sustainability

MDPI

Article

Protected Users: A Moodle Plugin To Improve Confidentiality and Privacy Support through User Aliases

Daniel Amo [1,*], Marc Alier [2], Francisco José García-Peñalvo [3], David Fonseca [4] and María José Casañ [2]

1 Departament d'Informàtica, Universitat Ramón Llull, La Salle, 08022 Barcelona, Spain
2 Departament d'Enginyeria de Serveis i Sistemes d'Informació, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain; marc.alier@upc.edu (M.A.); mjcasany@essi.upc.edu (M.J.C.)
3 Departamento de Informática y Automática, Instituto Universitario de Ciencias de la Educación, Grupo GRIAL, Universidad de Salamanca, 37008 Salamanca, Spain; fgarcia@usal.es
4 Departament d'Arquitectura, Universitat Ramón Llull, La Salle, 08022 Barcelona, Spain; david.fonseca@salle.url.edu
* Correspondence: daniel.amo@salle.url.edu or daniel.amo@salle.url.com; Tel.: +34-932-902-400

Received: 21 February 2020; Accepted: 20 March 2020; Published: 24 March 2020

Abstract: The privacy policies, terms, and conditions of use in any Learning Management System (LMS) are one-way contracts. The institution imposes clauses that the student can accept or decline. Students, once they accept conditions, should be able to exercise the rights granted by the General Data Protection Regulation (GDPR). However, students cannot object to data processing and public profiling because it would be conceived as an impediment to teachers to execute their work with normality. Nonetheless, regarding GDPR and consulted legal advisors, a student could claim identity anonymization in the LMS, if adequate personal justifications are provided. Per contra, the current LMSs do not have any functionality that enables identity anonymization. This is a big problem that generates undesired situations which urgently requires a definitive solution. In this work, we surveyed students and teachers to validate the feasibility and acceptance of using aliases to anonymize their identity in LMSs as a sustainable solution to the problem. Considering the positive results, we developed a user-friendly plugin for Moodle that enables students' identity anonymization by the use of aliases. This plugin, presented in this work and named Protected users, is publicly available online at GitHub and published under GNU General Public License.

Keywords: LMS; Moodle; GDPR; plugin; data privacy; confidentiality; alias; digital identity; sustainability

1. Introduction

Every Learning Management System or Virtual Learning Environment (VLE) (that in this work we will use as synonyms) [1,2] uses and manages personal information about every student. This encompasses data such as their name, surname, email address and other personal details like a profile image. The LMS also stores personal and sensitive information, such as the grades of the student for every course and online activity, plus the feedback from the teacher. Last, but not least, the LMS logs every interaction of the student with the LMS: every time s/he logs in, every click, every document read, for how much time, every word written, every chat. All data and metadata are recorded.

Not only do these systems allow a teacher to see personal information about students, but they also enable students to see the information of other students enrolled in their course. This double role feature is pervasive in all the interface: list of participants, forums, chats, history of edits in wiki pages,

group activities, etc. The information shown can include the name, picture, email address, links to social media profiles, when the user last logged in, activity in the course (entries in the forums, etc.), list of courses where the user is enrolled, full student profile, etc. To point out a specific LMS, this data openness is part of the very design of Moodle inspired by the principles of social constructionism [3]. Social constructivism per se is not a problem. Our claim is that the use of social constructivism in online learning without enabled data privacy protection measures could lead to undesired situations for students. Hence, this problem, which is built into the very design of the LMS in terms of data privacy protection, may result in cyber stalking and cyber-bullying, among other inappropriate behaviors [4–8].

Every information system that manages personal information in the European Union (EU) is affected by the General Data Privacy Regulation (GDPR). This includes LMSs and online educational applications.

The GDPR [9] is a regulation in EU law on data protection and privacy for all individual citizens of the EU and European Economic Area (EEA) adopted in April 2016 and applicable since May 2018. It aims primarily to give individuals control over their data, simplifying and unifying the regulation within the EEA. The GDPR also addresses the transfer of personal data outside the EEA. The regulation contains provisions and requirements related to the processing of personal data of individuals inside the EEA (called "data subjects" in the text of GDPR) and applies to any enterprise established that is processing the personal information of data subjects inside the EEA.

In the sector of education, the "data subjects" are the students (and also the teachers and support staff) who are in many cases minors. LMSs have to comply with the GDPR and provide options and functionalities to let students execute their data protection rights.

Every student has a fundamental right to the protection of her or his personal information. This right is manifested explicitly in points 1, 2 and 28 of GDPR [9], as well as in the section on the right to objection in article 21. Article 25 of the GDPR states that the protection of data by default is mandatory. All the GDPR rights should be assured in the LMSs using modifications on core codebase or by plugins [10].

Most LMS installations are not handling the digital identity and confidentiality of the students properly [11]. Such is the case of Moodle, which provides limited support for the GDPR [12]. In 2018, the 3.4 release of Moodle included support for compliance with the GDPR. This support allows the terms of service about data confidentiality and privacy for the Moodle installation to be configured. Moodle will ask the students to accept the privacy settings and will keep track of their choice. Those who do not accept the terms will not be able to use the service.

This all or nothing approach is not taking into consideration the full extension of the right to object to certain kinds of treatment of personal information. A student can object to sharing her or his information with peer students for several valid reasons (for example victims of (cyber)bullying or gender violence, or for whatever reason need to remain anonymous). Two of the interviewed lawyer profiles say that these gender violence cases are exceptions; even anonymity is needed due to work reasons. To give a solution to these undesired and exceptional situations, we should re-design our virtual campuses and services around these exceptions. Keep the following considerations in mind:

- For the last 40 years, we have been redesigning our brick and mortar campuses and schools to make them accessible for persons with disabilities.
- We are making the students (unintentional) custodians of the personal information of their peers and enabling them to be digital surveillance agents. In cyber-bullying or gender violence scenarios, this is scary.

Moodle offers two plugins to address GDPR compliance: Policies [13] and Data Privacy [14]. The Policies' plugin provides:

- A new user login process.
- Multiple policies definition (site, privacy, third parties, etc.).
- User consent tracking.

- Policy updates and version management.

The Data Privacy's plugin provides:

- The workflow for users to submit requests for data access and deletion.
- To Moodle administrators and data protection delegates, options for processing user requests.
- Options to configure retention period for data stored on a Moodle site.

Both plugins resolve some aspects pointed out by the GDPR, however, and as noted, do not allow a user to be anonymous. Moreover, they offer an all-or-nothing approach, where students only have the option of accepting all the conditions if they want to enter the learning platform. Exceptions in Moodle cannot be solved as there is no functionality to do so.

Based on our methodology, we implemented a plugin that pseudonymizes students' data. The pseudonymization consists of assigning an alias to a student such as a double or multiple identities associated with a specific course. This approximation allows students to remain anonymous in any single course, feel comfortable with the solution, act freely with no pressure in bullying or gender violence situations, and log in easily with their aliases.

In summary, our key contributions are as follows:

- We provide a Moodle opensource implementation in Moodle, named Protected users, that solves the presented problem for undesired situations in online education such as cyber-bullying, which also complies with the GDPR.
- We want the solution to be installed and uninstalled at the convenience of the Moodle administrator.
- We develop a working prototype based on Moodle's two privacy plugins (Policies and Data Privacy). Building on already tested features is faster than developing without reference.
- We avoid modifying the Moodle source code or delivering an update patch.
- We choose to develop a plugin that is operable for this format as opposed to others, to solve the problem easily, for both Moodle managers and students with a low technical profile.

2. Materials and Methods

Our aim is to design and implement a solution based on a student's data pseudonymization through aliases to enable adequate levels in confidentiality issues imposed by the GDPR in regard to students' personal data during the use of Learning Analytics in Virtual Learning Environments.

We divided the process into two phases:

- The first phase has a qualitative epistemology focus, where a series of interviews are carried out with actors from the educational context, and legal to collect perceptions about our second identity in VLEs.
- The second phase is framed in an iterative and incremental methodological proposal to develop an evolutionary prototype of a software solution. In this second phase, we developed a prototype that allows us to exercise specific legal rights not currently available in a virtual learning environment such as Moodle and detected in the first phase.

We chose to work with Moodle as the VLE platform to create the prototypes of the detected problems because it is the most used platform in Spain. According to Hill [15], more than 65% of VLE installations in Europe are Moodle.

2.1. First Phase

In order to collect perceptions of the use of aliases to protect the anonymity of users in online learning processes, we chose a qualitative approach through the design and execution of a series of structured interviews.

This process is framed within the possibilities and area of influence of the field known as User Experience [16,17]. Contributions are collected from different user perspectives to make a

development decision based on the results. Consequently, different interviews are conducted with different profiles to ensure a result that is consistent with the observations and perceptions of users in VLEs. This process consists of direct questioning interviews, online questionnaires and finally, Bipolar Laddering (BLA) [18], a mixed combination that has previously demonstrated its scientific validity in the evaluation of all types of methodology and systems applied to education without the need of a large sample of participants [19–22]. This first approach will serve to analyze the validity of the use of aliases in relation to the GDPR.

2.1.1. Interviews with A Legal Profile

Below is the script of the interview conducted with experts from the legal field related to personal data protection laws. Table 1 shows the structure of the interview, and Table 2 shows the questions of the interview with the experts on legality in data protection matters. The answers (n = 3) can be found in the Supplementary Material section and are analyzed in the Results section.

Table 1. Structure of the interview with lawyer profiles.

Interview Criteria	Description
Expert user profile	Legal expert
The objective of the interview	To know the viability of the use of aliases to ensure the anonymity of the students who use the VLE
Approximate time	15–20 minutes

Table 2. Lawyer profile interview questions.

Question	Response Type
PA1. Do you think that the use of aliases in a virtual learning environment ensures an adequate level of anonymity?	Open
PA2. Do you think that there is a more convenient solution?	Open
PA3. Do you consider that the task of managing the creation and assignment of aliases at the express request of the user should be assigned to the Data Protection Officer?	Open
PA4. Do you consider that the use of algorithms such as Deep Fake to generate the pseudonymized information of the aliases is a valid method?	Open

2.1.2. The Results of the Survey Conducted on Students

Below is the script of the survey conducted to students. Table 3 shows the structure of the survey, Table 4 shows the questions of the survey. The answers (n = 110) are analyzed in the Results section.

Table 3. Structure of the survey conducted with students.

Interview Criteria	Description
Expert user profile	Student
The objective of the interview	Assess students' opinions on using aliases in purely online and virtual learning environments to ensure their anonymity
Justification	Assess the student's perception
Method	Online form survey
Approximate time	15–20 minutes

Table 4. Student profile survey questions.

Question	Response Type
PA1. Would you mind introducing yourself to other students in an online course under an alias?	Yes/No
PA2. Have you ever used an alias to maintain anonymity?	Yes/No
PA3. What about using an alias to safeguard your anonymity in virtual learning environments?	Likert 5 points

2.1.3. Interviews with Moodle Technical Administrators

Below is the script of the interview conducted with Moodle technical administrators. Table 5 shows the structure of the interview, and Table 6 shows the questions of the interview. The answers (n = 5) can be found in the Supplementary Material section and are analyzed in the Results section.

Table 5. Structure of the interview with Moodle technical administrators.

Interview Criteria	Description
Expert user profile	Moodle technical administrator
The objective of the interview	To assess the technical concerns regarding the use of aliases and their possible application as a plugin in managed virtual learning environments
Justification	Assess the perception of the Moodle technical administrator
Method	BLA method
Approximate time	15–20 minutes

Table 6. Moodle technical administrator profile interview questions.

Question	Response Type
PAT1. Do you think that a plugin is a technical solution compatible with your virtual learning environment?	Open
PAT2. Do you think that a plugin of this kind is the most suitable solution?	Open
PAT3. What other complimentary solutions do you think could be developed?	Open
PAT4. Have you ever used an alias to keep your anonymity?	Open

2.1.4. Interviews with Data Privacy Officers

Below is the script of the interview conducted with Data Privacy Officers (DPO). Table 7 shows the structure of the interview, and Table 8 shows the questions of the interview. The answers (n = 4) can be found in the Supplementary Material section and are analyzed in the Results section.

Table 7. Structure of the interview with Data Privacy Officer.

Interview Criteria	Description
Expert user profile	Data Privacy Officer
The objective of the interview	To assess the comfort with the process of generating and assigning aliases to students in virtual learning environments that are expressly requested, taking into account that the communication with the user follows standard channels already established
Justification	Assess the perception of the Data Privacy Officer
Method	BLA method
Approximate time	15–20 minutes

Table 8. Data Privacy Officer profile interview questions.

Question	Response Type
PD1. Do you think that your profile is adequately configured to handle anonymity requests?	Open
PD2. Do you think that your profile is the right one to manage user aliases?	Open
PD3. What other solution do you think could be applied to solve the anonymity problem?	Open
PD4. Have you ever used an alias to maintain anonymity?	Open

2.1.5. Interviews with Teachers

Below is the script of the interview conducted with teachers. Table 9 shows the structure of the interview, and Table 10 shows the questions of the interview. The answers (n = 13) can be found in the Supplementary Material section and are analyzed in the Results section.

Table 9. Structure of the interview with teachers.

Interview Criteria	Description
Expert user profile	Teacher
The objective of the interview	To assess the perception from the perspective of teachers of using aliases in online and virtual learning environments to ensure their anonymity
Justification	Assess the perception of the teachers
Method	BLA method
Approximate time	15–20 minutes

Table 10. Teacher profile interview questions.

Question	Response Type
PP1. Would the use of aliases complicate classroom management?	Open
PP2. What do you think the use of aliases as a measure of anonymity brings?	Open
PP3. What other solution do you think could be applied to solve the problem of anonymity?	Open
PP4. Have you ever used an alias to maintain anonymity?	Open

2.2. Second Phase

Moodle offers the plugins Policies and Data Privacy to help Moodle installations comply with the GDPR. The applied methodology builds on these publicly available plugins. Hence, both architecture's plugins are used to develop our solution. The plugin Policies is used to set the access point of our plugin in the administration console of the DPO. The Data Privacy plugin is used to set roles and permission needed to use the plugin, so our plugin uses the same checking process. In every and each script of our plugin that needs to assure that the DPO is authorized to perform the action, a check is performed through the use of the already installed Data Privacy plugin using the following piece of code:

```
if (!\tool_dataprivacy\api::is_site_dpo($USER->id)) {
    $message = get_string('privacyofficeronly', 'tool_dataprivacy', $dponamestring);
    echo $OUTPUT->notification($message, 'error');
}
```

We envision DPOs to use in our work and help students avoid situations of harassment and cyber-bullying. A student needs to make an explicit request of anonymity to the DPO (or designed responsible) to enable an alias user. The alias user is associated with a course or multiple courses so students can be anonymous in each of them. To do so, we consider a tree architecture to enforce anonymity by request. Figure 1 shows the tree architecture that the plugin implements to allow the DPO the approval or denial of students' anonymity requests.

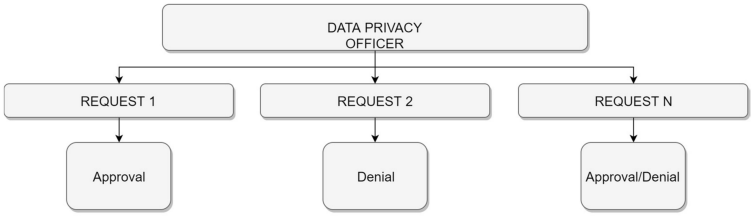

Figure 1. Decisional tree architecture of the new plugin.

Figure 2 shows the tree architecture that the plugin implements to allow the DPO the creation of aliases and course assigning.

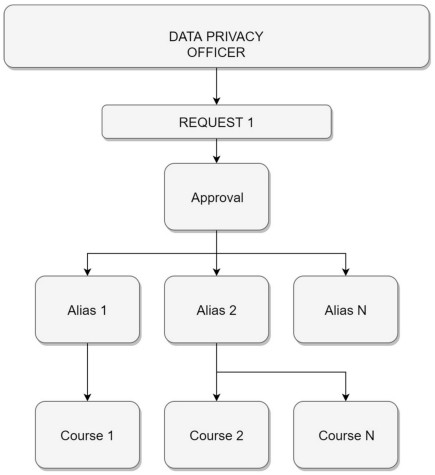

Figure 2. Full decisional tree architecture of the Protected Users plugin by request.

The table relationship design shown in Figure 3 shows some of the tables created during the installation of the Moodle's Policies and Data Privacy plugins, and the only table created by our Protected Users plugin.

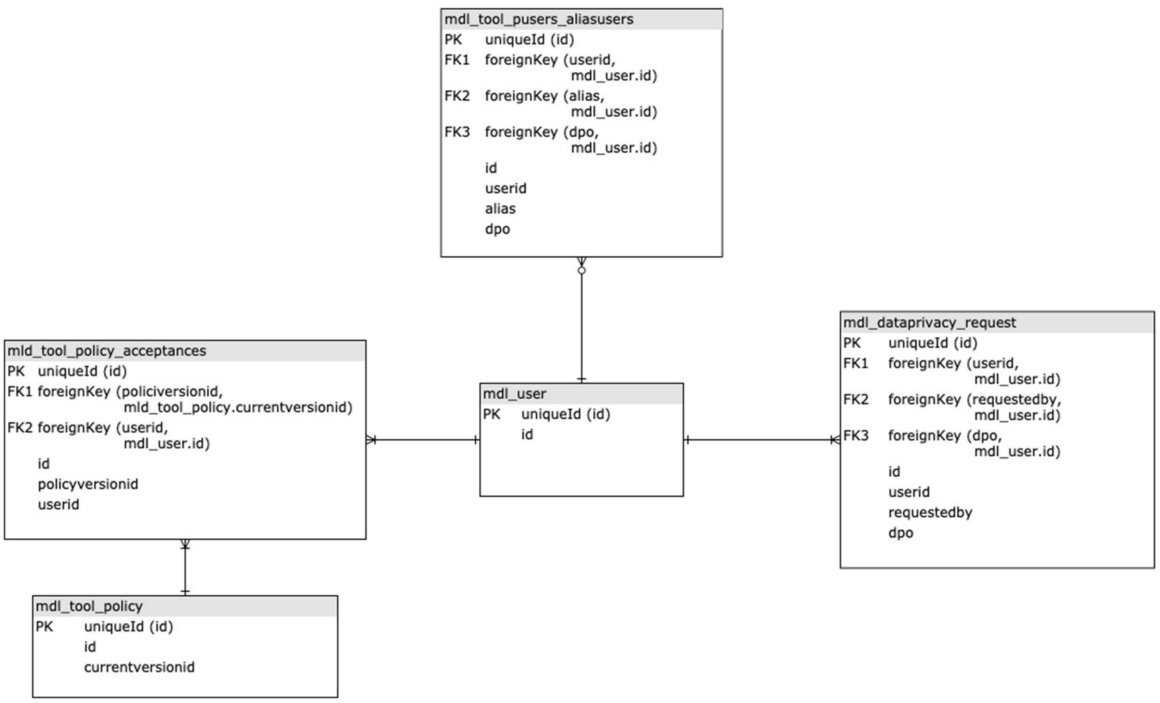

Figure 3. Full decisional tree architecture of the new plugin by request.

The design demonstrates how the three plugins depend on the user table *mdl_user*. The DPO manages:

- The students' acceptance of privacy policies and legal notices through the Policies plugin, which uses the tables *mdl_tool_policy* and *mdl_tool_policy_acceptances*.
- The student's data requests through the Data Privacy plugin, which uses the table *mdl_dataprivacy_request*.
- The student's alias and course assignations through our Protected Users plugin, which uses the table *mdl_tool_pusers_aliasusers*.

The *mdl_tool_pusers_aliasusers* table stores data for each alias assigned to a student. In this table, there are stored an identifier for:

- The student's user who made the request.
- The alias' user to log in anonymously.
- The DPO's user who performed the assignment.

All the prior specifications are integrated into the implementation shown in the Results section.

3. Results

It is considered that every user of a VLE can have the opportunity to anonymize her or his identity in accordance with the data protection rights of natural persons and pseudonymization set out in points of the regulation 1, 6 and 28 of the GDPR. Therefore, the use of aliases to protect the anonymity of a user in a virtual learning environment is a correct approach to ensure an adequate degree of anonymity for VLE users. This is because pseudonymized data continues to be personal data that identifies a person, and its use is correct within the current legislation to ensure an appropriate level of confidentiality of the personal data of those affected.

Answers from legal experts denote a positive use of user aliases as an anonymity assurance for a user in a VLE. Consequently, the solution to aliases makes complete sense in online learning. However, we need to define the perception of trust that this approach generates in the different roles of users of a VLE. Otherwise, our solution could be mistrusted. Hence, we interviewed and surveyed different VLE user roles.

The results of the students' survey, shown at Figure 4, Figure 5, and Figure 6, highlight that a large percentage of students feel comfortable using an alias (84%), and indeed many have already used it (76%), and a high percentage of students would use it on an online course (69%).

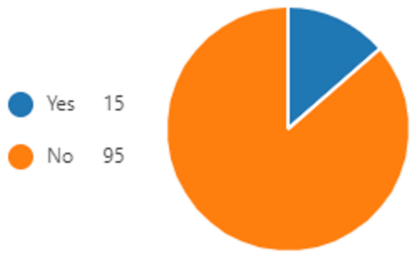

Figure 4. Answers to question PA1 of the student survey.

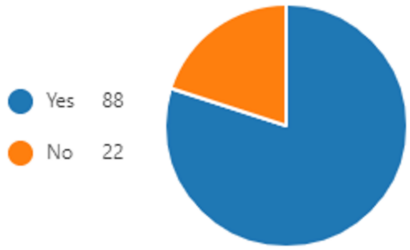

Figure 5. Answers to question PA2 of the student survey.

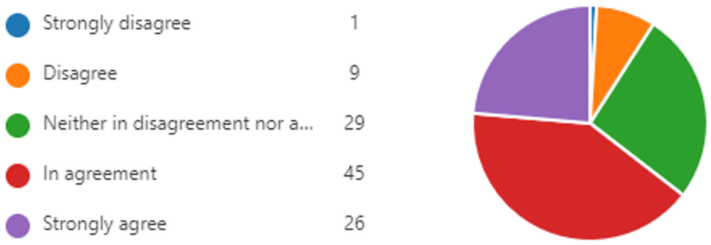

Figure 6. Answers to question PA3 of the student survey.

The results of interviews with teachers manifest a positive perception about the use of user aliases. Furthermore, the use of aliases by students generates confidence in solving in-classroom social problems. In general, teachers consider the use of aliases as a valid and very simple solution. Some teachers' perceptions indicate that aliases can prove difficult or limit some kind of classroom activities if they ignore the students with aliases.

The results of the interviews with Moodle technical administrators highlight that the use of aliases is perceived as positive in those environments that require student participation and interaction. Some answers are against the default use of aliases. However, the use of aliases depending on the environment and/or circumstances is perceived as convenient. The format of the solution is debatable, whether it is distributable as a plugin or as product functionality, although there is a tendency towards the latter. This position is based on the logical fact that functionality integrated into the product is preferable since it has direct support from the supplier and will evolve in line with product updates. Despite this trend, the use of the solution as a plugin is considered positive due to its simplicity of installation and uninstallation.

The DPO profiles consider the use of aliases as positive in determined cases such as when seeking to avoid spam. However, there is uncertainty about being able to handle a large volume of requests and technical support is proposed as a possible assistant. It is inferred that it is acceptable for the Data Privacy Officer, or members of her or his department, to manage the requests and assignation of aliases, but not the creation of user aliases.

After the analysis of the interviews conducted on different types of VLE user profiles, we can conclude that assigning an alias to a user of a VLE generates enough confidence to foster the development of a plugin as a potential solution to VLE students' anonymity requests. The results of the analysis are used to develop the solution where:

- The DPO (or another person of their team as stated in the answers) is the only one who has the permission to access data requests and assign aliases.
- Technical administrators are the only ones who can create aliases (as the DPO stated in the answers).
- The students have access to an alias in an easy manner.

3.1. Implementation

In a Moodle environment, all students registered on a determined course can see who is enrolled. Moreover, students also see the coursemates' public profile which usually contains personal data. We aim to provide students with digital mechanisms to execute their right of anonymity in any course. Accordingly, we have developed a plugin to help the DPO to manage aliases and to allow students to log in with those aliases.

In this work, we present an open source plugin implementation of our solution named Protected users [23]. Moodle administrators can install the plugin Protected users under their supervision and criteria.

We developed the plugin to assure the anonymity of students while complying with the GDPR. For this reason, we named the plugin as Protected users, to imply that there is the need to protect students in Moodle that require special attention.

The final development consisted of a total of 35 files with a total of 2778 lines of code. The technologies used have been heterogeneous, some of them enforced by the LMS environment in which the plugin runs, both frontend and backend, and compatibility requirements when building on top of the Policies and Data Privacy plugins. Table 11 shows the summary of programming languages, affected files, and lines of code written.

Table 11. Summary of programming languages, affected files, and lines of code written.

Language	Files Affected	Code Lines	Comments Lines	Blank Lines	Total Lines
PHP	30	1022	1031	367	2420
JavaScript	1	175	64	33	272
XML	2	41	0	1	42
CSS	1	26	3	6	35
Markdown	1	6	0	3	9

The plugin developed is functionality. However, considering possible design issues, we have taken the "cognitive path" approach [24]. In this way, the original design of the screens is carried out before moving on to a usability validation phase. The validation of usability is a long process that is transferred to future works. The plugin design undergoes two evolutions before being functional and ready for a first release. We proceed to expose its evolution and final state.

3.1.1. First Design

In the first stage, we propose the creation of a new special role that allows students to configure what they want to be shown publicly in their profile. This proposal requires a modification in the source code of Moodle in order to be fully functional. Therefore, we discarded the development of this stage as we consider it a contradiction to our aim. Nevertheless, we show the designs of the different screens to foster Moodle to integrate this proposal in future updates. Figure 7 shows the flow diagram of the plugin in its first design.

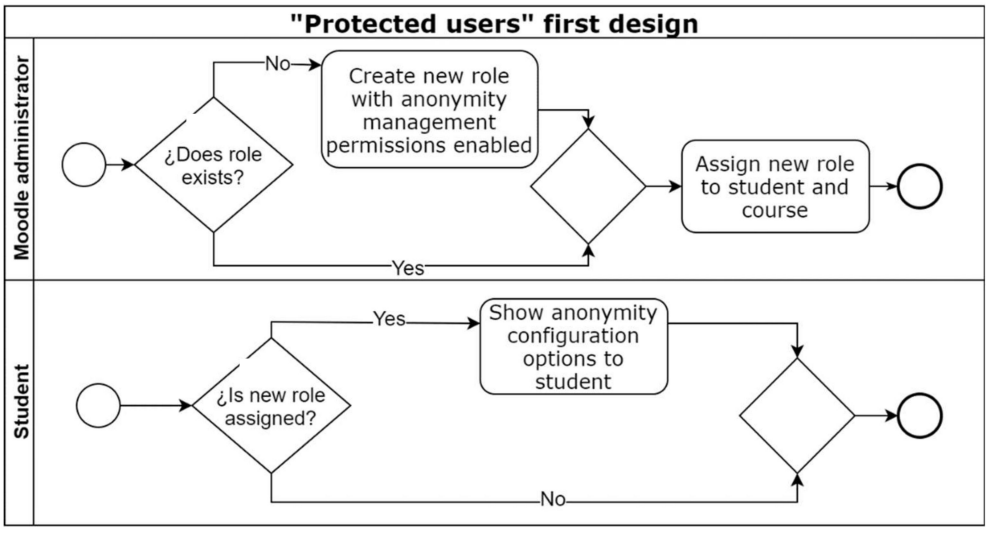

Figure 7. Flow diagram of the plugin in its first design.

- The Moodle administrator can create a student role with the new profile management permissions.
- The Moodle administrator assigns the role to the student and the course. Then the student can hide or show personal data at their own convenience.
- The student manages the options of the anonymity of his data from the header of the course.

3.1.2. First Evolution

In the second stage, we eliminate the excessive granularity in the anonymity configuration for the student profile. We focus on assigning an alias to a student to connect to any course anonymously. We make a series of decisions consisting of:

- Eliminating special permissions and roles assignable to students.
- Assigning a user alias for any students who need anonymization.
- Transferring alias management responsibility to the DPO.
- Allowing a student to log in with her aliases from the main page of the platform.

The above decisions allow the student, considered a protected user, to voluntarily communicate the requirement of anonymity in the course s/he wishes to the DPO. It is the DPO who creates an alias and assigns it to the protected user. The protected user can then automatically configure the aliases from her or his Moodle student profile. Figure 8 shows the flow diagram in this first evolution of our plugin.

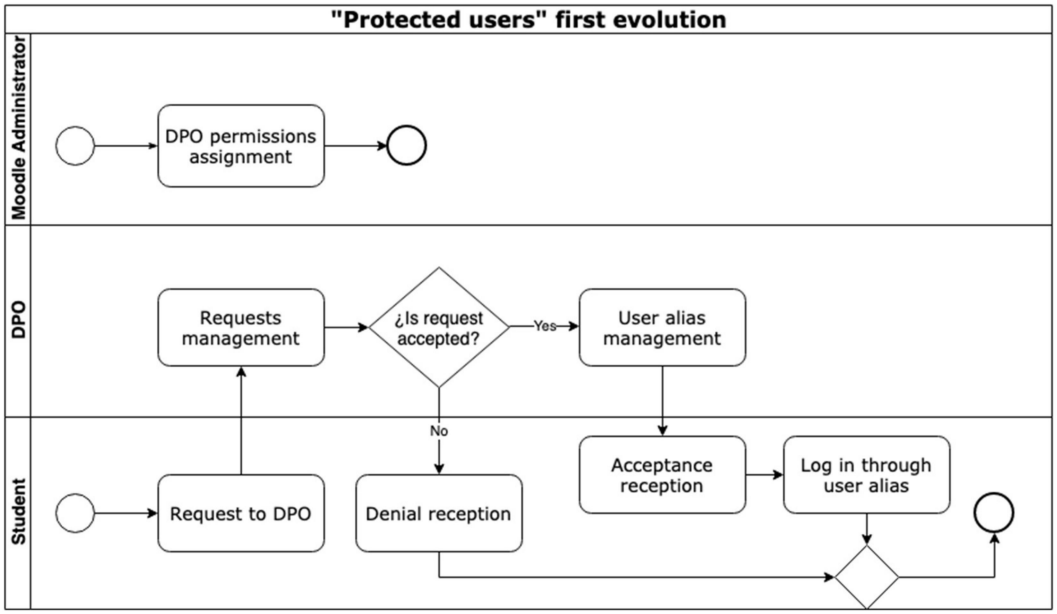

Figure 8. Flow diagram of the plugin in its first evolution.

- The Moodle administrator assigns alias management permissions to the DPO.
- The student to be protected uses the contact form to send the DPO an anonymity request.
- The DPO manages the requests, studies the cases, and validates or rejects them.
- The DPO assigns different aliases to the student to be protected.
- The protected user logs in with her alias from the main page.

3.1.3. Final State

In the third stage, we make different changes to improve the interface and the process of management, assignment, and log in with the aliases. We eliminate the Moodle administrator intermediation, make the management of the alias easier for the DPO, and we enable students to log in with the protected users' aliases from their student profile. We aim to show the information in a form which is as simple, minimalist, and clear as possible. The development of the interface ends in this second evolution. Figure 9 shows the flow diagram in this second evolution of our plugin.

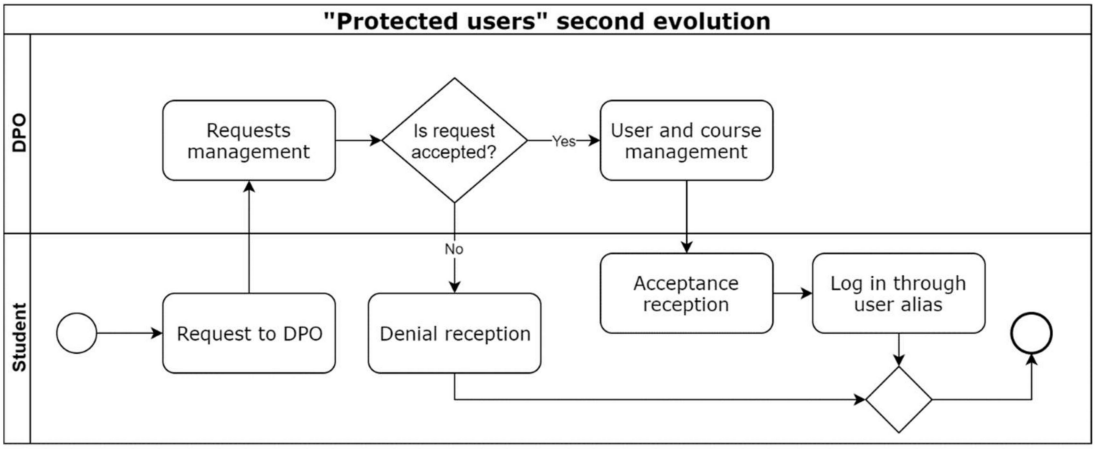

Figure 9. Flow diagram of the plugin in its second and final evolution.

- The DPO manages the requests sent from students. Afterwards, DPO studies the cases and validates or rejects them (see Figure 10).
- The DPO assigns the aliases to the students (see Figure 11).
- The protected user logs in to her or his alias from an option on the profile page (see Figures 12 and 13).

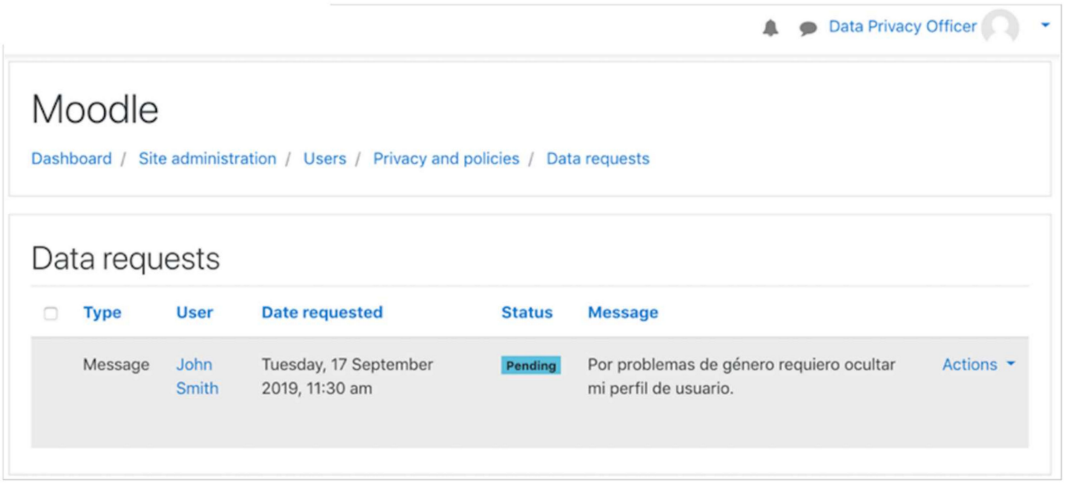

Figure 10. The DPO manages the sent requests from students.

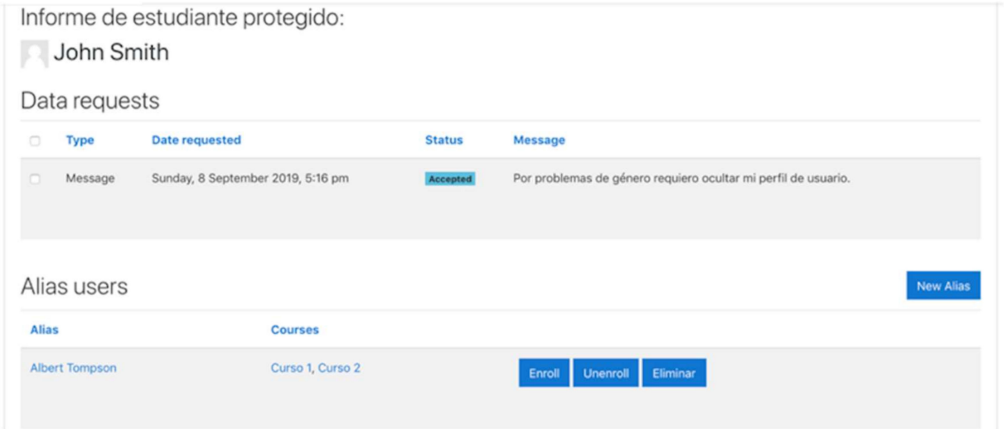

Figure 11. The DPO assigns the aliases to the student.

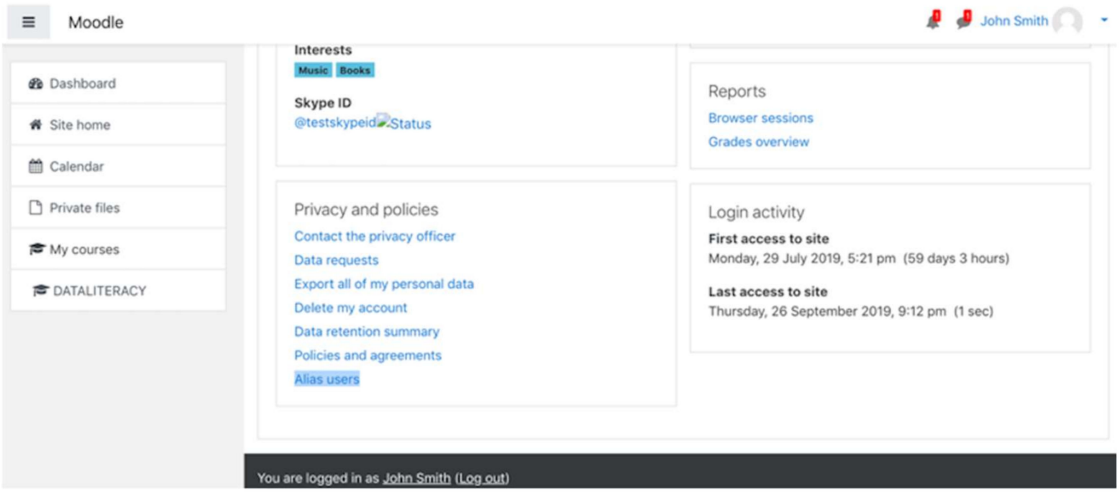

Figure 12. The protected user has access to their aliases list from an option on the profile page.

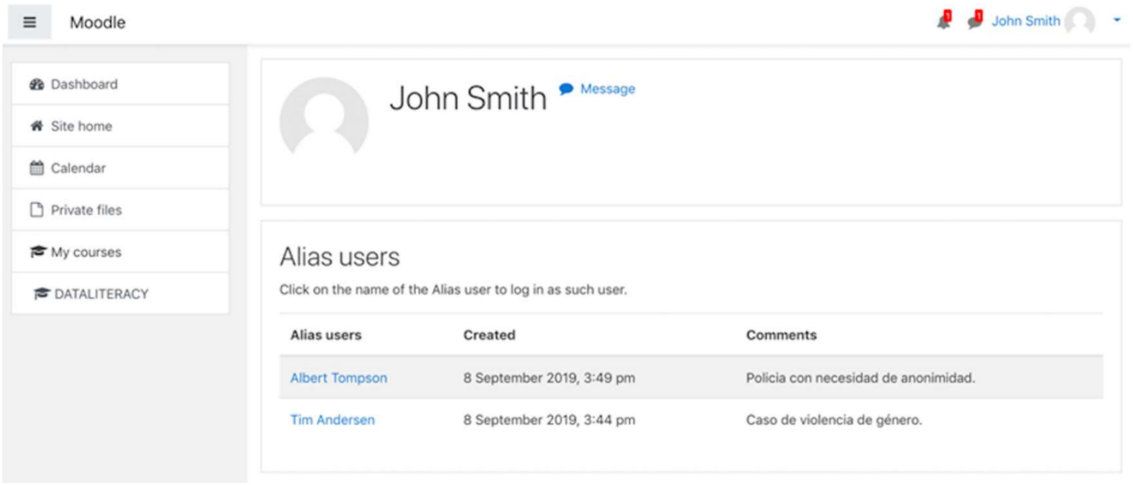

Figure 13. The protected user can log in to her alias from a list.

4. Discussion

Our implementation of the solution in plugin format demonstrates that it is possible to solve specific privacy and identity protection problems in LMSs. Our plugin allows any student to request the DPO to ensure their privacy in the LMS through an alias.

These cases were considered exceptions and were not contemplated in the LMS, until our development. On the one hand, we bring advances to the area. On the other hand, we open up new sustainable possibilities for the implementation of solutions at the LMS level.

The work is restricted to the possibilities of governance of LMS by administrators and our position as external developers of the Moodle platform. We are aware that the ideal scenario for a Moodle administrator is the integration of our solution as part of Moodle instead of it being offered as a plugin. After the presentation of the plugin in the Moodlemoot Global 2019 [25], we hope to start conversations with Moodle HQ to propose such integration in future versions of the LMS. Meanwhile, Moodle administrators can install and uninstall our plugin at their convenience, both when the problem arises or before it.

We use Moodle as the development platform due to different reasons. First, to demonstrate that the proposal can be developed in an LMS. Second, Moodle is an Open Source LMS and has an architecture that supports authentication plugins and extensions for the administration dashboard. Third, Moodle is the most used LMS in Spain. Fourth, our centers are using Moodle as the main LMS.

Fifth, the projects we are executing in collaboration with different schools use this system. Hence, we adopted Moodle as our work standard for future research sample collection.

Moreover, our proposed solution is replicable to other open LMSs. Therefore, similar approaches could be implemented in other Open Source LMSs like Sakai or Canvas.

For closed source systems like Blackboard, it is not possible to do this kind of customization beyond Blackboard's developers itself. However, the functionalities of the plugin can be implemented outside the LMS. With this externalized approach, all the aliases need to be managed in a software layer outside the LMS. The LMS will host alias users as if they were real. The management of grades for students with aliases would be more cumbersome depending on the way the LMS is integrated with the Academic Information System.

Our proposed plugin provides a simpler architecture that handles all the complexity.

5. Conclusions

In the present work, we underline the importance for LMSs to comply with the GDPR laws. This law regulates the processing of personal data of students. We show that the LMS platforms do not completely implement the GDPR requirements. For example, Moodle provides the institution with the opportunity to present privacy policies and terms of use as digital contracts. At the same time, the institution can track students who have accepted their digital contracts and prohibit access to those who have not yet done so.

Access to Moodle, therefore, implies prior acceptance of digital contracts. However, this acceptance does not provide anonymity to students. In detriment to some students, this implies public exposure of their digital student profiles, as well as access to other academic data of their peers. A student using Moodle cannot protect her or his identity from other students. This conflicts with students who may need to remain anonymous for justifiable personal reasons, such as gender-based violence or a post in public sectors.

The LMS is legally regulated by the GDPR, which requires institutions to offer safe anonymity to students who justifiably request it. In our work, we propose an easy and elegant solution to the problem in plugin format. Our contribution provides Moodle with a plugin that solves the problem presented. The solution allows Moodle system administrators to install and uninstall the plugin at their convenience. The plugin is developed based on developments provided by Moodle, ensuring compatibility with the system.

We are aware that the ideal solution is to integrate the code of our solution into the Moodle code in future distributions of the platform. We decided to develop a plugin in the same way Moodle did in order to resolve aspects of the GDPR, and started conversations to make further integration possible in the near future.

Supplementary Materials: The following are available online at https://lasalleuniversities-my.sharepoint.com/:x:/g/personal/daniel_amo_salle_url_edu/EWh6ESgHCLlGmeSPW5P_d8YBquokTmYcAi-JrGpBUkFqeg?e=Dml7yz, Table S2: Lawyer profile interview questions, Table S4: Student profile survey questions, Table S6: Moodle technical administrator profile interview questions, Table S8: Data Privacy Officer profile interview questions, Table S10: Teacher profile interview questions.

Author Contributions: Conceptualization, M.A. and D.A.; methodology, D.F. and F.J.G.-P.; software, D.A.; validation, D.A. and M.J.C.; formal analysis, D.A.; investigation, M.A. and D.A.; resources, D.A.; writing—original draft preparation, D.A.; writing—review and editing, D.A. and M.J.C.; supervision, M.A. and D.F.; project administration, F.J.G.-P.; funding acquisition, F.J.G.-P. and D.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partially funded by the Spanish Government Ministry of Economy and Competitiveness throughout the DEFINES project (Ref. TIN2016-80172-R), with the support of the Secretaria d'Universitats I Recerca of the Department of Business and Knowledge of the Generalitat de Catalunya with the help of 2017 SGR 934.

Acknowledgments: This work is carried out in the Doctorate Programme Formación en la Sociedad del Conocimiento de la Universidad de Salamanca [26–28]. The program is regulated by the Real Decreto 99/2011 [29].

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. García-Peñalvo, F.J.; Seoane-Pardo, A.M. Una revisión actualizada del concepto de eLearning. Décimo Aniversario. *Educ. Knowled. Soc.* **2015**, *16*, 119–144. [CrossRef]
2. Gros, B.; García-Peñalvo, F.J. Future trends in the design strategies and technological affordances of e-learning. In *Learning, Design, and Technology. An International Compendium of Theory, Research, Practice, and Policy*; Springer International Publishing: Basel, Swissland, 2016; pp. 1–23. [CrossRef]
3. Dougiamas, M. A Journey into Constructivism. Available online: https://dougiamas.com/archives/a-journey-into-constructivism/ (accessed on 1 January 2017).
4. Mayes, R.; Natividad, G.; Spector, J. Challenges for Educational Technologists in the 21st Century. *Educ. Sci.* **2015**, *5*, 221–237. [CrossRef]
5. Chahal, R.; Kumar, L.; Jindal, S.; Rawat, P. Cyber stalking: Technological form of sexual harassment. *Int. J. Emerg. Technol.* **2019**, *10*, 367–373.
6. Kambourakis, G. Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art. *Int. J. u-and e-Service Sci. Technol.* **2013**, *6*, 67–84.
7. Isabwe, G.M.N.; Reichert, F. Revisiting students' privacy in computer supported learning systems. In Proceedings of the International Conference on Information Society, i-Society, Toronto, ON, Canada, 24–26 June 2013; pp. 256–262.
8. Eskey, M.; Taylor, C.; Eskey, M. Cyber-Bullying in the Online Classroom: Instructor Perceptions of Aggressive Student Behavior. *Online J. Distance Learn. Adm.* **2014**, *17*, n4.
9. EP and the CEU: Regulation (EU) 2016/679 GDPR. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679 (accessed on 27 June 2019).
10. Amo, D.; Alier, M.; García-Peñalvo, F.J.; Fonseca, D.; Casañ, M.J. GDPR Security and Confidentiality compliance in LMS' a problem analysis and engineering solution proposal. In Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality, TEEM, León, Spain, 16–18 October 2019; pp. 253–259. [CrossRef]
11. García-Peñalvo, F.J. Modelo de referencia para la enseñanza no presencial en universidades presenciales. *Campus Virt.* **2020**, *9*. in press.
12. Amo, D.; Fonseca, D.; Alier, M.; García-Peñalvo, F.J.; Casañ, M.J.; Alsina, M. Personal Data Broker: A Solution to Assure Data Privacy in EdTech. In Proceedings of the International Conference on Human-Computer Interaction, HCII, Orlando, FL, USA, 26–31 July 2019; pp. 3–14. [CrossRef]
13. Téllez, S.A.; Moodle, H.Q. Moodle Plugin Policies. Available online: https://moodle.org/plugins/tool_policy (accessed on 1 October 2018).
14. Moodle, H.Q.; Pataleta, J.; Monllaó, D. Moodle Plugin Data Privacy. Available online: https://moodle.org/plugins/tool_dataprivacy (accessed on 1 October 2018).
15. Hill, P. New Release of European LMS Market Report. Available online: https://eliterate.us/new-release-european-lms-market-report/ (accessed on 1 June 2018).
16. Bevan, N.; Carter, J.; Harker, S. Iso 9241-11 revised: What have we learnt about usability since 1998. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 143–151. [CrossRef]
17. Hassenzahl, M.; Tractinsky, N. User experience-a research agenda. *Behav. Inf. Technol.* **2006**, *25*, 91–97. [CrossRef]
18. Pifarré, M.; Tomico, O. Bipolar laddering (BLA): A participatory subjective exploration method on user experience. In Proceedings of the 2007 Conference on Designing for User eXperiences, DUX'07, Chicago, IL, USA, 5–7 November 2007; p. 2. [CrossRef]
19. Llorca, J.; Zapata, H.; Redondo, E.; Alba, J.; Fonseca, D. Bipolar laddering assessments applied to urban acoustics education. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 287–297. [CrossRef]

20. Villagrasa, S.; Fonseca, D.; Durán, J. Teaching case: Applying gamification techniques and virtual reality for learning building engineering 3D arts. In Proceedings of the ACM International Conference Proceeding Series, Salamanca, Spain, 1–3 October 2014; pp. 171–177. [CrossRef]
21. Fonseca, D.; Pifarre, M.; Redondo, E.; Alitany, A.; Sanchez, A. Combination of qualitative and quantitative techniques in the analysis of new technologies implementation in education: Using augmented reality in the visualization of architectural projects. In Proceedings of the Iberian Conference on Information Systems and Technologies, CISTI, Lisboa, Portugal, 19–22 June 2013; pp. 1–7.
22. Villagrasa, S.; Fonseca, D.; Redondo, E.; Duran, J. Teaching case of gamification and visual technologies for education. *Ophthalmol. Break. Res. Pract.* **2018**, *16*, 205–226. [CrossRef]
23. Amo, D.; Alier, M.; García-Peñalvo, F.J.; Fonseca, D.; Casañ, M.J. GitHub of Protected Users a Moodle Plugin to Protect Studens Identity. 2019. Available online: https://github.com/danielamof/protected_users (accessed on 19 November 2019).
24. Granollers, T.; Perdrix, F.; Lorés, J. Incorporación de usuarios en la evaluación de la usabilidad por recorrido cognitivo. In Proceedings of the Interacción'04, Lleida, Spain, 4–7 May 2004.
25. Alier, M.; Amo, D. Modding Moodle to improve confidentiality and privacy support. 2:10pm (PROGRAM – DAY 2). Available online: https://moodlemoot.org/mootglobal19/day-2/ (accessed on 17 November 2019).
26. García-Peñalvo, F.J. Education in Knowledge Society: A new PhD Programme approach. In Proceedings of the First International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'13), Salamanca, Spain, 14–15 November 2013; García-Peñalvo, F.J., Ed.; Association for Computing Machinery: New York, NY, USA, 2013; pp. 575–577. [CrossRef]
27. García-Peñalvo, F.J. Formación en la sociedad del conocimiento, un programa de doctorado con una perspectiva interdisciplinar. *Educ. Knowl. Soc.* **2014**, *15*, 4–9.
28. García-Peñalvo, F.J. Programa de Doctorado Formación en la Sociedad del Conocimiento. Kick-off de la Edición 2019–2020. Presented in Seminarios del Programa de Doctorado en Formación en la Sociedad del Conocimiento. 2019. Available online: https://www.researchgate.net/publication/336687137$\delimiter"026E30F$_Education$\delimiter"026E30F$_in$\delimiter"026E30F$_the$\delimiter"026E30F$_Knowledge$\delimiter"026E30F$_Society$\delimiter"026E30F$_PhD$\delimiter"026E30F$_Programme$\delimiter"026E30F$_2019$\delimiter"026E30F$_Kick-off$\delimiter"026E30F$_Meeting (accessed on 21 October 2019). [CrossRef]
29. Gobierno de España: Real Decreto 99/2011, de 28 de enero, por el que se Regulan las Enseñanzas Oficiales de Doctorado. In Ministerio de Educación. pp 13909–13926. Gobierno de España. 2011. Available online: https://goo.gl/imEsz6 (accessed on 11 November 2019).