المؤتمر العلمي الدولي السابع لكلية الاعمال بالتشارك مع عمادة البحث العلمي والدراسات العليا بعنوان

رقمنة الاعمال والبحث العلمي: رؤى مستقبلية

Legal protection of students' personal data

الحماية القانونية للبيانات الشخصية للطلاب

Hamouti Nadia: Professor at university Sidi Mohamed Ben Abdellah

El bakouhi Safae: Phd student at university Sidi Mohamed Ben Abdellah

safae.elbakouhi@usmba.ac.ma

Abstract:

The legal protection of student's personal data is a crucial priority. Educational institutions must obtain informed consent from students before collecting, processing or sharing their data. Robust security measures are needed to prevent unauthorized access, and data collection must be restricted to what is strictly essential, encouraging data minimization. Transparency of privacy policies is essential to establish trust, and students are guaranteed rights of access and rectification. Data retention periods must be limited, followed by secure deletion. Regular evaluations are necessary to adjust policies in line with technological developments and legal changes, ensuring solid legal protection of student personal data.

ملخص:

تُعد الحماية القانونية للبيانات الشخصية للطلاب أولوية حاسمة. يجب على المؤسسات التعليمية الحصول على موافقة مستنيرة من الطلاب قبل جمع بياناتهم أو معالجتها مشاركتها. هناك حاجة إلى اتخاذ تدابير أمنية قوية لمنع الوصول غير المصرح به، ويجب أن يقتصر جمع البيانات على ما هو ضروري للغاية، مما يشجع تقليل البيانات إلى الحد الأدنى. شفافية سياسات الخصوصية ضرورية لإرساء الثقة، ويجب ضمان حقوق الطلاب في الوصول إلى البيانات وتصحيحها. يجب أن تكون فترات الاحتفاظ بالبيانات محدودة، يليها الحذف الآمن. من الضروري إجراء تقييمات منتظمة لتعديل السياسات بما يتماشى مع التطورات التكنولوجية والتغيرات القانونية، بما يضمن حماية قانونية قوية للبيانات الشخصية للطلاب.

Introduction

Since the early 2000s, Morocco has introduced reforms to strike a balance between security and privacy. The protection of privacy is a key issue for Morocco, and the reforms underway are designed to strengthen guarantees for citizens. Privacy protection reforms are constantly evolving to adapt to new technologies and new security challenges.

Thanks to the constitutional reform of July 2011, Morocco has taken a stand to strengthen the protection of citizens against the abusive use of automated personal data processing, and has strengthened its legal and institutional arsenal through several laws and institutions, in particular Law No. 09-08 on the protection of individuals with regard to the processing of personal data, and the National Commission for the Supervision of Personal Data Protection, which is the national institution responsible for ensuring the protection of personal data in Morocco.

However, there are concerns about the protection of personal data in relation to this, as massive data analysis can reveal very personal information about individuals, threatening their privacy. It is therefore crucial to put in place regulations and security measures to ensure that personal data is used responsibly and in a way that respects the privacy of individuals.

On the other hand, the development of data volumes and the intensification of the exploitation of this data by companies have radically transformed the digital economy. This transformation has not been without first changing the relationship that users have with their personal data. More profoundly, it is the image of privacy that seems to have been turned upside down.

Problem, importance and objectives of the research

Our subject is of interest because of the efforts made by the Moroccan legislator to promote the effectiveness and efficiency of the legal arsenal ensuring the protection of personal data.

The underlying problem concerns the effectiveness of Moroccan legislation on the protection of personal data, with a view to ensuring adequate protection of this sensitive data, which leads us to ask the following question: How can we ensure adequate protection of students' personal data in Morocco by assessing the gaps in current legislation and proposing measures to strengthen the protection of this sensitive data?

To address this issue, we will use an analytical methodology that involves examining the legal framework relating to the protection of personal data in Morocco.

On the basis of this observation, it would then be legitimate to consider the legal framework for the protection of students' personal data, and secondly we will deal with offences and sanctions relating to personal data.

Results and discussion

1- The legal framework for protecting students' personal data

1-1 Conditions for processing personal data

Several conditions are taken into consideration to ensure that students' personal data is processed. These conditions are generally the consent of the student**,** *the purpose of the processing and the principle of proportionality, fairness and lawfulness in the processing as well as* limiting the duration of the processing.

With regard to ***student consent***, a manifestation of free, specific and informed will, by which the data subject accepts that personal data concerning him or her may be processed. In accordance with article 4 of **Law 09.08 in Morocco**, personal data may only be processed if the data subject has given his/her consent to the operation or operations envisaged.

As regards **the purpose of the processing and the principle of proportionality.**

Personal data must be processed for a clearly defined purpose. Personal data may only be collected for a specific purpose and must not be further processed in a way that is incompatible with that purpose. The principle of proportionality implies that the personal data collected must be appropriate to the purpose of the processing. Data must therefore be "*adequate, relevant and not excessive in relation to the purposes for which they are further processed*" (Article 3, law 09.08).

As regards **fairness and lawfulness in processing, this is** a fundamental principle that is mandatory for any processing operation involving personal data (Basdevant, 2019). We must ensure that data is collected fairly, i.e. that data subjects are properly informed and that their rights are respected. Data must also be protected against any external attack by putting in place the human and technical means to protect it.

And lastly, for **the limitation of the duration of processing**, Data must be kept for no longer than is necessary to achieve the purposes for which it was collected.

1-2 Effects of collecting personal data

About students

When students' data is collected, they must be informed in particular of the identity of the data controller, the purposes of the processing, the recipients of the data and the existence of a right of access, rectification and deletion. Students also have the right to object to the processing of their personal data for legitimate reasons. This information must be mentioned on any medium intended to collect users' personal data:

- Compulsory consent: the right of students to give or refuse consent allows individuals to retain control over their private lives and their personal data;
- the right to information when data is collected: all students have the right to be informed in a precise, express and unequivocal manner of the use or storage of data concerning them. This right to information also covers the data controller collecting the data and the intended recipients (Türk, 2007);
- the right of access: this right is recognised by article 7 of the law **(law 09.08)** and allows any person to access information concerning him or her in order to ensure that it is accurate;
- the right of rectification: in addition to the right of access, this enables students to demand that information concerning them be rectified, particularly if it is inaccurate or incomplete;

- the right of deletion: this enables students to demand that information concerning them be deleted;
- the right to object: this allows students to object to their data being collected and used.

Data controller

The data controller must comply with the obligations set out in the Law **(Law 09.08)** and implement appropriate technical and organisational measures to protect the data collected. These measures must ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

Data protection therefore does not stop at students' rights alone, but also obliges the collector to put in place a high-performance information and security system in order to avoid loopholes in the protection of personal data (Kettani, 2020).

2- Offences and penalties relating to personal data

2.1 Infringements

The following are considered as breaches of **law 09.08** :

- any processing that undermines public order, security, morality or decency;
- the implementation of processing without the required authorisation or declaration;
- refusal of the right of access, rectification or opposition;
- any incompatibility with the declared purpose;
- failure to comply with the data retention period;
- failure to comply with data processing security measures;
- failure to obtain the consent of the data subject, particularly in the case of direct marketing for commercial purposes, with increased penalties in the case of sensitive data;

- any transfer of personal data to a country that is not recognised as providing adequate protection;
- any hindrance to the exercise of the supervisory functions of the National Data Protection Supervisory Commission;
- any refusal to apply the decisions of the National Data Protection Supervisory Commission .

2.2 Sanctions

-Without prejudice to civil liability towards persons who have suffered damage as a result of the offence, anyone who implements a personal data file without the declaration or authorisation required under Article 12, or who continues to process personal data despite the withdrawal of the receipt for the declaration or authorisation, shall be liable to a fine of between DH10,000 and DH100,000. (Article 52).

- Any controller of personal data who refuses the rights of access, rectification or opposition provided for in Articles 7, 8 and 9 shall be liable to a fine of between DH20,000 and DH200,000 per offence.

- Anyone who: - retains personal data beyond the period stipulated by the legislation in force or that stipulated in the declaration or authorisation; - retains the aforementioned data in breach of the provisions of article 3 of this law, shall be punished by imprisonment of between three months and one year and a fine of between Dhs 20,000 and Dhs 200,000, or by one of these two penalties only. The same penalties shall apply to the processing, for purposes other than historical, statistical or scientific purposes, of personal data kept beyond the period referred to in the first paragraph. (Article 55).

- Any person who processes personal data in breach of the provisions of Article 4 shall be liable to imprisonment of between three months and one year and a fine of between Dhs 20,000 and Dhs 200,000, or to one of these two penalties only (Article 56).

- Any person who, without the express consent of the persons concerned, processes personal data which, directly or indirectly, reveal the racial or ethnic origins, political, philosophical or religious opinions or trade union membership of persons or which relate to their health, shall be punished by imprisonment of between three months and one year and a fine of between DH50,000 and DH300,000, or by one of these two penalties only. The same penalties shall apply to anyone processing personal data relating to offences, convictions or security measures (Article 57).

- Any person who transfers personal data to a foreign State in breach of the provisions of Articles 43 and 44 of this Act shall be liable to imprisonment of between three months and one year and a fine of between Dhs 20,000 and Dhs 200,000, or to one of these two penalties only. (Article 60).

- Any controller, subcontractor or person who, by virtue of his or her duties, is responsible for processing personal data and who, even through negligence, causes or facilitates the improper or fraudulent use of the data processed or received or communicates it to unauthorised third parties, shall be punished by imprisonment of between three months and one year and a fine of between Dhs 20,000 and Dhs 200,000, or by one of these two penalties only. The court may also order the seizure of the equipment used to commit the offence and the deletion of all or part of the personal data forming the subject of the processing that gave rise to the offence. (Article 61).

The law sets out the civil and criminal penalties applicable, which in the event of a repeat offence may include up to four (4) years' imprisonment and a fine of 300,000 Dirhams.

Where the perpetrator of one of these offences is a legal entity, and without prejudice to the penalties that may be applied to its directors, the fines may be doubled (article 64).

Conclusion and recommendations

We must stress the need to strengthen good governance within the campuses of the institutions in general and within the National Supervisory Committee for the Protection of Data of a Particularly Personal Nature. To begin with, it is essential that the necessary human and financial resources are available for legal proceedings.

Duplication of the roles of the members of the National Data Protection Supervisory Committee must be avoided in order to ensure that they make the maximum effort in the Committee's activities. They also face a large number of organisational challenges, as they have to learn a new profession quickly and keep up with the frantic renewal of technologies, responding professionally to requests and trying to instil a new culture among citizens. A more transparent and open commission must be envisaged for citizens. In fact, while the latter pursues an awareness-raising strategy through radio advertisements or agreements signed with specific sectors when these activities were not external is sufficient given the lack of human and financial resources. It is therefore necessary to remedy this shortcoming in order to strengthen the image of the National Commission for the Protection of Personal Data. For their part, citizens must adapt to the new regulations on the protection of personal data.

With regard to the challenges posed to the implementation of Convention No. 108 and the Budapest Convention of the Council of Europe, the application of Convention No. 108 of the European Council and its additional protocol on Morocco will require several

Legal and institutional reforms. Initially, as mentioned above, Law 09-08 excluded data collected in the context of defence and security activities covered by its scope, and the law had to be amended to comply with Convention 108. In addition, the Kingdom of Morocco had begun the process of acceding to the Budapest Convention, but before ratifying its accession it had to put an end to its creation of a specialised investigation unit and make legislative amendments, in particular to the Code of Criminal Procedure.

As far as the school sector is concerned, transparency and communication are essential. When schools clearly explain to students and their families what data is being collected, for what purpose and how it is being used, this helps to establish a climate of trust. Families must feel informed and able to give their informed consent to the collection and processing of their children's data.

If families feel that their personal data is not being adequately protected or is being used inappropriately, this can lead to concerns about the confidentiality and security of their children's personal information. It can also damage the relationship of trust between pupils, families and the school.

It cannot be repeated often enough, but it is essential that schools adopt robust protection practices (François, 2021). These practices must guarantee security, confidentiality and respect for individual rights.

To protect personal data: the essential behaviours to adopt are as follows:

Raising awareness and training those involved in education; Regular training sessions can be organised to explain good practice in data collection, use and protection. These sessions are aimed at all those involved in a school: teachers, administrative staff and management.

Implement data confidentiality and security policies; A clear policy on the collection, use and storage of data within a facility helps to protect data. These policies can include security measures such as password management within the establishment.

Use data protection technologies (Gosselin, 2019); Technologies such as data encryption, anonymisation and pseudonymisation enhance data security. Encryption makes data unreadable to any unauthorised person. Anonymisation and pseudonymisation reduce the risk of individuals being identified from the data collected.

Monitoring data collection and processing practices: A data protection strategy may work at a given moment. However, there is no guarantee that this strategy will work in the medium or long term, particularly in the light of technological advances. It is crucial to put in place monitoring and audit mechanisms to evaluate practices on an ongoing basis. This may include periodic reviews of confidentiality policies, security assessments of IT systems and internal or external audits of data management processes.

References :

- Adrien Basdevant , "Data, the new engineering of power, what consequences for the rule of law?", AI and Law Breakfasts conference, Council of Europe, 2019.

-Alex Türk , International Conference of Data Protection Commissioners in London, CNIL, Rapport d'activités 2006, Paris, La Documentation française, 2007.

- Camille Gosselin , "La police prédictive - enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique", Institut d'Aménagement et d'urbanisme d'Ile de France, 2019.

Cazals François , Cazals Chantal, "Intelligence artificielle: L'intelligence amplifiée par la technologie", Ed. De Boeck Supérieur, 2021.

-- Law no. 09-08 promulgated by dahir no. 1-09-15 of 18 February 2009 - 22 Safar 1430, on the protection of individuals with regard to the processing of personal data

- Marine Kettani , "*Predictive policing and rule of technology*", Webinar AI and Law Breakfasts, organised by the Council of Europe,2020.