PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021
162

LATE ADOPTION OF PREVENTIVE MEASURES OF ONLINE PRIVACY IN MEXICAN AND COLOMBIAN UNIVERSITY STUDENTS

Carlos Arturo Torres-Gastelú
University of Veracruz, Mexico
E-mail: ctorres@uv.mx

Abstract

One of the educational challenges faced by Latin American universities is the development of digital citizenship competence in their students on issues of digital identity, security and privacy online. The aim of the study was to identify the perception of Mexican and Colombian university students towards the preventive measures of online privacy. For that purpose, a mixed-cut study was carried out. For the quantitative part, a survey made up of 20 items was applied to 1,245 university students. Meanwhile, for the qualitative part, 42 university students were asked to answer open questions. The quantitative analysis was carried out using descriptive and inferential statistics for data by country and gender. In order to test the hypotheses about the existence of significant differences, the Kruskal-Wallis test was chosen. While for the qualitative part, the university student responses were transcribed, the information was organized, and the main contributions of the students were presented. The results indicate that Mexican and Colombian university students have a favorable attitude towards preventive measures of online privacy. No significant differences were detected in the items on preventive measures of online privacy with respect to the variables Country, and Gender. The stories of the university student show a late development in the attitudes and skills regarding preventive measures of online privacy that begins with entering university, and that is consolidated over time. In addition, inconsistencies were detected between the favorable attitude expressed by students towards a broad use of online care with respect to the informants' narratives.

Keywords: *comparative studies, digital competence, digital citizenship, online privacy, university students*

Introduction

The development of digital competence in the educational community becomes the vehicle that encourages the training of students who can act as responsible digital citizens. In this sense, one of the educational challenges faced by Latin American universities is the development of digital citizenship competence in their students on issues of digital identity, security and privacy online. Therefore, identifying the perception of university students towards online privacy preventive measures allows providing information for the design of institutional educational strategies to improve digital competences of the students.

Digital competence is the "set of knowledge, skills, attitudes, strategies and values what are required when using ICT and digital media to perform tasks, solve problems, communicate, manage information, collaborate, create and share content, and build knowledge…" (Ferrari, 2012, p. 43). Through the European project DIGCOMP, a common framework of digital competences based on knowledge, skills and attitudes is proposed. It encompasses five areas: information, communication, content creation, security, and problem solving. With regard

https://doi.org/10.33225/pec/21.79.162 ISSN 1822-7864 (Print) ISSN 2538-7111 (Online)

to safety, it implies the protection of devices, personal data, health and the environment or environment (Ferrari, 2013).

In the same way, other international organizations such as ISTE (International Society for Technology in Education) have developed standards to help educators and educational leaders around the world prepare students to prosper in work and life. In this standard there is an item on the development of digital citizenship in students: The ISTE standard states that "Digital Citizen Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act in ways that are safe, legal and ethical". Two key aspects of the standard are closely related to online privacy: "Students manage their digital identities and reputations within school policy, including demonstrating an understanding of how digital actions are never fully erasable"; and also "Students demonstrate an understanding of what personal data is and how to keep it private and secure, including the awareness of terms such as encryption, HTTPS, password, cookies and computer viruses..." (ISTE, 2016).

In the cases indicated, both the European standard (DIGCOMP) and the United States (ISTE) highlight the relevance of the development of digital competence in both teachers and students, including aspects related to security and privacy management digital. Hence, the university understood as an institution that generates social inclusion, has the responsibility to assume the commitment that the management of digital skills implies in its academic community and in the society in which it is immersed. Likewise, it should be considered as one of the fundamental professional competencies in the profile of the university graduate. According to these international standards, the development of digital competences of both teachers and students in any educational institution includes the assimilation of protection mechanisms on aspects of security and privacy online.

Various researchers pointed out that the expression of online privacy is related to the establishment of controls over personal information, as well as the freedom to decide when and how to disclose certain information to others, determination of being able to control the information (Herrera-Aguilar and Sepulveda, 2018; Saldaña 2007). In this way, security is distinguished as the general measures to protect information, while privacy is related to the visibility of personal information and the content that is published, as well as the people with whom they interact and are authorized to share information.

According to Matzner et al. (2015), Internet users rarely implement privacy and data protection strategies, so online privacy literacy emerges as a potential solution for this topic. In this way, there was an increasing attention to identify the individual´s skills and knowledge to navigate the Internet safely and responsibly. For instance, Morrison (2013) found that the level of literacy was rather low, and that people often overestimated their knowledge. Meanwhile, Park (2013) analyzed three dimensions of online privacy literacy and found that higher levels in all three dimensions predicted data protection.

Mansur (2018) proposed a comprehensive model of online privacy literacy that outlines several factual privacy knowledge areas, privacy-related reflection abilities, privacy and data protection skills, and privacy-related critical thinking abilities. Factual privacy knowledge is related with: (1) Knowledge about data collection, data analysis, and data sharing practices of online service providers; (2) Knowledge about data collection and surveillance practices of institutions and governments; (3) Technical knowledge about privacy and data protection; (4) Knowledge about privacy and data protection law; (5) Knowledge about horizontal dynamics and related privacy risks.

Privacy related reflection ability is related with: (1) Ability to reflect privacy needs in different online environments; (2) Ability to identify privacy risks in different online environments; (3) Ability to reflect and evaluate one´s own behavior and relation to one´s privacy needs. While Privacy and data protection skills are related with: (1) Awareness about and implementation of data parsimony as a form of passive privacy regulation; (2) Implementation

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

of preventive data protection strategies on the vertical level; (3) Privacy-related media selection in light of privacy-affecting characteristics of different media; (4) Implementation of platform or media-specific privacy and data protection strategies. Finally, Privacy-related critical ability is related with: (1) Ability to critically analyze and question societal structures, processes, norms, and practices related to privacy; (2) Realization of social responsibility and implementation of practices that can influence individual and/or societal change.

In this regard, in a study published by Chamarro et al. (2016), the researchers found three privacy patterns: protective, in which users only receive messages from friends and from friends of friends; restricted, in which teens are open to meeting new friends; and exposed, which highlights the exhibition of information and content open to the entire public. In the same way, Herrera-Aguilar and Sepulveda (2018) identified in their study four categories that collected the reflection on how students handle privacy on the Internet. Most of the participants refer to an informative self-management; another significant part points to the implementation of a regulation and a self-regulation; a third widely supported position is the impossibility of privacy on the Internet; finally, a small part indicates the importance that should be given to it for full use of the different devices on the network.

Research Problem

Various institutions such as UNESCO, UNICEF, and the OECD recognize that digital security is a difficult challenge in all areas, particularly in the generation of digital competences in both teachers and students so that they can interact digitally in a safe and responsible way. In the same way, educational institutions in various countries have recognized the relevance of online privacy both within school and outside of it (Gallego-Arrufat et al., 2019). This recognition of the relevance of online privacy in students is manifested in aspects such as the use of protection and prevention measures for their personal data as well as avoiding online risks (harassment, virtual intimidation, among others).

In the Latin American context, there is a need for digitally competent teachers so that they can train their university students to act as responsible digital citizen (Gisbert et al., 2016; INTEF, 2016; Llorente, 2008; Lugo and Ruiz, 2016; Maris et al., 2008; Salinas and Silva, 2014; Selwyn, 2013; Silva et al., 2016; Suárez et al., 2010). In this sense, Morales et al., 2020 has pointed out that the greatest challenge in many of the Latin American countries is that educational institutions sponsored by a national educational public policy include in their teacher training programs, the development of digital competence, its evaluation, and its eventual certification.

Few studies have focused on the development of online privacy and security competence in university students, or on the training of teachers on this topic. Instead, an important part of the literature has focused on the assessment of technological or information literacy. In this sense, research by Yan (2009) and Shin (2015) have highlighted that both students and teachers do not receive sufficient training on issues of security and privacy online.

The current Latin American Society characterized by a gradual but growing adoption of a digital culture requires useful teachers, experts, and oriented to train critical and responsible citizens. This situation has also been reported in other regions of the world. Various studies have pointed out the need for educational institutions to adopt a coherent approach that ensures training to promote safety as a high priority issue in education, especially in teacher training programs (Barrow and Heywood-Everett, 2006; Woollard et al., 2009; Chou and Peng, 2011; Engen et al., 2015; Shin, 2015).

De-Waal and Grösser (2014) have analyzed the level of mastery of students and teachers towards topics related to digital security. These researchers found that the two groups analyzed showed a low level of mastery on these topics. For its part, Gallego-Arrufat et al. (2019) have

highlighted the need to strengthen the development of digital competences oriented to security and privacy in university teachers with a view to transmitting these knowledge and skills to their students so that they can perform as responsible digital citizens.

Hence, a growing need has been revealed to develop both training courses for teachers and the adaptation of curricular plans in universities to include specialized topics and subjects that allow the development of competence in security and digital privacy both in teachers as well as in students. (Chou and Peng, 2011; Chou and Chou, 2016; Engen et al., 2015; Shin, 2015).

Morales et al. (2020) has pointed out the need to deepen the teaching of digital security, as well as the promotion and inclusion of security content in university curricula. It should be noted that this measure has already been implemented in other educational levels, such as: the PIES model (Šimandl and Vaníček, 2017), the CIPA program (Yan, 2009) and the TAIS project (Chou and Peng, 2011).

Research Focus

The literature review revealed that in general terms Internet users frequently overestimate their ability to manage their security and privacy online (Morrison, 2013). Besides, there are studies that revealed that on rare occasions Internet users implement strategies to manage their privacy and protect their data. (Matzner et al., 2015).

For the purposes of this research, it was decided to consider the guidelines proposed by Masur, (2018) about Privacy related reflection ability related with: (1) Ability to reflect privacy needs in different online environments; (2) Ability to identify privacy risks in different online environments; (3) Ability to reflect and evaluate one´s own behavior and relation to one´s privacy needs, considering that they attend to the various preventive measures of online privacy that were raised in the survey, and that are related to the security considerations that may be feasible for university students to handle.

Unlike what other studies have reported that have shown that people have relatively low levels of privacy knowledge, which is often associated with a lack of effort to protect privacy (Bartsch and Dienlin, 2016), or individuals have an apathy attitude (Baruh et al., 2017). In the same way, in the study carried out by Trepte et al. (2015) about how much people know about privacy and data protection strategies they found that even though women want to protect their online privacy, they do not possess sufficient knowledge or have confidence in their ability to do so.

Another aspect that is interesting to address has to do with the role that the university has played in the learning process of preventive measures of online privacy with a view to establishing to what extent the family, social and academic environment have influenced the use of these measures. In this sense, the study carried out by Boyd and Hargittai (2010) to university students about online skills suggests that privacy behavior and digital literacy or skills are related. They found that after a year in college, these students became more aware of Facebook's privacy settings and changed them more frequently, indicating learning effects. The researchers showed that highly skilled Facebook users modified their privacy settings more often than less skilled users.

According to the study carried out by Hurwitz (2013), the decision to disclose information relies heavily on individual sensitivities towards what is perceived as privacy invasive. However, international reports such as World Bank Group (2016) have pointed out that young people are aware of the risks to which they are exposed when surfing the Internet, although it is not specified what young people are doing to take care of themselves online. Hence, the relevance of this study lies in the fact that it shows to what extent university students feel identified using a set of preventive measures of online privacy on a daily basis.

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Research Aim and Research Questions

The aim of the research was to identify the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they take when they are connected to the Internet. Hence, the research questions addressed were: What preventive measures of online privacy do Mexican and Colombian university students use?; Are there differences in the perceptions of university students regarding preventive measures of online privacy for the variables Country and Gender?; How consistent is the quantitative data analyzed with respect to the qualitative evidence collected on preventive measures of online privacy?.

The hypothesis developed in the document regarding quantitative data were the following:
H_{01}: There is no significant difference in the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they use when connected to the Internet.
H_{02}: There is no significant difference in the perception of men and women regarding the preventive measures of online privacy they use when connected to the Internet.

Research Methodology

General Background

This empirical research is part of a comprehensive study whose aim was to identify the perception of university students towards their digital citizenship. The manifestations of the students' digital citizenship were analyzed through several dimensions: online participation and practices, online security and privacy, ethical-technological behavior, personal data management, and digital identity management (Torres-Gastelú, 2020; Torres-Gastelú et.al., 2020, Torres-Gastelú et al., 2019; Torres-Gastelú, 2018). This text presents the perceptions of university students towards the items related to preventive security and privacy measures online, as well as the narratives of Colombians and Mexicans.

A mixed approach was used through the application of a survey as well as the collection of the narratives of the university students of some open questions. The quantitative part sought to identify the perception of university students towards preventive measures of online privacy. While the qualitative part tried to understand the ways that university students use to control their digital privacy. The type of sampling was non-probabilistic under the criterion of convenience. Data collection was done in two stages. In Mexican universities in 2018, and in Colombian universities in 2019. Descriptive and inferential statistics were used. Also, the data triangulation was carried out with the answers to the open questions.

The relevance of the research in an international context lies in the identification of the similarities and differences that exist in the ways in which university students manage privacy online in the Latin American region. This region is characterized by sharing a common heritage expressed in the use of the same language, similar idiosyncrasies, and similar social, political and economic situations. Therefore, it is feasible to generate regional educational strategies that meet specific common needs.

Sample

Data collection was done at two different times. First in 2 Mexican public universities in 2018 and then in 4 Colombian public universities in 2019. Face-to-face stays were held in each of the universities for the application of the qualitative surveys and interviews. Authorization was obtained in the universities for the application of various surveys related to the competence

https://doi.org/10.33225/pec/21.79.162 ISSN 1822-7864 (Print) ISSN 2538-7111 (Online)

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

of digital citizenship. One of them was the online security and privacy survey, part of this survey is presented in this document.

It was agreed with the authorities of each university to apply a minimum of 100 surveys since the researcher had to apply them on his own. Each university facilitated access to a certain number of groups and students. Therefore, it was not possible to obtain a probabilistic sample of clusters considering the size of each educational institution for various reasons: 1) it was not possible to know the exact number of students; 2) it was not feasible to access all groups due to different school activities; 3) the short stays carried out by the research in each of the universities did not allow a statistically significant sample.

Despite this, it was tried to make the sample as homogeneous as possible considering the following aspects: 1) students from public universities; 2) similar distribution of students from Mexico and Colombia; 3) similar distribution of male students and female students. Therefore, for this research convenience sampling was used. The sample consisted of 1,245 university students (Table 1). 52.6% were Mexican and 47.4% were Colombian. Of which, 58.4% were male students and 41.6% were female students. It should be noted that participants were randomly selected students assigned to 26 different educational programs. However, 76.6% of the participants were from 7 bachelor's degrees (Administration, Industrial Engineering, Mechatronics Engineering, Software Engineering, Psychology, Computer Science, Business Management). The preponderant age range is between 19 to 24 years, reaching 78.6% of the sample.

Table 1
Characteristics of the Sample

Characteristics	***n***	***%***
Country		
Mexico	655	52.6
Colombia	590	47.4
Gender		
Male Students	727	58.4
Female Students	518	41.6
Age		
16-19	367	29.5
20-23	633	50.8
24 or more	245	19.7
Semester		
1-3	509	40.9
4-6	435	34.9
7-10	301	24.2

Research Process

The research was carried out in compliance with ethical procedures. The selection of participating universities and countries was governed by two research calls in which the resources and authorization were obtained to carry out the research project. Therefore, when the researcher made the stays, the university authorities already had knowledge about the research. In addition, the students voluntarily participated after being informed of the aim of the research, as well as the confidentiality of the results. In the same way they were informed of the scientific and non-profit nature of the research.

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Instrument and Procedures

For the quantitative study, a survey on the management of digital security and privacy was applied. The survey comprised three dimensions (attitude towards security and privacy management, preventive measures of online privacy, events experienced against the integrity of their digital identity) assessed through a 5-point Likert scale: Strongly disagree, Disagree, Indifferent, Agree, Strongly agree. It should be noted that this document only presents the results of the second dimension on preventive measures of online privacy considered by students. Data capture and statistical processing was done with SPSS Software. The level of reliability of the 20 items that comprise the dimension under study reported by the Cronbach's Alpha test was .906.

As for the qualitative part, 42 students who were studying a bachelor's degree related to computing (21 Mexicans and 21 Colombians) were asked to develop open questions with a view to triangulating the data. The main question was how they controlled their digital privacy. In the same way, they were asked other questions that tried to review the role that various actors had played in the learning process about security and privacy online, such as: their teachers at the university, their family, their close circle of acquaintances and friends, as well as the situation of violence that exists in Colombian and Mexican societies. The evidences of the university students are indicated in this text anonymously by means of the acronym USID (University Student ID) and a consecutive number ranging from 1 to 42.

Table 2
Description of the Items and Levels of the Survey

	Item	Level
1	I keep only friends or acquaintances in my social networks (I-13)	1
2	In my social networks I do not accept, nor do I add strangers (I-14)	1
3	I'm careful with my posts on the web (I-22)	1
4	I use my real data on the network (name, date of birth, etc.) (I-23)	1
5	I think and review before what I am going to publish, chat, upload or download (I-26)	1
6	I configure the privacy elements in the services I use on the Internet (I-12)	2
7	I avoid sharing my passwords for my service accounts, applications, social networks and websites with family or friends (I-15)	2
8	I make sure I know who I chat with when I'm online (Example: Facebook, WhatsApp, Twitter, etc.) (I-24)	2
9	I knowingly give permission for the use of the Webcam in applications, games, etc. (I-25)	2
10	I know and use the pattern that a password must follow in order to be secure (symbols, letters and numbers) (I-29)	2
11	I usually review the type of permissions that I am going to grant to an application, which I just downloaded, correspond to the required functionality (I-17)	3
12	I know and configure my privacy in social networks in detail (I-18)	3
13	I restrict the consultation of my personal data stored on the Internet to only certain people (I-19)	3
14	I grant only the necessary permissions when sharing a document in the cloud (edit / view) (I-21)	3
15	I use a different password for each website (I-30)	3
16	When I enter my personal data in an online form, I check that the web page (URL) is secure (https: // ...) (I-20)	4
17	I make sure to configure the privacy and security settings every time I install an application or browse a website where I use an access account (I-16)	4
18	I deactivate the geo-location functions that are activated by default in web browsers, on my computer or on the mobile devices that I use (I-27)	4
19	Given the security warning to access a website, I avoid accessing it (I-28)	4
20	When I make a purchase on the Internet, I check that the web page (URL) is secure (https: // ...) (I-31)	4

https://doi.org/10.33225/pec/21.79.162 ISSN 1822-7864 (Print) ISSN 2538-7111 (Online)

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Table 2 shows the 20 items with their corresponding classification regarding the level of knowledge about preventive measures of online privacy. It is assumed that at a higher level number a greater experience and / or knowledge was expected in the student because it is a more complex measure or that it was expected to be less known. Four levels were established: Level 1 for Beginners (Items 1 to 5); Level 2 for Basic (Items 6 to 10); Level 3 for Intermediate (Items 11 to 15); and Level 4 for Advanced (Items 16 to 20).

Data Analysis

The quantitative analysis was carried out using descriptive and inferential statistics. In order to test the hypotheses on the existence of differences by country and gender, the Kruskal-Wallis test was chosen. While for the qualitative part, the students' responses were transcribed, the information was organized, and the main contributions of the students were presented. To carry out the triangulation of the data obtained, the data collected by the application of the survey to 1,245 students of various degrees were considered, as well as the narratives of the answers to the open questions answered by 42 students of a degree related to computing selected at the investigator's convenience. Hence, the quantitative perspective did represent a diversity of options with different profiles of university students, while the qualitative part reflected evidence of the learning process and maturity in the assimilation of preventive measures of online privacy of a certain profile of university students.

Research Results

Average values of Online Privacy Preventive Measures

The percentage average of the 20 items on preventive measures of online privacy of Mexican and Colombian university students reflected a favorable attitude represented by 62.2% (28.8% agree and 33.4% strongly agree). While 16.8% of university students adopted an indifferent stance. Meanwhile, 21% of the participants expressed an unfavorable attitude (10% disagreed and 11% strongly disagreed).

Table 3
Average Values of Online Privacy Preventive Measures Levels

Level	Item	Favorable Attitude		Indifferent	Unfavorable Attitude	
		Strongly agree	Agree		Strongly disagree	Disagree
Beginner	1-5	30.9	36.8	15.3	7.4	9.6
Basic	6-10	26	38.1	13.4	13.4	9
Intermediate	11-15	30.1	27.2	19.1	12.5	11.1
Advanced	16-20	28.2	31.5	19.6	10.4	10.4

Table 3 shows the average values of the four levels in which the items on preventive measures of online privacy were organized. For the beginner level, a favorable attitude of the students was observed, represented by 67.7%. While 15.3% of university students adopted an indifferent stance. Meanwhile, 17% of the participants expressed an unfavorable attitude. Also, similar results were presented at the basic level. 64.1% of the students expressed a favorable attitude, 13.4% chose to remain indifferent, and 22.5% of the students expressed an unfavorable attitude. On the other hand, in the intermediate and advanced levels there

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

was a less favorable attitude (57.3% Intermediate Level and 59.6% Advanced Level). There were very similar preferences towards an indifferent stance on the part of the students (19.1% Intermediate Level and 19.6% Advanced Level). In the same way, similar tendencies towards an unfavorable attitude occurred in students for this set of items (23.6% Intermediate Level and 20.8% Advanced Level).

Below is a detail of the results for each of the items. Seven out of ten students expressed a favorable attitude in the following items: I think and review before what I am going to publish, chat, upload, or download (78.5%); I make sure I know who I chat with when I'm online, such as: Facebook, WhatsApp, Twitter, among others (73.1%); I avoid sharing my passwords for my service accounts, applications, social networks and websites with family or friends (70.2%).

While six out of ten university students opted for a favorable attitude in the items: I use my real personal data on the network such as my name, date of birth, among others (68.6%); I am careful with my publications on the net (68.4%); I restrict the consultation of my personal data saved on the Internet to only certain people (66.4%); I know and configure my privacy in social networks in detail (66%); I make sure to configure the privacy and security settings every time I install an application or browse a website where I use an access account (65%); I know and use the pattern that a password must follow in order to be secure, for example the one formed by symbols, letters and numbers (64.7%); I keep only friends or acquaintances on my social networks (62.7%); I configure the privacy elements in the services I use on the Internet (61.4%); When I make a purchase on the Internet I check that the web page (URL) is secure (https://…) (61.2%); Given the security warning to access a website, I avoid accessing it (61%); In my social networks I do not accept, nor do I add unknown people (60.4%).

Meanwhile, five out of ten of the university students expressed a favorable attitude in the following items: I deactivate the geo-location functions that are activated by default in web browsers, on my computer or on the mobile devices that I use (56.5%); When I enter my personal data in an online form I check that the web page (URL) is secure (https://…) (54.5%); I grant only the necessary permissions when sharing a document in the cloud (edit / view) (54.1%); I usually review the type of permissions that I am going to grant to an application, which I just downloaded, correspond to the required functionality (52.6%); I consciously give permission for the use of the Webcam as in applications, games, among others (51.3%); I use a different password for each website (47.3%).

Results by Country: Online Privacy Preventive Measures

Table 4 shows the results of the Kruskal-Wallis test in order to test the hypothesis about the existence of a significant difference in the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they use when are connected to the Internet (H_{01}). The significance values of 18 items are less than .05, so the null hypothesis is accepted, and it is concluded that in most of the items there is no significant difference in the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they use when connected to the Internet. Only two of the twenty items are greater than .05, and therefore the alternative hypothesis is accepted that there are significant differences in the perception of university students from Mexico and Colombia regarding: I consciously give permission for the use of the Webcam in applications, games, etc. (item 9 I-25); and Given the security warning to access a website, I avoid accessing it (item 19 I-28).

https://doi.org/10.33225/pec/21.79.162 ISSN 1822-7864 (Print) ISSN 2538-7111 (Online)

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Table 4

Kruskal-Wallis Test: Online Privacy Preventive Measures (Country / Gender)

Item	Code	Level	Country			Gender		
			Statistic	*df*	*p*	Statistic	*df*	*p*
1	I-13	1	33.413	1	.001*	39.589	1	.001*
2	I-14	1	11.692	1	.001	49.928	1	.001*
3	I-22	1	99.636	1	.001*	22.081	1	.001*
4	I-23	1	48.448	1	.001*	4.587	1	.032
5	I-26	1	7.823	1	.001*	18.646	1	.001*
6	I-12	2	20.320	1	.001*	26.090	1	.001*
7	I-15	2	166.036	1	.001*	5.033	1	.025
8	I-24	2	90.245	1	.001*	20.100	1	.001*
9	I-25	2	1.693	1	.193	.923	1	.337
10	I-29	2	113.688	1	.001*	7.746	1	.005
11	I-17	3	14.646	1	.001*	10.108	1	.001
12	I-18	3	13.734	1	.001*	23.402	1	.001*
13	I-19	3	12.513	1	.001*	21.885	1	.001*
14	I-21	3	109.303	1	.001*	9.641	1	.002
15	I-30	3	29.418	1	.001*	8.368	1	.004
16	I-20	4	5.609	1	.018	6.617	1	.010
17	I-16	4	7.188	1	.007	20.399	1	.001*
18	I-27	4	20.988	1	.001*	10.435	1	.001
19	I-28	4	.906	1	.341	25.201	1	.001*
20	I-31	4	91.806	1	.001*	7.032	1	.008

*p<.001

Regarding the hypothesis about the differences by gender, Table 4 shows the results of the Kruskal-Wallis test. The significance values of 19 items were less than .05, so the null hypothesis is accepted, and it is concluded that in most of the items there is no significant difference in the perception of men and women regarding preventive measures of online privacy they use when connected to the Internet (H_{02}). Only in one of the twenty items was a significance value greater than .05 obtained. Hence, for this item, the alternative hypothesis is accepted that there are significant differences between men in terms of: I consciously give permission for the use of the Webcam in applications, games, among others (item 9 I-25).

Table 5 summarizes the items in which differences did occur considering the proposed levels considering the variables Country and Gender. The common element is the item on I consciously give permission for the use of the Webcam in applications, games, among others (Item 9 I-25).

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Table 5
Items that Presented Significant Differences Organized According to Levels

No.	Level	Country	Gender
1	Beginner	No differences	No differences
2	Basic	(Item 9) I-25 .193>.05	(Item 9) I-25 .337>.05
3	Intermediate	No differences	No differences
4	Advanced	(Item 19) I-28 .341>.05	No differences

Findings from Open Questions

In order to contrast the perceptions of university students, the findings of the responses to various questions are presented below. The main question had to do with how university students controlled their digital privacy. To do this, the evidence is organized in two tables according to the country in which the students were born. In each table a consecutive number is placed, the degree of privacy preventive measures used by the student, as well as the description of the contribution. The classification of the grade is as follows: Grade 1 for the use of a preventive measure; Grade 2 for two or three preventive measures; Grade 3 for four or more preventive measures of online privacy. Table 6 presents the degree of preventive measures, as well as the comments of Colombian students.

Table 6
Description of the Qualitative Evidence of Colombian Students on How They Control Their Digital Privacy

No.	Grade	Description of the qualitative evidence of the students
1	1	*I use the browser's search engine in private mode so that it does not keep a history of the sites I visit. When an app asks for my credentials, I use the on-screen keyboard to enter (USID-1).*
2	1	*The way I control digital privacy is by being cautious or making sure that the page I'm going to enter is legal (USID-2).*
3	1	*With the use of mechanisms such as security pins, patterns, use the keys different to the year of birth, ID number, etc. (USID-3).*
4	3	*The way I control my privacy is I grant the necessary permissions, I configure my privacy, I am careful about the pages that I enter, and I like to delete the pages and the cache. (USID-4).*
5	3	*I browse incognito, change my passwords periodically. I use licensed antivirus. I enter trusted browsing portals (USID-5).*
6	1	*I use browsers, rare and little known to people, this in the field of Internet; since they allow not to be tracked and it generates confidence to browse the web since you are not afraid of being spied on or that your data will be stolen (USID-6).*
7	2	*I do not share my passwords with people, or with websites (USID-7).*
8	1	*I use passwords with letters, numbers and sometimes with characters (USID-8).*
9	2	*I change passwords monthly. I delete history. I use official pages of the platforms (USID-9).*
10	3	*I use different passwords for each account, limiting what I post on the network about my personal life, I don't sign up for non-recommended pages, I avoid browsing pages that have the padlock and the S after https: //, I don't use my institutional account to register (USID-10).*
11	3	*I browse incognito mode. I dock the logins with the fingerprint. I delete the browsing history. I do not go online in public places to open or consult my bank accounts (USID-11).*
12	2	*I use the browser tabs in incognito mode and clear my search histories. I also change my passwords constantly (USID-12).*

13	3	*On Facebook I do not accept requests, my information is very little and I have it hidden. In browsing I use incognito mode, I constantly delete the history, I do not open any suspicious messages, I have different passwords and I change them constantly (USID-13).*
14	2	*I do not go to websites that are not secure, I only connect to a Wi-Fi network that is secure. I also manage social networks with advanced settings (USID-14).*
15	2	*I use complicated passwords, I avoid entering pages where they ask me for a lot of personal information (USID-15).*
16	3	*I avoid opening a link sent to me through chat, I do not accept strange requests, I avoid sending photos or videos of sexual content, I close my session when I open my accounts in public places (USID-16).*
17	2	*I control my passwords on social networks, I keep an eye on what devices my social network is on, occasionally see the login location. I maintain privacy in photos or publications so that it is only seen by my friends or acquaintances (USID-17).*
18	2	*I put long passwords, I do not share passwords or emails to strangers. I usually download applications that help to have a little more security, in this case security patterns or passwords for each application or social network (USID-18).*
19	1	*I avoid giving relevant information to strangers or friends who allow them to clone my information (USID-19).*
20	1	*I try not to post personal data, family photos, I do not share the fact that other people post when they bought their clothes or when they are traveling or post photos of their children, I am not one to share those things, I prefer to share informative things (USID-20).*
21	1	*I am a very reserved person. I think there is a lot of insecurity today in social networks. I avoid posting personal photos a lot, even my Facebook profile picture is from many years ago. I avoid using many applications a lot, I use the basics for my daily life: WhatsApp and Facebook (USID-21).*

The quantification of the degree of preventive privacy measures used by the student represented in Table 6 indicates that 38% of Colombians expressed using only one preventive measure. While 33.4% of Colombians indicated that they used two or three preventive measures. For their part, 28.6% of Colombian university students indicated that they used four or more preventive measures of online privacy.

Table 7

Description of the Qualitative Evidence of Mexican Students on How They Control Their Digital Privacy

No.	Grade	Description of the qualitative evidence of the students
22	1	*I use passwords and I do not leave a session open when I browse the Internet. I only log in when I know I will occupy it (USID-22).*
23	2	*I manage my passwords and accounts meticulously, I manage app location permissions, I regulate my public information on networks (USID-23).*
24	2	*I do not allow my accounts to be public, I set strong passwords, I visit secure Internet sites (USID-24).*
25	2	*Through the privacy settings on the platforms, passwords, I publish little information about my personal data (USID-25).*
26	2	*I do not put all my personal information on the sites I use, I do not allow some applications to have my location or access to my files, I also verify that where I enter is a safe site and does not have any threat (USID-26).*
27	1	*I change my passwords every so often (USID-27).*
28	2	*I do not register my primary or educational e-mail, I do not provide real information unless I know what it will be used for (USID-28).*
29	2	*I browse secure pages and restrict the personal information I share (USID-29).*
30	1	*Remembering my passwords and configuring the applications to show only the information I indicate (USID-30).*

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

31	1	*Through the constant change of passwords, as well as the protection of the same through servers that encrypt said data (USID-31).*
32	1	*Not giving access to the network to save my passwords (USID-32).*
33	2	*I check the https domain and use an incognito browser to avoid cookies (USID-33).*
34	1	*I do not share specific data in my profile that I have on social networks or another platform, that way I decide what to share and what not (USID-34).*
35	1	*I configure my devices and private accounts so that they can notify me when my accounts are being accessed from other devices (USID-35).*
36	2	*I have a complex password that not everyone could remember or recognize, in terms of social networks I do not share the same password for all my networks, in one I have no privacy in terms of viewing my images, and in another I try to only accept people that I really know (USID-36).*
37	3	*I avoid that others can visualize what I share on my social networks. I try not to join open wi-fi networks in very crowded places, I check the permission accesses for each of the applications on my devices. I frequently change my email and social media passwords, I use different passwords for each one, I have two-step verification turned on for most of my accounts (USID-37).*
38	2	*I do not share my passwords, I put my private information on social networks (USID-38).*
39	2	*I do not disclose private data to untrustworthy web pages, and I use password encryption systems (USID-39).*
40	1	*I keep my personal information hidden, either by lying about my data or simply not giving it away. Unless it is an important website (like a bank) then I would give my information (USID-40).*
41	2	*When I access Internet pages, if they contain cookies, I simply exit and look for another. In the same way when I download programs or applications, I deny them the permissions to access certain information that I do not want to share (USID-41).*
42	2	*I try to restrict the automatic access of the applications to my data, in social networks I put my private profiles so that only the people that I add and / or accept see my information, which I decided to make public (USID-42).*

Table 7 presents the comments of the Mexican students. The quantification of the degree of privacy preventive measures used by the student represented in Table 7, indicates that 38% of Mexicans expressed using only one preventive measure. While 57% of Mexicans indicated that they used two or three preventive measures. For their part, 5% of Mexican university students indicated that they used four or more preventive measures of online privacy.

Other questions that were addressed sought to review the role that various actors had played in the learning process about online security and privacy, such as: his teachers at the university, his family, his close circle of acquaintances and friends, as well as the situation of violence that exists in Colombian and Mexican societies.

In the Mexican case, the role that teachers have played in the university to increase the attitudes, skills and knowledge of students about security and privacy online was indicated by several positions. First, there was a group of students who indicated the support they received from various teachers:

> "*Fortunately, I have had good teachers concerned about sharing the idea of protecting the information we make public on our social networks and when surfing the net*" (USID-22).

According to the students, the teaching received consisted of advice aimed at preserving the privacy of their personal data:

> "*I would say that the role of my teachers has been very important, several of my teachers have taught me about some measures to secure my data or they have taught me to use the tools that help us keep our data safe*" (USID-23).

Another group of university students said that the role of teachers has been discreet:

"*Only one teacher has told us about the importance of protecting our personal data, as well as keeping us up to date with suspicious emails that arrive at our institutional emails*" (USID-24).
"*A moderately relevant role. In the first year of university with the Digital Literacy subject, they mentioned some ways to prevent others from accessing our information, although I do not remember that it was a specific class topic, they were superficial comments*" (USID-27).

Or, they have received little information on this topic:

"*The role of teachers has been little relevant on security issues, only one teacher has mentioned the importance of digital security and our data*" (USID-26).

Hence, a third group of students highlighted that their teachers have not contributed much in their training process on security and privacy online:

"*Teachers only make comments like: Take care, or Do not upload personal information to your network, but they do not really teach us to have a good protection strategy*" (USID-29).
"*They only tell us to take care of our information on Internet networks*" (USID-31).

Student evidence reveals that not all youth have the same opportunity to receive instruction on safety and privacy issues online:

"*So far we have not had a teacher who has addressed directly to the topic of how to have greater security online*" (USID-25).
"*A very minor role since no teacher has touched upon that specific topic*" (USID-30).

In the Colombian case, the teacher's profile has played a key role in encouraging the development of a culture of digital security and privacy. In this sense, a student pointed out:

"*During the bachelor's degree, they did mention certain things to me, for example, in the eighth semester, a teacher who was an engineer addressed things about computer security, he was a specialist in that regard. He gave us some Social Engineering, he even taught us how hackers hurt and made us aware of the dark web where there is organ trafficking, how they are sold there and hitmen are hired, that is, he put us fully into that world. He taught us many things that by means of cell phones you can do a lot of damage by sending only an image and that kind of thing, that's why I already said at that time, Oh, that's serious!, Let's say that they send you an image for you is creepy and horrible, and with that being able to hack into your camera, that they steal an image, that for me is violating your privacy in every way, usually one is involved in everything all day on the cell phone ... it was a very cool and important experience for us*" (USID-16).
"*In the bachelor's degree in different subjects because those topics are touched upon in terms of security and privacy online since I started, as in the second or third semester we were in software architecture, the teacher did focus a lot on the security of digital media to take care of ourselves when we use these digital tools and other. Also, the Artificial Intelligence teacher taught us a lot about how we should protect ourselves when we surf the Internet…*" (USID-18).

Another group of students revealed the role that a family member of the students had played, by instilling them to take care of themselves both in their face-to-face social environment and in virtual social networks:

"*Because it was an aspect partly like nurturing, my parents from a very young age have instilled in me that kind of thing, that I must take great care of myself both in the face-to-face social environment and in virtuality and on social networks*" (USID-20).

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

The students' narratives allowed us to understand the assimilation and learning process they went through. Informants noted that they had learned to take care of themselves online over time, to a large extent retro feeding on things that had happened to other people, especially in their close circles. As one student recounted:

> "*I have partly learned to take care of myself online from what I have seen that has happened to other people who have suffered more than anything from scams, for example, when making transactions over the Internet or purchases through platforms such as the Mercado Libre site, and this has perhaps happened to family or friends, so one already with that knowledge one avoids it*" (USID-20).

Some students considered that the development of their learning about security and privacy online was associated with the profiles of the bachelor's degrees they studied. This aspect was thus highlighted by Colombian students:

> "*I think that professional training influences, perhaps because in different careers (degrees) we are taught about online security, but I think that more in systems-oriented bachelor's degrees, electronics, telecommunications, I think these topics are touched upon more than in other bachelor's degrees, and even in different ways that, as a person, they open their minds more and also because we have been in contact with cases of acquaintances who have happened to them about that situation*" (USID-19).
> "*As a systems bachelor's degree student, I believe that our teachers at the university have taught us a lot. They have instilled in us a lot about how we should do things, such as making safe purchases online, let's say entering a portal that is reliable, has https security and is highly recognized. Even when we enter platforms, we make sure to see the comments of other people, to see if they are good comments, or see if they have good stars on the products or in what we are interested. In addition, we have also learned to make purchases or handle secure platforms mostly because cases have happened to other people and we have found out, so we have learned about that*" (USID-21).
> "*Through the bachelor's degree courses I am learning many things, for example, about how social engineering has to do with the ways of obtaining confidential information through the manipulation of legitimate users. In other words, through social networks then they follow up on people what they publish or do not publish and from that they take their environment, their life, their friends.*" (USID-20).

Regarding the situation that has prevailed in both Mexico and Colombia in recent decades characterized by strong indications of violence, drug trafficking, extortion, kidnappings and murders that have affected various sectors of society, it was considered pertinent to question students about whether this situation had influenced them to adopt preventive measures for security and privacy online. The response of the university students was forceful, highlighting this factor as a key element that has led them to adopt precautions as they have understood and internalized their reality:

> "*Very high influence, since currently insecurity in Mexico is very high, which is why taking measures is very important"* (USID-22).
> *"It has greatly influenced. Since all personal data has had to be hidden, so as not to be a victim of a case of cyber-attack"* (USID-23).
> "*The high number of kidnappings of people who accept strangers on social networks has made me see that I should not accept anyone, much less talk to them*" (USID-30).
> "*I have taken online security measures because in recent years there have been many cases of kidnapping and extortion due to the insecurity generated by the Internet*" (USID-31).
> "*The high rate of violence was the main reason for opting for strong online security measures, especially because of having a family who was the victim of extortion*" (USID-34).

https://doi.org/10.33225/pec/21.79.162 ISSN 1822-7864 (Print) ISSN 2538-7111 (Online)

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

Students have learned to take precautions to interact in the virtual world through the story of experiences lived by third parties. As related below:

> "*I had a very close case of a daughter of my brother who was contacted by a young man through Facebook, over time they fell in love, then he started using her and the girl ended up committing suicide. The family never knew until they entered Facebook here and checked all her updates, then this person published many photos of her, of the family, then they tried to scam the parents, then there are cases that reveal the misuse of the social networks from near, that one knows ... so I learned and then I take care of that kind of thing*" (USID-20).

In this sense, university students from both countries highlighted the importance they attach to managing their privacy online as a mechanism to have safe virtual spaces in which they can act.

Another question sought to know the position of students with respect to whether they considered that most university students took care of themselves when they used the Internet, and if they believed that the type of bachelor's degree students coursed at the university had an influence on their obtaining a greater knowledge and greater adoption of preventive measures of security and privacy online:

> *"I think that there are not many students who take care of their online safety mainly because we believe that nothing will happen to us; I consider that the bachelor's degree has a lot to do with it since it determines what tools or environment you will be surrounded by"* (USID-43).
> *"I believe that the majority of university students do not take care of themselves on the Internet, but I do believe that the bachelor's degree has an influence to be more aware of the dangers involved in the use of personal data on the Internet, since they know in a certain way how the way to steal information or how easily that data can be accessed"* (USID-44).
> *"I consider that the majority of university students are very careless when handling the information we have on the Internet. I believe that bachelor's degrees, including those related to computers, are not so focused on educating or teaching the student special methods for the use of electronic media"* (USID-47).
> *"There are many university students who have no idea about some topics about their care on the Internet or the sites they visit, I don't know how many actually, but I know some. I think that the bachelor's degree we study has a lot to do with what we know or do, some if they are interested in knowing more about the subject without it being their branch, but it does not apply to everyone"* (USID-48).
> *"I consider that the type of bachelor's degree that is studied is not a determining variant for preventive measures to be adopted, any student can implement the measures they consider pertinent to take care of their navigation"* (USID-50).

The demonstrations of university students agreed that they considered that the majority of university students took care of themselves when they used the Internet, and a good part of the informants indicated that they believed that the type of bachelor's degree they were studying had an influence as a factor that allowed them to achieve a greater knowledge and greater adoption of preventive security and privacy measures online.

Apparently, the sense of good sense about what is published, and the corresponding security restrictions are gradually assimilated as the age and academic training of students advance:

> "S*ince I started studying as a systems technician at CENA, I became aware of all the security issues. Little by little I learned about maintaining my privacy, I was putting restrictions on security and establishing limits. For example, I was deleting my photos that were very personal from my Facebook profile, I was recommending to my friends that if I am there in some perhaps very compromising photos, I told them that they were personal and not for the public ... or else*

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

configure the options of the Facebook tools and all that part, so I think that the bachelor's degree was very important because it opened my mind a lot, until I entered university I was enabling restrictions and setting limits, I learned how to behave on the networks" (USID-18).

Discussion

The aim of the research was to identify the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they took when they were connected to the Internet. The quantitative results indicated a favorable attitude towards preventive measures of online privacy in most items in at least six out of ten students. In the same way, no significant differences were detected between the countries and gender. The common element is the item on I consciously give permission for the use of the Webcam in applications, games, among others (Item 9 I-25).

However, there are several aspects to consider. First of all, that four out of ten students do not feel identified with the adoption of these privacy measures online. These findings are consistent with other studies that have found that users lack understanding and awareness about the risks on the Internet regarding sharing personal and private data (Bartsch and Dienlin, 2016; Hoofnagle et al., 2010; Trepte et al., 2015). This lack of understanding and awareness may be due to the lack or deficiency of digital skills of the users (Dienlin and Trepte, 2015; Park, 2013).

If we add to this aspect that the university students in the study who did use this type of measures did so until they were in university, there is evidence of a deficit in the training process on online security and privacy in students. This aspect coincides with the findings of García et al. (2018), in terms that students are increasingly aware of online privacy issues since they recognize that they must protect part of their private life. These researchers also highlighted that the perception of privacy increases with age, and that students, aware of this, demand both training and information for the use of the networks.

Secondly, the qualitative evidence reflected that there is a marked late adoption of these preventive measures until admission to university, and precisely in at least 40% of the cases this situation is not occurring. The late adoption of university students towards these measures coincides with that indicated by Bartsch and Dienlin (2016) when they conclude that having extensive experience in the use of the Internet results in greater knowledge about the dangers to privacy on the Internet, which in turn produces a more cautious behavior on social networks.

Thirdly, there is a clear contrast between the quantitative data that reflected an apparent extensive use of preventive measures of online privacy by university students (Table 3) with respect to the qualitative findings that indicate few privacy preventive measures online (Tables 5 and 6) both by Colombians and by Mexicans. Besides, many of the measures they indicated are aimed at avoiding actions that cause an intrusion and not so much in the use of tools or settings that favor the integrity of the privacy of users.

These findings on the apparent use of privacy measures and what users actually do coincide with what was pointed out by Barth and De Jong (2017) and Kolokakis (2017) who have ensured that incorporate privacy knowledge into research on privacy concern may help to understand how individuals declare to be highly concerned about privacy yet do little to protect personal information. In their study, Bartsch and Dienlin (2016) have shown that people have relatively low levels of privacy knowledge, which is often associated with a lack of effort to protect privacy. Another explanation about why individuals may fail to protect their privacy include desensitization and lack of efficacy, represented in an apathy attitude (Baruh et al., 2017).

The qualitative evidence allowed identifying that the learning process about digital privacy was related to three factors. In the first place, because of the role that a family member of the students had played, by instilling them to take care of themselves both in their face-to-

face social environment and in virtual social networks. Secondly, for having studied a subject in his bachelor's degree that made it easier for him to understand the relevance of taking care of himself virtually. The third factor is related to the internalization of learning through the account of experiences lived by third parties.

This finding coincides with that indicated by Rodríguez and Magdalena (2016) when they argue that the privacy and security measures that teens use to protect their information are strengthened as they acquire more experience in using the Internet, being an empirical process based on tests and error. Thus, being a constant learning that is strengthened as preventive and corrective measures are used in terms of security and privacy online.

The assimilation of a culture of security and digital privacy has been partly caused by belonging to the university environment, the specific knowledge acquired during their training, as well as the role played by some teachers who have been in charge of sensitizing university students about digital security and privacy aspects.

Despite this apparent incipient culture in security and digital privacy, there is no consensus for it to apply to all students of the different bachelor's degrees in both Mexico and Colombia. Even among students of the same bachelor's degree there were cases of university students who had been victims of identity theft and studying a bachelor's degree related with computers.

Hence, the learning process about preventive measures in digital privacy is individual and is associated with socio-economic characteristics, experiences lived with close people, approach with some teachers, among other aspects. In this sense, the study carried out by Brandtzæg et al. (2010) highlights that as individuals get older, the use of social networks changes and focuses on maintaining contact with acquaintances and family.

The role that the university has played in the training process of the interviewed students of the bachelor's degree in systems on digital security and privacy has been addressed by various subjects throughout their academic career. In the Colombian case, the teacher's profile has played a key role in encouraging the development of a culture of digital security and privacy. While in the Mexican case, teachers have played a more conservative role.

It should be noted that not all university students have access to the same teachers in their subjects. Hence, possibly those who did not manage to develop skills and knowledge about security and privacy online has to do simply with the fact that they did not have the same teachers from the group of university students who did manage to develop skills and knowledge on this aspect. Perhaps that is one of the reasons why four out of ten university students have expressed an unfavorable attitude towards preventive measures of online privacy.

This aspect contrasts with the findings of the study by Young and Quan-Haase (2013) where they argued that students are supposed to be better able to manage application settings and options to protect their privacy. However, the evidence from this study highlighted a late adoption of the majority of university students in part due to the knowledge received at the university, due to events that have addressed the security and privacy in their close social circle, as well as the process of gradual maturity as an Internet user.

In this sense, the qualitative evidence indicated that there were differences between Mexicans and Colombians regarding the role that their teachers and their university had played. On the one hand, the Mexican students showed divided positions on the role of these actors. Meanwhile, Colombians indicated that both their teachers and their university had been key elements in acquiring greater knowledge about security and privacy online. Despite this, both Mexicans and Colombians agreed on the late adoption of preventive measures of online privacy that takes place up to the university level. There was also coincidence in the evidence on the influence of the levels of violence as a factor that has made them reflect on adopting restrictive measures on the control of their personal data, as well as the publications they make when they are connected to the Internet.

PROBLEMS
OF EDUCATION
IN THE 21st CENTURY
Vol. 79, No. 1, 2021

In general terms, university students stated that they used a variety of preventive measures to maintain their privacy online. Among which are: configuration of privacy elements in the services they use on the Internet; make adjustments to privacy options both in applications and browsers; they limit themselves to keeping their friends, acquaintances and family members on their virtual social networks, avoiding accepting anyone who sends them an invitation; they usually review the types of permissions both in the applications and tools they use on the Internet; if it is necessary to capture their sensitive personal data in an online form, they make sure that it is a secure site (// https); they point out that they are careful with the publications they make on the Internet; they ensure that they avoid using false profiles and that the data they publish is real; they try to make sure they know who they are chatting with when online; they argue that they disable geolocation functions; and they take into account the security warnings that appear in the browser when they try to access a site on the Web, so they avoid entering those sites.

In this sense, the study carried out by Herrera-Aguilar and Sepulveda (2018) coincides with some of the online preventive measures adopted by university students, such as: the use of security filters on platforms and applications, not accepting interactions with strangers on social networks, not sharing photos or personal data and using the privacy options on the pages themselves; in other words, be informed and be aware of what is published. They incorporate a measure that was not mentioned in this study: the need for users to carefully read the privacy policies of the different platforms.

Another key aspect in which the informants agreed is that just before entering the university they maintained a high level of publication of photos and personal aspects on social networks such as Facebook. This aspect coincides with the results of other studies that have argued that the youngest are supposed to be more likely to reveal personal information and share experiences (Steijn and Schouten, 2013; Urista et al., 2009).

The narratives of the students indicate that the maturity on the Internet about what was published, and the corresponding security restrictions are gradually assimilated as the age and academic training of students' advance. However, this finding contrasts with the study by Lee et al. (2013), they found that users actively shared personal information despite their concerns, due to the expected benefits of information sharing. According to these researchers, it seems that self-disclosure related to information inherent to privacy in social networks did not decrease substantially over the years, despite constant reports of high concern for user privacy.

Conclusions

The perception of Mexican and Colombian university students about preventive measures of online privacy reflects a favorable attitude in six out of ten students. However, four out of ten university students indicated that they had not adopted preventive measures or that they adopted an indifferent stance in this situation. Hence, in addition to the fact that they are incorporating security strategies until they come of legal age, almost half recognized that they did not use them or were not interested in doing so. For most items, there was no significant difference in the perception of Mexican and Colombian university students regarding the preventive measures of online privacy they used when connected to the Internet. Only one common item was detected that was different in all cases (Country and Gender), the item was I consciously give permission for the use of the Webcam in applications, games, among others (Item 9 I-25).

Regarding the proposed levels of preventive measures of online privacy, from the perspective of the perceptions of university students, they indicated a favorable attitude without denoting any prevalence of any specific level. However, the students' narratives focused on a few preventive measures and for the majority of the informants they are at the beginner and basic levels. The evidence was concentrated on the following items: I keep only friends

or acquaintances on my social networks; in my social networks I do not accept, nor do I add unknown people, I am careful with my publications on the network; I configure the privacy elements in the services I use on the Internet; I avoid sharing my account passwords with family and friends; and I use the pattern that a password must follow to be secure (symbols, letters and numbers).

In the same way, the students' narratives highlighted the extensive use of the following preventive measures of online privacy that can also be cataloged at a basic level: such as: (1) frequent password change; (2) generation of long passwords in which they try to use characters such as letters and numbers; (3) browsing in incognito mode in browsers; (4) verification in online inquiries that the page they visit is legal; (5) routine deletion of browsing history; (6) avoid leaving a session open with their passwords active; (7) Restrict the shared personal information; (8) they make sure to navigate on secure pages; (9) privacy settings in Web services and applications; and (10) avoiding posting personal information on their social networks.

In this same sense, the percentage diversification on the degree of preventive measures of online privacy is aligned with the beginner and basic levels, allowing a positive triangulation of the data between the quantitative and qualitative data, reflecting that despite the apparent prevalence towards the assimilation of preventive measures of online privacy, there is an incipient level of control in Mexicans and Colombians over the management of their privacy when they are connected to the Internet.

University students indicated that their attitude and ability to manage security and privacy online is associated with a gradual learning process that in many cases coincides with entering the university, partly because of having received formal instruction on the subject and partly because of a maturity process in the use of social networks on the relevance of taking care of their personal data and their digital identity, induced to a large extent because they were aware of various risks to digital security such as extortion, cyberbullying, fraud, and identity theft that happened to acquaintances, friends, or family.

Evidence reveals a late development in online security and privacy attitudes and measures in university students, considering that on average they adopted this cyber commitment around the age of 18. In most of the cases interviewed, they indicated that before entering the university, they did not adopt almost any security measures, they made multiple publications that compromised their personal data and digital identity. Even at university level, the qualitative evidence denotes little use of preventive measures of online privacy in contrast to the favorable attitude expressed by students, indicating that in practice they do not take much care into account when surfing the net. Hence, it is pertinent to assess not only the attitude but the skills and knowledge that they really have about security and privacy online at the university level, as well as at previous educational levels.

Acknowledgements

The data gathering process was supported by a scholarship for a research stay in Colombia through the Pacific Alliance in 2019. While the information collected in Mexico was supported by a sabbatical stay granted by CONACYT in 2018.

References

Barrow, C., & Heywood-Everett, G. (n.d.). *The experience of English educational establishments: Summary and recommendations*. British Educational Communications and Technology Agency (BECTA). https://bit.ly/2Gz6aoD

Barth, S., & De Jong, M. D. (2017). The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telemat Inform, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. https://doi.org/10.1111/jcom.12276

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8), 265-288. https://doi.org/10.5210/fm.v15i8.3086

Brandtzæg, P., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook "Friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction, 26*(11-12), 1006-1030. https://doi.org/10.1080/10447318.2010.516719

Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education, 14*(1), 44-53. https://doi.org/10.1016/j.iheduc.2010.03.006

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers´ problematic information security behavior. *Computers in Human Behavior, 65,* 334-345. https://doi.org/10.1016/j.chb.2016.08.034

De-Waal, E., & Grösser, M. (2014). On safety and security in education: Pedagogical needs and fundamental rights of learners. *Educar, 50*(2), 339-361. https://doi.org/10.5565/rev/educar.44

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*, 285-297. http://dx.doi.org/10.1002/ejsp.2049

Engen, B. K., Giaever, T. H., & Mifsud, L. (2015). Guidelines and regulations for teaching digital competence In schools and teacher education: a weak link? *Nordic Journal of Digital Literacy, 10*(2), 172-186.

Ferrari, A. (2012). *Digital competence in practice: An Analysis of Frameworks*. JRC-IPTS. https://ifap.ru/library/book522.pdf

Ferrari, A. (2013). *DIGCOMP: A framework for developing and understanding digital competence in Europe*. Scientific and Policy Reports. https://ec.europa.eu/jrc/en/publication/digcomp-framework-developing-and-understanding-digital-competence-europe

Gallego-Arrufat, M. J., Torres-Hernández, N., & Pessoa, T. (2019). Competence of Future Teachers in the Digital Security Area. *Comunicar, 61,* 57-67. https://doi.org/10.3916/C61-2019-05

Gisbert, M., Esteve, F., & Lázaro, J. (2016). La competencia digital de los futuros docentes: ¿cómo se ven los actuales estudiantes de educación? [The digital competence of future teachers: How do current students of education see themselves?]. *Perspectiva Educacional, 55*(2), 34-52. http://dx.doi.org/10.4151/07189729-Vol.55-Iss.2-Art.412

Herrera-Aguilar, M., & Sepulveda, A. T. (2018). Los jóvenes y la privacidad en Internet [Young people and privacy on the Internet] *Technologies mobiles, innovation et développement, 6*, 1-14. https://doi.org/10.4000/ctd.514

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN,* 1-20. https://repository.upenn.edu/cgi/viewcontent.cgi?article=1413&context=asc_papers

Hurwitz, J. B. (2013). User choice, privacy sensitivity, and acceptance of personal information collection. In *European data protection: Coming of age* (pp. 295-312). Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_13

Instituto Nacional de Tecnologías Educativas y de Formación de Profesorado INTEF (2016). *Uso de las tecnologías por niños de hasta 8 años: Un estudio cualitativo en siete países* [*Use of technologies by children up to 8 years: A qualitative study in seven countries*]. https://intef.es/wp-content/uploads/2016/03/2016_0220-Informe_TIC_ninos_8years-INTEF.pdf

ISTE (2016). *International Society for Technology in Education*. https://www.iste.org/es/standards

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862-877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Llorente, M. C. (2008). Aspectos fundamentales de la formación del profesorado en TIC [Fundamental aspects of teacher training in ICT]. *Pixel-Bit: Revista de medios y educación, 31*, 121-130.

Lugo, M., & Ruiz, V. (2016). Reflexiones en torno a los escenarios educativos de integración TIC [Reflections on the educational scenarios of ICT integration]. En Unesco / Fundación Telefónica (Ed.), *Experiencias Evaluativas de Tecnologías Digitales en la Educación* (pp. 87-96). Fundação Telefônica Vivo.

Maris, S., Martínez, M., Siñanes, G., & Rivero, M. (2008). Nuevos espacios de interactividad para la práctica pedagógica universitaria [New spaces of interactivity for university pedagogical practice.]. *Pixel-Bit. Revista de Medios y Educación, 33*, 165-172.

Masur, P. K. (2018). Mehr als Bewusstsein für Privatheitsrisiken: Eine Rekonzeptualisierung der Online-Privatheitskompetenz als Kombination aus Wissen, Fähig- und Fertigkeiten. *Medien & Kommunikationswissenschaft, 66*(4)*,* 446-465. https://doi.org/10.5771/1615-634X-2018-4-446

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2015). *Self-Data-Protection – Empowerment or burden?*. Data Protection on the Move. https://doi.org/10.5771/1615-634x-2018-4-446

Morales, M. J., Rivoir, A., Lázaro-Cantabrana, J. L., & Gisbert-Cervera, M. (2020). ¿Cuánto importa la competencia digital docente? Análisis de los programas de formación inicial docente en Urugay [How does the digital teaching competence matter? An analysis of initial teacher training programs in Uruguay]. *International Journal of Technology and Educational Innovation, 6*(2), 128-140. https://doi.org/10.24310/innoeduca.2020.v6i2.5601

Morrison, B. (2013). Do we know what we think we know? An exploration of online social network users' privacy literacy. *Workplace Review*. http://www.library2.smu.ca/handle/01/25696#.X3KW4NlKi00

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. https://doi.org/10.1177/0093650211418338

Rodríguez, G. L., & Magdalena, B. J. R. (2016). Perspectiva de los jóvenes sobre seguridad y privacidad en las redes sociales [Young people's perspective on security and privacy in social networks.]. *Revista ICONO14 Revista científica de Comunicación y Tecnologías emergentes*, *14*(1), 24-49. https://doi.org/10.7195/ri14.v14i1.885

Saldaña, M. (2007). La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos [Protecting Privacy in the Technological Society: The Constitutional Right to Privacy of Personal Information in the United States.]. *Revista Iberoamericana de Filosofía, Política y Humanidades, 9*(18), 85-115.

Salinas, J., & Silva J. (2014). Innovación con TIC en la formación inicial docente en Iberoamérica. En J. Silva & J. Salinas (Eds.), *Innovación con TIC en Formación Inicial Docentes: Aspectos teóricos y casos concretos* [Salinas, J., & Silva J. (2014). Innovation with ICT in initial teacher training in Latin America. *Innovation with ICT in Initial Teacher Training: Theoretical aspects and specific cases.* Ministry of Education Chile.] (pp. 1233). Ministerio de Educación Chile.

Selwyn, N. (2013). *Education in a Digital World: Global Perspectives on Technology and Education*. Routledge.

Shin, S. K. (2015). Teaching critical, ethical, and safe use of ICT in pre-service teacher education. *Language Learning & Technology, 19*(1), 181-197. https://doi.org/10125/44408

Silva, J., Miranda, P., Gisbert, M., Morales, M., & Onetto, A. (2016). Indicadores para evaluar la competencia digital docente en la formación inicial en el contexto Chileno – Uruguayo [Indicators to assess the digital competence of teachers in initial training in the Chilean - Uruguayan context.]. *RELATEC: Revista Latinoamericana de Tecnología Educativa, 15*(3), 55-67. http://dx.doi.org/10.17398/1695-288X.15.3.55

Šimandl, V., & Vaníček, J. (2017). Influences on ICT teachers' knowledge and routines in a technical e-safety context. *Telematics and Informatics, 34*(8), 1488-1502. https://doi.org/10.1016/j.tele.2017.06.012

Steijn, W., & Schouten, A. (2013). Information Sharing and Relationships on Social Networking Sites. *Cyberpsychology, Behavior, and Social Networking, 16*(8), 582-587. https://doi.org/10.1089/cyber.2012.0392

Suárez, J. M., Almerich, G., Gargallo, B., & Aliaga, F. (2010). Las competencias en TIC del profesorado y su relación con el uso de los recursos tecnológicos [ICT skills of teachers and their relationship with the use of technological resources]. *Archivos Analíticos de Políticas Educativas, 18*(10), 1-33. https://doi.org/10.14507/epaa.v18n10.2010

Torres-Gastelú, C. A. (2020). Participación en línea de los jóvenes en México, Colombia y Perú [Online Participation of young people in Mexico, Colombia and Peru.]. *Campus Virtuales. Revista Científica Iberoamericana de Tecnología Educativa, 9*(1), 69-83.

Torres-Gastelú, C. A. (2018). Formas de participación en línea en estudiantes de la Facultad de Administración de la Universidad Veracruzana, México [Forms of online participation in students of the Faculty of Administration of the Veracruzana University in Mexico]. *Actualidades Investigativas en Educación, 18*(2), 1-28. https://doi.org/10.5517/aie.v18i2.33131

Torres-Gastelú, C. A., Cuevas-Salazar, O., Angulo-Armenta, J., & Lagunes-Domínguez, A. (2020). Incidencia y frecuencia de la participación en línea de estudiantes universitarios mexicanos. El caso de la Universidad Veracruzana [Online Participation: Incidence and frequency in mexican university students: The case of veracruzana university.]. *Revista Formación Universitaria, 13*(1), 71-82. http://dx.doi.org/10.4067/S0718-50062020000100071

Torres-Gastelú, C. A., Cordero-Guzmán, D., Soto-Ortiz, J. L., & Mory-Alvarado, A. (2019). Influencia de factores sobre la manifestación de la ciudadanía digital [Influence of factors about the manifestation of Digital Citizenship.]. *Revista Prisma Social,* (26), 27-49.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the online privacy literacy scale (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law.* https://doi.org/10.1007/978-94-017-9385-8_14

Urista, M. A., Dong, Q., & Day, K. D. (2009). Explaining why young adults use myspace and Facebook through uses and gratifications theory. *Human Communication, 12*(2), 215-229.

Woollard, J., Wickens, C., Powell, K., & Russell, T. (2009). Evaluation of e-safety materials for initial teacher training: Can 'Jenny's Story make a difference? *Technology, Pedagogy and Education, 18*(2), 187-200. https://doi.org/10.1080/14759390902992659

World Bank Group. (2016). *World Development Report 2016: Digital Dividends*. World Bank Publications.

Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the Children's Internet Protection Act? *Journal of Applied Developmental Psychology, 30*(3), 209-217. https://doi.org/10.1016/j.appdev.2008.10.007

Young, A., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information Communication and Society, 16*(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757

Received: *November 01, 2020* Accepted: *January 30, 2021*

Cite as: Torres-Gastelu, C. A. (2021). Late adoption of preventive measures of online privacy in Mexican and Colombian university students. *Problems of Education in the 21st Century*, *79*(1), 162-184. https://doi.org/10.33225/pec/21.79.162

Carlos Arturo Torres-Gastelú
PhD Administration Sciences, Academic, University of Veracruz, Calle Puesta del Sol S/N. Fracc. Vista Mar. Veracruz, Ver. México.
E-mail: torresgastelu@gmail.com
Website: http://catg66.blogspot.com
ORCID: https://orcid.org/0000-0003-2527-9602