Ethical, Legal and Privacy Considerations for Adaptive Systems

Knockaert, Manon; De Vos, Nathan

Published in:
Engineering Data-Driven Adaptive Trust-based e-Assessment Systems

Publication date:
2019

Document Version
le PDF de l'éditeur

Chapter 12: Ethical, Legal and Privacy Considerations for Adaptive Systems

Manon Knockaert and Nathan De Vos[1]

Abstract:

The General Data Protection Regulation (GDPR) is the new EU legal framework for the processing of personal data. The use of any information related to an identified or identifiable person by a software will imply the compliance with this European legislation. The objective of this chapter is to focus on the processing of a specific category of personal data: sensitive data (mainly face recognition and voice recognition) to verify the user's identity. Indeed, the GDPR reinforces requirements for security measures to ensure the integrity and confidentiality of these personal data. We analyze three privacy aspects: the possibility to obtain a valid consent from the user, how to ensure the transparency principle and the implication of openness and the framework to implement in order to use the feedback given by the system to the user. From an ethical point of view, the request for consent is legitimized by the existence of a real assessment alternative left to the student. Then the different components of the right to transparency are illustrated by examples from the field. Finally, the question of feedback is expressed in the form of a dilemma highlighting the possible risks of poorly justified decisions due to the way feedback is exposed.

Keywords: Biometrics- GDPR – Privacy- Personal Data – Ethics – Consent – Transparency - Right to information

1. Introduction

As members of the Research Centre in Information, Law and Society (CRIDS), we have worked on both the legal and ethical aspects of the TeSLA (Trust-based authentication and authorship e-assessment analysis) project[2]. As the software is using personal data of the students from the involved institutions (face recognition, voice recognition and keystroke dynamics), it was necessary to adopt a reflection on both the legal and ethical aspects of data processes involved – and this, from the beginning of the project, to ensure that the outcomes are legally valid and well received

[1] M. Knockaert
University of Namur, CRIDS/NADI
manon.knockaert@unamur.be

N. De Vos
University of Namur, CRIDS/NADI
nathan.devos@unamur.be

[2] To learn more about the project: https://tesla-project.eu/

by society.

Our Research Centre is used to dealing with these two aspects both in research and development projects. Based upon our experience in the field and long-standing reflection on how to make legal and ethical interventions in this context, we have adopted a particular stance towards the other members of the project. Indeed, being neither engineers nor pedagogues, our expertise could tend to place us on sort of an external position. However, our credo is to try to collaborate as much as possible with all the partners, despite the diversity of the profiles we have to deal with. This modus operandi avoids the trap of an overhanging attitude that would consist in prescribing from the outside a series of directly applicable injunctions. We worked together with the project members to stimulate collective reflection on a number of issues that we found necessary to address.

The legal approach intends to put in place the safeguards required by the law to legalize the processing of personal data. The major objective was to implement the technical measures to ensure the proportionality, the confidentiality and the security of the personal data processes. The first guarantee implemented is that the system can only process the data of the students that give their consent. The second major guarantee concerns the rules of access. The system must be designed to allow each institution to have access only to its own data and only to the relevant data. Furthermore, the system must be designed to facilitate deletion or anonymization of the personal data when it is no longer necessary to store the data in a form permitting the identification of the student. Next to the technical considerations, the GDPR also foresees key principles surrounding the processing of personal data. In this chapter, we will mainly focus on this second aspect of the legislation, with a particular attention to the transparency principle.
Conversely, the ethicist's contribution is less related to operational aspects. It aims more to open the project, to bring a broader point of view to it, to see how the object created would interact with the rest of society. The ethical approach highlights hypotheses on the various potential impacts of the technology, sheds light on the societal choices embedded in the object and invites other partners to think about them. The product of ethical work therefore takes the form of a reflection rather than a recommendation.

For a project such as TeSLA, the legal aspects already provide a solid basis to be taken into account to ensure the possibility of implementing the system. However, the Law will not necessarily enlighten us about all the critical technical choices (especially given the novelty of the object, some legal gaps may exist). The ethical approach can also be used to complete the legal approach when it does not have the resources to effectively advise partners. In this sense, but also because of the two

aspects mentioned above, the legal approach and the ethical approach are complementary.

The first part of this chapter is dedicated to the consent of the students to process their personal data. As TeSLA is using biometrics data, it is important to obtain an explicit consent. We will analyze the legal conditions to obtain a valid consent and how the ethical considerations could reinforce the requirements to have a free, specific, informed and unambiguous consent. The second part is dedicated to the transparency principle. This principle involves a right for the students to receive specific information and a corollary obligation for the data controller to provide that information. In this second part of the chapter, we will analyze what information has to be given and how they can be adapted to the user. Finally, as a third part, we will focus on the result given by the TeSLA system. The result of matching or non-matching is personal data but ethical considerations could help the teachers to work with these indicators. For each part, we will firstly expose the GDPR requirements, and secondly explain the ethical considerations.

2. Ethical preliminary remarks

Three methodological approaches were undertaken in order to question the project from an ethical point of view.

First of all, a state-of-the-art report was produced regarding the potential social effects TeSLA could have on the learning and teaching experience. It was based on an interdisciplinary approach, ranging from academic texts on e-learning to the sociology of technology. This state of the art aimed to introduce initial reflections with a more global aim into the project (both through reports and direct discussions) and to get familiar with the subject of study. To this end, our analytical framework was informed by the work of key authors in the field of sociology of techniques such as Feenberg[3] or Akrich[4].

Following this theoretical approach to the above concerns, an ethical fieldwork was developed, based on individual semi-structured interviews of teachers and learners involved into the pilots (which consist of the experimental and gradual integration of the TeSLA system in 7 consortium member universities). These interviews aimed to help us to concretely and pragmatically understand the social effects the TeSLA project could have on teaching and learning experiences of the participants. Four pilot institutions were implicated in the ethical fieldwork: two full distance universities (the Open University of Catalunya UOC and The Open University of the Neth-

[3]Feenberg 2012.
[4]Akrich 1987.

erlands OUNL) and two blended ones (Sofia University SU and the Technical University of Sofia TUS). Dutch OUNL stakeholders were interviewed at the end of Pilot 2, the other pilot stakeholders at the end of pilot 3A (not earlier because we needed to interview users who tested a sufficiently advanced version of the system). The choice of these universities was made to collect contrasted social contexts with respect two criteria (distance versus blended Higher Education Institutions HEI – technical backgrounds versus humanities backgrounds of teachers and learners).

Table 1. Interviews conducted in each pilot university

Number of participants	UOC	OUNL	SU	TUS
Learners	6	5	1	5 (focus group)
Teachers	3	3	2	3

Each interview lasted an average of 1.30 hours. Two specific features characterized those interviews: first of all, they were based on the TeSLA experience of the interviewees, i.e. their understanding of the system and the activities undertaken with the system (what we call 'situated interviews'). Secondly, they were explorative and not representative: the ambition was just to help us to pragmatically understand concerns 'theoretically' pointed out by the literature or through the discussions experienced during the project. The number of interviewees is too low to expect some statistical representativeness and this is not the point of this study. The aim was to discuss, with users of the system (professors and students), the uses they have made of a new system. The reactions should allow the technical partners to see how their system is received by the public.

In this respect, the interview methodology is inspired by sociologists such as Kaufmann, who claims a very open approach to interviews[5]. This openness allows interviewees to address the aspects that they consider most relevant and not to confine the debate to the interviewer's pre-conceptions. This is how our fieldwork differs from other fieldworks accomplished in the context of this project: this methodology allows us to report the sense of the practices, the deep reasons why users act a specific way. It enables us to consider diversity among users and to ask specific questions according to the issues they are more sensitive about. This wider freedom in the way to answer questions presented by our methodology is complementary to the pilot partners questionnaires which are more formalized and gather more standardized quantitative data.

To do this, interview grids were designed: they include a set of sub-themes to explore in order to deal with the system in a comprehensive way and examples of

[5]Kaufmann 2011.

questions that can help the conversation to move forward (interviewees are not required to answer each of them if they find them uninteresting). Here are simplified versions of these grids both for teachers interviews and students' interviews.

Table 2. Teachers' interview grid

Topic	Why approaching it?
Background of the teacher (both global and more specifically about e-learning)	Allows a very contextualized analysis
Understanding of TeSLA	Observing whether they really understand what is TeSLA and how it is supposed to be used is a prerequisite to analyse other issues
Pedagogical integration of TeSLA	Their feeling about the principles of use of the system, the different instruments, why did they use this/these instrument(s) in place of others...
Feedback interpretation	Their use of the numbers sent back by TeSLA. Are they a sufficient prove? Are they reliable?
Monitoring aspect	The surveillance induced by TeSLA, their eventual fear of "slides"
Defence against a decision coming from the system	What would they do if the system accuses them of cheating? Would they like to be added in the system to allow this defence?
Regulation of the judgement	The relation between the use of TeSLA and the internal regulation of institutions, the role allocated at the teacher in the management of TeSLA

Table 3. Learners' interview grid

Topic	Why approaching it?
Background of the learner (both global and more specifically about e-learning)	Allows a very contextualized analysis
Understanding of TeSLA	Observing whether they really understand what is TeSLA and how it is supposed to be used is a prerequisite to analyse other issues
Explanation of the use	Their feeling about the principles of use of the system, the different instruments, and their integration with the activities they are asked to do...
Monitoring aspect	The surveillance induced by TeSLA, their eventual fear of "slides" …

Defence against a decision coming from the system	What would they do if the system accuses them of cheating? Would they like to be added in the system to allow this defence?
Regulation of the judgement	How are the teachers supposed to deal with the feedbacks sent by TeSLA?

The information collected during the ethical fieldwork have been compared (where possible) with the observations from other partners, particularly the data collected in the surveys and focus groups organized to assess the pilots experiences, to widen our point of view.

3. Legal preliminary remarks

Privacy law concern TeSLA. Indeed, the General Data Protection Regulation[6] (hereafter the "GDPR") defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[7]. TeSLA implies the processing of personal data when using face recognition, voice recognition and keystroke dynamics to verify students' identity during distance exams and pedagogical activities. One of the objectives is to develop strong privacy features that will prevent unnecessary identification of persons during the e-assessment. The project began under the rules of the Directive 95/46/EC[8] and continued under the GDPR which is applicable from 25 May 2018. For the purpose of this chapter, we only focus on the processing of face and voice recognition. Indeed, even if keystroke dynamics are personal data, they do not fall into the specific category of sensitive personal data (see section 5.1.2 of this chapter).

In order to establish the responsibilities of each partner and the architecture of the system, a first step was to identify the data controller and the data processor. Let us indicate that the *data controller* is the natural or legal person that determines

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016, L 119/1, p. 1.

[7] Article 4.4 of the GDPR.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281, p. 0031.

the means and the purposes of the personal data processing[9]. When using TeSLA, the institutions are the solely responsible for the processing of personal data of their students.

On the other hand, the *data processor* is the natural or legal person, which processes personal data on behalf of the controller[10]. TeSLA is the third party, which develops the tools needed to perform the e-assessment. It will be the interface executing the *privacy filters* and sending alerts of fraud detection to the institution. The privacy filters are the guarantees developed in the system to ensure the compliance with GDPR requirements.

Each institution willing to use TeSLA is in charge of the major part of the obligations provided by law and is the main contact for data subjects. The obligations are mainly:

- Getting the consent from students. The plug-in, in the university domain, verify that the student signed the Consent Form;
- The internal determination of who can have access to what data, and send these rules of access to the TeSLA system. The combination of the VLE (Virtual Learning Environment) and LTI (Learning Tools Interoperability) provider establish this privacy filter. The infrastructure has to be conceived in a way that limits access to the relevant teacher and only to the relevant data;
- The period of retention of personal data by the system;
- To keep the table of conversion between the TeSLA ID and the real identity of students. The TeSLA ID is a unique and secure identifier assigned to each student in TeSLA.

The processing by the data processor must be governed by a binding legal act that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the obligations of each party. The data processor can only act if the data controller provides documented instructions[11].

The project uses a hybrid model of cloud. The TeSLA system has student's biometric data but only through the coded identity of the students. The institutions, on their servers, have the uncoded samples and the table of conversion between the TeSLA ID and the real identity of the students. The TIP (TeSLA Identity Provider)

[9] Article 4.7 of the GDPR.
[10] Article 4.8 of the GDPR.
[11] Articles 28.1 and 28.3 of the GDPR.

converts the identity of the student into a pseudonymized TeSLA ID. The main function is to reduce as much as technically possible the identification of unneeded information. TeSLA only works with pseudonymised data and it sends the coded data to the relevant institution only when there is an abnormality detected during the exam. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. This additional information needs to be kept separately and be subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. On the contrary, anonymization means that there is no possibility, with reasonable means, to identify a person.

Each instrument has its own database. It permits to separate the data (face recognition, voice recognition, and keystroke dynamics) in order to send only the relevant data to verify the cheating. The combination of TEP (TeSLA E-assessment Portal) and the RT (Reporting Tool) constitute service brokers that gather-forward requests and learner's data. Furthermore, the system is designed to facilitate deletion or anonymization of the data when it is no longer necessary to store them in a form permitting identification of the corresponding person. Another filter is applied over the results. If the instrument does not detect a dishonest behavior, the teacher will not have access to the audited data, but only to the score itself. Furthermore, both data controller and data processor are in charge of data accuracy. In case of incorrectness, they have to take reasonable steps to rectify or erase the concerned personal data[12].

The data processor is liable for damages caused by processing which do not comply with the GDPR requirements. TeSLA will also be liable if it has acted outside or contrary to lawful instructions of the controller. Nevertheless, a data processor will be exempt from any liability if it proves that it is not responsible for the event giving rise to the damage[13].

The GDPR considers also the situation where there is more than one controller or processor involved in the same processing. Each controller or processor will be held liable for the entire damage in order to ensure a full and effective compensation for the data subject. The person who has paid full compensation has the possibility to claim back from the other controllers or processors involved in the same processing the part of the compensation corresponding to their part of responsibility in the damage[14]. The division of responsibility is tackled after the full data subject's compensation.

4. Personal data processing key principles

[12] Article 5.1, d) of the GDPR.

[13] Articles 82.2 and 82.3 of the GDPR.

[14] Articles 82.4 and 82.5 of the GDPR.

In this section, the aim is not to explain all the legislation but to re-examine the general principles of protection in order to understand the next steps in the development process. Therefore, we focus on the obligation of transparency, purpose limitation, minimization principle, storage limitation and security. All these principles related to the processing of personal data ensure the lawfulness of each software development.

4.1 Lawfulness, fairness and transparency

Article 5.1, a) of the GDPR provides that: "*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*".

The GDPR provides for six legitimate assumptions for data processing. Note that the TeSLA project uses biometric data, such as face and voice recognition tools. According to the GDPR, biometric data means "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*"[15].
These kinds of personal data fall in the special categories of personal data. Consequently, we identified the consent of the student as a way of legitimizing the processing, according to article 9 of the GDPR.

The obligation of transparency requires that the information about the recipient or category of recipients of the data must be disclosed to the data subject. It means that the student has to be informed about TeSLA as the data processor and has the right to access the data processing contract[16].

4.2 Purpose limitation

Article 5.2, b) of the GDPR provides that: "*Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". For example, biometric data can be useful to identify the user of the TeSLA system or to check if the user is cheating or not[17].
In addition, the GDPR prohibits further processing in a manner that is incompatible with the original purpose. To determine the lawfulness of a further processing, the GDPR establishes a list of factors that should be taken into account. Here are some examples of relevant factors (this list is not exhaustive[18]):

- The existence of a link between the original purpose and the new one,

---

[15] Article 4.14 of the GDPR.

[16] See article 12 of the GDPR.

[17] Notice that the traceability of the learner and the correlation between data collected are a process by themselves and need to respect all privacy legislation. Consequently, the student must be informed and consent.

[18] Recital 50 of the GDPR.

- The context in which the data was collected,

- The nature of the data and the possible consequences of the processing,

- And the existence of safeguards such as encryption or pseudonymisation.

Concerning TeSLA, the purpose could be defined as follow: the personal data from students who gave their consent (face recognition, voice recognition and keystroke dynamics) will be collected and processed by the institution in order to certify the real identity of the student.

4.3 Minimization principle

Article 5.1, c) of the GDPR states that: "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

To analyze the necessity to use biometrics data, we consider whether there are less privacy-invasive means to achieve the same result with the same efficacy and if the resulting loss of privacy for the students is proportional to any anticipated benefit[19]. To minimize the risk, we put in place one database for each instrument to avoid the use of a centralized database that could lead to a single point of failure, and we use the technique of pseudonymisation[20].

Pseudonymisation means "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the personal data are not attributed to an identified or identifiable natural person"*[21].

The GDPR encourages the use of this method because it is a technique to implement privacy by design and by default[22]. Indeed, the GDPR implements these two notions. It implies that the principles of data protection have to be taken into account during the elaboration and conception of the system. Furthermore, it may contribute to meeting the security obligations[23].

We established that the TeSLA project would adopt a hybrid system, which would consist of having pseudonymized (or coded) data in the cloud and uncoded data in institution servers (data controller).

---

[19] Article 29 Data Protection Working Party-WP193 2012, p.8.

[20] Belgian Commission for the protection of privacy 2008, pp. 14-16.

[21] Article 4.5 of the GDPR.

[22] Article 25 and Recital 58 of the GDPR.

[23] See article 6.4 (e) of the GDPR.

4.4. Storage limitation

Article 5.1, e) of the GDPR states that: "*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*". The retention period could be the time required to verify the fraud alert if any or the extinction of recourse by the student. For each type of collected data and in consideration of the relevant purposes, it is necessary to determine if the personal data needs to be stored or whether it can be deleted.

4.5. Security

Finally, article 5.1, f) of the GDPR states that: "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". In other words, personal data should be processed in a manner that ensures appropriate data security. The data processor is also responsible for the security of the system, in particular for preventing unauthorized access to personal data used for processing such data. The security system should also prevent any illegal/unauthorized use of personal data. The GDPR imposes no specific measure.

According to article 32 of the GDPR, the data controller and data processor shall implement appropriate technical and organizational measures to ensure security of personal data, taking into account the state of the art, the costs of implementation, the type of personal data, and the potential risks. According to the GDPR, the data processor should evaluate the risks inherent in the processing such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, which may lead, in particular, to physical, material or non-material damages.

The GDPR gives some examples of security measures:

- Pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensure the security of the processing.

5. Consent

In the TeSLA system, each student has to consent to the processing of his/her biometrics data. In order to be legally valid, the consent needs to fulfil legal obligations. These are mainly the obtention of a free, specific, informed and unambiguous consent. Ethical considerations strengthen and reinforce legal obligations arising from the GDPR. After describing each of the conditions, we will expose their implementations in the TeSLA system.

5.1. Legal considerations

5.1.1 Definition and objectives

The GDPR provides that: *'Processing shall be lawful only if and to the extent that at least one of the following applies: (a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes".* The consent of the data subject is: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

The GDPR intends to stop the abusive use of uninformed and uncertain consent. In order to ensure a true reflection of individual autonomy, the GDPR has strengthened its requirements[24]. Consent must now be free, specific, informed and unambiguous[25].

Consent is also enshrined in Convention 108+. This is currently the only international legislation on personal data protection[26]. Having in mind the increase and globalization of the use of personal data as well as the vast deployment of technologies, the Convention 108 wants to give more power to citizens. As stated in the Explanatory Report: "*A major objective of the Convention is to put individuals in a position to know about, to understand and to control the processing of their personal data by others*"[27].

5.1.2. Conditions

The data controller must therefore prove compliance with four conditions.

- Free consent

[24] de Terwangne et al. 2017, p. 306.

[25] Article 4.11 of the GDPR. See also Article 29 Data Protection Working Party-WP259 2018.

[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg the 28 January 1981, ETS No.108.

[27] Explanatory Report, p. 2, pt. 10. Available at : https://rm.coe.int/16808ac91a.

The objective is that the data subject has a real choice to consent. To ensure a real expression of willingness, three elements must be taken into account: the imbalance of power, the granularity and the detriment[28]. Recital 43 states that: « *Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*". It is up to the controller to determine and specify the different purposes pursued and to allow an opt-in of the data subject for each one. Furthermore, if the data subject feels compelled, afraid to face negative consequences in case of refusal or to be affected by any detriment, the consent will not be considered as freely given. As stated in Recital 42, "*consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*"[29].

- Specific consent

Secondly, consent must be specific. In case of multiple purposes for several data processing, the data controller must receive a separate consent for each purpose.

- Informed consent

Thirdly, the consent must be informed. Articles 13 and 14 of the GDPR list the information that the controller must provide to the data subject. At least, it concerns information about the data controller's identity, the purpose of each of the processing operations for which consent is needed, the collected and processed data, the existence of the rights for the data subject, notably the right to withdraw the consent and the transfers of personal data outside the European Union if any.

The objective is that the person who consents must understand why, how and by whom his or her personal data will be collected and used[30]. The information must be concise, transparent, intelligible and easily accessible. The information has also to be given in a clear and plain language, avoiding specialist terminology. Therefore, the data controller should adopt a user-centric approach and to identify the "audience" and ensure that the information is understandable by an average member of this audience[31]. As best practice, the Article 29 Working Party encourages the data controller to provide an easy access to the information related to the processing

[28] Article 29 Data Protection Working Party-WP259 2018, p.5 and seq.

[29] Article 29 Data Protection Working Party-WP259 2018, pp. 5-10.

[30] Article 29 Data Protection Working Party-WP259 2018, p. 13.

[31] Article 29 Data Protection Working Party-WP259 2018, p. 14. The Article 29 Working Party gives some methods to target the audience, such as panels, readability testing and dialogue with concerned groups; Article 29 Data Protection Working Party-WP260 2018, p. 7.

of personal data. The data controller has also to take into consideration the possibility to provide express reminders to data subject about the information notice[32].

- . Unambiguous consent

Fourthly, the consent must be unambiguous and must be the result of a declaration by the data subject or a clear positive act. Consent is therefore not presumed. In addition to the quality requirements, consent may be withdrawn at any time and the GDPR specifies that it must be as easy to withdraw consent as to give it[33].

- Implementation in TeSLA

In TeSLA, we process biometrics data. As it is information related to an identified or identifiable person, biometrics data are personal data in the meaning of the GDPR. In addition, biometrics data enter into a particular category of personal data: sensitive personal data. Sensitive data is defined as data relating to specific information on the data subject. These are mainly listed in Article 9 of the GDPR and include the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural per-son's sex life or sexual orientation.

For the processing of this special category of personal data - which is in principle prohibited - the GDPR requires an explicit consent. It implies that the data subject must give an express statement of consent[34]. As examples, the Article 29 Working Party recognizes the use of an electronic form, the sending of email or using electronic signature. The explicit consent implies for the data controller to be careful when providing information to the data subject. The institution willing to use TeSLA, as data controller, has to ensure that all the necessary information are given to the data subject to understand the processing and the personal data used, without submerging the data subject with information[35].

TeSLA's particularity is the collection of both personal data such as students' surnames and first names and special categories of personal data such as face and voice recognition. In view of the factual circumstances, consent seems to be the only basis for legitimization.

---

[32] Article 29 Data Protection Working Party-WP260 2018, p. 18.

[33] Article 7.3 of the GDPR.

[34] Article 9.2, a) of the GDPR.

[35] Article 29 Data Protection Working Party-WP259 2018, p. 18.

The consent form elaborated during the project includes the following information: the identity of the controller and of the processor, goals of the project, personal data collected, purposes, data retention, privacy policy signature and rights of the data subjects. We have been vigilant in balancing the obligation of transparency with the obligation to obtain valid consent and the requirement not to inundate the person concerned with information[36]. We suggest that the period of conservation is the duration of the project TeSLA. In case of duration of TeSLA over the end of the project, the retention period for both types of personal data could be the time required to verify the alert of fraud.

This consent form must be completed and approved by each student. This form is offered to them by a visual display on the user's computer screen at the beginning of the service's use to respect the timing for provision of information[37]. This method has also the advantage to include the information in one single document in one single place[38]. This is intended to facilitate the accessibility and the communication of information by ensuring that the data subject has at least once taken note of all information relating to the processing of his or her personal data[39].

The consent is also specific because the student receives a clear information about the privacy policy, which is separate from other text or activities and the student has to click in order to give his/her consent. In the text of the consent form, we avoided to use unclear terms like “may’, “might”, “possible” as it is pointed out by the Article 29 Working Party. These terms are subject to interpretation and do not allow the data subject to have a concrete understanding of what is done with his or her data[40].

5.2. Ethical considerations

In order to enrich the definition of consent given in the law, we will take up one by one the different characteristics it cites: consent must be free, specific, informed and unambiguous.

The necessity of freedom implies that a request for consent to provide private data must include a real possibility of alternative in case of refusal. This may stand to reason, but what would be the point of asking for a student's consent to provide biometric data if he or she were unable to take the test if he or she refused?

---

[36] Article 29 Data Protection Working Party-WP260 2018, p. 18.

[37] Article 13 GDPR and Article 29 Data Protection Working Party-WP260 2018, pp. 14-16.

[38] Article 29 Data Protection Working Party-WP260 2018, p. 11.

[39] Article 29 Data Protection Working Party-WP260 2018, p. 11.

[40] Article 29 Data Protection Working Party-WP260 2018, p. 9.

Ethical analysis makes it possible to enrich the contribution of Law at this level. As we have said, ethics can help to refine our response to technical partners when the law remains somewhat vague. Indeed, the latter informs us of the obligation to provide a viable alternative but remains vague as to the definition of what constitutes a real alternative able to guarantee the free aspect of a consent.

What is actually the situation for TeSLA? The system asks the student if he/she wishes to be authenticated by the system using the modalities chosen upstream by the professor. It is therefore a question of agreeing on a combination of biometric / textual analysis instruments, in other words on a set of samples of data to be made available. TeSLA, as it was originally conceived, provides two possibilities:

- The teacher provides the possibility of an examination completely outside the context of TeSLA (for example, a classic face-to-face examination).

- The teacher allows the student to take the exam with another combination of TeSLA instruments.

We noted that this approach derived by the technical partners had certain shortcomings.
First, it consists in delegating a large part of the very functioning of the system to the teacher. They are faced with a system that would require a fairly substantial logistical effort in cases of massive refusals, whereas the purpose of the system is precisely to avoid the organizational burdens caused by face-to-face examinations. This aspect needs to be clarified for reasons of transparency towards future TeSLA user institutions. Indeed, it is important that they know what they will incur if consent is not given by the student. One thing that can be done at this level is to further clarify these aspects (the necessity to develop an alternative way of exam and the limitations of the internal alternative options) in the description of TeSLA to future customers, as well as clear warnings in the operating instructions. For the institutions, it is a question of being able to perceive how the system could be implemented in their own regulation.

Second, it is clear from our ethical investigation that a significant proportion of the students are unconvinced by the alternative system embedded in TeSLA. They believe that if they have little confidence in the way the system processes their data or in the reliability of the instruments, switching from one combination of instruments to another will not necessarily reassure them. Concerning this problem, we had suggested to the partners to standardize and clarify the uses that would be made by teachers by giving indications on the following aspects: Who can access to which data? For which purpose? How do TeSLA's instruments process data? These indications go beyond the simple question of consent but they would make consent more informed if they were put forward at the time of the request.

Finally, this second way of considering an alternative is ethically questionable because it does not guarantee equivalence criteria between students. Indeed, on

which legitimacy is based an examination that has been passed by students with different monitoring criteria? Various abuses are conceivable: students could consciously choose the method that makes it easier for them to cheat, or on the other hand they could feel aggrieved by having to take an exam with a heavier supervisory method than their classmates. This would impact the very legitimacy of the past examination, and by extension the reputation of the institution that proposes it.

The specificity of consent implies that the nature of the data and the way in which the data covered by it are used must be explicitly indicated. We stressed the importance of clearly defining how feedback is treated (more explanation about feedbacks in the next section).

The question of feedback and its processing will be dealt with more precision in the seventh section, but it is important to specify that the definition of this feedback processing affects in particular the quality of the request for consent. In this respect, we have insisted on the need to extend this concern for clarity in the request for consent to the way feedback are exposed and used (and not only basic biometric samples).

Regarding the need to have an informed consent, we fed the reflection with findings of our survey about students' concerns about their understanding of the system. These must be taken into account when writing the consent request in order to make it both user-centred and easier to access. Highlights from our findings include:

- The activation period of biometric instruments.

- The type of data that is collected (picture, voice recording...).

- The way the data is collected (the continuous aspect).

- And so, certain behaviors can be avoided to allow the instruments to correctly collect the necessary and sufficient data.

Consent is therefore an important issue to be addressed because it conditions the very use of the system. Indeed, the very purpose of TeSLA is to generate trust between professors and students. To do this, it uses biometric recognition instruments to identify students remotely. However, these instruments do not provide confidence in a purely mechanical or automatic way through their use. It is worth considering the potential drift of such a system if it claims to bring confidence to users through a strong and widespread monitoring system. Working on the transparency of consent makes it possible to avoid justifying ever greater and deregulated surveillance based on the need for trust.

However, a good request for consent is not limited to a transparent list of the private data collected and the work done with it. The system itself must operate clearly and unambiguously in order to submit a meaningful request for consent. This principle

probably applies to any system requiring private data, but is all the more important for TeSLA, whose biometric instruments provide feedback that teachers must interpret.

6. Transparency

The transparency obligation is a core requirement of the GDPR. After explaining this principle and its objectives, we focus on how this obligation imposes to the software developers the openness of their system. Finally, ethical considerations give a good overview of possible difficulties in users' understanding and therefore of the transparency efforts needed to guarantee the right to information.

6.1. Legal considerations

6.1.1. Principle and objectives

The objective of the transparency obligation is to strengthen the citizens' control over the processing of their personal data. The transparency of the data controller permits data subjects to understand the use of their information. In addition, this key principle allows individuals to effectively exercise the rights granted by the GDPR[41].

To respect the obligations for Member States to processed the personal data fairly, we assisted to the emergence of long and unintelligible general conditions of use. Needless to say, every citizen accepted them without understanding, or even knowing, what he/she was engaging with, without knowing that he/she had just exchanged aspects of private life for a service.

The GDPR intends to reinforce the transparency requirement. It is now clearly written in the text that transparency is an obligation for the data controller. Article 5 states that: "*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*".

Recital 39 adds: "*Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of*

[41] de Terwangne 2018, pp. 90-94.

risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing." .

Transparency promotes and develops the empowerment of citizens and is interpreted as a mean of enhancing the privacy of users and facilitating the exercise of their rights[42]. Furthermore, the obligation of transparency is intrinsically linked to trust. As stated by Article 29 Working Party, "*It is about engendering trust in the processes which affect the citizen by enabling them to understand and, in necessary, challenge the processes*"[43].

[42] Article 29 Data Protection Working Party-WP260 2018, p. 4.

[43] Article 29 Data Protection Working Party-WP260 2018, p. 4.

Fig. 1. Informations requirements

6.1.2. Transparency and openness

The obligation of transparency is often presented as the cornerstone of the data subject's right to information and a duty of communication of the controller. It includes:

- Providing information to the data subject in a clear and plain language, at the beginning and all along the processing of personal data. In addition, the data controller must adopt a proactive approach for providing information and not waiting for an intervention of the data subject[44] (see as detailed above and Fig. 1.).

[44] Article 29 Data Protection Working Party-WP260 2018, p. 6 and p. 18.

- The data controller has to give a permanent access to privacy information, even if there is no modification in the terms and conditions. In addition, the Article 29 Working Party encourages the data controller to provide express reminders, from time to time, to the data subject about the privacy notice, and where this is accessible[45] (see as detailed above).

However, the obligation of transparency indirectly entails other obligations for the controller and a certain openness of the system in order to permit the verification of compliance with the GDPR.
The duty of transparency has two faces. On the one hand, the data subject have some rights, such as the right to be informed, the right to have access to some information and the right to erasure. On the other hand, the data controller has to prepare himself/herself by technical and organisational measures, to answer to the data subject. It implies *de facto* to open the system to the data subject. These two faces are illustrated by Table 4.

Table 4. Right for the data subject and corresponding obligations for the data controller

Rights for data subject	Duty for data controller
Right of access	To give a secure and online access to one's personal data
Right to be informed	Transparency about the logic and how the system works
Right to have a human intervention and contest the decision	• Procedural rules • To receive a clear and comprehensive feedback from the tools
Right to erasure	To facilitate the deletion in all servers

This duty of transparency could be a constraint on the shoulders of the data controller, who must identify the type of persons concerned and the most intelligible way of fulfilling the obligation to inform. However, it could be also a decision-making tool for the data controller in the use and management of personal data. In order to

[45] Article 29 Data Protection Working Party-WP260 2018, p. 18.

fulfil its obligation of information, the data controller has to understand how the system works. Thereby, the data controller must know the limits of the tools used and can therefore take an enlightened decision on the basis of the outputs of the TeSLA system. Transparency then becomes, not only a legal constraint, but a real contribution in the academic procedure of decision-making in the case of suspicion of cheating by a student.

6.2. Ethical considerations

The GDPR gives the right to information as a fundamental prerogative, but this dimension needs to be further explored ethically. This will then make it possible to provide a richer contextual dimension, in a way to relate the standard legal definition of this right into a practical reality.

The GDPR's definition of the right to information is not totally satisfactory because it cannot (and this is normal for a legal definition) take into account the diversity of human behaviors. Indeed, the right to information implies a need of understanding on the side of stakeholders. Our ethical fieldwork gives us a good overview of possible difficulties in users' understanding and therefore of the transparency efforts needed to guarantee the right to information.

The comprehension problems demonstrated by our survey participants are diverse. On the student side, these concerns lie both in the understanding of biometric instruments and the architecture of the system and how it affects the teacher's judgment behind the scenes.

Although many factors may have influenced this lack of understanding regarding how the TeSLA instruments work (the lack of explanations received upstream, the sometimes confusing context that characterizes a test phase...), it is worrying to note how difficult it is for some to access the basic principles of these instruments. The capabilities of these instruments were sometimes overestimated, considered at a level that goes beyond simple authentication. For example, many students believed that the face recognition instrument was able to interpret their actions which is way more than only matching enrolment biometric samples with data samples collected during assessment activities. Some even thought that someone was watching them live via webcam. These interpretations led these students to ask themselves what behaviors were expected of them (should we stay in front of the screen during the entire activity or not? Should we remove the presence of sheets of paper on the desk?). These uncertainties potentially cause a form of anxiety about the system. Taking these understanding shortcomings into account is necessary to ensure the right to be informed in the context of TeSLA.

These aspects concern the understanding of the algorithmic underlying the system (the software attached to the instruments are black boxes from the TeSLA system perspectives), but the opacity that potentially blurs the vision of student users is not limited to them. The feedback that these instruments send back to the teachers is also a veil of opacity towards the students. Legal and ethical issues regarding the feedback will be addressed in the following section. We would like to stress the potential lack of access by students to these data (cfr: the "right of access"). Indeed, these feedback data are subject to the right of information. Students are seeking an opportunity to see how professors manage them and whether they are able to justify their possible charges with supporting evidence.

Another legal aspect that also concerned our research was the right to a human intervention and to challenge the decision taken on the basis of TeSLA's indications. The students' concerns, or even defeatism, about the difficulty to challenge a decision that would have been taken on the basis of the system led us to highlight the importance of implementing TeSLA according to the rules specific to each university. Of course, we could not study all the possibilities of interaction between TeSLA and internal regulations on a case-by-case basis, but we are contributing to the implementation of an instruction manual. This will contain general principles of use allowing universities to easily set up a clear modus operandi. By clarifying TeSLA's role in the teacher's judgment of his or her students, the notice should enable each student to challenge the charges against him or her and hold the teacher accountable if necessary.

The issue of transparency is crucial because it highlights a common dilemma in the development of such systems. On the one hand, it must be easily accessible in order to allow as many people as possible to use it (and this aim of "democratizing" university courses is an argument claimed by TeSLA project) and on the other hand the use of technical tools (here biometric instruments) necessarily leads to a certain complexity of the system. This complexity can hinder users with the least technological literacy (both from the teacher and student point of view).

In this case, the ethical approach raises questions that go beyond the scope of the Law. Beyond the processing of private data, there is the question of the usability of the system and its potentially discriminatory nature. Ethically speaking, it is obvious that it is necessary to ensure the greatest possible accessibility to it, whatever the level of technological literacy of the person. This is of course also linked to the question of trust that we have previously mentioned: how the system can claim to generate trust if it excludes some of the users to whom it potentially addresses? We have tried to favor an approach that would not simply consider that “people have to adapt to technologies, period” by the comprehension of their fears.

The use of TeSLA by teachers must be understood in terms of "clues". As TeSLA's feedbacks do not constitute self-evident evidence, a possible accusation of

cheating must be based on more solid materials than the mere presence of a litigious number returned by one of the biometric instruments.

As a result, TeSLA interacts with the cheating regulations previously in place in each university. On the institutional side, it is important to understand what TeSLA produces before integrating it. The latter already includes, in a way, a specific "definition" of what is considered as cheating. Authentication using face recognition implies, for example, that a third party cannot take the place of the student "in front of the screen" for the duration of the evaluation activity. However, TeSLA does not regulate the interactions that these two people would have outside the duration of the assessment, or even during the assessment (if speech recognition is not enabled, there is nothing to prevent them from talking during the activity).

Before any integration of TeSLA, the following two questions must therefore be asked by the institutions:

- What are the typical fraud situations facing our institution? After detailing them field by field (the way of cheating is not the same depending on the field of study, of course), institutions must look at which of these situations TeSLA potentially thwarts or not.

- Are the detections made by TeSLA instruments relevant to our institution? It is in fact the opposite question. The system user guide should contain a detailed description of each instrument and what it is capable of reporting. On the basis of this, the institutions will be able to see which instrument is potentially useful for them or not.

7. Feedback

The aims of this section are to explain the legal framework surrounding automated decision-making and the related rights for the students, in particular the right to obtain, on request, knowledge of the reasoning underlying data processing. A particular point of attention is the possibility of using the results given by the TeSLA system to profile students that are repeatedly cheating. It is also important for teachers using the software to understand the delivered indicators as well as how to interpret and integrate them into internal rules of each institution.

7.1. Definition

As showed in Fig. 2., Feedback consists of confidence indexes comparing enrolment sample(s) (of biometric or text-based data) with samples collected during an

activity for each learner. The feedback is classified by instrument (a tab by instrument) and showed chronologically for each activity in the case of biometric instruments (one index is sent for each sample collected every 30 seconds/1 minute more or less).

Each metric included in tables appear in green, yellow or red according to their value in comparison with a threshold. This aims to facilitate teachers' interpretation of these abstract numbers, giving a simple indication. However, even if the teachers are supposed to interpret freely these numbers, the thresholds and the coloration of feedback will influence his/her later decision and perception of learners' work.

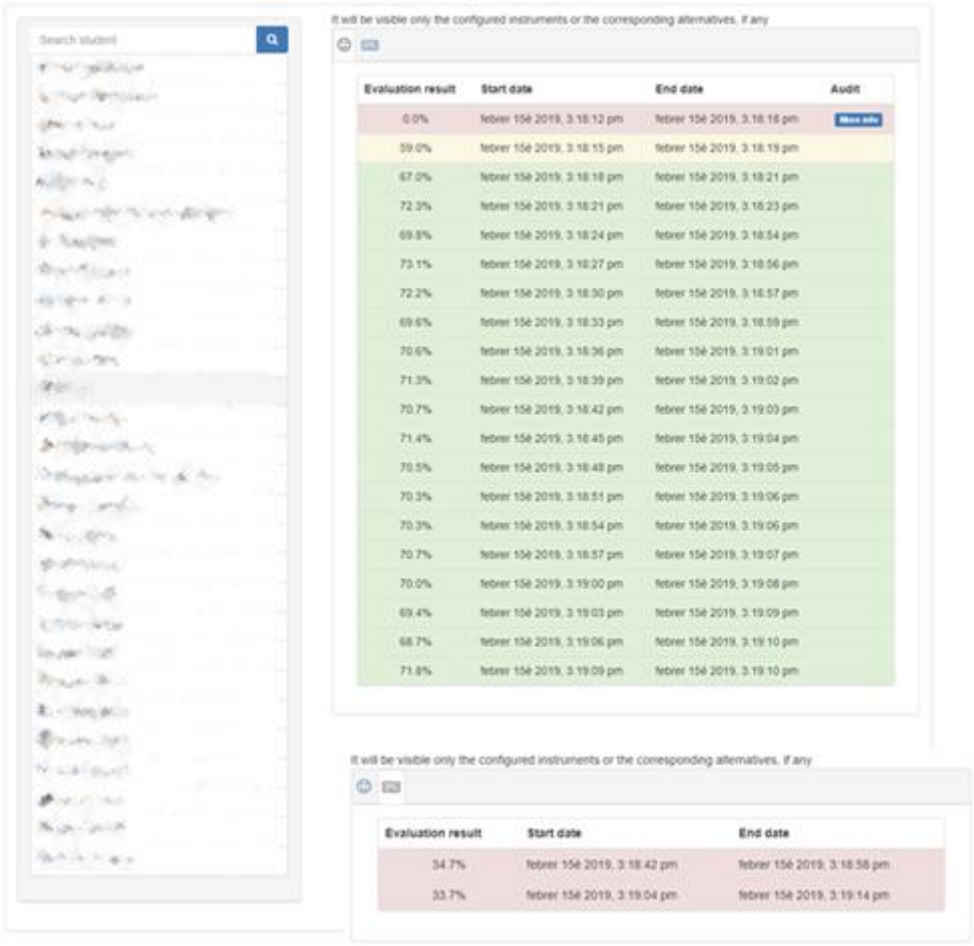

Fig. 2. Screenshot of Feedback interface

7.2. Legal considerations

The result given by TeSLA is a personal data in the sense that it is information relating to an identifiable person[46]. Consequently, all regulations relating to the protection of personal data must be respected.

7.2.1. Legal guarantees

The Article 29 Working Party defines the concept of automated decision-making as "*the ability to make decisions by technological means without human involvement. Automated decisions can be made with or without profiling*"[47].

The Article 29 Working Party is sensitive to a decision that has "*the potential to significantly influence the circumstances, behaviour or choices if the individuals concerned*"[48].
If by an algorithmic method the TeSLA system is able to determine a result of cheating, or at least a percentage of probability, of non-matching between the exam and the enrolment process, it seems that this can potentially affect significantly the student's situation in that it may lead to a refusal to grant the diploma or certificate.

In the TeSLA project, the collection and use of personal data from the learners are based on their freely given, specific and informed consent. The consent, that needs to be confirmed by an express statement and a positive action, is an exception that permits the use of automated decision-making. There are several safeguards. Firstly, the data controller has to inform properly the data subject about the existence of an automated decision-making[49]. They have the right to be informed about the logic involved, the explanation of the mechanism and how the system works. It is not mandatory to enter into details on the functioning of algorithms[50]. These information must be provided by the data controller when the data are collected. As a consequence, it does not concern information about how the decision was reached by the system in a concrete situation[51].

---

[46] Article 4.1 of the GDPR.

[47] Article 29 Working Party-WP251 2017, p. 8.

[48] Article 29 Working Party-WP251 2017.

[49] See articles 13 and 14 GDPR

[50] Article 29 Working Party-WP251 2017, p. 14.

[51] Wachter et al. 2016, pp. 82-83.

Secondly, students have the right to obtain a human intervention, to express their opinion and to contest the decision[52]. This is of a crucial importance considering the fact that special categories of personal data from students are used in the project. Recital 71 of the GDPR specifies that they need to have the possibility to obtain an explanation of the decision reached. It goes beyond a simple right of information as it requires to give an *ex post* information on the concrete decision. It implies for the data controller to understand and to be able to explain in a comprehensive way the algorithmic functioning of the system[53]. In the context of TeSLA, the teacher has to receive a clear and comprehensive feedback from the tools.
The possibility to obtain an explanation of the decision reached is not mandatory as it is in a recital and not in the article itself, but permits a real and meaningful possibility to express an opinion and to decide to contest the decision or not. The Article 29 Working Party insists on the role of the controller in the transparency of the processing[54].

Thirdly, the data controller must ensure that someone who has the authority and ability to remove the decision will review the automated decision[55].

Fourthly, the Article 29 Working Party advises the data controller to carry out frequent assessments on the personal data collected and used. The curacy of the personal data and the quality of the tools used for the processing are core elements of the lawfulness of the system. This is particularly relevant when special categories of personal data, such as biometrics, are processed. The data controller, with the help of the data processor, should not only check the quality and prevent errors or inaccuracies at the time of the collection and the technical implementation of the system but in a continuous way as long as the data is not deleted or anonymized[56].

Beside the right not to be subject to and automated decision, the right of access for the student includes the right to know "*the existence of automated decision-making (…) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*"[57]. It implies for the data controller to understand and to be able to explain in a comprehensive way the algorithmic functioning of the system but is not a plenary algorithmic transparency[58].

---

[52] Article 22.3 of the GDPR.

[53] Wachter et al. 2016, pp. 92-93.

[54] Article 29 Working Party-WP251 2017.

[55] Article 29 Working Party-WP251 2017, p. 10.

[56] Article 29 Working Party-WP251 2017, pp. 16-17.

[57] Article 13.2 of the GDPR.

[58] See Wachter et al. 2016.

In the TeSLA context, the teacher has to receive a clear and comprehensive feedback from the tools. So there is a right for the students to know the data being processed, the criteria and the importance of each criteria but it is not a real full algorithmic transparency because we need also to take into account potential intellectual property rights on the software and trade secret on algorithms[59].

The modernization of the Convention 108+ gives the right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her[60].

In conclusion, if the teacher or the institutional committee have suspicions, it is important that they are able to explain to the students how the system works and to give, on student's request, knowledge of the reasoning underlying the data processing and the possibility to obtain an explanation of the decision reached.
To respect the right to rectification and to object, it is also important that the student can demonstrate that his or her behaviour was not optimal for the functioning of the system but it is not for that much a case of fraud.

7.2.2. Feedback and profiling

The aim of this subsection is to consider the possibility to use the feedback given by TeSLA system for profiling activities

According to article 4.4 of the GDPR, profiling means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

If the data controller wants to collect the repeated cases of fraud from the same student with TeSLA (the biometrics data will be used to certify the identity of the student), there is no explicit and clear mention of profiling or collection of personal data in order to combine them with others to establish a certain profile of a student in the consent form. Furthermore, it is important to keep in mind that the consent can never legitimate a disproportionate processing[61].

We can take a second hypothesis: If the envisaged activity is the establishment of blacklists[62] with identities of students that are considered as cheaters, there is no

[59] de Terwangne 2015, p. 107.

[60] Article 9.1 c) Convention 108+.

[61] Belgian Commission for the protection of privacy 2008, p. 10.

[62] The Article 29 Working Party defines a blacklist as : " *the collection and dissemination of specific information relating to a specific group of persons, which is compiled to specific*

prohibition as such for that. However, these listing need to be done in accordance with the GDPR; transparency, data minimization, exercise of the right of access, information to the data subject on the fact that he/she is on the list, limited time of conservation, accuracy and mechanisms to avoid errors in the identification of students included and errors in the information mentioned and a secured access[63].

Nevertheless, if the database needs to contain also biometrics data to prove the identity of the learner, there is no explicit consent from the students. Consequently, the data controller has no ground to legitimate such activity. Moreover, this is subject to the condition that the processing of personal data is not contrary to the exercise of the fundamental right to education and therefore could not be regarded as unlawful[64].

7.3. Ethical considerations

Addressing the feedback system is important because we do not know in advance how teachers will use this feature. This raises questions in terms of fair treatment of students. How can an accusation of cheating be justified in front of them if the teacher is not able to explain how he used the system? How can we avoid a totally hazardous use of the system that could produce uncontrollable effects of judgement? This is a major issue regarding the second aspect cited by the legal approach: the right to have a human intervention.

One of the topics we discussed with the professors during our ethical survey was their understanding and use of these index tables. Five out eight teachers found the feedback hard to understand and had difficulties to answer the following questions: What does each number mean? How are you supposed to interpret them concretely? What does the green/yellow/red coloration of the feedback really mean? Their answers were often unclear, and based largely on the idea that this has to be judged on a case-by-case basis. Some others, however, complained head-on about the way feedback was presented in the interface. The comments of some professors even suggested that they would use this feedback in a way that goes beyond the framework initially imagined in the project, for example by developing a long-term student profiling based on the confidence indexes returned by the TeSLA instruments. Then, it was necessary to intervene ethically on this aspect of the system.

---

criteria according to the kind of blacklist in question, which generally implies ad-verse and prejudicial effects for the individuals included thereon and which may be discriminate against a group of people by barring them access to a specific service or harming their reputation" ; Article 29 Working Party-WP65 2002, pp. 2-3.

[63] See article 5 and Recitals 39 and 50 of the GDPR. See also, Article 29 Working Party-WP65 2002, pp. 8-12.

[64] Burton and Poullet 2006, p. 109.

A dilemma has arisen in the face of this observation: what should we do to make the use of feedback less ambiguous and what is the status that should be attributed to them? Should they have decision-making and justification powers or are they just indicators that need to be informed by other evidence?

This dilemma is materialized in the way trust indicators are presented in the teacher's interface. These are exposed in a very raw way, as we have explained. However, some professors imagined that they would actually be presented in a more aggregated and summarized form, allowing for more immediate use and requiring less interpretation work. The advantage of this second way to perceive feedback would be to reduce the random aspect of teachers' understanding of the indexes. On the other hand, this version of the system would tend to “pre-decide” who is a cheating student and who is not in the teacher's place, and so contribute to an even more automated decision process. It is to avoid this pitfall and leave each institution free to decide how to use the system that the project has kept a very rough exposure of the data.

However, it is our ethical responsibility to insist on the limits of these indexes (that they must be assisted with other means to justify a suspicion of fraud) and to give advice on the use of these index tables. These should help to answer the following questions: What to consider when there is a whole spot with numbers written in red on the interface (which would correspond to a long while without a correct matching)? What could be the reasons for red numbers outside the attempt to mislead the system (e.g., a non-optimal biometric data collection environment)? On the other hand, which cheating scenarios seem to be difficult to deal with via TeSLA?

TeSLA's feedback raises the question of how to interpret the results returned by biometric instruments in the context of continuous authentication. Indeed, the specificity of TeSLA is that biometrics is not used from time to time (for example, in an airport to authenticate passengers when crossing the border) but throughout an activity. Biometrics, in the context of TeSLA, goes beyond its usual role of authentication, in fact: student behaviour can be attributed to certain feedbacks. What does a negative result mean? That the student was replaced? That someone else passed in front of the webcam field? That the student went away for a few moments?

This diversion from the more "traditional" uses of biometrics raises many questions. Such as the fact that use of biometrics in decision-making could lead to random and arbitrary forms of decisions: it is difficult to know how professors will deal with such feedbacks if they are not provided with a minimum of clarification.

In this regard, it should however be noted that an argument in favor of the project is its flexibility and the fact that it does not impose a way of using it. The system provides "clues" that the student may have cheated (the teacher must then still prove it with means that exceed TeSLA). The feedbacks do not therefore say head-on "this

student cheated", teachers are free to interpret feedbacks differently depending on the context. Nonetheless, this argument in favor of TeSLA may mask the potential pitfalls of a completely deregulated use. If no minimal standardization of the use of TeSLA feedback (e. g. through a user manual for teachers) is developed, how can students trust the decisions that will be made using the system?

8. Conclusions

TeSLA involves the processing of personal data when using face recognition, voice recognition and keystroke dynamics to verify student's identity during distance examinations and pedagogical activities. In this chapter, we focused on three privacy aspects: the need to have a valid consent, the transparency principle and the feedback given by the system to the user.

Firstly, as TeSLA is working with a special category of personal data, the GDPR requires an explicit consent. The consent form established during the project includes information that helps the students understand what will be done with their personal data. The consent form must be completed and approved by each student. The consent is also specific because the students receive a clear information about the privacy policy, which is separate from other texts, and the students have to click to give their consent. From ethical surveys, we learned that students require clear information about who can have access to their personal data, the activation period of biometrics instruments, the continuous or non-continuous collection of personal data and the behaviors to be avoided to ensure the proper functioning of the system. This information has to be given to the students to have a real and informed consent and to adopt a user-centric approach.

Secondly, the transparency principle involves a right, for the data subject, to receive information, and a corollary obligation for the data controller to provide information in a clear and plain language. The information should be given at the beginning and all along the processing of personal data. While the GDPR establishes a list of information to be provided, ethical analysis could highlight some particular requirements from the data subject. In TeSLA, the students seem to have difficulties to really understand how the system is working and what the TeSLA possibilities are. Ethical considerations may therefore justify the provision of additional information to that required by law, in order to ensure a non-discriminatory use of the system.

Thirdly, we focused on the feedback given by TeSLA and the teachers that used it. A concern is that the students cannot effectively exercise their right to object if they do not receive information about how the system works and how the decision was made by the professor. Accordingly, a decision had to be made between giving raw information and leaving the interpretation of these feedback to teachers, on the one hand, and giving immediately interpretable results, on the other hand. As this

second option would lead to pre-decide for the teachers, it has been decided to keep a very rough exposure of the data.

From the above, it stems that if the law regulates the processing of personal data, ethical considerations make it possible to concretize the rules imposed by the GDPR in order to facilitate the integration of TeSLA into an institution and its pedagogical activities.

References

Akrich, M. (1987). Comment décrire les objets techniques?, *Techniques et culture*, (9), 49-64.

Burton, C. & Poullet, Y. (2006). Note d'observations à propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires, *Revue du droit des technologies de l'information*, 102-122.

de Terwangne, C. (2015). La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. In C. Castets-Renard (Ed.). *Quelle protection des données personnelles en Europe ?*, 425-451, Larcier.

de Terwangne, C., Rosier, K. & Losdyck, B. (2017). Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ?, *Journal de droit européen,* 302-316.

de Terwangne, C. (2018). Les principes relatifs au traitement des données à caractère personnel et sa licéité. In C. de Terwangne & K. Rosier (Eds.), *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie*, 87-142, Larcier.

Feenberg, A. (2012). *Questioning technology*, Routledge.

Kaufmann, J.C. (2011). *L'entretien compréhensif*, Paris: Armand Colin.

Wachter, S., Mittelstadt, B. & Floridi, L. (2016). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*,76–99.

Article 29 Working Party, Working Document on Blacklists, 3 October 2002, WP65.

Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03 October 2017, WP251.

Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 10 April 2018, WP259.

Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 11 April 2018, WP260.

Article 29 Data Protection Working Party, Opinion 03/2012 on developments in biometrics technologies, 27 April 2012, WP193.
Belgian Commission for the protection of privacy, Opinion 17/20008 on biometrics data processing, 9 April 2008.

Glossary

Biometrics data Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person (Article 4.14 of the GDPR).

Consent Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4.11 of the GDPR).

Data controller The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4.7 of the GDPR).

Data processor The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4.8 of the GDPR).

Data subject The identified or identifiable natural person.

Personal data Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4.1 of the GDPR).

Processing Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4.2 of the GDPR).

Profiling Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4.3 of the GDPR).

Pseudonymisation The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4.5 of the GDPR).

Index

Acronyms list

GDPR General Data Protection Regulation

HEI Higher Education Institution

LTI Learning Tools Interoperability

TEP TeSLA e-Assessment Portal

TIP TeSLA Identity Provider

VLE Virtual Learning Environment