ANTI-CYBER AND INFORMATION TECHNOLOGY CRIMES LAWS AND LEGISLATION IN THE GCC COUNTRIES: A COMPARATIVE ANALYSIS STUDY OF THE LAWS OF THE UAE, SAUDI ARABIA AND KUWAIT

Rahima Aissani, Al Ain University

ABSTRACT

The paper will focus on analyzing and comparing the laws governing the use of "IT Crimes and cybercrime" in three countries of the GCC Countries: UAE: The Law "Combating Information Technology Crimes" was passed in 2012 by Decree Law No: 5 / 2012, which was published in the Official Gazette No: 540, attached to the 42nd year, on 26/8/2012, and included amendments to the provisions of the law Federal No: (2) for the year 2006 establishing the Law "Combating Information Technology Crimes". Saudi Arabia Through the "Anti-Information Crime System", which was issued by the Council of Ministers No: 79 dated 7/3/1428 H corresponding to March 26, 2007, and was ratified by Royal Decree No: M /17 dated 8/3/1428 H, 27 March 2007. Kuwait, which approved the Law "Combating Information Technology Crimes", No: 63 / 2015, which was published in the Official Gazette on 7/7/2015, was activated as of 12/1/2016.

The study will be based on a content analysis methodology for the basic articles of the legislation governing cyber-crimes in the context of the "Combating Information Technology Crimes" in: UAE, Saudi Arabia, and Kuwait.

The study came up with the following conclusions: The UAE's "Combating Information Technology Crimes" legislation includes more legal articles than the Saudi and Kuwaiti laws, and has more details of cyber-crimes and penalties than other laws. Most of the drafting of legal articles in the "Combating Information Technology Crimes" in the three countries have come in the form that obliges users to be responsible for morality and social responsibility in the communication of information technologies. "Combating Information Technology Crimes" in the three countries revealed the evidence of four basic ethics involving Respect for the Privacy and Dignity of Persons, and three basic ethics under the principle of "Respect for Community Values".

Keywords: New Media Ethics, Laws against IT Crimes, Cybercrime, New Media Uses.

INTRODUCTION

Several international bodies and organizations, as well as governments around the world and in the Arab world, have been engaged in the enactment of laws and legislation regulating the

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

use of information, media, and technology tools in an advanced effort to mitigate the negative effects of the lack of legislation governing and controlling this open space. The Gulf States have pursued the path that most other countries in the world have taken to protect information using laws on intellectual property, so that the protection of such laws extends to include computer software and applications, before some of them have taken the path of issuing anti-cybercrime laws and regulations.

The United Arab Emirates was the first Arab country to issue a special law on combating information technology crimes, when Federal Law No. 2 of 2006 was issued, and the Federal Legal Decree No. 5 of 2012 promulgating the Law on "*Combating Cyber Crimes*", which was published in Official Gazette No. 540, supplement of the year Forty-Two, dated 26-08-2012, setting out amendments to the Federal Law No. (2) of 2006 promulgating the Law on "*Combating Cyber Crimes*", which is one of the model laws that dealt with most of the types of information cyber-crimes.

Saudi Arabia issued the "*Anti-Cyber Crime Law*" (1993), under the Council of Ministers Decision No. 79, dated 7 /3 /1428 AH, and it was approved by Royal Decree No. M /17, dated 8 /3 /1428 AH. The "*Anti-Cyber Crime Law*" in the Sultanate of Oman was issued in the first quarter of 2011, under Royal Decree 12 /2011. Bahrain announced the start of control of social networking sites in August 2013. Sheik Fawaz Al Khalifa, Minister of State for Bahraini Communications Affairs, announced the establishment of a monitoring and coordination office to "*apply legal procedures against anyone who misuses social media and tampers with Bahrain's security and stability*", as recommended by the National Council Against Terrorism. The Ministry has established a hot line for citizens and residents to report any social network sites or accounts that incite or endorse violence and terrorist activities, endanger the safety of citizens and residents, harm their public interests, threaten national unity, or negatively affect civil peace and security.

Based on the decisions of the Gulf Cooperation Council Summit held in Manama on December 24-25, 2012, which stipulated the need to strengthen control over the Internet as part of efforts to combat terrorism, the State of Kuwait approved Law No. 63 of 2015 on "*Combating Information Technology Crime*", published in the Official Gazette on 7 /7 /2015 and effective as of 12 / 1/2016.

New technologies of communication and information have imposed a completely new reality in media and communication. It has shifted to the level of absolute sovereignty in terms of prevalence, penetration of all space and time barriers, the infinite variety of messages and content with its unlimited universal access capabilities and outreach, and its diverse techniques, tools, uses and applications, open-ended cyberspace, without any boundaries, barriers, or differences.

The internet, with its instant messaging tools and social networks, has become a crucial meeting place where children can exercise their right to freedom of expression by connecting with friends and family and with other children who share their interests. In the 11 countries surveyed, many children can be considered ‘active socializers’, in that they take part in a range of social activities online each week-such as chatting with friends and family, using various messaging tools and networking with people who have similar interests. Some children also report that they find it easier to express their true selves online (United Nations Children's Fund,

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

2019).

New challenges dictate the balance between the right to use and the prevention of a threat to community security. That is why it is crucial to have controls governing and guiding the use process and to ensure that these risks are addressed according to their distinct characteristics, which require a holistic strategy that focuses not only on the security solution but also on all other dimensions (social, economic, and cultural). Academic studies have sought to find solutions to this and have introduced the concept of global knowledge ethics as an appropriate context for the development of a framework for knowledge ethics, while other researchers have proposed the development, renewal, and development of existing ethical guidelines, such as pragmatism, virtue ethics, ethics of care and moral concerns.

Several researchers and experts stressed the need to take account of the ethics and general customs on the Internet, and its uses for media and communication. Each user must assume responsibility for these platforms. Researchers and experts indicated that the freedom of expression offered by social media platforms demands, in particular, that everyone respects his/her conscience in writing, reflects on the implications of the words he/she shares on his/her own page or account, and does not establish biases or words that might hurt others (International Telecommunication Union, 2020).

Saudi Arabia, the UAE and Kuwait have demonstrated legislative and regulatory interest in social networking sites and what is published on them. Some social networking sites have been officially included in the regulatory tools, considering the posts they share as reports, requiring investigation of those who violate the rules of integrity. At the same time, they have committed government institutions to increase their involvement in the issues presented in newspapers and TV shows that may be evidence of violations.

Based on the foregoing, this study will discuss the legal articles included in those legislations and their indicators on the ethics of the use of information technology, through an analysis study of the laws of "*Combating Information Technology Crimes*" in the UAE, Saudi Arabia, and Kuwait. In the analysis, three questions were raised.

1. What legal content do the three countries of which the study sample is comprised, have in their "*combating information technology crimes*" legislation?
2. What is the ethics of the use of information technology in accordance with the wording and concept of such legislations and laws?

The study aims to achieve the following:

1. Cognitive Outcomes: Its basis is to contribute to the creation of a sound knowledge system in the field of specialization (media and communication) and to the enrichment of empirical research on new media and its tools, represented by most of the uses of information technology, and the challenges it poses to users, particularly in our Arab countries and our social and cultural systems.
2. Practical Outcomes: Most important of which are: Introduction of all media laws and legislation in the field of the Internet and its applications in the countries of the Gulf Cooperation Council and the Arab Region, Research and analyze these laws and legislation, and their implications for ethics, principles, and community values. Thus, developing a perception of the laws and ethics of the use of information technology in the countries of the Gulf Cooperation Council in particular.

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

METHODOLOGY AND SAMPLE

Since our research belongs to the Descriptive and Explanatory Research, we will therefore use the content/method analysis tool (quantitative and qualitative) for the basic articles of the legislation governing cyber-crimes in the context of the "*Combating Information Technology Crimes*" in three Gulf Cooperation Council countries, namely: UAE, Saudi Arabia, and Kuwait. In order to familiarize ourselves with the laws and ethics of the use of information technology in the countries of the Gulf Cooperation Council, we have adopted two categories of analysis:

1. Form of laws/legislation: In order to know the legal articles governing the use of information technology, the following analysis units were included: Form of law/legislation Substance and its contents.
2. Substance of laws/legislation: And its relevance to the ethics of the use of information technology in the countries of the Gulf Cooperation Council.

Anti-Cyber and Information Technology Crimes Laws and Legislation in the UAE, Saudi Arabia, and Kuwait: Form of Law/Legislation

Number of articles included in each law and legislation on "*combating information technology crimes*" in the three countries of which the study sample (Figure 1) is comprised:

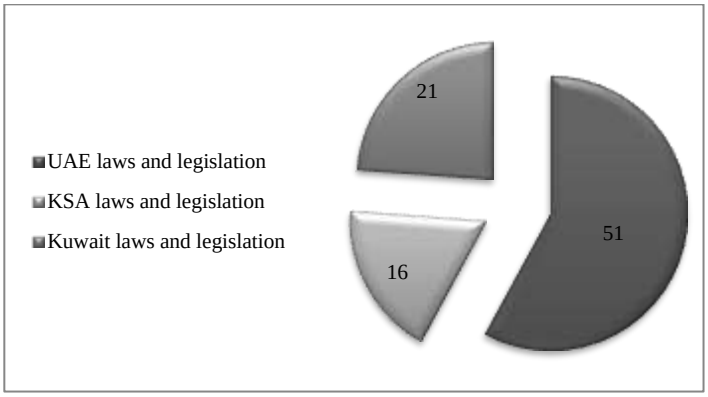

FIGURE 1
SHOWS THE NUMBER OF ARTICLES INCLUDED IN EACH LAW AND LEGISLATION ON "*COMBATING INFORMATION TECHNOLOGY CRIMES*" IN THE THREE COUNTRIES

Federal Law No. 2 of 2006 was issued, followed the UAE Law on "*Combating Cyber Crimes*" of 2012, which included 51 legal articles. The Law on Anti-Cybercrime in Saudi Arabia was issued in 2007 and included 16 articles (Al-Laban, 2014).

The State of Kuwait passed the Law on "*Combating Cyber Crimes*" in 2015. The Government of Kuwait, represented by the Ministry of Interior, has announced the start of its implementation and enforcement as of (12 January 2016). The law included 21 articles.

The "*Riyadh Document*", adopted at the 2012 Manama Summit, is a unified law to combat information technology crimes in the six countries of the Gulf Cooperation Council. It prohibits "*the*

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

promotion of ideas that violate public order and public morality". It prohibits "*the promotion of ideas that threaten public order and public morality*". It preserves the rights resulting from the legitimate use of computers and information networks and protects the national economies of the GCC States and acts against those who maintain a website and publish information on the Internet or a means of information technology for a terrorist group to facilitate contact with its leaders, members, promote or finance their ideas (Riyadh Document, 2013).

Figure 1 show that the UAE's "*Combating Information Technology Crimes*" legislation included a larger number of legal articles compared to Saudi and Kuwaiti legislation, as several types of cyber-crimes have been detailed, as in Figure 2 indicates. Federal Law No. (5) of 2012 amended the UAE Law No. (2) Of 2006 with a view to keeping abreast of local, regional, and international changes and developments. Therefore, the new legislation includes crucial additions for the following issues (Hassan, 2015):

1. Acts related to terrorist crimes, electronic transactions, e-commerce, and human trafficking crimes, and those relating to tourism, antiquities, firearms, ammunition, explosives, and cybersecurity, which are not covered by the old legislation.
2. Adding new definitions that were not included in the old legislation, where the definitions included the following terms: (Financial, Commercial or Economic Institutions, Electronic, IT Protocol, Juvenile Pornography, Secret, Capturing, Abuse), the purpose of which was to include illegal electronic activities and acts, as well as commercial transactions using technical systems.
3. The tendency of the UAE legislator has been to increase freedom-restricting penalties and to increase the value of financial penalties. It also provided for certain accessory and complementary penalties and measures in the new legislation, contrary to what was stated in the 2006 legislation, in that it approved life imprisonment for freedom-restricting crimes and life imprisonment in the new legislation. The law also provides for a penalty of half of the total penalty for offenses committed in the event of an attempted offence, as provided for in Article (40).
4. As for the fine, it was not more than 200 thousand dirhams in the old legislation, while the new value amounted to 3 million dirhams.

Therefore, the UAE project has in fact aligned itself with the technological, informational, economic, and social changes that have led to the emergence of electronic crimes at the global level and their prevalence in many countries of the world, and the prediction of their damages and risks. The UAE legislator has been concerned with the adoption of a criminal legislative policy aimed at describing all the actions and behaviors that are considered cyber-crimes, with the establishment of the necessary sanctions for it, as concluded by study of the "*UAE project policy to combat cyber-crime*" (Hassan, 2015).

Substance and Its Contents

The UAE law includes a number of articles that provide legal protection for the privacy of information, data, and numbers published and circulated on the Internet (Figure 2). These articles include the criminalization of the following (Aissani, 2018):

1. Whoever creates, operates, maintains, transmits, disseminates, republishes, or reproduces, via the Internet, pornographic or gambling activities and everything that might prejudice public morality, induces or incites others to commit acts of pornography or indecent acts, or assists others to do the same, and whoever, through the use of information networks or an IT medium, insults other persons or attributes to them an incident that would render them punished or despised by others.

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

2. Whoever uses an information network or an information technology device to attack the privacy of people, whether such attack was carried out by eavesdropping, intercepting, recording or transmitting conversations or communications or audio or video materials, or taking pictures of others or preparing electronic pictures, transferring, disclosing, copying, maintaining, or publishing news, electronic pictures or photographs, scenes, comments and/or data, even if the information is true and correct.
3. Whoever establishes, manages, or oversees a website or disseminates information via a network or a means of information technology with the intention of carrying out human or human organ trafficking, or dealing in the same illegally, or promotes or motivates the use of any programs or ideas that cause hatred, racism or sectarianism, or harm national unity or social peace or disturb public order or public morals, or promote the use of firearms, ammunition or explosives in circumstances other than those authorized by law, or promotes terrorist groups and their ideas.
4. Whoever, by using any information network or an information technology means, publishes information, news, data or rumors on a website, to ridicule or harm the reputation, prestige or status of the State or any of its institutions, its president or his deputy, the rulers of the emirates, their crown princes, deputy rulers of the emirates, the flag, the national salute, the national emblem, the national anthem or symbols, or incites acts, or publishes or broadcasts information, news, cartoons or any other images that may endanger the security of the State and its supreme interests or prejudice public order, or extorts or threats another person to get him to act or refrain from acting by using a network or an information technology means.

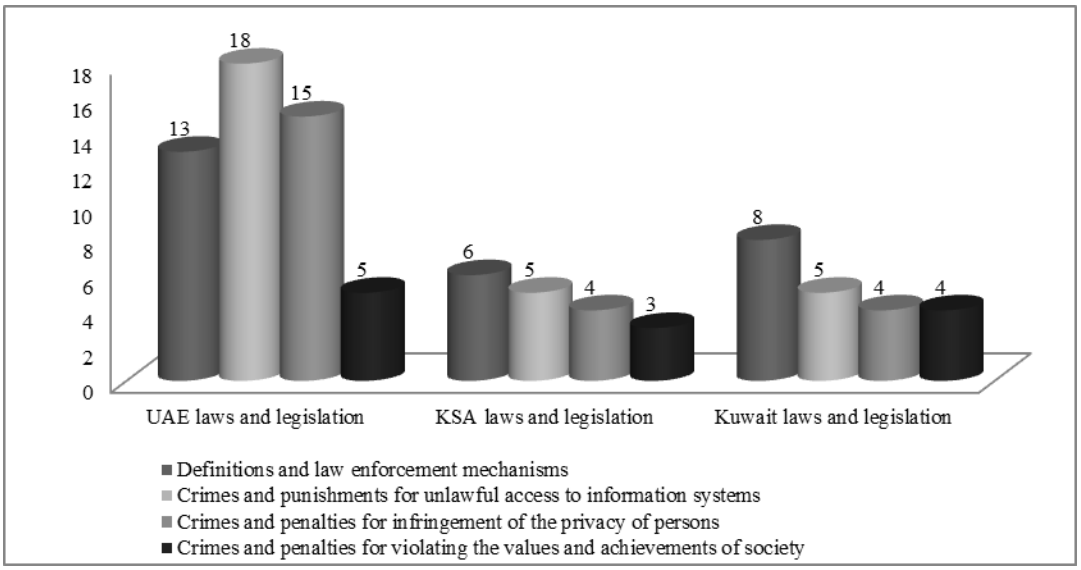

FIGURE 2
OUTLINES THE SUBSTANCE AND CONTENTS OF THE LAWS AND LEGISLATION ON COMBATING INFORMATION TECHNOLOGY CRIMES IN THE THREE COUNTRIES

The Law on "*Anti-Cyber Crime*" in Saudi Arabia included (16) articles:

1. Article One included the definition of ten terms of information technology terms such as; cyber-crime, information system, information network, unauthorized access, website, and others.
2. Article Two dealt with the purposes of the legislation and the law.
3. Articles from Three to Ten included crimes that could be committed by any of the various means of information technology, and their punishments: Crimes of unauthorized use of data stored on a computer, Computer hacking crimes that destroy programs and data, Crimes committed through the use of computers

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

to plan or commit a specific crime, and Crimes of illegal use of computers by individuals authorized to use them: Employees working in computer centers, Employees who are dissatisfied with their organizations or companies, the abuser category, like hackers and crackers, and People involved in organized crime through the use of computers.

4. Articles Eleven to Thirteen are concerned with the procedures and powers of the Court.
5. Article Fourteen stipulates that the Communications and Information Technology Commission, pursuant to its powers, shall provide the assistance and technical support to competent security agencies during the investigation stages of such crimes and during trial.
6. Article Fifteen stipulates that the Bureau of Investigation and Public Prosecution shall carry out the investigation and prosecution of crimes stipulated in this Law.
7. Article Sixteen stipulates that the Law shall be published in the Official Gazette and shall enter into force one hundred and twenty days after the date of publication.

The Kuwaiti law included 21 articles:

1. In its first chapter, the first article dealt with definitions of the technical terms included in the Law.
2. Chapter Two deals with crimes and penalties. Article (2) in this chapter provided for a crime of unauthorized access to computers or information systems by means of information technology, and the second and third paragraphs increased the penalty in the event that such access resulted in the cancellation or destruction of data or in the case of personal information, and the fourth paragraph stipulated that the penalty should be increased if the crime is committed during or because of the performing of the job.
3. Article (3) also provides for an aggravating penalty in the event that the data in question are governmental or related to the accounts of clients in banking facilities. The same Article criminalizes the forgery or destruction of electronic documents, both private and public, including those relating to medical examinations, as well as the use of any means of information technology to threaten or extort persons, and increases the penalty if there is a threat of felony or infringement of the dignity or honor of persons.
4. Article (4) provides for the punishment of those who deliberately obstruct or disable access to websites, whoever eavesdrops on what is being transmitted through the information network, and whoever has created a site that contains an infringement of public morals or incitement to prostitution and debauchery.
5. Article (5) provides for the punishment of anyone who, by means of information technology, has access to credit card data and has used it to obtain funds from other persons. Articles (6) and (7) require that any person who has committed any of the prohibitions set out in the Press and Publications Act, by means of electronic means, be punished.
6. Articles (8), (9) and (10) punished anyone who uses any of these means to promote human trafficking, or narcotic substances, or facilitate contact with terrorist organizations, or promote their ideas or promote money laundering. Articles (11) to (19) included general provisions, including cases of exemption from punishment, the decision to confiscate or close a shop or site, the criminal responsibility of the legal person, the sole competence of the Public Prosecutor to investigate, act in connection with and prosecute such crimes, and provisions for the extinction of penal and civil claims.

The explanatory note of Law No. 63 of 2015 on Kuwaiti anti-cybercrimes explained the reasons for the promulgation and operation of the Law and its importance. The use of international information networks in the modern age as a means of communication, in all areas of life, has been extended to achieve what humanity aspires to in terms of saving time, distance, and physical and mental effort. These networks provide infinite information that relates to all fields of life, including personal, economic, and scientific information.

On the other hand, however, the increased use of these networks and information systems has led to many risks, as they have resulted in new types of crimes known as "*information crimes*" such as embezzlement and counterfeiting crimes committed by electronic means, crimes against ethics and

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

public morals, information theft, and the penetration of confidential systems.

"*Traditional criminal law does not help in dealing with these newly committed crimes, which depend on modern technologies, and does not help in protecting the rights, dignity, and reputation of individuals or in defending against the aggression of public and private property. In order to help international efforts to counter these crimes, and to comply with the provisions of the Arab Convention to Combat Crimes of Information Technology, ratified by the State of Kuwait under Law No. (60) Of 2013, an annexed legislation has been drawn up*" (Explanatory Note, 2015).

A comparative analysis of the content of the legal articles in the three sample countries (United Arab Emirates, Saudi Arabia, and Kuwait) showed that UAE law has more penalties than that of the law in Saudi Arabia and Kuwait.

1. For example, the UAE legislator has drawn up, in 18 articles, crimes and penalties relating to access to information technology systems, while the Saudi and Kuwaiti legislators have drawn up (only five articles for each legislation).
2. The UAE legislator has drawn up 15 articles on crimes and penalties against privacy and properties, while the Saudi and Kuwaiti legislators have drawn up (only four articles for both legislations).
3. The UAE legislator has drawn up five articles on punishments for violating the values and achievements of society, while the Saudi and Kuwaiti legislators have drawn up (three articles and four articles, respectively).

Type of Punishments Imposed by Law and Legislation in the Three States

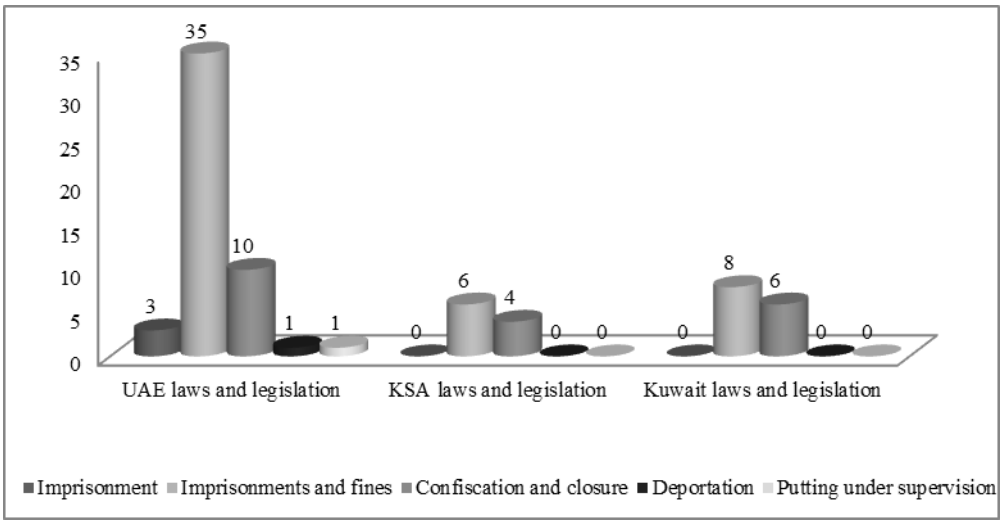

FIGURE 3
DESCRIBES THE TYPE OF PENALTIES FOR VIOLATORS OF THE LAWS AND LEGISLATION ON "*COMBATING INFORMATION TECHNOLOGY CRIMES*" IN THE THREE COUNTRIES

The Figure 3 and data of the above Figure 3 indicate that the penalties imposed by the UAE, Saudi and Kuwaiti legislators on the perpetrators of the cybercrimes, as set out in the articles of their laws and legislations for combating information technology crimes, ranged mostly between two types, including.

1. Imprisonment with a fine.

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

2. The confiscation of the equipment, software, tools used or funds collected therefrom, as well as the closure of the shop or site where any of these crimes has been committed, either by complete closure or for a time determined by the court. In UAE law, prison sentences ranged from one year to life imprisonment, while in Saudi law, prison terms ranged from one to ten years, and in Kuwaiti law, prison terms ranged from 6 months to 10 years. The fine ranged from 100 thousand dirhams to 3 million dirhams under UAE law and from 500,000 riyals to 5 million riyals under Saudi law and from 500 dinars to 50 thousand dinars under Kuwaiti law.

Ethics of the Use of Information Technology

Article 17 of the International Covenant on Civil and Political Rights stipulates that: No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The Code of Ethics for Electronic Journalists of the International Federation of Electronic Journalism defines the principles and ethics of electronic publishing as follows: Defend the principles of freedom to access and disseminate information, guarantee the right to respond and criticize, express opinions and comment on information, Follow honest means in obtaining information, pictures, and documents, Dependence on well-known sources, protecting them and preserving their confidentiality, Not engaging in defamation, slander, and harassment campaigns, Refrain from taking gifts and donations, or from offering press coverage, in exchange for special financial benefits, and Provide the right to respond to those affected.

On the basis of the two previous documents, the ethics of the use of information technology will be defined in three key groups: 1) Demonstrating a sense of responsibility, 2) Ethics of Respect for the Privacy and Dignity of Persons Including: Refraining from insulting, slandering, and defamation, refraining from threats and blackmail, refraining from spreading ideas of hatred and racism, 3) Respect for Community Values.

In the light of the previous identification of IT ethics, the analysis study of the laws in the UAE, Saudi Arabia and Kuwait has demonstrated their focus on guiding IT users in the three countries to commit themselves to a set of ethics that can be specified in three major groups.

Demonstrating a Sense of Responsibility

Most of the drafting of legal articles in the "*Anti-cybercrime legislation*" in the three countries has come in forms that lead the user to be responsible for morality and social responsibility when communicating with social networks or other information technologies (Figure 4).

1. In most of its articles, it used the threat form, with a phrase that was repeated in almost all articles, namely: "*shall be punished with imprisonment ... and a fine*".
2. The form of generalization has been used in some of its articles, such as: "*without prejudice to the criminal liability of the perpetrator, the legal person shall be punished...*"

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

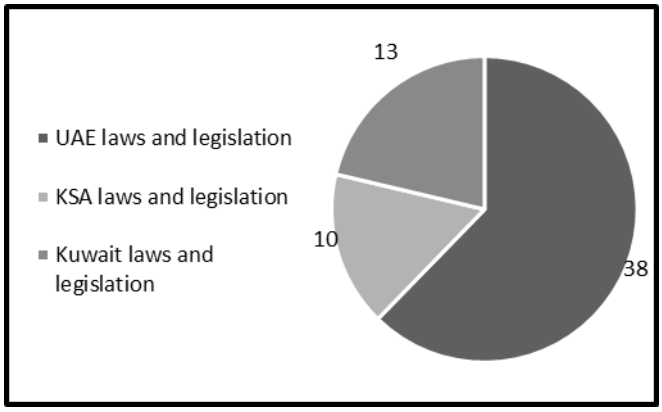

FIGURE 4
OUTLINES THE BASICS OF RESPONSIBILITY ACCORDING TO THE DRAFTING AND CONCEPT OF THE LEGAL PROVISIONS OF ARTICLES OF THE "*COMBATING INFORMATION TECHNOLOGY CRIMES*" LEGISLATION IN THE LAWS OF THE THREE COUNTRIES

Respecting the Privacy and Dignity of Persons

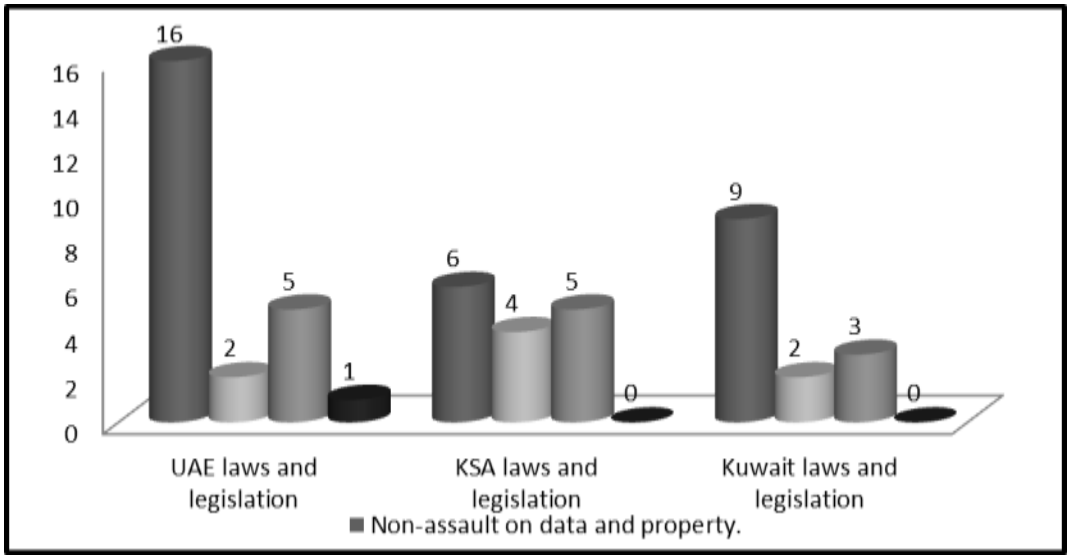

FIGURE 5
OUTLINES THE BASICS OF RESPECT FOR THE PRIVACY AND DIGNITY OF PERSONS ACCORDING TO THE WORDINGS AND CONCEPT OF LEGAL ARTICLES IN THE LEGISLATION ON "*COMBATING INFORMATION TECHNOLOGY CRIMES*", IN THE THREE COUNTRIES

The analysis study of the articles of the laws and legislation (Figure 5) "*Combating Information Technology Crimes*" in the three countries of which the study sample is comprised,

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

revealed the evidence of four basic ethics involving Respect for the Privacy and Dignity of Persons, namely.

1. Non-assault on data and property: Refrain from unauthorized access to any computer device or system, to an electronic data processing system, or to an automated electronic system, or to an information network, or directly to a website or other information system.
2. Refraining from: Forging, destroying, changing, seizing, fraud, disabling, damaging, eavesdropping, capturing, or deliberately intercepting, publishing, sending, storing documents, records, electronic signatures, electronic data processing system, automated electronic system, website, computer system or electronic system. All such acts/ethics were demonstrated in: Articles 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, 37, 41 of UAE Law, Articles 3, 4, 5, 8, 9, 10 of KSA Law, and Articles 2, 3, 4, 5, 6, 7, 8, 11, 14 of Kuwaiti Law.
3. Refraining from insulting, slandering, and defamation: These articles require IT users, including users of social networks, to have the following ethics: Refrain from insulting people or attributing to others incidents that render them subject to punishment or ridicule by others; Refrain from eavesdropping, intercepting, recording, or transmitting, broadcasting, disclosing conversations, communications, or audiovisual material, and Refrain from taking pictures of others or preparing electronic pictures, transferring, disclosing, copying, maintaining, or publishing news, electronic pictures or photographs, scenes, comments and/or data, without their permission, even if the information is true and correct. All such acts/ethics were demonstrated in: Articles 20, 21 of UAE law, Articles 3, 8, 9, and 10 of Saudi law, and Article 3 of Kuwaiti law.
4. Refraining from threats and extortion: These articles require IT users, including users of social networks, to refrain from using any means of information technology to threaten or extort a natural or legal person to get him to act or refrain from acting. Such acts/ethics were demonstrated in: Articles 16, 23, 25, 26, and 36 of UAE law, Articles 3, 7, 8, 9, and 10 of Saudi law, and Articles 3, 9 and 10 of Kuwaiti law.
5. Refraining from spreading ideas of hatred and racism: or promoting the use of any programs or ideas that cause hatred, racism, or sectarianism, or harm national unity or social peace, or disturb public order or public morals. Such acts/ethics were demonstrated in: Article 5 of the UAE law only.

The findings of the comparison between the number and content of legal articles that reflect the ethics of "*Respecting the Privacy and Dignity of Persons*" and the laws on "*Combating Information Technology Crimes*" of the three countries of which the study sample is comprised, indicate that they were almost similar in many of them and were, in certain aspects, equal in terms of numbers and content. Except for the ethics of "*Non-assault on data and property*": The UAE legislator has detailed (16) legal articles, The Saudi and Kuwaiti legislators mentioned them in (6 articles and 9 articles, respectively).

Respect for Community Values

The analysis study of the articles of the laws and legislation on "*Combating Information Technology Crimes*" in the three countries, of which the study sample is comprised, also revealed the evidence of three basic ethics under the principle of Respect for Community Values. The Figure 6 above indicates that the three laws require IT users to respect these values by adhering to the following ethics:

1. Refrain from inciting or seducing anyone to commit acts of prostitution and debauchery or to assist in doing so, or to promote trafficking in human beings or narcotics or psychotropic substances and the like, or to facilitate the same in cases other than those permitted by law, or to promote or fund terrorist organizations,

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

or to publish the manufacture of incendiary devices, explosives or any tools used in terrorist acts, as well as refraining from intentionally possessing pornographic materials by means of an electronic information system, an information network, a website, or one of the means of information technology. Such acts/ethics were demonstrated in: Articles 18, 19 of UAE law, Articles 6, 8, 9, and 10 of Saudi law, and Articles 4, 11, 14, and 15 of Kuwaiti law.

2. Refraining from rumors, publishing or disseminating information, news, cartoons, or any other form that would endanger the security of the State and its supreme interests or prejudice public order. Such acts/ethics were demonstrated in: Articles 4, 26, 27, 28, 29, 30, 31, 32, 28, 39, 44, 45, and 46 of UAE law, Articles 7, 8, 9, and 10 of Saudi law, and Articles 4, 11, 14, and 15 of Kuwaiti law.
3. Refrain from offending God-Almighty, prophets, messengers, Islamic sanctities and rituals or any other rites prescribed in other religions if such sanctities and rituals are protected under Islamic Sharia law, and refrain from mitigating sins. Such acts/ethics were demonstrated in: Article 35 of the UAE law, and Articles 6, 8, 9, and 10 of Saudi law.

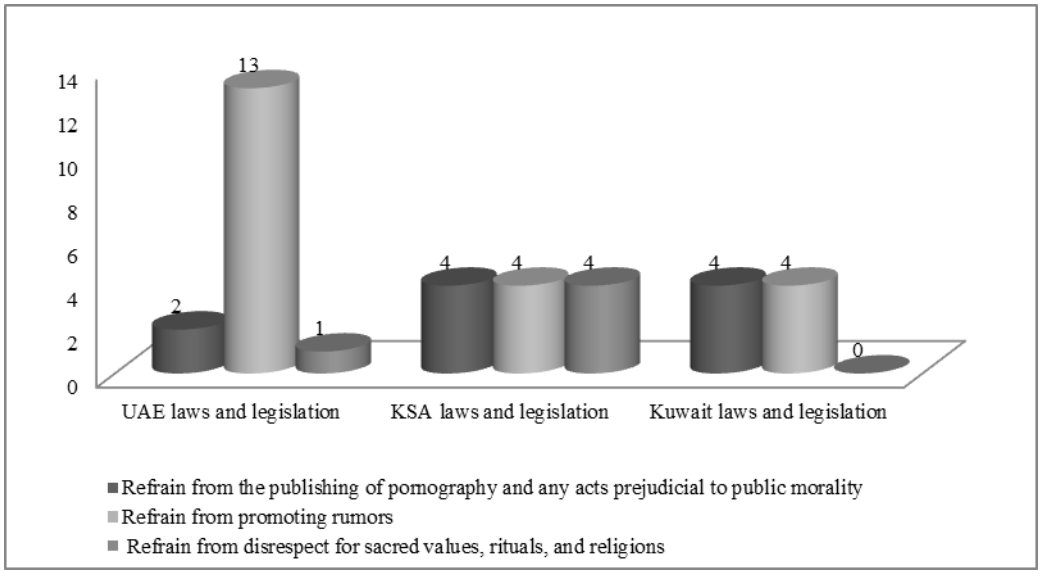

FIGURE 6
OUTLINES THE BASICS OF RESPECT FOR COMMUNITY VALUES ACCORDING TO THE WORDINGS AND CONCEPT OF LEGAL ARTICLES IN THE LEGISLATION ON "*COMBATING INFORMATION TECHNOLOGY CRIMES*", IN THE THREE COUNTRIES

The findings of the comparison between the number and content of legal articles reflecting the ethics of "*Respect for Community Values*" in the law on "*Combating Information Technology Crimes*" in the three countries of which the study sample is comprised, demonstrates that they were equal in terms of numbers and content.

CONCLUSION

The study came up with the following conclusions. The UAE's "*Combating Information Technology Crimes"* legislation includes more legal articles than the Saudi and Kuwaiti laws, and has more details of cyber-crimes and penalties than do the laws of Saudi Arabia and Kuwait.

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

For example, the UAE legislator has drawn up, in 18 articles, crimes and penalties relating to access to information technology systems, while the Saudi and Kuwaiti legislators have drawn up (only 5 articles for each legislation). The UAE legislator has drawn up 15 articles on crimes and penalties against privacy and properties, while the Saudi and Kuwaiti legislators have drawn up (only 4 articles for both legislations). The UAE legislator has drawn up five articles on punishments for violating the values and achievements of society, while the Saudi and Kuwaiti legislators have drawn up (three articles and four articles, respectively). Most of the drafting of legal articles in the "*Combating Information Technology Crimes*" in the three countries has come in the form that obliges users to be responsible for morality and social responsibility in the communication of information technologies.

The analysis study of the articles of the laws and legislation on "*Combating Information Technology Crimes*" in the three countries of which the study sample is comprised, revealed the evidence of four basic ethics involving Respect for the Privacy and Dignity of Persons, namely: Non-assault on data and property, Refraining from insulting, slandering, and defamation, Refraining from threats and extortion, and Refraining from spreading ideas of hatred and racism. The findings of the comparison between the number and content of legal articles that reflect the ethics of "*Respecting the Privacy and Dignity of Persons*" and the laws on "*Combating Information Technology Crimes*" of the three countries of which the study sample is comprised, indicate that they were almost similar in many of them and were, in certain aspects, equal in terms of numbers and content, with the exception of the ethics of "*Non-assault on Data and Property*", as the UAE legislator has detailed (16) legal articles, while the Saudi and Kuwaiti legislators mentioned them in (6 articles and 9 articles, respectively). Also revealed the evidence of three basic ethics under the principle of "*Respect for Community Values*" and indicated that the three laws require IT users to respect these values by adhering to the following ethics:

Refrain from inciting or seducing anyone to commit acts of prostitution and debauchery or to assist in doing so, or to promote trafficking in human beings or narcotics or psychotropic substances and the like, or to facilitate the same in cases other than those permitted by law, or to promote or fund terrorist organizations, or to publish the manufacture of incendiary devices, explosives or any tools used in terrorist acts, as well as refraining from intentionally possessing pornographic materials by means of an electronic information system, an information network, a website, or one of the means of information technology.

Refraining from rumors, publishing or disseminating information, news, cartoons, or any other form that would endanger the security of the State and its supreme interests or prejudice public order.

Refrain from offending God-Almighty, prophets, messengers, Islamic sanctities and rituals or any other rites prescribed in other religions if such sanctities and rituals are protected under Islamic Sharia law and refrain from mitigating sins.

REFERENCES

Aissani, R. (2018). The ethics and legislation of the new media use in the United Arab Emirates. *AAU Journal of Business and Law, 2*(1), 72-98.

Al-Laban, S.D. (2014). Professional, ethical and legal controls of new media. *Strategic Insights Journal*, *2*(7), 96-135.

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.

Anti-Cyber Crime Law. (1993). *Communications and information technology commission, KSA*. Article (1) Dictionary Hachette. Paris Ed. Hachette.

Hassan, U.S. (2015). The UAE project policy on combating cyber-crime. *Al-Fikr Al-Sharti Journal, 24*(4), 21-52.

International Telecommunication Union. (2020). *Guidelines for parents and educators on child online protection.*

Riyadh Document. (2013). *The Unified Law (regulation) for combating information technology crimes in the countries of the gulf cooperation council, Riyadh*. The Cooperation Council for the Arab States of the Gulf (General Secretariat).

United Nations Children's Fund. (2019). *Growing up in a connected world.*

Citation Information: Aissani, R. (2022). Anti-Cyber and information technology crimes laws and legislation in the GCC countries: A comparative analysis study of the laws of the UAE, Saudi Arabia and Kuwait. *Journal of Legal, Ethical and Regulatory Issues, 25*(1), 1-14.