CRIMINAL PROTECTION OF CORPORATE WEBSITES: AN ANALYTICAL STUDY

Mohammad Amin Alkrisheh *

* Public Law Department, College of Law, Al Ain University, Al Ain, UAE
Contact details: Public Law Department, College of Law, P. O. Box 64141, Al Ain University, Al Ain, UAE

OPEN ACCESS

How to cite this paper: Alkrisheh, M. A. (2022). Criminal protection of corporate websites: An analytical study. *Journal of Governance & Regulation, 11*(3), 148–154. https://doi.org/10.22495/jgrv11i3art12

ISSN Print: 2220-9352
ISSN Online: 2306-6784

Received: 26.03.2022
Accepted: 26.07.2022

JEL Classification: K200, K220, K240
DOI: 10.22495/jgrv11i3art12

Abstract

In the light of the state's economic revolution and tremendous techniques sweeping the communication in the recent years which seeks to establish the concept of e-government practically, and the huge increase in using the Internet by all member of society including companies that depend on e-commerce, the UAE legislator is keen to report on criminal protection of a website by issuing the Federal Decree-Law No. 34 for the year 2021 on Combating Rumours and Cybercrime. This research aims to demonstrate the effectiveness of the UAE law in combating hackers who attack and spy on sensitive data of financial, commercial, or economic establishments. To achieve that, the researcher examined the concept, legal nature, and components of a website similar to a previous study conducted in Ukraine (Nekit, Ulianova, & Kolodi, 2019). The researcher opted to check what the website means and state its advantages and disadvantages, and then dealt with all forms of penal protection of the website in the UAE law as well as the general rules of responsibility for the crimes of hacking, and finished the research by conclusion including the most important findings and recommendations such as that the UAE legislator needs to amend the text of Article 75 of the Code of Criminal Procedure, so as to monitor wired and wireless conversations including the website. A command should be issued from the judge, so as to be justified and useful in revealing the truth.

Keywords: Cybercrimes, Website, Federal Law No. 34 of 2021, Combating Rumors and Cybercrime, Penal, Protection, Hacking, Corporate

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

1. INTRODUCTION

The development of information technology and modem communication appears every day in new forms, making the electronic means the nerve system of activating the e-commerce. Most financial and trade transactions have been made electronically and, therefore, the traditional means suitable for modem contracts in electronic form is no longer available, so, the website has recently been used as a substitute for it, so as to comply with the nature of legal contracts in addition to contracts being made by the means of modem electronic devices.

In the light of economic revolution and tremendous techniques sweeping the country in recent years seeking to establish the concept of e-government practically and with the expansion of its use and access to all segments of society including the list of users and large corporations which own sites for e-commerce, the process of communication is conducted among them electronically and fully carried out relying on the website, so, the requests, invoices, and contracts are sent electronically as well as taking advantage of the multi-banking services provided by banks through the website as well as the use of the website

in the process of marketing, advertising or delivering of products destined for the consumer.

Under that, the crimes began to appear on the network and have increased through time and multiplied their forms, through penetrating websites and accessing information as well as destroying them or capturing them and then stealing the data or information or just tampering with them by programmed viruses or other means.

The protection of websites will not be achieved unless there is a new legal rule facing this rapid development, so, the UAE legislator has responded to this development by issuing the new Cybercrime Law, adopted by Federal Decree-Law No. 34 of 2021, which went into effect on January 2, 2022, replacing the Emirates' former Federal Law No. 5 of 2012 on Combating Cybercrime. The law included many materials that would provide legal protection for the privacy of what is published and circulated on the network as information, data, and figures relating to credit card numbers and bank account data or any other means of electronic payment as well as all the use of any means of information technology by rigging, imitating or copying credit cards or any attack on a website.

Although many studies discussed online shopping and consumer rights in the Middle East, the study conducted by Dahiyat (2019) explored the existing legislation in the UAE to determine whether or not this legislation gives due attention to consumer protection in an online environment. Another study by Dahiyat (2011) from Jordan explored how the electronic transactions law deals with such rights and determines whether or not this law gives due attention to consumer protection in an online environment. There is a big gap in the literature discussing the criminal protection of corporate websites in world countries in general and in Middle Eastern countries in particular. Only one study examined the website as an object of legal protection by Ukrainian legislation (Nekit, Ulianova, & Kolodi, 2019). This study used a similar methodology to the Ukrainian study which examined the legal website as an object of legal protection by Ukrainian legislation (Nekit et al., 2019).

The importance of this research appears through the statement of criminal protection of the website and the limits of these parameters and the scope of protection through clarifying the criminal acts that undermine it. The aim of this research is to show the effectiveness of Emirati legislation specifically the new Cybercrime Law, adopted by Federal Decree-Law No. 34 of 2021 in the criminal protection of corporate websites. The aim of the research is achieved by analyzing the penal protection forms of websites in the following crimes: hacking entry to a corporate website, illegal entry with the intention of tampering with the website, creating a fake website or a fake online account, obtaining a secret number, code or password for a website without permission, attacking the data of financial, commercial or economic establishments, and crime of assault on privacy.

The structure of this paper is as follows. Section 1 is the background information and introduction. Section 2 discusses the previous literature. Section3 includes a detailed research methodology applied in this article. Section 4 presents and analyses the UAE legislation that ensures the criminal protection of the website Section 5 highlights the conclusion and recommendations to achieve the highest level of criminal protection of corporate websites in the UAE.

2. LITERATURE REVIEW

The concept, legal character, and components of a website were investigated in a prior study in Ukraine. The objects of intellectual property rights, as well as such a separate object of civil rights as information, can be detected in the website's structure. The website and the domain name are considered to be separate and independent items. A domain name is not an essential component of a website and should not be sent along by default when a website is abandoned. Protecting the website's material against plagiarism and piracy, as well as accountability for erroneous information uploaded on the site, receives special attention (Nekit et al., 2019).

Another study conducted by Nofianti (2017) discussed the legal protection of website copyright in preventing copyright violation on the Internet and the extended role of the license in preventing copyright violation through registering the copyright although the registration is not an obligation. The registration should be conducted by the copyright owner of the website (Nofianti, 2017).

The importance of website protection is extensively studied by many researchers and from different perspectives other than law. A previous study analyzing the website contents of the top 350 companies listed on the London Stock Exchange concluded the importance of corporate social responsibility disclosure and information accuracy and website protection (Basuony, 2021).

In an international study across 23 worldwide countries, El-Halaby, Hussainey, Marie, and Mohsen (2018) seek to examine disclosure levels in the annual report and websites related to Islamic accountability pillars which are Sharia, social and financial. The researchers investigated a holistic framework about Islamic accountabilities for Islamic banks around the world. The study measured the responsibility sections in the annual report for Islamic banks as well as their websites.

3. RESEARCH METHODOLOGY

Thematic content analysis of the UAE laws based on general observation of the legal texts that outline the criminal liability as per the UAE legislator was used in the process of research. This study examined the legal nature of corporate websites based on the Emirates' new Cybercrime Law, adopted by Federal Decree-Law No. 34 of 2021, which went into effect on January 2, 2022, replacing the Emirates' former Federal Law No. 5 of 2012 on Combating Cybercrime. Methods of descriptive analysis and synthesis were used to determine the nature of the website and statement of criminal protection of the website and the limits of these parameters and the scope of protection by clarifying the criminal acts that undermine it and the statement of the adequacy and effectiveness of the UAE legislator plan to criminalize any acts that impair the website. The thematic content analysis of the UAE legislation was applied.

4. RESULTS AND DISCUSSION

4.1. What does a website mean?

The development of the Internet and the increasing number of users of websites in the world is seen everywhere. So, we find that most legislators have resorted to determining the meaning of a website as a necessary indispensable means in the field of electronic transactions. To identify the nature of a website, the researcher has to make a definition of the website and then clarify its most important advantages and disadvantages.

4.1.1. Definition of a website

A website is defined by jurisprudence as "a group of web pages linked together and stored on the same server, and can be visited over the Internet" (Al-Fariji, 2017, p. 3). A website is a collection of publicly accessible, interlinked web pages that share a single domain name. Although it is sometimes called a "web page", this definition is wrong, since a website consists of several web pages. A website is also known as a "web presence" or simply a "site". Websites can be created and maintained by an individual, group, business, or organization to serve a variety of purposes (Al-Fariji, 2017).

The definition of websites varies according to the use of these sites: if you have a company or organization, the definition of the website is a set of fixed pages under the name of your site (the domain), these pages contain information about the company, are accessible 24 hours a day, seven days a year on the Internet, and are available to all web surfers from all countries of the world (Ibrahim, 2017). If the website is for a person, it is a group of pages that fall under the website name (the domain), these pages contain your CV, in addition to any audio or video recordings or written lessons, which could give the possibility of site visitors to interact with lessons and recordings, comment on them, and talk to you directly (Ibrahim, 2017).

On the other hand, the Emirati legislator under Article 1 of Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime defines some terms of an electronic nature as a website. A website is defined as a place where electronic information is made available on the computer network, including social communication sites, personal pages, and blogs.

The legislator defined electronic attacks as any deliberate and planned attack targeting information systems, infrastructure, electronic networks, or information technology tools that result in reducing the capabilities and functionality of any of them, whether for a personal purpose or the purposes of interception, intrusion, hacking, leaking or for exposing data or information to danger or disabling operations, etc.

Some examples of means of information technology are such as magnetic, optical, electrochemical, or any other tool used to process data, perform logic, arithmetic, or storage functions, and include any ability to store data or communications related to working in conjunction with such a tool.

4.1.2. Advantages and disadvantages of a website

A website has several advantages that distinguish it from traditional mail (Khalid, 2010; Al-Awadi, 2005). The most important is that it is an asynchronous communication way which means that there is no synchronization in the presence of people on both sides of contact because the caller via the Internet and through the website can contact and get what he wants from the opposite side whenever he wants without interfering in that person. Therefore, sending messages via the website does not require the presence of the addressee and then having to call again in case of non-existence as the sender can let what he wanted to be conveyed by a text or graphic, through sound or image in part of the sender computer memory to a dedicated website box is called a website box.

It is also a quick, easy, and cheap communication means that works all the time without leave, formal or informal holidays with the possibility of sending more than one message to more than one person at one time, that is the most popular Internet application and that is most widely used by lawyers because it facilitates the exchange process files with anyone in the world of the attorney office. Consequently, the practice of law depends on the rapid transfer of information and documents across geographic space (Masur, 1999).

Despite these advantages of a website, there are some disadvantages (Abdel-Fattah, 2004). Sending subversive and disturbing messages loaded with viruses to cause harm to a website and the seriousness of the website is also reflected through that access from non-owner which leads to the disclosure of secrets in a manner that makes serious damage to the website and there is no real guarantee that the sent message has not been tampered with.

In addition to this, there is another disadvantage. For example, in some website messages, the signature of the owner does not appear so that his website-related link cannot be known in advance or the way that the message will be received or proven to receive it if the other party communicated with him denies these messages.

But these defects do not impair the advantages of the website in the presence of legal and technical (see Austin, 2003 for technical protection methods (inscription)) means by which we protect the website from penetration and tinker and also protecting the private lives of individuals (see Warren and Brandeis, 1890 for the discrepancy in defining privacy expression).

4.2. Penal protection forms of a website

The development of information technology and modem communication in everyday new situations needs to be organized. This will not be achieved unless new legal rules face this rapid development. The UAE legislator has responded to this development and managed to add the penal protection for websites by issuing Federal Decree-Law No. 34 of 2021, which went into effect on January 2, 2022, replacing the Emirates' former Federal Law No. 5 of 2012 on Combating Cybercrime. The law included many materials that would provide legal protection for the privacy of

what is published and circulated on the information network and, therefore, the researcher will discuss the penal protection forms for the website which was described in the above-mentioned law as follows.

4.2.1. Hacking entry to a corporate website

The act of compromising digital devices and networks by gaining unauthorized access to any account or computer system is a popular definition of hacking (Lenhard, 2022). Hacking is not always a negative act, although it is most often linked to illicit activities and data theft by cybercriminals. Hacking is the exploitation of technology such as computers, smartphones, tablets, and networks to harm or destroy systems, collect information on users, steal data and documents, or disrupt data-related activity ("What is 'hacking'," n.d.).

This crime is mentioned in Article 2 of Federal Decree-Law No. 34 of 2021, a penalty of imprisonment and a fine of not less than 100,000 dirhams and not more than 300,000 dirhams, or one of these two penalties, for anyone hacking a website, electronic information system, information network, or information technology means. The legislator intensified the penalty to six months in prison and a fine of not less than 150,000 dirhams and no more than 500,000 dirhams, or any combination of these two penalties, for anyone who disrupted a website, electronic information system, information network, or information technology by canceling, deleting, destroying, disclosing, destroying, changing, copying, publishing, re-publishing, or obtaining any data or information. The Emirati legislator also intensified the penalty further to reach imprisonment for a period of not less than one year and a fine of not less than 200,000 dirhams and not more than 500,000 dirhams, or one of these two penalties if this breach was for the purpose of obtaining data or information to achieve an illegal purpose. The UAE legislator has stressed punishment in any event that will be resulted through the entry, staying into the system, canceling, destruction, disclosure, damaging, or modifying the data contained on the system for the availability of these circumstances there should be a causal relationship between the act of illegal entry or staying in the system and also a relationship between erasing, modifying data or disabling the system from doing its work. But if this erasure or modification is due to other reasons that led to it like outside power or a sudden event, the causal link will be interrupted and the culprit, in this case, will not be required for the aggravating act It strengthened the punishment according to Article 3 of the same law. It made it jail for a period of not less than l year and a fine of not less than 250.000 dirhams but not exceed 1 million dirhams or by both penalties if crimes were committed during doing this research. It made the penalty a fine of not less than 200,000 dirhams and no more than 500,000 dirhams as well as temporary imprisonment if the hack entry was intended to a governmental institution's website, electronic information system, information network, or information technology methods.

It is noted that the UAE legislator does not emphasize achieving a certain finding resulting from entry into the database or information systems by the offender and all what the legislator requires is that the entry has been conducted without permission or transcend permit or staying there illegally.

This crime is classified as a dangerous crime in which the behavior is criminalized without stopping by a particular result because this crime is not a crime of damage that its punishment is linked to causing harm to the victim. This is a form of intentional crime, the form of the mental element in it is the general criminal intent connected by racist awareness and will where the offender should know that accessing the website to someone else without permission, transcending permit, staying there illegally or moving his free will to do this activity, so that, the offender is aware that his entry may be legitimate if it was done by accident or mistake or omission and in this case, this person is required to cut his connection and withdraw immediately but if remained, he should have punishment.

It must be noted here that the UAE legislator made the punishment for this crime by imprisonment and a fine and also the escalation of the punishment value because of losses arising from illegal entry but punished for embarking on offense by half penalty for the full offense (Article No. 57 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime).

4.2.2. Illegal entry with the intention of tampering with the website

The legislator offended illegal entry intending to tamper with the data inside the website, so as to erase, change, delete some of them or re-deploy it (Issa, Ismail, & Aamar, 2019). Article 5 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime on combating information technology crimes penalizes the other forms of illegal entry by saying:

"Anyone who intentionally damages, destroys, stops, or disables a website, electronic information system, information network, or information technology means, shall be punished by imprisonment for a period of not less than one year and a fine of not less than 500,000 dirhams and not more than 3,000,000 dirhams, or one of these two penalties".

The penalty shall be temporary imprisonment and a fine of not less than 500,000 dirhams and not more than 3,000,000 dirhams if the damage was caused to a banking, media, health, or scientific entity, or if the purpose of that was to investigate an illegal matter, or if the crime occurred as a result of an electronic attack. The UAE legislator emphasized the punishment if the illegal entry intent to obtain data affecting national security or the national economy by saying:

"… shall be punished by temporary imprisonment and a fine of not less than 500,000 dirhams and not more than 3,100,000 dirhams whoever accesses a website, electronic information system, computer network or information technology means without authorization whether such access is intended to obtain government data or confidential information relating to a financial, commercial or economical facility" (Article 5 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime).

4.2.3. Attacking the data of financial, commercial, or economic establishments

The crime of attacking the data of financial, commercial, or economic establishments is mentioned in Article 8 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime: "Whoever obtains, possesses, alters, destroys, discloses, leaks, cancels, deletes, alters, copies, publishes or re-publishes without authorization confidential information or data of a financial, commercial or economic facility using information technology or an information technology means shall be punished by temporary imprisonment for a period of not less than (5) five years in addition to a fine, not less than 500,000 dirhams and not more than 3,000,000 dirhams".

From the above article, we clearly note that the UAE legislator has tightened the penalty to a higher degree compared with other previous penalties, as it classifies it as a felony crime. This is because the attack on the data of financial, commercial, or economic establishments constitutes prejudice against the higher interests of the country, its security, and its national economy, which causes harm to the whole country, the financial system, and the climate of investment.

4.2.4. Creating a fake website or a fake online account

Article 11 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes stipulates that any person, who creates a fake website, online account impersonating a natural or legal person, shall be subject to imprisonment and a fine of not less than 50,000 dirhams and not more than 200,000 dirhams, or one of the two penalties.

The offender shall be imprisoned for a minimum of two years if they use or allow any person to use the fake website, online account to cause harm to the impersonated victim.

A penalty of imprisonment of not more than five years, and a fine of not less than 200,000 dirhams and not more than 2,000,000 dirhams shall be applicable if such fake website, online account impersonates any UAE entity.

4.2.5. Obtaining a secret number, code, or password for a website without permission

The UAE legislator emphasized the confidentiality of website data and offended obtaining a secret number, code or password for a website without permission. The text of Article 14 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes referred to this by saying:

"… shall be punished by imprisonment and a fine of not less than 200,000 dirhams and not more than 500,000 dirhams or either of these two penalties whoever obtains without legal right, a secret number, code, password or any other means to have access to an information technology means, website, electronic information system, computer network or electronic information.

… shall be punished with the same penalty whoever prepares, designs, produces, sells, buys, imports, displays for sale or make available any computer program or any information technology means or promotes by any means links to websites, computer program or any information technology means designed for the purposes of committing, facilitating or abetting in the commission of the crimes specified in this Decree-Law".

4.2.6. The crime of assault on privacy

The Constitution of the United Arab Emirates has referred to the privacy of the individual and the sanctity of his private life within its provisions. The text in Article 26 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime referred that personal freedom is guaranteed to all citizens. Article 31 says that everyone has the sanctity of postal, telegraphic correspondence or any other means of communication, emphasizing that viewing, controlling, stopping them is prohibited except in circumstances prescribed by law because the seriousness of this right, Islam religion granted it the most importance. In Holy Quran, Surat Al-Noor, Verse 27: *"O ye who believe! enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you, in order that ye may heed (what is seemly)"*. And it is also included in Surat Al-Hujurat, Verse 12: *"O ye who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it… But fear Allah: For Allah is Oft-Returning, Most Merciful"*. It is also included in the Universal Declaration of Human Rights of 1948. Article 3 cited that everybody has the right to life, freedom, and personal safety. Article 12 stated that nobody is exposed to any kind of interference in his private life, his family, his correspondences, or any campaigns against his honor or reputation and everybody has the right to protect the law against any interference or any campaign (Coleman, 2006; McArthur, 2001). The UAE legislator followed the same approach under the aforementioned law in Article 6 saying:

"Whoever obtains, possesses, alters, destroys, discloses, leaks, cancels, deletes, copies, publishes, or re-publishes without authorization electronic personal data or information using information technology or information technology means will be punished by imprisonment for not less than (6) six months and a fine of not less than 20,000 dirhams and not more than 100,000 dirhams, or any combination of these two penalties. If the data or information referred to in Clause (1) of this Article is related to examinations, diagnosis, treatment, care, medical records, bank accounts, data, and information of electronic payment methods, this shall be considered an aggravating circumstance".

The questions here are as follows: Is the principle of the privacy of website messages an absolute principle and not to be touched? Are there some exceptions to that exception that allow compromising that privacy?

The UAE legislator defined the cases in which penetrating the right to private life is illegible when the interests of the right holder contradict the interests of the community; the provisions of Article 75 of the Code of Criminal Procedure says that the member of the public prosecution has the right to inspect the accused but not the others who are not accused as well as their house. However,

if it turns out from powerful signs that the offender possesses items related to the crime in this case, he has the right and with the consent of the Attorney General to control all correspondences, letters, newspapers, publications, parcels and telegrams, all cables and telecommunications through post offices as well as watching wire and wireless talks when necessary for the requirements of the investigation. Article 76 of Federal Law No. 35 of 1992 Concerning the Criminal Procedural Law defined the limits conducted by a member of the public prosecution by saying that the public prosecutor alone has the right to see correspondences, letters, and other controlled papers and he has the right to order the annexation of those papers to the case file or turning it back to those who possessed them or to those who they were destined to.

The researcher can emphasize the possibility of the application of those texts on website messages. This means that the member of the public prosecution does not have the right to check out those messages unless obtaining the approval of the Attorney General. This procedure should be useful to show the truth in a particular crime. In the case of the availability of these conditions, the public prosecutor determines the website letters they want to check that the investigator chooses which is only related to the crime.

4.2.7. General rules of responsibility for the crimes of assault on a website

The UAE legislator cited in the law of the fight against crimes of information technology which shows the general lines of responsibility for the crimes of abuse of a website, particularly with the substantive provisions of criminal responsibility for information technology crimes law in the following manner.

The UAE legislator stressed maintaining a website with full protection and offended every attack against it even if not included in the law of the fight against cybercrimes, but it is cited in other valid legislation. This means that the punishment should be according to this text provided that this is conducted by using electronic means and the application of the prejudice should not violate any penalties cited in this act to any severer penalty in any other law (Article 72 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime).

The UAE legislator authorized the court to order putting the convict under supervision or control and deprive him of using any information network, information system, or any technical device other information or putting him in a therapeutic shelter or rehabilitation center for a period of time determined by the court (Article 59 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime).

The legislator put a punishment to those misdemeanors who embark on a crime with a half penalty of the complete offense (Article 57 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime).

The legislator strengthened the punishment in case of the availability of some aggravating circumstances. The law cited some circumstances that need emphasizing punishment for the original penalty for the actor of such offenses. Article 60/3 of Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime states that it is also an aggravating circumstance of committing any offense under this law for the account or the benefit of a foreign state, any terrorist group, any association organization or any illegal body.

5. CONCLUSION

As seen earlier, the UAE legislator is keen to report on the criminal protection of websites by issuing Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrime. The aim of this research was to demonstrate the effectiveness of the UAE law in combating hackers who attack and spy on sensitive data of financial, commercial, or economic establishments. The researcher concluded the most important findings and recommendations. With the development of the Internet and the increasing numbers of website users in the world, we find that most state legislations have resorted to determining the meaning of a website as a necessary and indispensable means in the field of electronic transactions.

The UAE legislator explained the website within the website that includes social networking sites and personal homepages.

The website has several advantages but it also has some disadvantages, these disadvantages do not impair the advantages in the presence of legal and technical means by which we protect the website from intrusion and tampering.

A website is one of the most important means of achieving e-government and facilitating its performance. A website can be exploited in committing many crimes, such as drug trafficking or human trafficking, crimes of religious blasphemy, crimes relating to state security internal and external, money crimes, and other crimes. So, the researcher found that the UAE legislator has responded to this development and managed to bring the penal protection for a website by issuing Federal Law No. 5 of 2012 on Combating Cybercrimes. The law included many materials that would provide legal protection for the privacy of what is published and circulated on the information network.

The legislator cited some texts in the fight against crimes of information technology which show the general lines of responsibility for the crimes such as abusing websites, particularly with the rules of the substantive provisions of criminal responsibility for information technology crimes.

The UAE information technology law is characterized by giving the judge wide discretion to choose between the type of penalty and its amount.

The UAE legislator determined the cases of excusing penetrating the right to private life in the case when the interests of the right holder contradict the interests of the community. It is cited in the provisions of Article 75 of the Code of Criminal Procedure.

Based on this study the researcher recommended the following actions in order to increase the level of legal criminal protection in the UAE. The researcher hopes that the UAE legislator can amend the text of Article 75 of the Code of Criminal Procedure to monitor wired

and wireless conversations including a website. A command should be issued from the judge to be justified and useful in revealing the truth. There is a need to train specialists, officers, public prosecutors, and judges in the area of law enforcement as well as the means and tools of electronic information technology to deal with cybercrimes and the ways of detecting attacks on the website. Moreover, supporting international cooperation in the field of combating information technology crimes that become cross-border crimes due to technical and technological development. This requires mutual judicial assistance and signing of extradition agreements between countries.

The key drawback of this study was the lack of legal studies that discussed the criminal protection of corporate websites in general and in the UAE in particular, which increased the time and effort required by researchers to develop a theoretical framework for the topic under consideration.

Future research should compare global legislation dealing with criminal protection of websites across nations and assess the effectiveness of these laws.

REFERENCES

1. Abdel-Fattah, B. H. (2004). *E-governrnent and its legal system.* Alexandria, Egypt: Dar al-Fikr al-Arabi Publisher.
2. Abdul-Muti Khayal, M. A. (2001). *Internet and some legal sides.* Beruit, Lebanon: Dar Annahdha Al-Arabieh.
3. Al-Awadi, F. A. H. (2005). *The legal aspects of website.* Alaraiah, Egypt: Dar Annahda Al Arabia.
4. Al-Fariji, R. N. (2017). The uses of social networks in charitable work in the Kingdom of Saudi Arabia: Reality and obstacles. Paper presented at the *Fourteenth Annual Meeting of Charitable Entities in the Eastern Province*.
5. Austin, L. M. (2003). Privacy and the question of technology. *Law and Philosophy, 22*, 119–166. https://cutt.ly/jHYMQjF
6. Basuony, M. A. K. (2021). Corporate governance: Does it matter for corporate social responsibility disclosure via website and social media by top listed UK companies? *Corporate Ownership & Control, 19*(1), 84–93. https://doi.org/10.22495/cocv19i1art7
7. Coleman, S. (2006). E-mail, terrorism and the right to privacy. *Ethics and Information Technology, 8*, 17–27. https://doi.org/10.1007/s10676-006-9103-5
8. Dahiyat, E. A. R. (2011). Consumer protection in electronic commerce: Some remarks on the Jordanian electronic transactions law. *Journal of Consumer Policy, 34*, 423. https://doi.org/10.1007/s10603-011-9170-9
9. Dahiyat, E. A. R. (2019). Online shopping and consumer rights in the UAE: Do we need a specific law? *Arab Law Quarterly, 33*(1), 35–57. https://doi.org/10.1163/15730255-12331014
10. El-Halaby, S., Hussainey, K., Marie, M., & Mohsen, H. (2018). The determinants of financial, social and Sharia disclosure accountability for Islamic banks. *Risk Governance and Control: Financial Markets & Institutions, 8*(3), 21–42. https://doi.org/10.22495/rgcv8i3p2
11. Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes. Retrieved from https://laws.uaecabinet.ae/ar/legislation-list?type=law&decision-page=2&law-page=9
12. Federal Law No. 35 of 1992 Concerning the Criminal Procedural Law. Retrieved from https://legaladviceme.com /legislation/156/uae-federal-law-35-of-1992-concerning-criminal-procedural-law
13. Ibrahim, A. H. (2017). *Media logic between globalization and globalization.* Amman, Jordan: Dar Al Moataz for Publishing and Distribution.
14. Issa, H. A., Ismail, M., & Aamar, O. (2019). Unauthorized access crime in Jordanian law (comparative study). *Digital Investigation*, 28, 104–111. https://doi.org/10.1016/j.diin.2019.01.006
15. Juridical aspects of email. (1999). Retrieved from https://cutt.ly/zH1NRvW
16. Khalid, M. I. (2010). Website guide in proving. *Law Philosophy, 22*, 119–166.
17. Lenhard, T. H. (Ed.). (2022). Website hacking. In *Data security* (pp. 69–71). https://doi.org/10.1007/978-3-658-35494-7_13
18. Masur, J. M. (1999). Safety in numbers: Revisiting the risks to client confidences and attorney-client privilege posed by internet electronic mail. *Berkeley Technology Law Journal, 14*, 1117–1162. Retrieved from https://btlj.org/data/articles2015/vol14/14_3/14-berkeley-tech-l-j-1117-1162.pdf
19. McArthur, R. L. (2001). Reasonable expectations of privacy. *Ethics and Information Technology, 3*, 123–128. https://doi.org/10.1023/A:1011898010298
20. Nekit, K., Ulianova, H., & Kolodi, D. (2019). Website as an object of legal protection by Ukrainian legislation. *Amazonia Investiga, 8*(21), 222–230. Retrieved from https://amazoniainvestiga.info/index.php/amazonia/article/view/97
21. Nofianti, N. (2017). Juridical review of website protection through copyright license agreement. *International Journal of Humanities, Religion and Social Science, 3*(1), 72–79. Retrieved from http://www.doarj.org/ijhrss/wp-content/uploads/2017/IJHRSS/12-2017/7.pdf
22. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160
23. What is 'hacking'? (n.d.). *The Economic Times.* Retrieved 2022, March 23, from https://economictimes.indiatimes.com /definition/hacking