Personal Data Broker: A Solution to Assure Data Privacy in EdTech

Daniel Amo[1](✉), David Fonseca[1], Marc Alier[2],
Francisco José García-Peñalvo[3], María José Casañ[2],
and María Alsina[1]

[1] La Salle, Universitat Ramón Llull, Barcelona, Spain
{daniel.amo,fonsi,maria.alsina}@salle.url.edu
[2] Universitat Politècnica de Catalunya, Barcelona, Spain
marc.alier@upc.edu, mjcasany@essi.upc.edu
[3] Universidad de Salamanca, Salamanca, Spain
fgarcia@usal.es

Abstract. Educational technologies (Edtech) collect private and personal data from students. This is a growing trend in both new and already available Edtech. There are different stakeholders in the analysis of the collected students' data. Teachers use educational analytics to enhance the learning environment, principals use academic analytics for decision making in the leadership of the educational institution and Edtech providers uses students' data interactions to improve their services and tools. There are some issues in this new context. Edtech have been feeding their analytical algorithms from student's data, both private and personal, even from minors. This draws a critical problem about data privacy fragility in Edtech. Moreover, this is a sensitive issue that generates fears and angst in the use of educational data analytics in Edtech, such as learning management systems (LMS). Current laws, regulations, policies, principles and good practices are not enough to prevent private data leakage, security breaches, misuses or trading. For instance, data privacy agreements in LMS are deterrent but not an ultimate solution due do not act in real time. There is a need for automated real-time law enforcement to avoid the fragility of data privacy. In this work, we take a step further in the automation of data privacy agreement in LMS. We expose which technology and architecture are suitable for data privacy agreement automation, a partial implementation of the design in Moodle and ongoing work.

Keywords: Smart contracts · Learning Analytics · Moodle · Data privacy · Digital identity · Blockchain · Educational data mining · Academic analytics

1 Introduction

In the last decades we have seen a fast-paced evolution in the way information technologies for education (Edtech) are used. This evolution goes from seeing the computer itself as the educational tool in – as first introduced by Seymour Papert in the late 1970's [1] - to software developed specifically with instructional purposes [2, 3], to the usage of computer and other technological devices as content delivery platforms, to

P. Zaphiris and A. Ioannou (Eds.): HCII 2019, LNCS 11590, pp. 3–14, 2019.
https://doi.org/10.1007/978-3-030-21814-0_1

blended and online learning applications like Virtual Learning Environments (VLE) and apps [4], and finally the usage of platforms not specifically designed for learning but providing powerful assets like video streaming, online maps, office tools, calendars, email or social networking. Each of these steps has not deprecated the previous one, but built upon it adding more layers of usefulness and complexity. During the last 15 years there has been a big push for interoperability between systems in education [5–9]. This is allowing for a transformation of the Edtech ecosystem from one based on products (the computer, the software, the content, the VLE …) to an ecosystem of services. These services can be self-provided by the institution, like the back-office management system (enrolment, syllabus and curriculum management, ed-ERP) and the VLE, and can also be services provided by vendors providing learning apps, contents and other services [10–12].

In the first stages of this evolution the learning device was a single computer, unconnected, using software locally executed to perform learning activities or access contents from a tape or disk. But in the early 2000's this shifted to continuous online experience where the device used by the student is just a means to connect to online webapps and content. The software that runs these services is running on servers elsewhere, either by the learning institution or vendors. And all interactions are tracked and logged, generating data, lots of data.

The availability of this data allows for the birth of Learning Analytics, that aims to track and better understand the behaviour of the students at a collective and individual level [13–17]. This knowledge can be given to teachers and instructors in the form of statistics, graphics, dashboards and even recommendations in written form automatically generated [18]. The information can also be given to managers and policy makers in order to make better informed decisions.

What could possibly go wrong? While is reasonable for the learning institution to gather and use data about the learning activities of its students, to a point. When the online learning services are provided by commercial vendors, and especially when minors are involved, there is a clear concern about what data is being gathered and for what purpose [19]. This concern is increased in the current situation where deep learning algorithms are being used to model and influence the behaviour and sentiments of people.

The control of privacy in education has become an important problem to solve in Edtech.

This paper is organized in four additional sections. Section 2 presents the context and the problem authors want to address. Section three explains the solution proposed. Section four describes the software that has been developed as well as the platform authors are using. Section five presents the conclusion of the work and presents future work.

2 The Problem: Data Privacy in EdTech

As we have introduced previously, today the use of Edtech implies that personal information about the students and about their activity is going to be gathered and moved around. This is going to happen in two ways:

1. **Internal data gathering:** The data and metadata about the student and her activity is kept within the servers managed by the learning institution. This information is kept unencrypted and can be accessed by most of the IT personnel with access to the databases and files in the servers. This personal information is highly vulnerable to hacking and lack of proper security. Sometimes a number of schools share an IT provider that hosts their VLE's on a server farm or cloud, and security audits show that in this situations the compromise of one install can spread to the rest of installations.
2. **External data gathering:** The students access a service provided by a vendor outside the learning institution. Sometimes the service is provided through an interoperable service integrated in the VLE – using IMS LTI or another standard [6] -, while there is no direct contract or agreement of terms of service between the student or his legal tutors, some personal information is transferred to the vendor in order to provide the service and the data about the student's interactions are gathered and kept outside the control of the institution, the students and their tutors. Even in the case that the identity of each student is hidden from the vendor, the IP address and cookies from tracking sites can allow the identification of the student via social network profiles and other means.

The students and their legal tutors are all the time agreeing to conditions- they most of the time don't understand the meaning and implications- that allow the collection, management and use – and even selling or sharing with other actors – their personal data and logs. The case of the inBloom schools is a clear example of bad practice with regards to data privacy by the providers of learning online services [20].

Several projects and regulations have been created to deal with data privacy and the current misuses or bad practices. GDPR, data privacy guides such as DELICATE or ethical principles have been created for this purpose [21, 22]. The importance of this issue has made possible the creation of data policies that uses Edtech in micro context (classrooms), medium context (institutions) and macro context (governments).

The formulation of laws, regulations, frameworks for service agreements and ethical codes is important and a step in the right direction to address the problem of data and metadata privacy in education. However, we need to have a technological solution to enforce the agreements and regulations. We need to integrate the privacy management in the very core of the design of our Edtech systems and interoperability standards.

In a previous paper the authors explored the possibility of using Blockchain technologies as a core technology to address this problem. Our findings reveal that most likely the Blockchain [23, 24] is not a good way to go. We also explored the main characteristics of a technological solution that can be introduced in the mix: a software component we have named provisionally Personal Data Broker PDB, outlined in the diagram in Fig. 1.

In the same paper we propose the use of Smart Contracts as technology that can be used to implement the proposed solution. We believe that this technology is a strong candidate to help automate privacy policies in a sound and secure way.

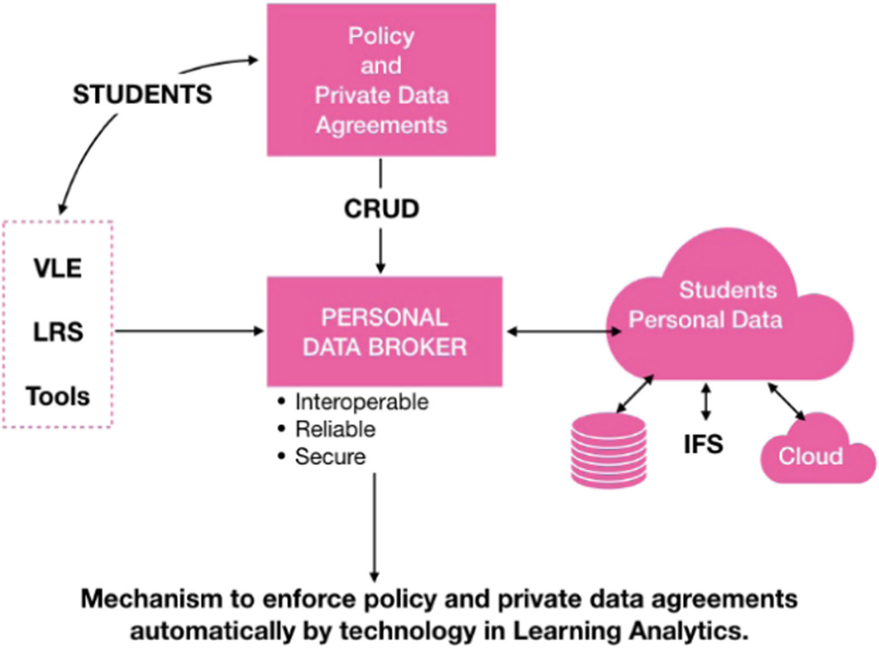
STUDENTS
Policy and Private Data Agreements
CRUD
VLE
LRS
Tools
PERSONAL DATA BROKER
• Interoperable
• Reliable
• Secure
Students Personal Data
IFS
Cloud
Mechanism to enforce policy and private data agreements automatically by technology in Learning Analytics.

Fig. 1. Personal data broker.

2.1 Research Question, Objectives and Scope

Our research question is: Is possible to implement a secure system that enforces privacy policies and agreements in real time in an Edtech environment?

For one part we are pretty sure that we could design from scratch a new VLE engine, and a family of apps and online services for education with privacy principles embedded in the core of its design. However, our aim is to propose a solution that could be implemented and used in production environments in a short span of time. This means that we have to contend with legacy systems. Fortunately, open source VLEs and interoperability standards can be tinkered with to find a solution and implement prototypes to test our ideas. Hence, our initial scope will be to propose a solution that works for an existing VLE.

Given the author's previous experience and background within the Moodle community we choose Moodle as the host system to implement the PDB.

The objectives we aim for are:

1. **Ensure privacy within the VLE.** The VLE stores personal information and information about the activity of the student in the platform. Our goal is to encrypt this information and make it accessible to software and users only on a need to know basis.
2. **Automate the enforcement of privacy agreements and regulations.** The privacy agreements, regulations and ethical codes of the learning institution need to be enforced by automation. In the same way Creative Commons created sets of legal

choices (licenses) that could be easily communicated to users without legal expertise and read by machines, we aim to define a set of patters of privacy agreements that we can implement with smart contracts within the VLE and its ecosystem of learning apps and services.

This is an ongoing research that has too great a scope to present in a single manuscript. So far we have only developed part of the first goal. The results are presented in the following sections. The development of the remaining part will be presented in future publications due to its greater complexity and extension. However, its approach is exposed and how different development possibilities will be addressed.

To complete the second goal we are conducting an analysis of the current laws and guidelines on data privacy. This will allow us to generate a questionnaire to conduct a series of interviews within the educational context. The results will be presented in future publications.

3 Development

In this section we present the technologies used in PDB as well as the VLE to develop it.

3.1 Smart Contracts

In order to execute policies and privacy agreements, in Edtech and in real time, digital automation technologies are needed. Smart Contracts are the most appropriate technology for this purpose, since their use does not break interoperability and security in the transfer of educational data.

The main goal of a Smart Contract is to automate the business rules between multiple entities, multiple subjects or subjects and entities. This technology is based on small programs whose activation depends on specific conditions.

It has been previously shown that using only laws and regulations is not a valid approach for technological environments. In technological environments, a technological solution is required. Szabo [19] stated in relation to the Smart Contracts: “Smart contracts […] provide us with new ways to formalize and secure digital relationships, which are much more functional than their paper-based inanimate ancestors.” Therefore, the Smart Contracts are useful to solve the problem of the control of the privacy of educational data.

The terms of use of Edtech tools and their data management can be found in the privacy contracts. These contracts are made between students and entities-educational institutions or providers. The Intelligent Contracts must execute the relevant actions declared in the agreements and conditions specified in the privacy contracts.

Intelligent Contracts can be used in VLEs to enforce regulations, laws, principles and good practices. This legal automatism can guarantee the privacy of student data. You can also make secure transfers between interoperable tools or even between independent tools. Therefore, the proposed solution incorporates Smart Contracts.

3.2 Selected VLE

To implement the PDB we are using Moodle. We have selected Moodle following a series of criteria from the research itself, from the knowledge and previous experience of the researchers and time and available resources. We summarize the criteria on which we based our decision as follows:

1. It must be open source.
2. It must be developed in a programming language knows by researchers.
3. It must be widely used by educational institutions.
4. It must have logs and a user table.

The previous criteria reduced the selection of the platform to Moodle and Sakai. After inspecting the source code of both, the architecture of their databases and the architecture of both VLEs, we verified that:

1. **Moodle has a serious problem of queries to the DB user table:** Most are scattered all over the code, visible and used at the discretion of the developers. This means that anyone who has access to the code can know and modify student data. On the other hand, since the queries are direct and built by the developers, serious security breaches can be generated.
2. **Sakai is less mature:** The development of this VLE is more recent. It is demonstrated with some comments inside the code. These comments confirms less maturity than Moodle. For instance "do we need these if we are all-webpack?", "Come up with a better solution for this." Or "these ones are questionable".
3. **Database security:** The Sakai database has an additional level of security because it anonymizes users with an intermediate table. The Moodle user table can be accessed with a direct query without anonymization or encryption.

Finally we decided to use Moodle for the following reasons:

1. It is open source.
2. There is a strong and consolidated community of developers and teachers.
3. It is the most used VLE in Spanish territory and in other countries compared to Sakai.
4. The research team is familiar with the code due to previous developments and direct relationships with the Moodle management team.
5. Moodle Headquarters is located in Barcelona, a city in which researchers develop their activity. This increases the chances of a meeting and faster progress.

We believe that it will be much easier to implement the proposal in Moodle. This will reduce the time, resources and development costs. The widespread use of Moodle will mean that the results of the research will have a greater impact on the educational community.

3.3 Development in Moodle

Our first goal is to ensure the security and privacy of student data in Moodle. After an exhaustive analysis we have detected two possible implementations that affect two different aspects: collection and storage. Our development in Moodle will have to ensure the security and privacy of student data in the data collection models as well as in the available stores.

In Moodle there are two tables related to the collection and storage of personal data of users. On the one hand we find the table where the interactions are stored (logs) and on the other the table where the users own data is stored, such as name or email. Our development focuses on securing these two tables.

Our second goal is the agreements between educational institutions and students. The development of this goal is currently underway. We expose at the end of this section how we are proceeding and what technologies we will use.

Logs

A log is a physical or virtual space where user interactions are stored with tools. The interaction of the students with the VLE generate logs with educational and personal data.

The VLE use a procedure called clickstream to capture the interactions of the students [2]. This procedure consists of saving all the clicks of the students in a table of the database (logs). These clicks are associated with additional information about the course and the student, such as date of interaction, access IP, course, activity, user id or any other related data.

The data collected in this log table allows educational analysts to perform analyzes, visualizations and extractions. With these reports you can act to improve both the learning of students and the environment. This is the foundation of Learning Analytics and the logs table is one of the first resources to analyze.

In Moodle, the logs are a table that is not encrypted. This means that the system administrator and even developers have access. In this table all the interactions of the users are saved. Therefore, anyone who has access to these data can alter, filter, trade with them and use them at their convenience.

Moodle configuration allows logs to be stored outside of your database. This opens up new opportunities for improvement in both the collection and storage of interactions.

Our purpose has been to develop a specific plugin to intervene each user interaction and save it in the Personal Data Broker, a plug-in for Moodle. A plugin is a development that is installed in the VLE and adds new features. The developed plugin captures any interaction by clickstream in Moodle, prevents it from being saved in Moodle's own log and sends it secure to the PDB. This procedure allows to:

1. Keep the data away from possible manipulations and leaks.
2. Secure the data with adequate encryption in the present and future.
3. Keep privacy and prevent unauthorized users from accessing data.

Figure 2 shows the data flow from the moment the user performs an interaction until it is securely and privately stored in the secured logs table of the PDB.

In a first stage we consider Blockchain as a possible solution to the problem. However, we detected a series of limitations that make it an unsafe and unstable candidate. Our new proposal in plugin format improves Blockchain's limitations in the security and privacy of educational data:

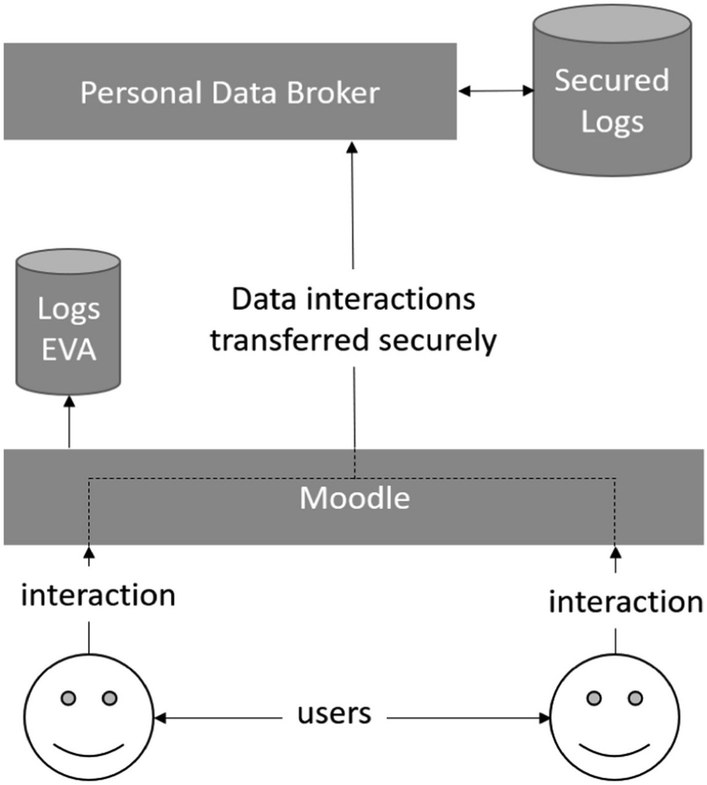

Fig. 2. Data flow PDB.

1. **The immutability of the data:** Blockchain does not allow new encryption algorithms to be applied. This is a danger when the computational capacity can break such algorithms with ease. The PDB plugin can re-encrypt data at your convenience.
2. **The privacy of the data:** in Blockchain all data is public. The users of the network have a copy of all the transactions. This foundation violates the principle of privacy of student data. The PDB plugin enables access to users who have appropriate permissions.
3. **Need for a database:** Blockchain is very bad database. It is very slow writing the blocks, there is no option to delete or modify data, and everyone has access to them. This means that instead of Blockchain we can use a relational database and all these problems are solved automatically. This is the reason why the PDB plugin uses a relational database.

User Table

The Moodle user table contains personal, configuration and relations between tables. In this way we find stored the Moodle user table the internal userId, the name and surnames, the address, an image and even data from social networks. Any access to these data, manipulation or filtering them is much more serious than doing it in the log table. The log table contains only some user data. The user table contains all the personal data of all users. In addition, the fact of having the social networks data of the each user allows may to extract a lot of intimate information. It is demonstrated that the data stored in the Moodle user table go beyond the academic life of the user.

From the Moodle user table comes out the user data that is displayed in Moodle. Any information, user profile visualization, grades chart, progress visualizations, interactions in a forum or delivery of tasks requires access to this table. Therefore, it is essential to secure and privatize access to the user table.

Despite the security limitations, the Moodle architecture manages to privatize the data through a hierarchy of permissions. A student cannot see students who are not from their course. In the same way, a teacher does not have access to the data of students who are not enrolled in their course. However, anyone can access information on the profiles of the visible users. If we jump at the administrator level, he has the ability to access all user information, without any restriction and without impeding the extraction of them outside of Moodle. Unfortunately, the data is not encrypted, a fact that shows a low security in the protection of personal user data.

The development related to the user table is not trivial. It requires much more advanced techniques that ensure a real security and privacy in accordance with the agreements established in the contracts and data policies. The fact that in the Moodle code there is a high dispersion of queries that Access the user table, makes the solution to be applied more complex. Our mission is not to solve this Moodle problem, but to provide a solution to the problem of data fragility.

In these moments we are developing different prototypes, testing and evaluating their efficiency and adequacy. In general terms, we are going to perform a hack in the Moodle architecture that allows us to add an additional layer of security to any query to the user table. The architecture we propose will be based on the following techniques:

1. **Triggers:** The databases work based on events. Each time one of these events happens, an action (trigger) is triggered. A set of code statements can be assigned to each action. From this point of view, any action of creation, reading, modification or elimination (CRUD) in the user table would be intercepted. Doing so would suppose a control of the security and privacy of the data subedited to the PDB, which would administer accesses and permissions.
2. **Outsourcing of the user table:** This measure is very drastic and consists in outsourcing the user table of the Moodle of the institution. This would require making a modification of the native Moodle code and changing the access system.
3. **Temporary tables:** Consists of creating temporary tables with extracts from the user table. In this way Moodle users would access the temporary table whose content would be the set of users to which they have access.
4. **Triggers and externalization of user data:** This measure is a hybrid between the use of events in the user table and the outsourcing of the same table. It consists in saving the data within the PDB and events would be responsible for retrieving that information that requires the user and also have access permissions.
5. **Triggers, outsourcing and temporary tables:** The complexity of the solution can lead us to implement different approaches at the same time. We are aware that there

is no single approach to solve the problem, since each one solves a specific casuistry. Therefore, we do not rule out using all the proposed approaches in the final solution.

The review of the possibilities denotes that the solution must be presented at the level of the database and specifically in the user table. We believe that modifying the native Moodle code is not the best option. In this sense, we focus our efforts on finding a solution less intrusive in code, but effective and that acts at the database level.

The complexity and supply of each of the possible solutions can even generate a publication. Therefore, the results of all the tests and final solution will be presented in future publications.

Law Automation

The above situations shows the limitations of laws to solve the detected problem. In addition, the laws are only effective considering a state of good faith on the part of all the actors. Therefore, the need to find a technological solution to the problem of fragility in data privacy is reaffirmed.

For the technological solution to be functional, all the agreements established in contracts and data policies must be applied automatically. In this way we reduce the possibilities of undue access to data and fraudulent uses.

These laws and agreements between students and educational institutions will be automated with the use of Smart Contracts. Before doing so, we must make sure of what must be automated. To achieve this, we will carry out a questionnaire that will allow us to interview different people in the educational field and in different roles. With the answers we can extract patterns to automate.

The questionnaire will be carried out based on the different regulations, frameworks, principles and good practices:

1. **Regulations:** LOPD (Spain) y GDPR (Europe)
2. **Policy frameworks:** DELICATE (LACE), LEA's Box (Europa), NUS, NTU, OU, CSU o Usyd (Australia)
3. **Ethical principles:** Como los expuestos por Abelardo Pardo y George Siemens
4. **Good practices and ethical codes:** SHEILA, ROMA, Jisc (UK)

This process is arduous and involves the participation of different educational agents and EdTech providers. These will be interviewed and their answers will be analyzed to extract automated conditions. These automations will be implemented in the Moodle code to be related to the PDB. The results will be presented in future publications.

4 Conclusions

Throughout the manuscript, we have exposed the biggest current problem in the use of Edtech and how to approach it technologically. The analytical capacity of the different Edtech tools highlights a large amount of educational data collected. These data, including from minors, are vulnerable in terms of their transfer, storage, and use. Consequently, we detected a serious problem of privacy control in education and in the use of Edtech.

Exposure to data can happen in internal and external environments of the educational institutions. The data transfer to Edtech providers increases the risk of misuse and disables the management and control of data by educational institutions.

The laws that regulate the collection and use of data are not enough to avoid leaks, exposures, and misuses. Students and teachers are constantly accepting terms of use and privacy agreements with Edtech tools providers. The content of such contracts is not understood at all or educational roles are not able to glimpse potential risks in some of the contractual conditions.

In the provider's context, there is evidence of entities that ignore the laws. This fact provokes undesirable situations of leaks and marketing of educational data. Therefore, there is a need to apply an automatic regulation system to solve the problem of privacy control.

In a virtual learning environment, there are different places where educational data is stored. We mainly find the logs and the user table. The interactions of the students are stored in the logs. The personal data of the students is stored in the user table. Securing and privatizing these two warehouses is key to avoid the problem detected.

We believe that Smart Contracts are the most appropriate technology to automatically assure the security and privacy of the data stored in the logs and user tables, of any EVA. We succeeded in developing a secure and private logs storage plugin for Moodle. Hence, a technological solution is a manner to solve the problem.

Part of the research is considered a work in process. We are designing the architecture and collecting the necessary information to carry out the following developments. However, throughout the manuscript, we have shown how it is possible to privatize the Moodle logs, from the conception of the architecture to its final functional development.

Acknowledgment. To the support of the Secretaria d'Universitats i Recerca of the Department of Business and Knowledge of the Generalitat de Catalunya for the help regarding 2017 SGR 934.

References

1. Papert, S.A.: Mindstorms: Children, Computers, and Powerful Ideas. Basic Books, New York (1980)
2. Filvà, D.A., Forment, M.A., García-Peñalvo, F.J., Escudero, D.F., Casañ, M.J.: Clickstream for learning analytics to assess students' behavior with Scratch. Futur. Gener. Comput. Syst. **93**, 673–686 (2019)
3. Busquets, F.: Clic: un proyecto cooperativo de producción e intercambio de software educativo. Prim. Not. Comun. y Pedagog. **20**, 40–41 (2000)
4. Calvo, X., Fonseca, D., Sánchez-Sepúlveda, M., Amo, D., Llorca, J., Redondo, E.: Programming virtual interactions for gamified educational proposes of urban spaces. In: Zaphiris, P., Ioannou, A. (eds.) LCT 2018. LNCS, vol. 10925, pp. 128–140. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-91152-6_10
5. Conde, M.Á., García-Peñalvo, F.J., Rodríguez-Conde, M.J., Alier, M., Casany, M.J., Piguillem, J.: An evolving learning management system for new educational environments using 2.0 tools. Interact. Learn. Environ. **22**, 188–204 (2014)

6. Alier, M.F., Guerrero, M.J.C., Gonzalez, M.A.C., Penalvo, F.J.G., Severance, C.: Interoperability for LMS: the missing piece to become the common place for e-learning innovation. Int. J. Knowl. Learn. **6**, 130 (2010)
7. García-Peñalvo, F.J., Conde, M.Á., Alier, M., Casany, M.J.: Opening learning management systems to personal learning environments
8. Casany, M.J., et al.: Moodbile: a framework to integrate m-Learning applications with the LMS (2012)
9. Alier, M., Casañ, M.J., Piguillem, J.: Moodle 2.0: shifting from a learning toolkit to a open learning platform. In: Lytras, Miltiadis D., et al. (eds.) TECH-EDUCATION 2010. CCIS, vol. 73, pp. 1–10. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13166-0_1
10. Williamson, B.: Decoding ClassDojo: psycho-policy, social-emotional learning, and persuasive educational technologies
11. Hirsh-Pasek, K., Zosh, J.M., Michnick, R., Gray, J.H., Robb, M.B., Kaufman, J.: Putting education in "educational" apps: lessons from the science of learning
12. Merriman, J., Santanach, F.: Next generation learning architecture
13. Amo, D., et al.: Using web analytics tools to improve the quality of educational resources and the learning process of students in a gamified situation. In: Proceedings of 12th Annual International Technology, Education and Development Conference, p. 5 (2018)
14. Peña, E., Fonseca, D., Marti, N., Ferrándiz, J.: Relationship between specific professional competences and learning activities of the building and construction engineering degree final project. Int. J. Eng. Educ. **34**, 924–939 (2018)
15. Campanyà, C., Fonseca, D., Martí, N., Peña, E., Ferrer, A., Llorca, J.: Identification of significant variables for the parameterization of structures learning in architecture students. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S. (eds.) WorldCIST'18 2018. AISC, vol. 747, pp. 298–306. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-77700-9_30
16. Peña, E., Fonseca, D., Martí, N.: Relationship between learning indicators in the development and result of the building engineering degree final project. In: ACM International Conference Proceeding Series (2016)
17. Chatti, M., Dyckhoff, A., Schroeder, U.: A reference model for learning analytics. Int. J. Technol. Enhanc. Learn. **4**, 318–331 (2013)
18. Amo, D., Alier, M., Casañ, M.J.: The student's progress snapshot a hybrid text and visual learning analytics dashboard. Int. J. Eng. Educ. **34–3**, 990–1000 (2018)
19. Lupton, D., Williamson, B.: The datafied child: the dataveillance of children and implications for their rights
20. Singer, N.: InBloom student data repository to close. New York Times **21** (2014)
21. Drachsler, H., Greller, W.: 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, pp. 89–98 (2016)
22. Hoel, T., Chen, W.: Implications of the European data protection regulations for learning analytics design (2016)
23. Forment, M.A., Filvà, D.A., García-Peñalvo, F.J., Escudero, D.F., Casañ, M.J.: Learning analytics' privacy on the blockchain. In: Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality – TEEM 2018, pp. 294–298. ACM Press, New York (2018)
24. Filvà, D.A., García-Peñalvo, F.J., Forment, M.A., Escudero, D.F., Casañ, M.J.: Privacy and identity management in learning analytics processes with blockchain. In: Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality – TEEM 2018, pp. 997–1003. ACM Press, New York (2018)