Article

Cyberethical Behaviour of High School Students in Selected Schools in uMhlathuze Municipality

Noxolo Nqobile Buthelezi
https://orcid.org/0000-0002-8338-7049
University of Zululand, South Africa
ButheleziNN@unizulu.ac.za

Dennis Ngong Ocholla
https://orcid.org/0000-0003-3860-1736
University of Zululand, South Africa
OchollaD@unizulu.ac.za

Lungile P. Luthuli
https://orcid.org/0000-0002-4310-8148
University of South Africa
luthulp@unisa.ac.za

Abstract

Cybertechnology has become a basic aspect of schools and universities with students' habitual use of these tools to communicate, learn, and play. However, schools and universities have faced numerous issues as a result of cyberethics activities in various settings. The study aimed to examine the cyberethical behaviour of high school students in selected schools in uMhlathuze Municipality. The objectives of this study were to explore the level of awareness about cyber ethical behaviour among the participants; identify the forms of cyberethics behaviour shown by the participants; demonstrate the application of the theory of planned behaviour (TPB) to the participants' cyberethical behaviour intentions; and ascertain the challenges that high school students face to act ethically when using the Internet and cybertechnologies. The study adopted a quantitative approach and a survey research design. Probability sampling was used to enrol grade 11 students from three conveniently selected high schools in the uMhlathuze municipality of KwaZulu-Natal. Data were collected by means of 214 questionnaires that were distributed to the participants. The study discovered a substantial number of challenges related to effective cyber ethical behaviour. The findings indicated a need for awareness of cyber ethical technology and how to mitigate its misuses. In addition, the study contributes to existing literature on the application of the TPB.

Keywords: cyberethical behaviour; cyberethics; cybertechnologies; grade 11 students; high schools; uMhlathuze Municipality

UNISA
Mousaion
#13249 | 18 pages

https://doi.org/10.25159/2663-659X/13249
ISSN 2663-659X (Online), ISSN 0027-2639 (Print)

Introduction

This article aimed to determine the importance of cyberethics awareness among grade 11 students in schools situated within uMhlathuze Municipality. Unfortunately, students are not sufficiently aware of their cyberethical behaviour (Aderibigbe 2019, 102). The concept of "cyberethics" has attracted several definitions. According to Polkowski (2015, 108), cyberethics is the study of computer ethics, including how people use computers, what computers are programmed to accomplish, and how they affect people and society. The terms "cyberethics," "information communication technology ethics," and "internet ethics" are often used to describe computing ethics (Jamal 2014, 26). However, "cyberethics" describes ethics in cyberspace. Thus, cyberethics is a concept that encompasses all types of applied ethics concerned with human actions that involve technology (Luppicini 2009, 39). In the application of technology to real-life circumstances, cyberethics attempts to find an appropriate worldview or philosophy (Shapiro and Gross 2013, 44).

Cyberethics was examined using the more well-known topics of computer and information ethics as a foundation. Computer and information ethics, as a part of applied ethics, can be defined as the field of study that examines the social and ethical implications of information and communication technology (ICT) (Aderibigbe 2019, 58).

Cyberspace is a dynamic environment that is constantly creating new and contentious ethical, social, and legal problems (Aderibigbe, Ocholla, and Britz 2021, 389). This study aimed to investigate the cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality and to gain knowledge of the factors that lead to such behaviour. The important factors influencing basic skills and concepts in ICT in the twenty-first century are generally recognised, and many schools have included these abilities in their teaching curricula (Barakabitze et al. 2019, 1). The use of the Internet leads to the unethical use of cybertechnologies. Therefore, studies such as the current one are very important in bringing awareness to the use of cybertechnologies.

Contextual Setting

The study was conducted among students from the three selected high schools in the Dlangezwa and Empangeni areas of the uMhlathuze local municipality in KwaZulu-Natal. A number of secondary private or state-supported high schools exist within the area.

Three schools were purposely chosen for this study. Dlangezwa High School for girls provides a rich learning environment enabling numerous students to study, develop, and grow. Ongoye High School is a rural public secondary school in a rural suburb of KwaDlangezwa; it offers tuition from grade 8 to grade 12 and is classified under quintile three as a no-fee institution. Empangeni High School was established in 1957 and is the largest and best-known high school in Zululand.

Problem and Purpose of the Study

The use of the Internet by high school students is currently posing challenges to cyberethics. It is critical to improve student knowledge of the importance of ethical problems surrounding cybertechnology in schools. Failure to identify solutions to this problem of unethical usage of cybertechnology can lead to more cyberbullying and children committing suicide because of things that have been said about them in cyberspace. Among identified gaps in the literature, as noted by Aderibigbe (2019, 11) referring to Africa, is that there is little research on cyberethics.

This study aimed to examine the unethical cyber behaviour of high school students in the three selected schools in uMhlathuze Municipality and gain knowledge of the factors that lead to such behaviour. The focus of this paper is based on the following research questions.

1. What is the level of awareness of cyberethical behaviour among students at the selected high schools in uMhlathuze Municipality?

2. What forms of cyberethics behaviour are revealed by the participants?

3. How does the theory of planned behaviour influence participants' behavioural intentions?

4. What are the challenges to the participants' efforts to act ethically when using the Internet and computers at the three selected high schools?

Theory and Literature Review

This study is informed by the theory of planned behaviour (TPB) developed by Ajzen (1991) which argues that an individual's purpose in undertaking a certain behaviour is a key aspect of the notion of planned behaviour. The theory considers that preferences capture the motivational variables that impact behaviour. They show how seriously someone is willing to try, and how much work they intend to put in, to exhibit the behaviour (Ajzen 1991, 180). Social, psychological, and knowledge factors have been shown to influence an individual's cyberethical decisions. Ajzen (2011, 1115) writes that the TPB is interested in predicting intentions and behavioural, normative, and control beliefs, as well as attitudes, subjective norms, and behavioural control perceptions, which are thought to influence and explain behavioural intents. It is true that the TPB is concerned with the regulated components of human information processing and decision-making. To defend this, Ajzen (2011, 1116) clarifies that it is largely concerned with goal-directed behaviour which is guided by conscious self-regulatory systems. This emphasis has been misconstrued to indicate that the theory assumes an unbiased, impassioned actor who evaluates all relevant information before making a behavioural decision (Ajzen 2011, 1116). Whether intentions predict behaviour is influenced by circumstances outside of the individual's control, that is, the

strength of the intended behaviour relationship is modulated by real control over the behaviour. Therefore, the stronger the intention to engage in conduct, the more likely its performance. The TPB has been used widely in related studies (Aderibigbe, Ocholla, and Britz 2021). TPB has been employed as an intervening theory in this study to evaluate and understand the cyberethical behaviour of students at selected high schools in uMhlathuze Municipality.

The association between the attitude toward the behaviour, subjective norms, perceived behavioural control, and behavioural intention is reflected in widely known graphical representations of the theory. As noted in a related study (Aderibigbe, Ocholla, and Britz 2021), all of these elements combine to impact students' willingness to engage in digital piracy and unethical use of cybertechnology. Furthermore, Aderibigbe (2019, 29) emphasises that students' perceptions of their capacity to control factors in their current situation, that either work with or restrain their ability to engage in unethical cyberbehaviour, are influenced by their previous experiences with computerised theft and dishonest use, as well as their perceptions of their ability to control factors, that either work with or restrain their ability, to engage in unethical cyberbehaviour. We found the theory to be applicable to this study.

High school studies associated with the use of learning technology primarily focus on its implementation and impact on the learning environment (Ozer, Ugurlu, and Beycioglu 2011). Similarly, younger children have caused increasing societal concerns about who bears the responsibility for guiding these children in the appropriate use of technology (Yamano and Jayne 2004, 86). The use of computers has transformed the teaching and learning process and has made education more accessible, independent, interactive, and interesting. According to Oyewole (2017, 69), university students in the twenty-first century cannot acquire knowledge without the assistance provided by using computers. For Oyewole (2017, 70), "most of the existing studies ascertained the level of awareness of students' ideas with regard to computer ethics, with some also considering the effect of gender." However, the level of awareness of issues associated with computer ethics could also determine the perceptions of students.

Many types of cyberethical behaviours lead to students being exposed to cybercrimes such as cyberbullying, which requires security. The growing list of cybercrimes includes crimes committed by computers, such as network intrusions and the spread of computer viruses, as well as computer-based variations of existing crimes, such as stalking, bullying, identity theft, and terrorism, which have become a major problem for individuals and the nation (Reddy and Reddy 2014, 58).

The literature review did not uncover any studies that focused on the study population and study area, yet high school students are quite vulnerable to cybercrime. We note recent studies in the domain focusing on university students (Aderibigbe and Ocholla 2020; Aderibigbe, Ocholla, and Britz 2021) whose cyberethical behaviour is likely to be different from those of high school students, largely because of demographic and

cognitive factors. There is a general assumption in related studies that students are not aware of cyberethical behaviours and the extent and level of awareness, where it exists, is not readily known.

Methodology

The concept of research methodology is widely understood. According to Goundar (2012, 10), research methodology is best defined as a systematic approach to problem-solving. In this quantitative study, a positivist paradigm was applied, a survey research design was used, and the data were collected using close-ended questionnaires. A sample for the study was drawn from the target population of high school students from the three high schools in uMhlathuze Municipality, namely Dlangezwa High, Ongoye High, and Empangeni High. The actual sample size was 480, which resulted in 214 targeted participants being invited to participate in the survey. The study adopted probability sampling and participants were selected using stratified and simple random sampling. The participants were drawn from each grade 11 class. The students were divided into subgroups and within each group, a simple random sampling was applied to get the desired sample. Data collected using the quantitative instrument were coded, and the analyses were carried out using SPSS version 28.0. The results are presented largely by descriptive statistics in the next section.

Findings and Discussions

This section focuses on the four research questions. Demographically, most of the students came from the Dlangezwa, Empangeni, and Ongoye high schools. Most of the participants were female in the age group 17–20, followed by 14–16-year-olds. The majority had spent less than one year in the grade.

Question 1: What is the level of awareness regarding cyberethical misbehaviour among students at the selected high schools in uMhlathuze Municipality?

There are different definitions of awareness, which is thought to be a precursor to the construction of attitudes and the eventual formulation of intentions prior to behaviour (Aderibigbe 2019). Determining participants' awareness and understanding of the concerns related to cyberethics misuse, which are highlighted in the survey instrument, is the foundation for eliciting participants' thoughts on the degree of their awareness of cyberethics misbehaviour (Ajzen 1993, 45). Children spend more time than any previous generation addicted to their gadgets and technology in the "age of screens." Undoubtedly, the Internet has provided a wealth of options for today's students to learn and develop their imaginations. The Internet's limitless knowledge also fosters creativity and fosters an environment that may help a child's intellectual growth in more ways than ever before.

The results revealed that the three high schools in the study have relatively high levels of awareness of cyberethics: 146 (68.2%) participants said they are aware of cyberethics, but when asked about their awareness of the teaching of cyberethics, 84.3% said "No," with a few saying "Yes" and others not responding to this question.

Table 1: Awareness of cyberethics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	The school does not teach us about cyberethical behaviour.	58	27.1	27.1	54.7
	I have never heard of this word before.	56	26.1	26.1	52.3
	Our teachers do not care if we face bullying or not.	27	12.6	12.6	72.0
	There are only two teachers who teach Life Orientation.	13	6.1	6.1	96.3
	They never mentioned it.	9	4.2	4.2	58.9
	It is because we are not taught enough about this, and it is quite a serious issue that needs to be addressed.	3	1.4	1.4	76.3
	Because they are also not that much educated about it.	1	.5	.5	73.4
	Because they do not want us to be fully aware of it and pay attention to it.	1	.5	.5	73.8
	Because it is the first-time hearing about it.	1	.5	.5	74.3
	Even they do not know.	1	.5	.5	74.8
	I am not exposed to some cyberbullying.	1	.5	.5	75.2
	I do not take the subject that deals with cyber ethical behaviour.	1	.5	.5	75.7
	I have never been taught about this.	1	.5	.5	76.2
	I have no idea.	1	.5	.5	76.6
	In this school, we are against bullying.	1	.5	.5	77.6
	Insufficient resources.	1	.5	.5	78.0
	It is because they do not want us to take pictures or videos at school.	1	.5	.5	78.5
	It is not in the curriculum.	1	.5	.5	79.0

It is because we are not taught enough about this and it is quite a serious issue that needs to be addressed.	3	1.4	1.4	80.4
It's not part of the curriculum	1	.5	.5	80.8
Occasionally, the school calls people to address the learners about cyberethics	2	.9	.9	82.2
The school does teach us about cyberethics.	1	.5	.5	86.0
The school has more than enough technological resources that are used for educational purposes.	1	.5	.5	86.9
The teachers do not teach us about cyberethics.	1	.5	.5	88.8
They have a tonne of work that has piled up	1	.5	.5	96.7
We learn about cyberethics but not frequently.	1	.5	.5	99.5
We usually come across cyberethics lecturing if one of our peers has been victimised.	1	.5	.5	100.0
Total	214	100.0	100.0	

The participants shared many reasons but most of them indicated they had never heard the words "cyberethics" or "cyberethical behaviour" mentioned in their school. This suggests an inadequate knowledge of cyberethics in schools. In a new era with the proliferation of social media and Internet technologies for daily use by students, such an omission can be catastrophic to teaching and learning in schools. The creation and expansion of awareness and education, for a comprehensive grasp of the ramifications of cyberethics abuse behaviour, should be a priority for every school seeking to secure its network and cyberspace. Therefore, a focus on education and training activities should be made for students who will begin their careers in higher institutions as cyber professionals, so that they can investigate in-depth both the fundamental aspects of cyberspace and acquire hands-on experience of the tools and techniques of the area (Schweitzer et al. 2009).

A focus on education and training activities is also supported by studies by the Council of the European Union (2015) and other developed countries on the awareness of the misuse of cyberethics. The European Union's decision-making body is more aware of cybercrime as a result of a project carried out by the data protection and cybercrime division to ensure a comprehensive response to cybercrime and other cyber offences involving the use of cybertechnology and electronic evidence. The project's significant

accomplishments include enhancing cooperation, introducing legal reforms, raising awareness, and establishing a network

Question 2: What forms of cyberethics behaviour were revealed by the participants?

There are many types of cyberethical behaviour that are reported in the literature (Aderibigbe and Ocholla 2020) and in this study (Table 2).

Table 2: Types of cyber ethical behaviours known to participants

No.	Cyberethics behaviour	Frequency	%
1.	Cyberbullying	122	57
2.	Using another user's password	35	16.4
3.	Dissemination of fake news	18	8.4
4.	Cybersquatting	8	3.7
5.	Cyberpiracy (software piracy: music and film downloading)	7	3.3
6.	Cyberstalking	7	3.3
7.	Hacking/carding/cracking	5	2.5
8.	Cybercrime	3	1.4
9.	Cybersex (Online pornography)	3	1.4
10.	Cyberfraud	3	1.4
11.	Cybervandalism	2	0.9
12	Plagiarism	1	0.5
13.	Identity theft	0	0
14.	Privacy violation	0	0
15.	Copyright violation	0	0

The participants were aware of more than one type of cyberethical behaviour, although it seems they experienced cyberbullying (57%) more than any other type of cyber unethical behaviour. Cyberbullying is quite common in schools. Evidently, cyberbullying, using another user's password, and disseminating fake news led the pack in this study in these three schools. This challenges schools to teach learners about the dangers of misuse of these types of behaviour. For example, raising awareness and implementing programmes that teach aspects of these types of cyberethics can reduce the high percentage of occurrence of these types. According to Khalil and Seleim (2012), users in colleges and at universities have engaged in a variety of abusive cyber behaviours. Aderibigbe (2019), Harris and Furnell (2012), and Oyewole (2017) write about the misuse of cybertechnologies by students. Harris and Furnell (2012) further emphasise that the utilisation of cybertechnologies in the academic setting is insecure owing to students' actions. Tavani (2013, 65) argues that by using these technologies, schools will be able to give their students an education that satisfies current industrial demands and teaches cutting-edge technical skills.

It is crucial to keep in mind that the current data depends on how much access the participants had to computers, laptops, tablets, and the Internet. It was evident that they

used smartphones more than laptops to connect to the technology. This simply means there are variations in the forms of cyberethics infractions committed by high school students. Owing to low access costs and wide availability, students are more prone to commit crimes and act unethically online. Peer pressure and other social forces are additional potential explanations for online infractions.

Question 3: How does the theory of planned behaviour influence participants' behavioural intentions?

The TPB is important and widely used in cyberethical research, as reported in a recent study (see Aderibigbe, Ocholla, and Britz 2021). Descriptive and inferential statistics were used to examine the impact of the TPB on the cyberethical behaviour of the high school participants in this study. The core concept of the TPB is that attitudes, subjective norms, and perceived behavioural control (PBC) all work together to establish behavioural intention and predict actual behaviour (Ajzen 1991). The study's findings prove that the three basic aspects of the theory—attitude, subjective norms, and PBC—are true, and considerably and uniquely influenced high school students' desire to violate cyberethics, which, in turn, was significantly connected with their actual behaviour (Table 3).

Table 3: Reactions to elements of TPB (N = 214)

No.	**Attitude towards cybertechnology behaviour**	**Yes**	**%**	**No**	**%**
1.	It is not essential to report instances of cyberethical violations.	60	28	154	72
2.	Learners regard incidents of cyberethical violation as commendable behaviour.	125	58.4	89	41.6
3.	It is tempting to engage in unethical cybertechnology behaviour.	118	55.1	96	44.9
4.	I will urge another learner to engage in the improper use of cyber-technology.	89	41.6	125	58.4
No.	**Influence of subjective norms on the use of cybertechnology**	**Yes**	**%**	**No**	**%**
1.	My classmates prefer carrying out this behaviour.	126	58.9	88	41.1
2.	My principal will want me to carry out the action.	62	29	152	71
3.	My religious community will back me up if I indulge in unethical cybertechnology behaviour.	83	38.8	131	61.2
4.	My family will be delighted to witness me indulge in unethical cybertechnology behaviour.	92	43	122	57
No.	**Influence of PBC on unauthorised use of cybertechnology**	**Yes**	**%**	**No**	**%**
1.	As a learner, it is quite easy for me to engage in unethical cyber behaviour.	114	53.3	100	46.7
2.	It would be relatively easy for learners at this high school to exploit cybertechnology unethically.	152	71	62	29
3.	I could easily carry out unethical use of cybertechnology and not get caught.	81	37.9	133	62.1

4.	My cybertechnology behaviour is neither controlled nor prevented by the school's cybertechnology policy.	124	57.9	90	42.1
No.	**Influence of BI towards cybertechnology acts**	**Yes**	**%**	**No**	**%**
1.	Friends and peers have an impact on a person's cyber-technology behaviour, both good and bad.	205	95.8	9	4.2
2.	The religious background of the student may influence some cyberethical goals and behaviour.	179	83.6	34	16.3
3.	The school's morale has little bearing on learners' cyber-technology behaviour.	133	62.1	81	37.9

The elements of the TPB have a considerable influence on students' behavioural intentions and, as a result, their cyberethical behaviour. The findings reveal that attitudes, subjective standards, and PBC all have a significant impact on students cyber ethical behaviour in high schools. The vast majority (95.8%) of participants believed that their peers had an influence on their cybertechnology behaviour. This alone shows that high school students are easily influenced by the people around them. Regarding PBC, half of the learners (53.3%) found it easy to engage in unethical cyber behaviour. Hence, high school learners find it easy to exploit cybertechnology unethically.

A study by Ibrahim (2016) found that rather than being affected by significant others, cyberethics misuse behaviour is more frequently caused by, or impacted by, structural or socio-economic factors. The intention was not predicted by the subjective norm. The best indicator of intention was PBC. The TPB is supported as a viable theory that might be used to account for users' propensity to engage in unethical online behaviour. Previous studies concur that attitude, subjective norms, and PBC all influence intention and behaviour. For instance, according to Peace, Galletta, and Thong (2003), user attitudes, subjective norms, and PBC all have a significant impact on online behaviour. Stone, Jawahar, and Kisamore (2010), Ajzen (1991), and Aderibigbe (2019) also found subjective norms to be a key factor influencing students' inclinations to engage in various unethical cyberactivities.

According to Aliyu et al. (2010), perceptions and attitudes concerning cyberethics behaviour have a substantial impact on how people utilise cybertechnology. They demonstrate how background elements, like general opinions, personality qualities, moral beliefs, and a sense of right and wrong all impact students' views on cyberethical behaviour. Other studies (Kreie and Cronan 2000; Leonard and Cronan 2005) have highlighted perceived personal gain, personal views, and qualities (i.e., religious ideals). Negative moral judgment, as well as economic and hedonistic benefits, have been cited as reasons for the public's attitude toward cyberethics (Cesareo and Pastore 2014). According to Chiang and Lee (2011), female students studying at a Chinese university placed great value on using cybertechnology effectively, especially when it comes to upholding laws, personal privacy, and intellectual property rights. Because there are few ethical and legal restraints, it is safe to claim that many undergraduate students have unfavourable sentiments about cybertechnology usage.

Russo et al. (2015), Cronan and Douglas (2006), Chatterjee, Sarker, and Valacich (2015), Chan and Wong (2015), and Chai, Wang, and Xu (2020) concur that attitudes and PBC affect high school students' cyberethical behaviour. Al-Rafee and Cronan (2006), Cronan and Douglas (2006), Cronan and Al-Rafee (2008), Chatterjee, Sarker, and Valacich (2015), and Chan and Wong (2015) report that a crucial antecedent of cyberethics misbehaviour is the subjective norm. This study supports claims made by Ajzen (1991), Snyder, Jones, and Bianco (2005), Aliyu et al. (2010), and Russo et al. (2015) that a person's attitude towards particular a behaviour influences the individual's participation; in this case, it is cyberethical behaviour.

Ajzen (1991, 2005), also found that people have a strong propensity to engage in behaviour when they have a reasonable amount of genuine control over it. The ease of access and the students' demonstrated proficiency in using cybertechnology, as evidenced by their experience, were used to perceive behavioural control. The availability of smartphones to learners pushes them to use the Internet and social networks.

Question 4: What are the challenges to the participants' efforts to act ethically when using the Internet and computers at the three selected high schools?

There are many challenges attributed to cyberethical behaviour in the subject literature and some are reported in this study (Table 4).

Table 4: Challenges of cyberethical behaviour among high school students

No.	Challenges of cyberethical behaviour among high school students	Yes	%	No	%
1.	Inappropriate use of cybertechnology owing to a lack of cyber-morality and ethical behaviour.	179	83.6	35	16.4
2.	There is a lack of policy guidelines on how to utilise and behave appropriately online.	181	84.6	33	15.4
3.	Appropriate understanding of cyberbehaviour is extremely limited.	142	66.4	72	33.6
4.	Inadequate security measures to ensure that cyberethics policy is followed.	136	63.6	78	36.4
5.	Breach of network integrity and confidentiality.	142	66.4	72	33.6

According to Stylianou et al. (2013, 44), individuals and organisations are challenged with new issues arising from unethical information activities, such as intrusions into personal privacy and intellectual theft, even beyond the undeniable benefits attributed to cybertechnology. The participants revealed that there is inappropriate use of cybertechnology owing to a lack of cyber morality and ethical behaviour, and some reported that appropriate understanding of cyber behaviour is extremely limited. The students are not aware of the cyberethical behaviour when they are using the Internet. Hence, not many studies have been conducted in high schools regarding cyberethical

behaviour. Inadequate security measures to enforce compliance with the cyberethics policy, a shortage of adequate alignment and education about the consequences of ethical violations, an overburdened teaching and learning syllabus, a dispute between authorship and access to information, a lack of cyber morality and ethical conduct in the use of cybertechnology, bureaucratic management processes, and breach of confidentiality are some of the challenges. Other obstacles to undergraduate students' efforts to behave morally online include a poor understanding of computer literacy and cybertechnology, insufficient understanding of the ethical aspects of cybertechnology, and a lack of training resources (Haughton et al. 2013). During the twenty-first century, students are able to use cybertechnologies for their personal matters and also for educational purposes. Consequently, concerns about cyberethical behaviours have been generated by limitless access to cyberspace. For instance, the rise in intellectual property crimes, such as software piracy and imitation of works of art in literature, music, movies, and videos, has grown alarmingly (Rujoiu and Rujoiu 2014).

Understanding security and privacy concerns, and the significant negative effects of cybertechnology on cyberspace, is particularly crucial. According to Gunarto (2003), a growing number of ethical issues, resulting from the detrimental effects of IT on our global society, must be addressed by global law enforcement, in addition to technical solutions like encryption, digital IDs, and firewall techniques. Despite the fact that ethical norms restrict the use of such technology to prevent ethical violations in so many schools, research suggests that students lack a grasp of ethical issues, awareness, and cybertechnology use.

Numerous studies of young individuals' use of cybertechnology in a university setting make use of moral theoretical notions. Some scholars (Calvani et al. 2012; Plaisance 2013; Vallor 2010) have argued that the moral aspects of cybertechnology should be considered. Some of the literature claims that, like previous technical breakthroughs and innovations throughout human history, cybertechnology has both positive and negative consequences on society and often creates moral and ethical dilemmas (Stahl, Eden, and Jirotka 2013; Von Schomberg 2012). There are not many studies on cyberethics in Africa, especially in high schools, and the study of recent patterns of unethical behaviour is still in its infancy in this area. As a result, the majority of African research on cyberethics adopts Western philosophical traditions as their points of reference.

This study concurs with previous findings by the National Cyber Security Alliance (2008) which found that financial constraints, time constraints, bureaucracy, and an overburdened syllabus were the barriers preventing students from acting in a morally proper manner. Some, on the other hand, have argued that separating ethical challenges will result in a lack of connections and a poor reflection of the entry of moral considerations and computing into the domain. This viewpoint was also expressed in a paper published by De Melo and De Sousa (2017), who expressed concern about the educational system's unresolved concerns, as a result of a lack of integrated courses in cyberethics education for undergraduate engineering students.

The study identifies an absence of cyberethics education in high schools and a shortage of specialists and experts to lead the courses. Thus, teachers are not paying much attention to this topic because they believe it does not affect them and the students, whereas it should be taught in high schools so that, as students get into the higher institutions, they are already aware of these unethical acts in cyberspace. Similarly, a study by Aderibigbe and Ocholla (2020) includes an absence of sufficient education for cyberethics educators, a lack of cyber morality, and unethical behaviour when utilising cybertechnology, among others.

Conclusions

The most relevant conclusions drawn from the findings are, first, that the students did not seem to be aware of the schools' cyberethics training requirements since the schools from the sample environment are not teaching enough about cyberethics. Second, among the several types of cyberethics behaviour, cyberbullying, using another person's password, and dissemination of fake news ranked highest, and most of the participants agreed that cyberethical behaviour is affected by skills and awareness of how to use cybertechnologies. The three main dimensions in the applied theory, namely attitude, subjective norms, and PBC exercised some importance and impact on cyberethics behaviour in the high schools under investigation. This supported the theory's applicability to the investigation of cyberethical behaviour in the study context. The students face many challenges (see Table 4) which require immediate intervention.

At least two limitations apply. First, the study was strictly directed to the grade 11 students at the selected schools in uMhlathuze Municipality. The case study, though it benefitted considerably from related global studies from comparison analysis, may not reflect the global trend. It does, however, reflect regional (Africa) trends.

The study recommends the following: high schools should provide information on cyberethics education; provide more knowledge on types of cyberethical behaviour, especially cyberbullying since it seems to be affecting learners; and should launch programmes that teach about cyberethics. This study discloses the hidden attitudes of a group of high school students concerning the use of cybertechnology and awareness of cyberethics among students in the uMhlathuze Municipality. The research is important in the context of the selected high schools in uMhlathuze Municipality for policy and decision-making, as well as for comparative research and practice in the domain.

Acknowledgements

This article is based on the first author's MA thesis (Buthelezi 2022).

References

Aderibigbe, N. A. 2019. “Cyberethical Behaviour of Undergraduate Students at University of Zululand, South Africa, and the Federal University of Agriculture, Abeokuta, Nigeria.” PhD diss., University of Zululand. https://uzspace.unizulu.ac.za/items/725e9053-d9a2-4232-b5f9-7285eb9b5531

Aderibigbe, N. A., and D. N. Ocholla. 2020. “Insight into Ethical Cyber Behaviour of Undergraduate Students in Selected African Universities.” *SA Journal of Information Management* 22 (1). https://doi.org/10.4102/sajim.v22i1.1131

Aderibigbe, D., D. N. Ocholla, and J. Britz. 2021. “Differences in Ethical Cyber Behavioural Intention of Nigerian and South African Students: A Multi-Group Analysis Based on the Theory of Planned Behaviour.” *Libri* 71 (4): 389–406. https://doi.org/10.1515/libri-2019-0062

Ajzen, I. 1991. “The Theory of Planned Behaviour.” *Organizational Behaviour and Human Decision Processes* 50 (2): 179–211. ResearchGate. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. 1993. “Attitudes Theory and the Attitude Behaviour Relation.” In *New Directions in Attitude Measurement*, edited by D. Krebs and P. Schmidt, 41–57. Berlin: Walter de Gruyter.

Ajzen, I. 2011. “The Theory of Planned Behaviour: Reactions and Reflections.” *Psychology and Health* 26 (9): 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Aliyu, M., N. A. Abdallah, N. A. Lasisi, D. Diyar, and A. M. Zeki. 2010. “Computer Security and Ethics Awareness among IIUM Students: An Empirical Study.” Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13–14 December. https://doi.org/10.1109/ICT4M.2010.5971884

Al-Rafee, S., and T. P. Cronan. 2006. “Digital Piracy: Factors that Influence Attitude Toward Behaviour.” *Journal of Business Ethics* 63 (3): 237–259. https://doi.org/10.1007/s10551-005-1902-9

Barakabitze, A., A. Kitindi, E., J. Sanga, C. Shabani, A., Philipo, J. and G. Kibirige. 2017. “New Technologies for Disseminating and Communicating Agriculture Knowledge and In-Formation: Challenges for Agricultural Research Institutes in Tanzania,” *Electronic Journal of Information Systems in Developing Countries* 70 (1): 1–22. https://doi.org/10.1002/j.1681-4835.2015.tb00502.x

Buthelezi, N. N. 2022. “Cyberethical Behaviour of High School Students in Selected Schools in uMhlathuze Municipality.” MA thesis, University of Zululand. https://uzspace.unizulu.ac.za/items/e8ddc60a-571d-46fc-bc97-5a83b968e7d6

Calvani, A., A. Fini, M. Ranieri, and P. Picci. 2012. “Are Young Generations in Secondary School Digitally Competent? A Study on Italian Teenagers.” *Computers & Education* 58 (2): 797–807. https://doi.org/10.1016/j.compedu.2011.10.004

Cesareo, L., and A. Pastore. 2014. “Consumer Attitude Behaviour Towards Online Music Piracy and Subscription-Based Services.” *Journal of Consumer Marketing* 31 (6/7): 515–525. https://doi.org/10.1108/JCM-07-2014-1070

Chai, C. S., X. Wang, and C. Xu. 2020. “An Extended Theory of Planned Behaviour for the Modelling of Chinese Secondary School Students’ Intention to Learn Artificial Intelligence.” *MDPI Journal Mathematics* 8 (11): 2089. https://doi.org/10.3390/math8112089

Chan, H. C. O., and D. S. Wong. 2015. “The Overlap between School Bullying Perpetration and Victimization: Assessing the Psychological, Familial, and School Factors of Chinese Adolescents in Hong Kong.” *Journal of Child and Family Studies* 24 (11): 3224–3234. https://doi.org/10.1007/s10826-015-0125-7

Chatterjee, S., S. Sarker, and J. S. Valacich. 2015. “The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use.” *Journal of Management Information Systems* 31 (4): 49–87. https://doi.org/10.1080/07421222.2014.1001257

Chiang, L., and B. Lee. 2011. “Ethical Attitude and Behaviours Regarding Computer Use.” *Ethics and Behaviour* 21: 481–497. https://doi.org/10.1080/10508422.2011.622181

Council of the European Union. 2015. Evaluation Report on the Seventh Round of Mutual Evaluations: The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime Report on Slovakia, Brussels, 22 September 2015, 9761/1/15 REV 1 DCL

Cronan, T. P., and S. Al-Rafee. 2008. “Factors that Influence the Intention to Pirate Software and Media.” *Journal of Business Ethics* 78 (4): 527–545. https://doi.org/10.1007/s10551-007-9366-8

Cronan, T., and D. Douglas. 2006. “Information Technology Ethical Behaviour: Towards a Comprehensive Ethical Behaviour Model.” *Journal of Organizational and End User Computing* 18 (1).

De Melo, C., and T. De Sousa. 2017. “Reflections on Cyberethics Education for Millennial Software Engineers.” In *2017 IEEE/ACM 1st International Workshop on Software Engineering Curricula for Millennials (SECM)*, 40–46. Buenos Aires: IEEE. https://doi.org/10.1109/SECM.2017.10

Goundar, S. 2012. *Research Methodology and Research Method*. Research Gate Publications.

Gunarto, H. 2003. *Ethical Issues in Cyberspace and IT Society*. Asia: Pacific University.

Harris, M., and S. Furnell. 2012. “Routes to Security Compliance: Be Good or Be Shamed?” *Computer Fraud & Security* 2012 (12): 12–20. https://doi.org/10.1016/S1361-3723(12)70122-7

Haughton, N. A., K. C. Yeh, J. Nworie, and L. Romero. 2013. “Digital Disturbances, Disorders, and Pathologies: A Discussion of Some Unintended Consequences of Technology in Higher Education.” *Educational Technology* 53 (4): 3–16.

Ibrahim, S. 2016. “Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals.” *International Journal of Law, Crime and Justice* 47: 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Jamal, A. 2014. *Computer Ethics*. Karnataka: Government Degree College.

Khalil, O. E., and A. A. Seleim. 2012. “Attitudes Towards Information Ethics: A View from Egypt.” *Journal of Information, Communication and Ethics in Society* 10 (4): 240–261. https://doi.org/10.1108/14779961211285872

Kreie, J., and T. P. Cronan. 2000. “What is Computer Ethics?” *Communications of the ACM* 43 (12): 66–67. https://doi.org/10.1145/355112.355126

Leornard, L., and T. Cronan. 2005. “Unethical Behaviour in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems* 1 (12): 25–43.

Luppicini, R. 2009. “Technoethical Inquiry: From Technological Systems to Society.” *Global Media Journal* 2 (1): 5–21..

National Cyber Security Alliance. 2008. “National Cyberethics, Cybersafety, Cybersecurity Baseline Study.” https://www.edtechpolicy.org/cyberk12ARCHIVE/Documents/C3Awareness/NationalC3BaselineSurvey_Extract_sept_2010.pdf

Oyewole, O. 2017. “Awareness and Perception of Computer Ethics by Undergraduates of a Nigerian University.” *Journal of Information Science Theory and Practice* 5 (4): 68–80.

Ozer, N., C. T. Ugurlu, and K. Beycioglu. 2011. “Computer Teachers’ Attitudes Toward Ethical Use of Computers in Elementary Schools.” *International Journal of Cyber Ethics in Education* 1 (2): 15–24. https://doi.org/10.4018/ijcee.2011040102

Peace, A. G., D. F. Galletta, and J. Y. Thong. 2003. “Software Piracy in the Workplace: A Model and Empirical Test.” *Journal of Management Information Systems* 20 (1): 153–177. https://doi.org/10.1080/07421222.2003.11045759

Plaisance, P. L. 2013. *Media Ethics: Key Principles for Responsible Practice*. Sage Publications. https://doi.org/10.4135/9781544308517

Polkowski, Z. 2015. “Ethical Issues in the Use and Implementation of ICT.” *Journal of Management and Research* 21 (2): 2–5.

Reddy, G. N., and G. J. Reddy. 2014. “A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies.” *International Journal of Engineering and Technology* 4 (1): 22–29. https://doi.org/10.48550/arXiv.1402.1842

Rujoiu, O., and V. Rujoiu. 2014. “Academic Dishonesty and Workplace Dishonesty: An Overview.” In *Proceedings of the 8th International Management Conference on Management Science and Engineering Management*, edited by Jiuping Xu, Virgílio António Cruz-Machado, Benjamin Lev, and Stefan Nickel, 928–938. Cham: Springer.

Russo, D., J. Stochl, M. Painter, and G. Shelley. 2015. “Use of the Theory of Planned Behaviour to Assess Factors Influencing the Identification of Students at Clinical High Risk for Psychosis in 16+ Education.” *BMC Health Services Research* 15 (1): 411. https://doi.org/10.1186/s12913-015-1074-y

Schweitzer, D., D. Gibson, D. Bibighaus, and J. Boleng. 2009. “Preparing Our Undergraduates to Enter a Cyber World.” In *Information Assurance and Security Education and Training*, edited by Ronald C. Dodge and Lynn Futcher, 123–130, Berlin: Springer. https://doi.org/10.1007/978-3-642-39377-8_13

Shapiro, S., and S. J. Gross. 2013. “Ethical Educational Leadership in Turbulent Times: Resolving Moral Dilemmas.” ResearchGate. Accessed 5 September 2022. https://www.researchgate.net/publication/286666985_Ethical_Educational_Leadership_in_Turbulent_Times_ReSolving_Moral_Dilemmas

Snyder, I., A. Jones, and J. Bianco. 2005. *Using Information and Communication Technologies in Adult Literacy Education: New Practices, New Challenges*. An Adult Literacy National Project Report. Adelaide: National Centre for Vocational Education Research Ltd.

Stahl, B. C., G. Eden, and M. Jirotka. 2013. “Responsible Research and Innovation in Information and Communication Technology: Identifying and Engaging with the Ethical Implications of ICTs.” In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, edited by Richard Owen, John Bessant, and Maggy Heintz, 199–218. New York: Wiley. https://doi.org/10.1002/9781118551424.ch11

Stone, T. H., I. M. Jawahar, and J. L. Kisamore. 2010. “Predicting Academic Misconduct Intentions and Behaviour using the Theory of Planned Behaviour and Personality.” *Basic and Applied Social Psychology* 32 (1): 35–45. https://doi.org/10.1080/01973530903539895

Stylianou, A. C., S. Winter, Y. Niu, R. A. Giacalone, and M. Campbell. 2013. “Understanding the Behavioural Intention to Report Unethical Information Technology Practices: The Role of Machiavellianism, Gender and Computer Expertise.” *Journal of Business Ethics* 117 (2): 333–343. https://doi.org/10.1007/s10551-012-1521-1

Tavani, H. T. 2013. “Cyberethics.” In *Encyclopaedia of Sciences and Religions*, edited by A. L. C. Runehov and L. Oviedo, 565–570. Dordrecht: Springer. https://doi.org/10.1007/978-1-4020-8265-8_279

Vallor, S. 2010. “Social Networking Technology and the Virtues.” *Ethics and Information Technology* 12 (2): 157–170. https://doi.org/10.1007/s10676-009-9202-1

Von Schomberg, R. 2012. “Prospects for Technology Assessment in a Framework of Responsible Research and Innovation.” In *Technikfolgen abschätzen lehren*, edited by M. Dusseldorp and R. Beecroft, 39–61. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-93468-6_2

Yamano, T., and T. S. Jayne. 2004. “Measuring the Impact of Working Age Adult Morality on Small Scale Farm Household in Kenya.” *Journal of World Development* 32 (1): 91–119. https://doi.org/10.1016/j.worlddev.2003.07.004