects of using cloud-based instructional and analytical technology, mixing or only using local technology. Technological methods that conform to this alternate viewpoint and new lines of study are also being suggested and created.

Keywords

I. Introduction

SCHOOLS and universities are experiencing rapid processes of digital updating where the adoption of third-party technology solutions results in changes in academic and learning processes. This digital evolution means the use of third-party hardware and software, which mostly resides and executes in cloud computing [1], [2], and forces changes to educational institutions. On the one hand, institutions require permanent Internet connectivity, and therefore the data generated becomes ubiquitous and available at any time and anywhere. On the other hand, changes in academic and educational processes raise new problems concerning generated data. Consequently, the new digital learning context is causing a profound change in educational organizations as well as new issues that need to be addressed.

The growth of educational technology based on cloud computing has led to the adoption of educational decisions based on data in line with the big data analytics movement [3]. This type of hyperconnected educational environment has a strong ability to collect, store, process, and analyze large amounts of data through cloud computing. Technological innovations and the cheapening of cloud computing have made Software as a Service (SaaS) [4], which resides in the cloud, the most attractive option for the distribution of digital tools in the industrial field. Even in educational terms, the philosophy of cloud computing and services also applies [5].

Business models seek IT solutions to save costs. Cloud computing helps to maintain an architectural design geared towards storing and processing large volumes of personal data, data, and metadata on remote servers. The educational context does not escape the adoption of cloud computing; universities and schools are working to reduce costs [6]. However, the use of the cloud in this context results in many negative results, from data leaks to misuse. Consequently, digital educational technology tools (EdTech) raise new challenges and issues related to privacy, identity, confidentiality, and security of data and metadata (PICSDM) for all educational roles and actors involved [7]-[13]. We need to ask ourselves:

- Do we need to send data to cloud computing?
- What data should be sent outside the institution and can be transferred without risking the PICSDM?
- Do we need to send unsecured data to cloud computing, or can we send it anonymously?
- Can local technology provide a trustworthy, private, and secure environment?

If it is necessary and justified to send data to cloud computing, it is mandatory to define and integrate both processes and technology that ensure ethical and legal treatment.

* Corresponding author.
E-mail address: daniel.amo@salle.url.edu

We present a framework named LEDA (Local Educational Data Analytics) and fathom into the "local first" principle. The LEDA framework builds in of seven principles with a big focus on considering local technology in any analytical solution design. Thus, in this work we make an extensive exposition of the LEDA framework to show how local technology should be considered, studied, and debated as one more to solve in new ways, or minimize, privacy problems known in analytical educational environments.

The LEDA framework principles enhance data privacy and security in the development or adoption of digital tools in education. First, it encourages the use of the "local technology without data transfer outside the classroom" premise, not excluding the "remote with data transfer to cloud computing" premise but relegating it to the last place. Between these two premises is a very wide range of options. Technologically you can work locally, integrate a mixed system that stores personal data locally and links to systems in cloud computing, to work absolutely in cloud computing. The authors of this paper seem to be against cloud computing. On the contrary, our proposal lies in inferring from those ultimately responsible for technological infrastructures a new vision of new perspectives and possibilities concerning the local-cloud binomial:

- First, indicate that the concept of "local" does not refer only to servers of the institution. Both the institutional services and the educational staff can work with technological solutions that can reside both in the servers of the institution and in the devices provided to teachers.

- Second, we propose that the premises be considered within the technological equation as one more option. Every educational institution has limited resources and it may seem a natural evolution to solve any short-term problem via the adoption of cloud computing. However, working locally can activate a distributed architecture within the institution that achieves the same results as a centralized architecture in cloud computing.

- Third, the concept of "local" is not opposed to cloud computing. Only local, mixed solutions between local and cloud computing, or only cloud computing can coexist in an institutional space. We want to prevent cloud computing from being used as a unique solution where the keys are the problems to be solved.

As mentioned, the "local first" principle is the most important of the LEDA framework. In the following sections, we will justify in what ways it contributes something different by opening new possibilities of doing not considered until now. We understand the rest of the principles as the necessary context that supports it from a legal and ethical perspective. That is why in this work we focus on exposing the "local first" principle extensively to make the benefits visible and encouraging people to turn their attention to local technology.

The structure of the paper consists of six sections. The first section is the introduction. In the second section, we present the pedagogical and technological transformation of the La Salle institution as the trigger of the LEDA principles development, and the risks raised with technology innovation in cloud computing as well. In the third section, we present the seven principles that underpin the framework. In the fourth section, we present how the local principle can solve in new ways some problems, expose some technical possibilities to develop "local first" principle compliance technologies, and show some actual solutions already developed or in development as well. In the next fifth section, we present both future and ongoing lines of research. Finally, we summarize the conclusions of the work as the last and sixth current section.

II. Context

A. Act Locally, Think Globally

The ARLEP district (Agrupación Lasaliana España - Portugal) of La Salle institution in 2017 began the design of a new pedagogical framework called NCA [14], [15] and in 2019 started the deployment of the framework among all their schools and universities. This pedagogical transformation provides new methodological, new didactic formulas, and an intense innovation through the use of digital technology. Related to the uses of digital technology in cloud computing some data risks emerge. In this risky context, the LEDA framework sets the principles to ensure privacy, identity, confidentiality, and security of your data, personal data, and metadata (PICSDM) in the NCA transformation acting locally but think globally considering solutions that can be beneficial to any educational institution of the world and beyond.

At the same time, this framework initiates different research related to digital competence and data literacy. Within digital competence, we find data literacy as the ability to interpret and analyze data. In educational settings, this knowledge is useful for both teachers and students to make data-driven decisions considering that it is an increasingly technicalization environment and surrounded by data. The research will extract indicators of the state of the situation on digital knowledge and data literacy as well as the creation of self-assessment tools and specific training. It is hoped that these indicators, self-assessment tools, and training will raise awareness of the various issues related to the sensitivity of data in educational settings and active action to prevent them.

B. Data as Sensible Educational Assets

The collection, storage, and treatment of educational data by third actors cause undesired situations that make them very sensitive and fragile. This context is due to the uncontrolled introduction of Big Data technology, consisting of Artificial Intelligence [16], Machine Learning, Deep Learning, and Neural Networking techniques in combination with Cloud Computing. This set of technologies and techniques applied to education has indeed revolutionized, especially in decision automation. However, it has also led to a strong distrust of educational institutions, as they correspond to a context with many open questions and loss of control. Some examples of these analytical technologies are the massive automatic decision-making, massive sensible data collection from students [12], unauthorized access to data [17], discrimination, filtering, analysis, and predictive tools against students will [18], and data transfer without a legally defined relationship [9]. There is an unstable situation in collecting, treating, sharing, and analyzing educational data [13].

Moreover, Cloud Computing enables Dark Data. Dark Data is all the collected but unused data. This data is stored waiting to be used for the benefit of technology. At first, it is not known how they will be used. That is why Dark Data presents an uncertain and probably frightening future if current issues are considered.

Data is fragile whether in the Cloud or anywhere else. Data may be more fragile in the Cloud because there are more actors involved. However, locally stored data is also fragile and open for misinterpretation and misuse. Considering this provides a different perspective on the collection, storage, and treatment of data, while it raises the importance of ethical behaviors. "Author et al." [19] delve into the concept of sensitive data and data fragility. They pointed out that there is definitely (more) sensitive data. Depending on the context, any data can become sensitive, e.g., location data, devices version, or any previous academic performance can depend on the context, escalate into sensitivity. What is explicating "Author et al." is metadata. This is the reason why the authors will always specify data as both

personal data and metadata, considering metadata all interactions and kind of other data than personal associated with them.

1. Power Asymmetries

It is a rapidly evolving trend to develop digital educational tools in cloud computing. The problem with these tools, such as ClassDojo or Snappet, as different authors point out [7], [11], [20], is that they generate situations of active surveillance and even manipulation. It means that they somehow modify the environment to generate arbitrary behaviors in students, which self-regulates the power-technology-teaching-learning relationships in an unbalanced way. As Williamson [21] points out, these technologies are governed by automatic decision-making algorithms [22], developed with Big Data technologies, finally harmful by regulating educational processes thanks to the ability to execute predictive algorithms in cloud computing.

Two examples of this are the analysis by Norwegian Consumer Councils and the Norwegian Data Inspectorate. On the one hand, Norwegian Consumer Councils highlights the Dark Patterns those technologies such as Google, Facebook, or Microsoft use to reduce the privacy options on their devices [23], and even forcing the users to accept being tracked continuously [24]. These situations generate an asymmetry of powers that tilts the balance in favor of the technology companies 'profits, leaving users who use their services at their mercy and without many desirable privacy settings. In general, there are no devices intended exclusively for education. Students use generic devices such as personal computers or smartphones from companies that apply dark patterns. Therefore, students are victims of dark patterns without being able to opt for devices that protect them from these asymmetrical and monopolistic practices. On the other hand, the guide published by the Norwegian Data Inspectorate is another example in an educational context of how to monitor and profile students when using Google tools [25]. Google has a specific license for education that specifies which tools and services the GDPR complies with. This license protects students and prevents them from being profiled to serve advertising on certain tools. ChromeOS, Google's operating system (Chromebooks), is not included in this license. However, Google promotes Chromebooks as suitable devices for education when Norwegian Data Inspectorate points to the opposite.

Algorithms are not neutral and are filled with cognitive biases [26] weakening the confidence in their adoption, which in the case of education is based on Learning Analytics [26]–[28], which offer visual data analytics to reduce data literacy and enhance educational processes, such as evaluation [30]. This is why the use of Learning Analytics has caused concern and generated debate [31], [32], giving way to the proposal of frameworks, guidelines, and recommendations for use such as DELICATE [11] and SHEILA [33]. Despite the great effort being made to restore confidence, regulate, and make the integration of Learning Analytics into EdTech ethical and ensure PICSDM, it can be shown that cases that degrade confidence in the use of algorithms and analysis of educational data continue to happen. The case of the A-levels in the UK [34] is an example where algorithms applied by the government have undermined the qualification of a large majority of students by preventing them from accessing the desired university studies. These disastrous results in the use of algorithms in education have aroused great disagreement among students and a strong rejection of such practices [34]; millions of pieces of sensitive student data have been leaked in recent years [35] relating to personal data, registration data and even financial data [36].

By now, it is clear that a "human in the loop" is needed [37]. Moore contrasts the concept of "algorithmic decision" with "algorithmic results" when she says that "... algorithmic decision not least that there is no human outside to act as the guarantor of the good..." but that "... they're always already also inside that new framework or paradigm of knowledge so then there's no decision as such in what societies have begun to call algorithmic decision, there are outputs...". Dark patterns, no educational-oriented devices, no human-in-the-loop, and active decisional biased algorithms are some of the untrustful situations that generate power asymmetries between big techs and educational roles. Perhaps the solution can be enforcing legality while maintaining a "human in the loop" to avoid algorithmic decisions and accept/decline algorithmic results.

2. Laws and Geopolitical Issues

The enthusiasm for integrating Big Data processes, data-based decision-making, data processing, and even international transfer between countries has, in some cases, led to problems of misuse, filtering, and improper access [38]. Regarding legal matters, legality, as of today is very far from regulating emerging technologies. We believe that legality is more corrective than preventive. There are still problems concerning trust and loss of control in managing educational data that are not avoided due to legal loopholes. We are aware that there are as many decrees and regulations (from now on, laws) as there are different jurisdictions, some of them more prone to protecting the citizens PICSDM, including educational roles, such as the GDPR in Europe, some less, such as the USA with very low data regulation. To reach a balance between correction and legal prevention and avoid power asymmetries, we believe that it is necessary to have a technological stack that automates every jurisdiction's legal framework, by default and by design. However, an automated ethic is needed, as well as "human-in-the-loop" with some ethical principles. Because legality as a new ethic only helps to privatize institutions and strengthen monopolies, especially when there is no strong regulation and there is strong pressure from lobbies [39].

In terms of geopolitics, we are in a situation of significant change and high sensitivity. The link between Europe and the USA in the search for a regulation of the international transfer of data, the so-called Privacy Shield [40], has been broken after Max Schrems took his original case against Facebook a step further [41] to the point of banning the sharing of data with US entities subject to surveillance laws by their government [42]. The second Schrems II judgment [43] puts the European Commission in focus on adequacy talks with the United States on Standard Contractual Clauses (SCCs). However, the privatization of adequacy assessment is a fact that is manifested in the round tables "Privacy, globalization and international data transfers: towards a new paradigm after "Schrems II" of the International Conference CPDP 2021 [44].

3. Monopolies, Privatization, and Basic Commodities

EdTech services are becoming a staple. Initial phrases such as "memory are not important if the internet is available" or "all knowledge is in your pocket (referring to the mobile phone)" justify the unnecessary work of certain skills. These premises give monopolistic power to the technological ones that have managed to be dependent in an interconnected world. Besides, two factors are accelerating the privatization of educational technology and therefore centralizing educational data on a few actors. On the one hand, the COVID-19 pandemic [45], [46] has accelerated the adoption of educational and business technology in a forced march towards online services and privatization [47]. On the other hand, Williamson [48] points to "learning loss", a reduction in qualified human capital, as the cause of the diversion of capital to EdTech. In Williamson's words, "De-valuations of national economies from 'learning loss' ... were mirrored by massive valuations of EdTech, and efforts to capitalize on more of total global education expenditure".

Privatization is compounded by a lack of regulation in the United States that limits the monopolistic power of technology [49]. Educational technology is being capitalized and centralized in a few actors. As found in a longitudinal survey conducted between 2018 and 2019 [13], the educational tools in-app or web platform format used in schools and universities in Spain come mostly from the United States. Specifically, most of the solutions used are companies accelerated at Imagine K12 (IK12) EdTech accelerator [50]. Y Combinator absorbed IK12 during 2016 and so forming its first specialized vertical in education. One company that IK12 worked with was LearnSprout, an online data insights software startup acquired by Apple [51], demonstrating that educational data analytics and insights are of high interest by big technological companies.

IK12 startups use cloud computing or private servers the run their services. Since 2011 more than 10 IK12 startups analyze data collected from students' interactions meaning that data is stored and treated out of the control of academic institutions. Inside LMS in schools and universities students' can be anonymized and respected for their privacy [13]. This is not the case in these EdTech tools when are developed without following the LEDA framework.

4. Mass Surveillance as the New Normal

Most of EdTEch is not open-sourced. This means that is not publicly available to being audited by anyone. Therefore, educational institutions cannot know what it does, how it stores data, how it processes or analyses data, or with whom it shares educational data. Educational actors are subject to blind trust towards these privately funded, and even publicly funded, tools. The LEDA framework considers open-source solutions that protect and secures whilst legally compliant, and entities behind expose an ethical idiosyncrasy. We find entities like Proton [52] and Cryptpad [53] that in some way meet the above four premises and therefore make it possible to create EdTech under these minimum requirements (BLOE):

- Business ethics
- Law compliance
- Open source
- Encryption

Proton and Cryptad are not the only useful tools to save our digital identity and prevent misuse of our data. There are collecting platforms for this type of tool such as ethical.net, operated by the Center for Applied Ethics Ltd. Its slogan "make ethical the new normal" is a definition of principles that puts it in the fight against the surveillance situation. current extreme. Ethical.net [54] is presented as "a collaborative platform for discovering and sharing ethical product alternatives - whether that means purchasing from a social enterprise, thrift shopping, or learning how to fix your old phone instead of buying a new one.". Unfortunately, this description confirms that we are not in an ethical world and that ethics is the alternative when it should be the other way around. Ethical.net is an entity that embraces different ethical issues, however, the technological resources it makes available consider, if not all four BLOE requirements, at least that of business ethics and law compliance. The normality of being monitored, usurped data and metadata, used by third parties as desired and to be used against us requires to be replaced by new normality both ethically and legally. Thus, the 4 BLOE requirements are a start to start changing the scenario, but not enough.

5. Ethics and Data Privacy

Privacy is almost a new term in our society that raises too many questions. It refers to manage sensitive data of students. The introduction of educational data methodologies, such as Learning Analytics [55], [56], raises a non-trustable context in education. Some

authors, such as Drachsler & Greller [11], Pardo & Siemens [32], or "Author et al." [19], [57], reflect on ethical issues and how checklists and principles can be useful to diminish data problems.

III. Principles

The seven principles of the LEDA framework [58] have to be seen as a guide for good practices concerning the treatment of educational data in EdTech with a moral basis to resolve concerns, worries, and mistrust in educational data analysis processes raised in the use of loud computing EdTech. Cloud computing is a useful technical architecture in many respects, but that it requires some technical measures and the motivation to redirect current issues related to the privacy and security of collected data.

Without intending to replace the set of interconnectivity and cloud technologies –quite the opposite- the framework of principles is used to generate or use a variant of EdTech that focuses on "local first" instead of "global first", but also considering a mix of both. It is not at all a variant that confronts local installing against the cloud execution, making them exclusive; we do not exclude the use of the cloud. Our alternative promotes in the first place and as a fundamental premise the installation and execution of local applications that can cut off connectivity to the outside for students and give control of the data to teachers, or even give more control to students of their educational interactions. We foster a new perspective in deploying and executing EdTech services.

Considering the above, LEDA principles are stated as:

1. Legality
2. Transparency, information, and expiration
3. Data control
4. Anonymous transactions
5. Responsibility in the code
6. Interoperability
7. Local first

A. Principle 1: Legality

EdTech has to be legally compliant [58], [59]. However, regulations [60] are not automated within EdTech. If regulations are the ultimate solution, we need to update and automate them. Besides, legality is not able to regulate innovations in technology since:

- It is 20 years behind and does not regulate EdTech consistently and correctly [61]
- It may be too restrictive and not allow technology companies to compete with big technologies, or it may be too lax and harm end-users [61]
- It changes considering interests of governmental roles related or not to technological companies [62]

It is complex for legality to contemplate future problems, so legality only embraces known and past problems, under a limited imaginary. Regulating new technologies becomes difficult when you can't imagine or predict what that technology will look like. Besides, strong regulation means that there can be no technological evolution and therefore it will be impossible for alternatives to compete with the ruling monopolies. With weak or non-existent legality, the current privatization of EdTech and other sectors is happening, which also endangers the privacy and confidentiality of data in educational roles. Technology developments must comply with the law and the principles of privacy, confidentiality, and data security must be automated by default and from within the design of the tool [60]. Moreover, automation must be flexible in anticipation of changes in laws and regulations.

Concerning legality and personal data, people share data in really regulated environments but do not fully understand the real consequences:

- Users do not know the laws in depth.
- Users would need an average of 244 hours (30 consecutive working days) [63] to read all privacy clauses and terms of use for each website or application they use daily.

Concerning the above, the concept of privacy paradox stands out, which consists of making decisions via balancing disadvantages and benefits in a situation where people's behaviors do not agree with the principles and values towards private data. However, authors deny the existence of the privacy paradox [64] arguing that people act in the face of the risk presented in each situation and that from these behaviors cannot be inferred the real assessment they have of privacy of your data. People accept legal clauses that otherwise would not be able to operate normally. Therefore, forcing legal protection is beyond the reach of the people themselves, thus reinforcing the argument of the need for automation that makes it possible.

B. Principle 2: Transparency, Information, and Expiration

All educational roles need to be informed of all aspects of data storage and treating. Students should know, among other aspects, what data and metadata will be collected, how long will be stored, who will have access, or which rights will have if technology jurisdiction is different from student jurisdiction. Legal documents are not suitable to understand those such things [64], [65], [66], however, icons can be useful as stated in recital 60 of the GDPR [60].

C. Principle 3: Data Control

Data control refers to:

- Understand how their data are curated, accessed, and shared, under what protocols
- Grant data usage permissions
- Manage data in terms of storage and transfer

Technologists need to understand that to gain trust and be respectful of the digital identity of educational roles, they need to develop solutions that do not require data or only those that are necessary to operate. Therefore, EdTech tools should be considered as mere interfaces with which to interact with local data. These interfaces, as before, might be available from cloud computing in web format or even on student devices. However, this paradigm shift where personal data and metadata reside locally would reduce the excess data transferred and decrease the actors involved.

D. Principle 4: Anonymous Transactions

Data have to be disclosed at will to those who agree with it and only to those who have access to it. Understand and personalize teaching and learning, may need not anonymized data, and this may lay a paradox. However, the act to reveal information to consent people and keep anonymity to others does not suppose a paradox, it supposes privacy by default.

Compliant technology with this LEDA principle uses by default and by design:

- Secure protocols such as SSH, SSL or TLS
- Encryption methods such as Asymmetric Encryption Method or specific encryption algorithms, e.g., AES
- VPN protocols such as OpenVPN

E. Principle 5: Responsibility in the Code

This LEDA principle prioritizes open-source solutions to be evaluated publicly. Responsibility in the code means debating and making questions about ethics and legality in the code [67]:

- What would developers do if asked to write code for an unethical purpose?
- How would developers report unethical code?
- Do developers have an obligation to consider the ethical implications of their code?
- Who is ultimately most responsible for code that accomplishes something unethical?

F. Principle 6: Interoperability

Interoperability protocols, models, techniques, and methodologies already exist. LTI is one of them, and some LMSs, such as Moodle, already carry this built-in technology to interoperate with external tools out of a desire for privacy and data security. However, interoperability alone does not guarantee confidentiality but allows data to be moved freely and at will under established, validated, and functional protocols in trusted environments.

G. Principle 7: Local First

1. Zero Distance

Technology that complies with the "local first" principle is such technology that reduces data transfer distance between devices. It implies that in the development and integration of EdTech, closer technologies are considered first, instead of distant ones such as cloud computing. This makes a shift in considering which technology adopt in academic organizations and also in developing EdTech solutions. "Local first" principle conceives EdTech tools as mere interfaces that process local data. This raises the question; how can the distance concept be used to develop and deploy EdTech tools as mere interfaces?

The "local first" approach does not exclude any other technology, it simply prioritizes how to solve different situations. Cloud computing offers huge opportunities and risks as well. The "local first" approach also offers huge opportunities in a new way of solving issues related to educational data. However, this "local first" new way of doing has to be evaluated. It must be said that an absolute local approach does not solve all problems, even can make solutions complicated and unusable in user experience sense. Therefore, in this "local first" approach, hybrid solutions with cloud computing are not excluded.

2. Protocols and Solutions

The EdTech that uses local storage in users' devices and no data transfer by default is set the maximum value; therefore, this EdTech complies with the most important LEDA principle "local first". Thus, one way to increase confidence in educational settings is to use zero-distance technology. Zero-distance technology is about:

- Communicating, as shown in Fig. 1 and Fig. 2, using near possibilities such as WI-FI, Bluetooth, or NFC. Technologies such as scanning images through mobile cameras would be allowed, e.g., the use of encrypted QR codes to read students' answers to questionnaires.
- Local storage technologies such as Web Storage API, IndexedDB API, or even Cache API for web browsers. These web browser available technologies are specially identified as zero-distance technologies because they enhance privacy and security in the development of EdTech.

As seen in Fig. 1 and Fig. 2, the "local first" concept allows the use of local server applications to keep data safe in rest inside educational organizations. Zero-distance technology enhances data control without allowing third-party actors to catch data generated in learning processes mediated by digital technology solutions. Teachers and students communicate with each other without transfer data to third-party servers. When zero-distance technology is used in EdTech, data is being transferred to company servers. An example of EdTech solutions

that partially use "local first" technologies is Plickers [68]. Teachers scan QR codes held by students, but answers and students' data are uploaded to Plickers' data servers, breaking the data control principle.
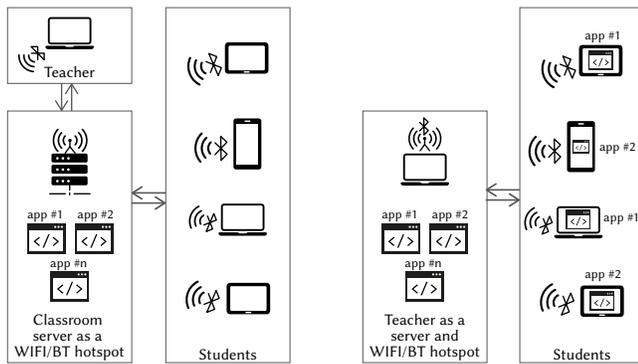

Fig. 1. The use of a WIFI or Bluetooth communication between educational roles where an in-class device (e.g., computer) is used as a server to keep data locally without transfers to third parties.
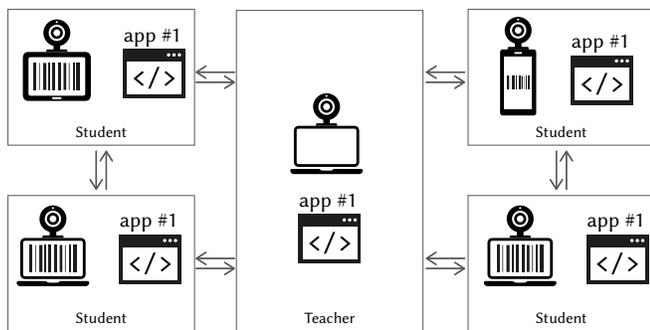

Fig. 2. The use of QR codes or Codebars to share information between educational roles both in-class and out-class to preserve data locally without express transfers to third parties.

3. Synchronization

"Local first" enables synchronization at will. EdTech that uses cloud computing incorporates automatic algorithms that continually communicate devices and servers sending data by default and with no settings to change how, what, and when to synchronize. Data is transferred automatically and constantly to remote company private servers. In the imaginary of LEDA framework, EdTech tools are mere interfaces and data transfer is one-way from student to teacher or student to LMS where students' data can be accessed.

To avoid continuous data streaming to remote servers, synchronization options are enabled but not activated by default. Automation simplifies processes but synchronizes with a local server or personal device when desired allows data management and control. Notwithstanding the evidence that reducing data transfer to cloud computing is the most convenient scenario, not all applications can work completely locally, and some data would be transferred to third-party servers to ensure the proper functioning of the solutions. Regarding "Author et al." that every single data point is fragile, some data points are inevitably shared but not necessarily those that identify persons. Therefore, makes sense to deploy a Personal Data Broker [69] to manage data sharing.

IV. New Looks at "Local First"

Looking into a "local first" approach means reducing two key elements in EdTech:

- Devices, in their broad aspect: servers, routers, hard drives, etc.
- Intermediaries, any actor that can access data from educational roles

Different actors are involved in the use of EdTech, such as classmates, teachers, system administrators of the educational institution, different people from different departments of the educational institution, staff associated with the educational services of third parties, and even third-party staff who have access to data that the educational services share for its proper functioning. Similarly, data navigates complex circuitry through a good set of devices such as proxy servers, switches, or routers where data is likely to be stored.

The EdTech scenario is a complex one and it is not easy to find a unique solution to the problem of fragility in PICSDM. We believe that this scenario can only be resolved through the adoption of standards, good practices, and forced automation under public audits. However, these standards should be based on principles that we believe the LEDA framework is a good starting point for.

The teacher must be able to view the student's data to address, communicate and tutor them, even if this data does not show the student's actual identity [12]. It should also be able Of course the teacher should be able to see academic data as results of questionnaires and other results of assessment instruments. The data that is generated on the student's device should go out. We have proposed possible solutions based on communication technologies within the classroom and others via QR code in case of working online. However, in some environments, there is no presence and QR codes do not solve all the cases. In this sense, given that the student's data will be transferred to another device or storage, principles 3, 4, and 5 take force so that the student has control over data transfers (e.g., acceptance), remain anonymous under the use of interoperable technologies.

A. Personal Data Record Store and Personal Data Brooker

Applying the "local first" principle in its entirety means that the student or any educational role can grant access to the data at will even without the person asking for it despite knowing the real identity. It is not even necessary for a teacher to know the identity of their students, as it will assess evidence of learning and not personalities. It would therefore make sense that in an LMS in absolutely online learning even the personal identifying information of each student is not needed. In any case, some scenarios require data to be transferred out of the student's device for the smooth running of the learning process.

We believe that the use of local storage that stores student interactions in sync with microservices can facilitate the scenario discussed. Fig. 3 shows how this scenario could be and what we are currently working on as a line of research for the LEDA framework:

- Apps as mere interfaces: EdTech tools running locally in the browser or as standalone applications without transferring data to the cloud or transferring anonymized data.
- Personal Data Record Storage (PDRS): local service that collects each interaction with EdTech tools synchronizing with a trusted and encrypted storage. This service installed in the device will have a proxy function between local data and the cloud.
- Personal Data Broker (PDB): some authors of this work worked on this concept [69] as a space managed by the student, or educational role, which connects with third party services such as LMS of the educational institution and share what is needed and at the right time. The stored data would be encrypted and served open or anonymized depending on the occasion. This PDB works as a microservice in which to make requests when needed.
- LMS: Although in Fig. 3 the PDB is connected to the LMS database, in reality, and depending on the situation, the data should not be stored. For instance, the teacher may have access to the student's

email, but the LMS system administrator does not need to have access to it. Other data will be interesting to store to streamline management, such as grades, however, these could be associated with a user identifier, even random, which allows the identity of the student to be anonymized.
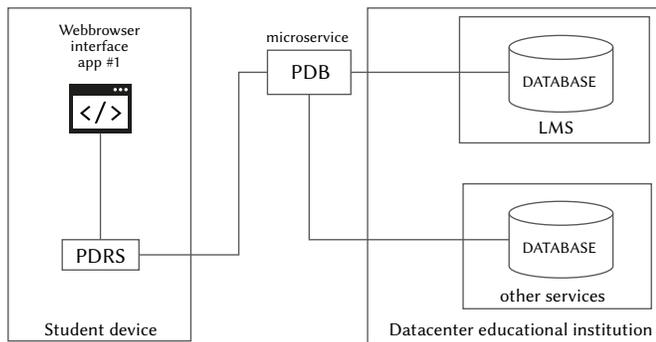

Fig. 3. Use of EdTech tools as interfaces that saves data locally in the Personal Data Record Storage synchronized with the service Personal Data Broker which serves data to educational services if needed.

Microservices such as the PRDS-PDB binomial open up new ways of doing things where data control lies with the student and inquiries can even be anonymous.

V. LEDA Developments

Developing educational tools and solutions following the LEDA framework is not complex, it is a matter of will. However, when designing some tools based on proximity technologies, we realize that usability can be very inconvenient. Cloud Computing makes the difficult easy by automating tedious manual processes. Instead, emulating the same functional behavior in the cloud on the premises becomes something manually if you want to ensure absolute control while using the solution. We present three examples that show how local technologies can add control to both data and processes without the user experience being affected, and how in some cases complexity and inconvenience in using the solutions are added if there are no automatisms. Therefore, the use of local, or zero-distance, technologies require a balance between:

- Complexity
- Automation
- Control

Balancing between one feature or another will depend on the configuration options set by the user. Therefore, the ethics of personalization via configuration options must be defined and implemented, without dark patterns that lead to confusion or wrong decisions.

A. QR Codes

One of the proposals defined in the "local first" principle is implemented, consisting of reducing as many devices as possible using QR codes. In this sense, servers are removed, and an application is designed with the following requirements:

- Teachers should be able to rearrange assessment forms with correct/incorrect questions and answers
- Teachers must be able to import students' answers
- Students must be able to receive the forms
- Students should be able to answer questions and send them to the teacher

- Enable communication between teachers and students via QR codes, either scanned or sent through a conventional communication channel such as email or Bluetooth

This mode of operation allows you to remove proxies and make sharing QR codes immediate by performing a scan. In the worst cases, QR codes can be shared via Bluetooth or other conventional services such as email or flash drive. Sending student responses to the teacher will be done by applying encryption to enable secure communication.

Teachers can enable a QR code repository so that other teachers can scan or import the QR code and dump the content to their devices. Therefore, both student forms and responses will be stored locally on the teacher's device; students will be able to keep their answers on their devices. Fig. 4 shows the teaching version with the on-screen QR code generated from a different question-and-answer form. A button allows you to download the QR and share it if it cannot be scanned. Fig. 5 shows the study version where once the questions have been answered, the QR code can be generated to be scanned by the teacher or sent with the encrypted information.

This solution, however, involves some problems related to the length of the content. Content capacity may require different QR codes to be generated. Therefore, reading by scanning or importing an image can be tedious depending on the number of QRs generated.

Fig. 4. QR code generated from questions and answers introduced by teacher in her device.

Fig. 5. Response of student ready to be qrcoded and scanned or send to teacher.

B. Bluetooth

Other proximity technologies such as Bluetooth connectivity are less cumbersome for users. We developed the Bpoll mobile app. It also consists of creating forms by teachers and responding to students. However, Bluetooth technology makes communication within the

classroom easier:

- QR codes are not shared or scanned
- The feeling is like being in a traditional cloud computing application
- Connectivity is local and data is transferred bidirectionally between teacher and student

In this type of technology, it is required to connect the devices expressly. This procedure is partly a control mechanism and partly an additional step that improves the user experience. However, control involves configuration, and configuration leads to a better understanding of technology and awareness of the dangers associated with data. Therefore, the execution process for each role within Bpoll is:

- The teacher creates the forms in the Teacher section
- Teachers warn of the availability of their device via "Advertise device"
- Students are asked to connect to the teacher's device to establish a connection
- Students access the forms and answer the questions presented

Fig. 6 and Fig. 7 show the main screen displayed by the teacher and the connectivity request screen for the student. The process is not far from a cloud computing application except for the pairing step between devices. However, with Bluetooth technology, this process could be automated and pairing reduced to just one and the first evaluation.
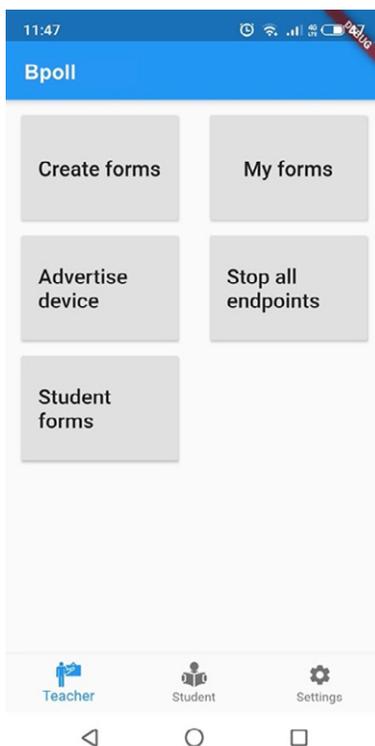

Fig. 7. Students in Bpoll pairing screen with teacher device.

C. Local Analytics

Following the premise of working with local data, we have developed a local execution application, with web technologies available on any personal computer, which allows the analysis of educational data from LMS exports. The development will show that it is possible:

- Distribute the analysis of educational data at the teacher level
- Work on the analysis of local educational data without the need for cloud computing
- In certain environments with a computing power that a browser and a personal computer, including a smartphone, can provide, it is sufficient to perform data analysis.

The tool is called Javascript Moodle Learning Analytics because it is supported by the Javascript Learning Analytics (JSLA) library developed ad hoc and adaptable to any data scheme. Moodle has served as a pilot LMS to use JSLA, build the JSMLA tool (view Fig. 8), and be able to view student interactions from an export of the interaction log.

Fig. 6. Bpoll's teacher screen with forms management and connectivity options.

The limitations of using only Bluetooth technology make it usable only in physical spaces due to the limited range. A hybrid technology between Bluetooth and QR codes could bridge these distances given the very limitations mentioned above about QR codes. It is a line of research to resolve these limitations via PRDS and PDB.
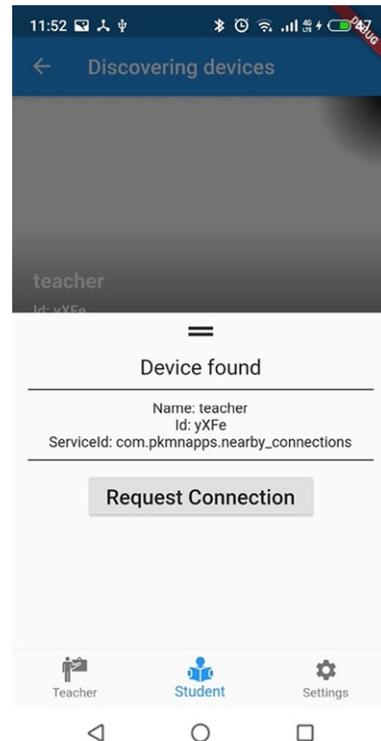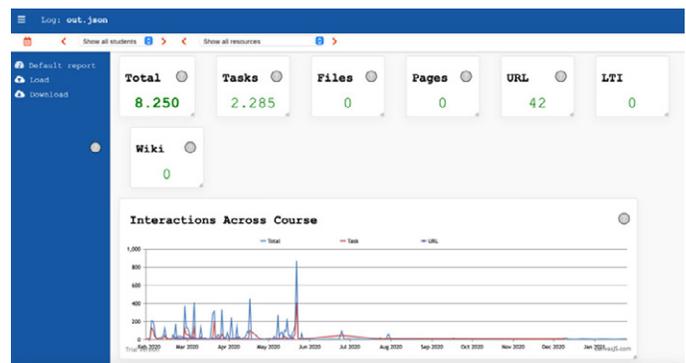

Fig. 8. JSMLA dashboard autogenerated by default.

The limitations are given by the computing power of personal devices concerning the amount of data that can be generated in an

online class. However, the tool analyzes logs of interactions that are not large in a standard environment. We will soon publish in more detail this open-source web library and all its possibilities.

VI. Research Lines

The LEDA principles open different fields to research on considering local technologies, encryption algorithms, legal considerations, or even ethical approaches. Here we present some research lines as a result of the seven principles:

- Provide an EdTech scoring platform concerning the principles of the framework. Distance between devices and data storage allows a score to be generated and also score EdTech solutions.
- Critically evaluate developments of technological solutions that meet the principles of the framework.
- Fathom the possibilities of the "Personal Data Record Store" and "Personal Data Broker" proposals to encourage the adoption of local technology.
- Detect educational community awareness of the risks related to data and cloud computing, as well as disseminate the seven principles of the LEDA framework as an attenuator and a solver.
- Develop solutions that include by design and by default the directed synchronization, with the possibility of automating the process.

VII. Conclusion

La Salle finds itself in the process of a methodological and technological transformation as well as confronting data issues. La Salle's situation is a very common situation on the educational stage. However, many institutions rely on legality to implement institutional changes that favor pedagogical aspects but also resource reduction in an attempt to balance. Political forces and private capitalism are pushing for the adoption of cloud technologies in an attempt to privatize education. However, when legality is branded as the new ethic, everything is worthwhile, and education is lost. We need technological initiatives and models that eliminate power asymmetries, give control to educational roles and institutions, as well as technologies that automate legality and ethics by omission and from design.

This work sets a framework of data protection and privacy principles to provide trust and confidence to minimize or solve data problems related to EdTech, Data Analytics, and Cloud Computing. This paper sets out the LEDA framework and its seven principles of legality, transparency, data control, anonymous transactions, code responsibility, interoperability, and "local first". This framework has been named LEDA after its seventh principle "local first.". This framework should be considered in the development and adoption of EdTech that collect, store, manage and analyze educational data.

The first six principles set the background to enable the seventh "local first" principle as the most impactful of all in terms of data confidentiality and privacy. The principle "local first" adds new perspectives to adopt ethical EdTech solutions and understand EdTech as interfaces. Data proxies such as personal data record storage enable data control to students allowing access under self-consideration and not by the EdTech tool. The synchronization with personal data brokers inside the LMS facilitates local data management and control to students.

In the framework, distance between devices and EdTech is a key factor to preserve educational data. The more the data is far away, the more perils arise. Zero distance is considered the more adequate scenario. Data proximity is therefore essential to ensure non-leakage, non-misuse, non-prohibited, or inappropriate storage, and non-processing without permission of any data generated in the interaction with the solution.

Considering the limitations of the framework, we envision different problems or educational situations to solve where zero distance makes the solution complex and unusable, considering the use of local-cloud hybrid developments. Local technologies can difficult the user experience and the teaching and learning processes, and even make all educational processes harder to execute. The comfort of cloud computing disappears and can be considered a stopper of local technologies adoption.

The LEDA framework allows institutions to consider issues related to the processing of student data in data-driven decision-making. At the same time, it offers a series of principles of action that minimize or even solve some of the problems present in the adoption of educational technology. These principles offer a change of perception that does not eliminate but ultimately relegates the integration of technologies in Cloud Computing by local technologies.

References

[1] F. J. García-Peñalvo *et al.*, "Mirando hacia el futuro: Ecosistemas tecnológicos de aprendizaje basados en servicios Looking into the future: Learning services-based technological ecosystems," in *La Sociedad del Aprendizaje. Actas del III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad*, Madrid, Spain, 2015, pp. 553–558.

[2] J. O. Islas-Carmona, "El prosumidor. El actor comunicativo de la sociedad de la ubicuidad," *Palabra Clave*, vol. 11, no. 1, pp. 29–39, 2008.

[3] P. Long and G. Siemens. "Penetrating the Fog: Analytics in Learning and Education." EDUCAUSE Review. https://er.educause.edu/articles/2011/9/penetrating-the-fog-analytics-in-learning-and-education. (accessed Jul. 24, 2018).

[4] D. Amo, M. Alier, M. J. Casan, and M. J. Casañ, "The student's progress snapshot a hybrid text and visual learning analytics dashboard," *International Journal of Engineering Education*, vol. 34, no. 3, pp. 990–1000, 2018.

[5] J. Navarro, A. Zaballos, D. Fonseca, and R. Torres-Kompen, "Master as a Service: A Multidisciplinary Approach to Big Data Teaching," in *Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality*, León, Spain, 2019, pp. 534–538.

[6] C. Bulla, B. Hunshal, and S. Mehta, "Adoption of Cloud Computing in Education System: A Survey," *International Journal of Engineering Science*, vol. 6, no. 6, pp. 6375-6380, 2016.

[7] D. Lupton and B. Williamson, "The datafied child: The dataveillance of children and implications for their rights," *New Media and Society*, vol. 19, no. 5, pp. 780–794, 2017.

[8] R. Mayes, G. Natividad, and J. Spector, "Challenges for Educational Technologists in the 21st Century," *Education Sciences*, vol. 5, no. 3, pp. 221–237, 2015.

[9] D. Amo, M. Alier, F. J. García-Peñalvo, D. Fonseca, and M. J. Casany, "GDPR security and confidentiality compliance in LMS' a problem analysis and engineering solution proposal," in *TEEM'19: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality*, León, Spain, 2019, pp. 253–259.

[10] D. Amo, D. Fonseca, M. Alier, F. J. García-Peñalvo, and M. J. Casañ, *Personal data broker instead of blockchain for students' data privacy assurance*, vol. 3. Switzerland: Springer Nature, 2019.

[11] H. Drachsler and W. Greller, "Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics," in *Proceedings of the sixth international conference on learning analytics & knowledge*, Edinburgh, United Kingdom, 2016, pp. 89–98.

[12] D. Amo, M. Alier, F. J. García-Peñalvo, D. Fonseca, and M. J. Casañ, "Protected users: A moodle plugin to improve confidentiality and privacy support through user aliases," *Sustainability*, vol. 12, no. 6, p. 2548, 2020.

[13] D. Amo, "Privacidad y gestión de la identidad en procesos de analítica de aprendizaje," PhD. dissertation, Programa de Doctorado Formación en la Sociedad del Conocimiento, Universidad de Salamanca, Spain, 2020. [Online]. Available: https://repositorio.grial.eu/handle/grial/1951

[14] L. S. D. ARLEP, *NCA, otra manera de hacer escuela*. Madrid, Spain: La Salle ARLEP, 2018.

[15] L. S. D. ARLEP, *NCA, Nuevo Contexto de Aprendizaje*. Madrid, Spain: La Salle ARLEP, 2020.

[16] J. C. Sánchez-Prieto, J. Cruz-Benito, R. Therón, and F. García-Peñalvo, "Assessed by Machines: Development of a TAM-Based Tool to Measure AI-based Assessment Acceptance Among Students," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 4, p. 80, 2020.

[17] D. Amo, M. Alier, F. García-Peñalvo, D. Fonseca, and M. J. Casañ, "Privacidad, seguridad y legalidad en soluciones educativas basadas en Blockchain: Una Revisión Sistemática de la Literatura," *Revista Iberoamericana de la Educación Digital*, vol. 23, no. 2, pp. 213-236, 2020.

[18] D. Amo, M. Alier, D. Fonseca, F.-J. García-Peñalvo, M. J. Casañ, and J. Navarro, "Evaluation of the importance of ethics, privacy and security in Learning Analytics studies, under the LAK conferences," in *Actas del V Congreso Internacional Sobre Aprendizaje, Innovación Y Competitividad*, 2019, pp. 343-348.

[19] S. Slade and P. Prinsloo, "Learning Analytics: Ethical Issues and Dilemmas," *American Behavioral Scientist*, vol. 57, no. 10, pp. 1510–1529, 2013.

[20] B. Williamson, "Decoding ClassDojo: psycho-policy, social-emotional learning and persuasive educational technologies," *Learning, Media and Technology*, vol. 42, no. 4, pp. 440–453, 2017.

[21] B. Williamson, *Big data in education: The digital future of learning, policy and practice*. London, UK: SAGE Publications Ltd, 2017.

[22] K. Peiró, "ADA en acció: treball de recerca a Catalunya," in *Intel·ligència artificial. Decisions automatitzades a Catalunya*, Autoritat Catalana de Protecció de Dades and Generalitat de Catalunya, Eds. Barcelona: Autoritat Catalana de Protecció de Dades, 2020, p. 100.

[23] Ø. H. Kaldestad, "New analysis shows how Facebook and Google push users into sharing personal data," Forbrukerradet, Sentrum, Oslo, 2018. [Online]. Available: https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/

[24] Ø. H. Kaldestad, "New study: Google manipulates users into constant tracking," Forbrukerradet, Sentrum, Oslo, 2018. [Online]. Available: https://www.forbrukerradet.no/side/google-manipulates-users-into-constant-tracking/

[25] P. Tranberg, "DPA Slams Norwegian Municipalities In Their Use of Google for Education,. DataEthics. https://dataethics.eu/dpa-slams-norwegian-municipalities-in-their-use-of-google-for-education/. (accessed Dec. 20, 2020).

[26] K. Peiró, "És possible acabar amb els biaixos dels algorismes? (1a part)." karmapeiro.com. https://www.karmapeiro.com/2019/06/17/es-possible-acabar-amb-els-biaixos-dels-algorismes-1a-part/. (accessed Sep. 16, 2020).

[27] F. J. García-Peñalvo, "Learning Analytics as a Breakthrough in Educational Improvement," in *Radical Solutions and Learning Analytics*, Springer, Singapore, 2020, pp. 1–15.

[28] M. A. Chatti, A. L. Dyckhoff, U. Schroeder, and H. Thüs, "A reference model for learning analytics," *International Journal of Technology Enhanced Learning*, vol. 4, no. 5–6, pp. 318–331, 2012.

[29] A. Martínez Monés *et al.*, "Achievements and challenges in learning analytics in Spain: The view of SNOLA," *Revista Iberoamericana de la Educación Digital*, vol. 23, no. 2, p. 187, 2020.

[30] A. Álvarez-Arana, M. Villamañe-Gironés, and M. Larrañaga-Olagaray, "Mejora de los procesos de evaluación mediante analítica visual del aprendizaje," *Education in the Knowledge Society*, no. 21, p. 9-13, 2020.

[31] H. Drachsler, "Ethics & Privacy in Learning Analytics - a DELICATE issue," Learning Analytics Community Exchange. http://www.laceproject.eu/blog/ethics-privacy-in-learning-analytics-a-delicate-issue/. (accessed Sep. 20, 2017).

[32] A. Pardo and G. Siemens, "Ethical and privacy principles for learning analytics," *British Journal of Educational Technology*, vol. 45, no. 3, pp. 438–450, 2014.

[33] Y.-S. Tsai, P. M. Moreno-Marcos, K. Tammets, K. Kollom, and D. Gašević, "SHEILA policy framework: informing institutional strategies and policy processes of learning analytics," in *Proceedings of the 8th International Conference on Learning Analytics and Knowledge - LAK '18*, 2018, pp. 320–329.

[34] L. Amoore, "Why 'Ditch the algorithm' is the future of political protest," The Guardian. https://www.theguardian.com/commentisfree/2020/aug/19/ditch-the-algorithm-generation-students-a-levels-politics. (accessed Sep. 16, 2020).

[35] J. Satisky, "A Duke study recorded thousands of students' faces. Now they're being used all over the world," The Chronicle. https://www.dukechronicle.com/article/2019/06/duke-university-facial-recognition-data-set-study-surveillance-video-students-china-uyghur. (accessed Sep. 16, 2020).

[36] D. MacMillan and N. Anderson, "College admissions officers rank prospective students based on web browsing, family finances and other data," The Washington Post. https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/. (accessed Sep. 16, 2020).

[37] L. Amoore and R. Raley, "Securing with algorithms: Knowledge, decision, sovereignty," *Security Dialogue*, vol. 48, no. 1, pp. 3–10, 2017.

[38] M. Grothaus, "Pearson data breach: details of hundreds of thousands of U.S. students hacked," Fast Company. https://www.fastcompany.com/90384759/pearson-data-breach-details-of-hundreds-of-thousands-of-u-s-students-hacked. (accessed Jan. 8, 2019).

[39] L. Kayali and V. Manancourt, "How Europe's new privacy rules survived years of negotiations, lobbying and drama," POLITICO. https://www.politico.eu/article/europe-privacy-rules-survived-years-of-negotiations-lobbying/. (available Feb. 10, 2021).

[40] M. A. Weiss and K. Archick, "U.S.-EU data privacy: From safe harbor to privacy shield," *The European Union: Challenges and Prospects*. Congressional Research Service, pp. 113–135, 2016.

[41] NYOB, "My Privacy is None of Your Business," None Of Your Business. https://noyb.eu/en. (accessed Sep. 16, 2020).

[42] P. Petit, "'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization," *Science as Culture*, vol. 29, no. 1, pp. 30–56, 2020.

[43] R. Á. Costello, "Schrems II: Everything is Illuminated?," *European Papers-A Journal on Law and Integration*, vol. 5, no. 2, pp. 1045–1059, 2020.

[44] ElDerecho.com, "CPDP 2021, los retos de las transferencias internacionales de datos tras Schrems II," ElDerecho.com. https://elderecho.com/cpdp-2021-los-retos-de-las-transferencias-internacionales-de-datos-tras-schrems-ii. (accessed Feb. 9, 2021).

[45] F. J. García-Peñalvo, A. Corell, V. Abella-García, and M. Grande, "Online assessment in higher education in the time of COVID-19," *Education in the Knowledge Society*, vol. 21, pp. 12-26, 2020.

[46] F. J. García-Peñalvo and A. Corell, "La COVID-19: ¿enzima de transformación digital de la docencia o reflejo de una crisis metodológica y competencial en la educación superior?," *Campus Virtuales*, vol. 9, no. 2, pp. 83–98, 2020.

[47] B. Williamson and A. Hogan, "Pandemic privatization and digitalization in higher education," code acts in education. https://codeactsineducation.wordpress.com/2021/02/10/pandemic-privatization-digitalization-higher-education/. (accessed Feb. 10, 2021).

[48] B. Williamson, "De-valuations of national economies," Message on Twitter. https://twitter.com/BenPatrickWill/status/1360322220132884481?s=20. (accessed Feb. 12, 2021).

[49] C. Doctorow, "How to destroy surveillance capitalism," OneZero. https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59. (accessed Aug. 26, 2020).

[50] Y Combinator, "Imagine K12," Imagine K12.http://www.imaginek12.com/. (accessed Sep. 16, 2020).

[51] C. Loizos, "Y Combinator Absorbs Edtech Accelerator Imagine K12, Creating Specialized Vertical," TechCrunch. https://techcrunch.com/2016/02/10/y-combinator-absorbs-edtech-accelerator-imagine-k12-creating-specialized-vertical/. (accessed Feb. 10, 2016).

[52] ProtonMail, "We have released an open source OpenPGP library - ProtonMail Blog." OpenPGP library. https://protonmail.com/blog/openpgpjs-3-release/. (accessed Sep. 16, 2020).

[53] CryptPad, "CryptPad Analytics & Privacy - What we can't know, what we must know, what we want to know." CryptPad Blog. https://blog.cryptpad.fr/2017/07/07/cryptpad-analytics-what-we-cant-know-what-we-must-know-what-we-want-to-know/. (accessed Sep. 16 2020).

[54] Ethical.net, "Ethical.net." Make ethical the new normal. https://ethical.net/. (accessed Jul. 11, 2019).

[55] C. Lang, G. Siemens, A. Wise, and D. Gasevic, *Handbook of Learning Analytics*. New York, USA: SOLAR, Society for Learning Analytics and Research, 2017.

[56] G. Siemens and R. S. J. d Baker, "Learning analytics and educational data mining: towards communication and collaboration," in *Proceedings of the 2nd international conference on learning analytics and knowledge*, 2012, pp. 252–254.

[57] C. Lang, L. P. Macfadyen, S. Slade, P. Prinsloo, and N. Sclater, "The complexities of developing a personal code of ethics for learning analytics practitioners implications for institutions and the field," in *LAK '18: Proceedings of the 8th International Conference on Learning Analytics and Knowledge*, 2018, pp. 436–440.

[58] D. Amo, R. Torres, X. Canaleta, J. Herrero-Martín, C. Rodríguez-Merino, and D. Fonseca, "Seven principles to foster privacy and security in educational tools: Local Educational Data Analytics," in *TEEM'20: Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality*, 2020, pp. 730-737.

[59] Boletín Oficial del Estado, "LOPDGDD BOE-A-2018-16673," *Boletín Oficial del Estado, núm. 294*, 2018. [Online]. Available: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. (accessed Sep. 6, 2019).

[60] EP and the CEU, "Regulation (EU) 2016/679 GDPR." Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. (accessed Jun. 27, 2019).

[61] A. Pedreño and L. Moreno, *Europa frente a EE.UU. y China. Prevenir el declive en la era de la inteligencia artificial*. Alicante, Spain: Amazon, 2020.

[62] J. P. Carlin and G. M. Graff, "Dawn of the code war: America's battle against Russia, China, and the rising global cyber threat." PublicAffairs. https://www.publicaffairsbooks.com/titles/john-p-carlin/dawn-of-the-code-war/9781541773813/. (accessed Sep. 16, 2020).

[63] A. M. Mcdonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, pp. 1–22, 2008.

[64] D. J. Solove, "The Myth of the Privacy Paradox," *SSRN Electronic Journal*, vol. 89, no. 1, pp. 1-51, 2020.

[65] P. Graßl, H. Schraffenberger, F. Z. Borgesius, and M. Buijzen, "Dark and bright patterns in cookie consent requests," *Journal of Digital Social Research*, vol. 3, no. 1, pp. 1-38, 2021.

[66] D. Machuletz and R. Böhme, "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR," *Proceedings on Privacy Enhancing Technologies*, no. 2, pp. 481–498, 2020.

[67] Stack Overflow, "Stack Overflow Developer Survey Results 2018." Developer Survey Results, 2018. https://insights.stackoverflow.com/survey/2018/. (accessed Jan. 1, 2019).

[68] Plicekers, "Plickers." Website of Plickers educational app. https://get.plickers.com/. (accessed Sep. 16, 2020).

[69] D. Amo, D. Fonseca, M. Alier, F. J. García-Peñalvo, M. J. Casañ, and M. Alsina, "Personal Data Broker: A Solution to Assure Data Privacy in EdTech," in *International Conference on Human-Computer Interaction*, Orlando, USA, 2019, pp. 3–14.

Daniel Amo

PhD in Education Sciences from the University of Salamanca (2020), with two master's degrees in education and educational technology, University Master's Degree in Teacher Training for Compulsory Secondary Education and Baccalaureate, Professional Training and Language Teaching (UNIR 2016) and University Master's Degree in Education and ICT, specialization in Research (UOC 2014). He currently focuses his professional career on University teaching in the Department of Computer Engineering at La Salle, Ramon Lull University, and Research in the established research group GRETEL (Group of REsearch in Technology Enhanced Learning) recognized by the Generalitat de Catalunya within the call 2017 SGR 934. Within GRETEL he coordinates the Educational Data Analytics research line with a special focus on the field of Learning, Feedback and Ethical Analytics. With his thesis dissertation "Privacy and identity management in learning analytics processes" he adds aspects related to Privacy, Identity, Confidentiality and Security of Personal Data, Data and Metadata in the educational context in his research career. Since 2014, it has published more than 30 scientific articles related to Education in areas such as Educational Analytics, Educational Technology, MOOCs, Educational Networks or Privacy and Ethics in Education. He actively participates in scientific congress committees (CISTI'21) and conferences to disseminate to society with knowledge resulting from his professional and personal research. He is the author of the books "Learning Analytics: the narrative of learning through data" (UOC OuterEdu), "Learning analytics: 30 experiences in the classroom with data", and of the Learning Analytics' divulgation blog eduliticas.com.

Paul Prinsloo

Paul Prinsloo is a Research Professor in Open and Distance Learning (ODL) in the College of Economic and Management Sciences, University of South Africa (Unisa). His academic background includes fields as diverse as theology, art history, business management, online learning, and religious studies. Paul is an established researcher and has published numerous articles in the fields of teaching and learning, student success in distance education contexts, learning analytics, and curriculum development. His current research focuses on the collection, analysis and use of student data in learning analytics, graduate supervision and digital identity. Paul was born curious and in trouble. Nothing has changed since then.

Marc Alier

Marc Alier (1971) received an engineering degree in computer science (1996) and a PhD in Sustainability (2009) in the Polytechnical University of Catalonia (UPC). He is an associate professor at UPC and deputy director at ICE http://www.ice.upc.edu. The last 25 years have worked in research and development related to the e-learning industry. Has participated in the development of several LMS, content authoring tools and interoperability standards. Since 2001, has taught software engineering, project management, information systems, and computing ethics at UPC's School of Informatics. Has been director of several master's programs. Has authored more than 120 papers in journals and conference proceedings. Since 2007 produces several podcasts about technology, science and its impact on society as a means of dissemination of his professional and personal research.

David Fonseca

Full Professor (2017) by La Salle Ramon Llull University, currently he is the coordinator of the Group of Research on Technology Enhanced Learning (GRETEL), a recognized research group of Generalitat de Catalunya (from 2014), and coordinator of the Graphic Representation Area in the Architecture Department of La Salle (where he is a teacher and academic tutor). Technical Engineer in Telecommunications (URL – 1998), Master in GIS (Universitat de Girona, 2003), Audiovisual Communication Degree (UOC, 2006), Master in Advanced Studies (URL-2007), Official Master in Information and Knowledge Society (UOC, 2008), PhD in Multimedia by URL (2011), also, he is Autodesk Approved and Certified Instructor from 1998. With extensive experience in project manager (from 2000 to act, he has coordinated more than 50 local, national, and international projects, both technological transfer and research funded projects), he has directed 7 PhD thesis and more than 10 other final degree and master projects. Currently he is serving as program or scientific committee in more than 15 indexed journals and conferences, as well as organizing workshops, special issues and invited sessions in different scientific forums.

Ricardo Torres Kompen

Lecturer, Coordinator of the Degree in International Computer Engineering. Researcher in the area of learning technologies and university professor since 1996. He is a chemical engineer (1991), a Master in Chemical Engineering (2000) and a PhD in Multimedia Engineering from the Polytechnic University of Catalonia–BarcelonaTech (2016). His research focuses on the personalization of learning through the use of multimedia and technology.

Xavier Canaleta

Dr. Xavi Canaleta has a degree in Computer Science from the Facultat d´Informàtica de Barcelona (Universitat Politècnica de Catalunya) and PhD from the Ramon Llull University. He has been developing academic functions in La Salle - Universitat Ramon Llull since 2001. He was Vicedean for Educational Innovation, Coordinator of the Degree in Computer Engineering, and the Master´s Degree in Teacher Training (Technology specialty). He is also professor of Operating Systems (Degree) and of Teaching Innovation and Educational Research (Master). In his academic trajectory he has been professor of different subjects of Engineering degrees (Advanced Operating Systems, Programming, and Introduction to Computers) and of masters (Technology in the Social Context and Practices in Educational Centers). Between 2003 and 2005 he was Coordinator of Computer Services at the Ramon Llull University. As far as research is concerned, he belongs to GRETEL (Group of Research in Technology Enhanced Learning) and has participated in various European projects and has written articles in national and international journals and conferences. His origins have a 14-year experience with teacher and coordinator in Secondary and High School.

Javier Herrero-Martín

PhD in Psychology. Vice Dean of Undergraduate Studies in Early Childhood Education and Primary Education at the La Salle Higher Center for University Studies (Autonomous University of Madrid). Professor at La Salle Campus Madrid, Faculty of Education and Education. Expert in cognitive and language psychology (Complutense University of Madrid). Director of the INAEX-La Salle research group. Member of the District Educational Innovation Team NCA-ARLEP (La Salle, Spain and Portugal).