The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.

UUM
Universiti Utara Malaysia

المشكلات الموضوعية والإجرائية المتعلقة بالجرائم الإلكترونية في دولة الإمارات العربية المتحدة

SUBSTANTIVE AND PROCEDURAL PROBLEMS RELATED TO CYBERCRIME IN THE UNITED ARAB EMIRATES

RASHED AHMED GHAREIB HUWASHEL ALSEREIDI

Universiti Utara Malaysia

MASTER'S OF LAW
UNIVERSITI UTARA MALAYSIA

2024

المشكلات الموضوعية والإجرائية المتعلقة بالجرائم الإلكترونية في دولة الإمارات العربية المتحدة

SUBSTANTIVE AND PROCEDURAL PROBLEMS RELATED TO CYBERCRIME IN THE UNITED ARAB EMIRATES

RASHED AHMED GHAREIB HUWASHEL ALSEREIDI
826728

Universiti Utara Malaysia

Thesis Submitted To The Ghazali Shafie Graduate School of Government In Fulfilment of The Requirements for The Master
Universiti Utara Malaysia

Kolej Undang-Undang, Kerajaan dan Pengajian Antarabangsa
(College of Law, Government and International Studies)
UNIVERSITI UTARA MALAYSIA

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

RASHED AHMED GHAREIB HUWASHEL ALSEREIDI (826728)

calon untuk Ijazah **MASTER OF LAW BY RESEARCH**
(candidate for the degree of)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

SUBSTANTIVE AND PROCEDURAL PROBLEMS RELATED TO CYBERCRIME IN THE UNITED ARAB EMIRATES

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada **27 OGOS 2023**
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:
AUGUST 27, 2023

Pengerusi Viva *(Chairman for Viva)*	:	**ASSOC. PROF. DR ALIAS AZHAR**	Tandatangan *(Signature)*	
Pemeriksa Luar *(External Examiner)*	:	**DR. AHMED A.A. SHEHAB (ISLAMIC UNIVERSITY OF GAZA)**	Tandatangan *(Signature)*	**AHMED SHEHAB**
Pemeriksa Dalam *(Internal Examiner)*	:	**ASSOC. PROF. DR. MOHD ZAKHIRI MD. NOR**	Tandatangan *(Signature)*	
Tarikh Date	:	**27 AUGUST 2023**		

Universiti Utara Malaysia

Nama Pelajar *(Name of Student)*	:	**RASHED AHMED GHAREIB HUWASHEL ALSEREIDI (826728)**
Tajuk Tesis *(Title of the Thesis)*	:	**SUBSTANTIVE AND PROCEDURAL PROBLEMS RELATED TO CYBERCRIME IN THE UNITED ARAB EMIRATES**
Program Pengajian *(Programme of Study)*	:	**MASTER OF LAW BY RESEARCH**
Penyelia Pertama (*First Supervisor*)	:	**DR. MUKHRIZ MAT RUS** Tandatangan *(Signature)*

UUM
Universiti Utara Malaysia

PERMISSION TO USE

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Perpustakaan Sultanah Bahiyah UUM may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Ghazali Shafie Graduate School of Government (GSGSG). It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean (Ghazali Shafie Graduate School of Government)

UUM College of law, Government and International Studies (UUM COLGIS)

Universiti Utara Malaysia

UUM Sintok 06010

Universiti Utara Malaysia

الملخص

تناولت الدراسة موضوعا حساسا يشكل خطرا على المجتمع في جميع جوانبه الشؤون الاجتماعية والاقتصادية والسياسية وحتى الدينية بتناول هذا الموضوع الجرائم الإلكترونية والشركات الموضوعية والإجرائية المتعلقة بهذا النوع من الجرائم في دولة الإمارات العربية المتحدة. تمت من خلال شرح تناولت هذه الدراسة من خلال شرح تناولت أساس المتمثل في شرط بعية الجريمة الإلكترونية لكي تعرف على الشركات الإجرائية العلمية التي تنجم عن الجريمة الإلكترونية والتي تهدف إلى معرفة تقنيات الجرائم الإلكترونية وإجراءات البحث والتحقيق والتعقب. وكذلك الشركات التي تطبق "القانون المختص والمنطبق على تلك الجرائم، والتي تهدف إلى معرفة القواعد الموضوعية والإجرائية للجرائم الإلكترونية وتحدثت الدراسة عن أنواع الجرائم وأركانها وتطرقها بوضع القانونية لحلت الدراسة مواد المرسوم رقم (5) لسنة 2012 المعدل بالقانون الاتحادي رقم (12) لسنة 2016 بشأن مكافحة جرائم تقنية المعلومات لمعرفة مدى نجاح أو فشل الشرع الإماراتي في تنظيم الجرائم الإلكترونية والتعامل معها. وفي الختام تناولت الدراسة الحلول العملية والتشريعية لمكافحة الجريمة الإلكترونية والتغلب على المشاكل الناتجة عن هذا النوع من الجرائم بالإضافة إلى الدور القانوني والدولي والوطني في مواجهة الجريمة المستحدثة ومكافحتها. كما بينت الباحثة أهم الحلول العملية في مواجهة هذه الجريمة من خلال عرض الإجراءات المطلوبة لمكافحة الجريمة الإلكترونية، وكذلك يمكن عرض بعض الشبكات التي تخدم في تقنين الجرائم. اعتمدت الدراسة المنهج النوعي التحليلي والمقارن. وخرجت الدراسة بعدد من النتائج والتوصيات، من أهمها خطورة الجرائم الإلكترونية وتنوعها، بالإضافة إلى أن المشرع الإماراتي نظم الجرائم الإلكترونية ضمن قانون اتحادي مكافحة الجرائم التقنية رقم 5 لسنة 2018. 2012 وتنص التهمة على القانون الاتحادي رقم 12 لسنة 2016 بشأن أنواع الجرائم الإلكترونية على أساس الجرائم التي ترتكب بالنظام، والجرائم المضلل النظام وفسره بالإضافة إلى ذلك، أوصت الدراسة بأن يضيف المشرع الإماراتي نصًا يوضح العقوبة المقررة لجريمة الإلكترونية، ويعتبرها جريمة ضد أمن الدولة. كما اقترحت الدراسة إضافة نص حول جواز فحص المكون المعرفي لحاسوب وضع العقوب المناسبة له.

الكلمات المفتاحية: الجرائم الإلكترونية، القانون الإماراتي، الشركات الموضوعية والإجرائية، الإمارات العربية المتحدة.

ABSTRACT

The study discussed a critical topic that poses a threat to society in all aspects of social, economic, political, and even religious affairs. This topic talked about cybercrime and the substantive and procedural problems related to this type of crime in the United Arab Emirates. This study was discussed by explaining the basic research points represented in explaining the nature of cybercrime and identifying the procedural and scientific problems that emanate from cybercrime, which aim to know how to prove electronic crime as well as the procedures for research, investigation, and tracking, as well as the problems associated with defining the "competent law and applicable to those crimes, which aim Knowledge of the substantive and procedural rules of cybercrime. The study talked about the types of crimes, their elements, scope, and legal nature. The study analyzed the articles of Decree No. (5) of 2012 amended by Federal Law No. (12) of 2016 related to combating information technology crimes to find out the extent of success or failure of the UAE legislator in organizing and dealing with cybercrime. In the end, the study discussed practical and legislative solutions to combat cybercrime and overcome the problems resulting from this type of crime, in addition to the regional, international, and national role in confronting and combating cybercrime. The researcher also showed the most essential practical solutions regarding confronting this crime with regard to some of the procedures required to combat cybercrime, as well as in relation to controlling and inspecting the methods used in the implementation of crimes. The study adopted the analytical and comparative qualitative approach. The study concluded with many results and recommendations, the most important of which is the seriousness of cybercrime and the diversity of their forms, in addition to the fact that the UAE legislator organized cybercrime within the Law of Combating Technical Crimes Union Law No. 5 of 2012 and its amendments to Federal Law No. 12 of 2016, regarding types of cybercrime on the basis of crimes committed by the system, and crimes against the system itself. In addition, the study recommended that the UAE legislator add a text clarifying the penalty prescribed for cybercrime, and considered a crime against state security. Furthermore, the study suggested adding text on the permissibility of inspecting the intangible components of the computer and establishing legal controls for them.

Keywords: Cybercrime, UAE law, Substantive and procedural problems, United Arab Emirates.

ABSTRAK

Kajian itu membincangkan topik kritikal yang menimbulkan ancaman kepada masyarakat dalam semua aspek sosial, ekonomi, politik, dan juga hal ehwal agama. Topik ini membincangkan tentang jenayah siber dan masalah substantif dan prosedur yang berkaitan dengan jenis jenayah ini di Emiriah Arab Bersatu. Kajian ini dibincangkan dengan menerangkan perkara-perkara asas penyelidikan yang diwakili dalam menerangkan sifat jenayah siber dan mengenal pasti masalah prosedur dan saintifik yang berpunca daripada jenayah siber, yang bertujuan untuk mengetahui bagaimana untuk membuktikan jenayah elektronik serta prosedur untuk penyelidikan, penyiasatan, dan pengesanan. , serta masalah yang berkaitan dengan mentakrifkan "undang-undang yang berwibawa dan terpakai kepada jenayah tersebut, yang bertujuan Pengetahuan tentang peraturan substantif dan prosedur jenayah siber. Kajian ini membincangkan jenis jenayah, elemen, skop dan sifat undang-undangnya. kajian menganalisis artikel Dekri No. (5) tahun 2012 yang dipinda oleh Undang-undang Persekutuan No. (12) tahun 2016 berkaitan memerangi jenayah teknologi maklumat untuk mengetahui sejauh mana kejayaan atau kegagalan penggubal undang-undang UAE dalam mengatur dan menangani jenayah siber. Pada akhirnya, kajian itu membincangkan penyelesaian praktikal dan perundangan untuk memerangi jenayah siber dan mengatasi masalah yang timbul daripada jenis jenayah ini, di samping peranan serantau, antarabangsa dan nasional dalam menghadapi dan memerangi jenayah siber. Penyelidik juga menunjukkan penyelesaian praktikal yang paling penting berhubung menghadapi jenayah ini berkaitan dengan beberapa prosedur yang diperlukan untuk memerangi jenayah siber, serta berkaitan dengan mengawal dan memeriksa kaedah yang digunakan dalam pelaksanaan jenayah. Kajian ini menggunakan pendekatan kualitatif analitikal dan perbandingan. Kajian itu diakhiri dengan banyak keputusan dan cadangan, yang paling penting ialah keseriusan jenayah siber dan kepelbagaian bentuknya, sebagai tambahan kepada fakta bahawa penggubal undang-undang UAE menganjurkan jenayah siber dalam Undang-undang Membanteras Jenayah Teknikal Undang-undang Kesatuan No. 5 tahun 2012 dan pindaannya kepada Undang-undang Persekutuan No. 12 Tahun 2016, mengenai jenis jenayah siber berdasarkan jenayah yang dilakukan oleh sistem, dan jenayah terhadap sistem itu sendiri. Di samping itu, kajian itu mengesyorkan agar penggubal undang-undang UAE menambah teks yang menjelaskan hukuman yang ditetapkan untuk jenayah siber, dan dianggap sebagai jenayah terhadap keselamatan negara. Tambahan pula, kajian itu mencadangkan menambah teks mengenai keizinan memeriksa komponen tidak ketara komputer dan mewujudkan kawalan undang-undang untuk mereka.

Kata kunci: Jenayah siber, undang-undang UAE, Masalah substantif dan prosedur, Emiriah Arab Bersatu.

ACKNOWLEDGEMENTS

Space will not be sufficient to acknowledge everyone that has contributed in one way or another, to the completion of the work of this magnitude. I must first and foremost, however, give thanks and glory to the Almighty Allah, who not only stood by me and guided me at every stage of this work, but also gave me the zeal and zest to successfully complete my study.

I am indebted to my supervisors, Dr. Mukhriz bin Mat Rus, whose mien and disposition towards me, encouraged me to work harder; and quest for perfection saved me a lot of worries that would have hounded me during the viva voce examination. I remain grateful to my internal reviewers for their insightful comments and suggestions.

I dedicate my dear wife, sons, brothers, and my sisters this modest work, to support me continue this scientific journey.

To all of you .... Thank you!

Universiti Utara Malaysia

جدول المحتويات /TABLE OF CONTENTS

PERMISSION TO USE ..... أ

الملخص ..... ج

ABSTRACT ..... ح

ABSTRAK ..... خ

ACKNOWLEDGEMENTS ..... د

جدول المحتويات /TABLE OF CONTENTS ..... ذ

CHAPTER ONE /الفصل الأول المقدمة 1

1.1 الخلفية الدراسة/ Background of Study 1

1.2 مشكلة الدراسة/ Problem Statement 6

1.3 أسئلة الدراسة/ Research Questions 11

1.4 أهداف الدراسة/ Research Objectives 11

1.5 أهمية البحث/ Significance of Study 12

1.6 منهجية البحث/ Research Methodology 15

1.6.1 تصميم البحث/ Research Design 16

1.6.2 نطاق البحث / Scope of the Study 18

1.6.3 بيانات الدراسة/ Data Collection 18

1.6.4 طرق جمع البيانات/ Data Collection Method 21

1.6.5 تحليل البيانات/ Data Analysis 22

1.7 حدود الدراسة/ Limitation of Study 22

1.8 الدراسات السابقة/ Literature Review 23

1.9 الخطوط العريضة للدراسة/ Outline of Chapters 39

Universiti Utara Malaysia

CHAPTER TWO / الفصل الثاني 42

بيان وتحديد لمشكلات الجرائم والاعتداءات الناشئة عن الجرائم الالكترونية 42

2.1 ماهية الجريمة الالكترونية 43

2.1.1 القصور في الجريمة الالكترونية 44

2.1.2 تعريف الجريمة الالكترونية 44

2.2 أنواع الجريمة الالكترونية 46

2.2.1 الجرائم الالكترونية الواقعة على النظام ذاته 47

2.2.2 الجرائم الواقعة على النظام ذاته 48

2.3 خصائص الجريمة الالكترونية 49

2.3.1 جريمة قيمية "ترتكب بواسطة الحواسيب بشبكات الانترنت" 49

2.3.2 جريمة عابرة للحدود 50

2.3.3 جريمة ليس له أثر مادي 50

2.4 الطبيعة القانونية وأركان الجريمة الالكترونية 52

2.4.1 الطبيعة القانونية 53

2.4.2 أركان الجريمة 54

2.5 الفرق بين الجريمة الالكترونية والتقليدية 60

2.6 المشاكل الموضوعية الناتجة عن الجرائم الالكترونية 63

2.6.1 جرائم الاعتداء على المراسل الشخصية "الحياة الخاصة" 64

2.6.2 جرائم الاعتداء على الأموال وسرقة المعلومات 65

2.6.3 جرائم التزوير وما يشرع عنها 67

2.7 المشاكل الجزائية الناتجة عن الجرائم الالكترونية 69

2.7.1 مشكلات الجريمة الالكترونية 69

2.7.2 المشاكل المتعلقة بالتحقيق والقانون الواجب التطبيق 72

CHAPTER THREE / الفصل الثالث 79

تحليل نصوص المرسوم رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 لمكافحة جرائم تقنية المعلومات 79

3.1 قانون الجرائم الإلكترونية 79
3.2 التكييف القانوني للجرائم الإلكترونية 103

CHAPTER FOUR / الفصل الرابع 105
الحلول العملية والتشريعية لمكافحة الجرائم الإلكترونية والتغلب على المشكلات الناتجة عن هذا النوع من الجرائم 105
4.1 الجريمة الإلكترونية في ظل التشريعات القانونية 105
4.1.1 القوانين الناظمة للجريمة الإلكترونية 105
4.1.2 الدور القانوني والدولي في مواجهة الجريمة الإلكترونية ومكافحتها 106
4.1.3 النص الدولي للجريمة الإلكترونية 107
4.2 الحلول العملية لمواجهة الجريمة الإلكترونية 110
4.2.1 صور الجريمة (حالات الجريمة الإلكترونية) 110
4.2.2 الجرائم الماسة بالإلكترونية 111
4.2.3 جريمة ابتزاز النساء الإلكترونية 113
4.2.4 الجرائم الرباعية الإلكترونية 115
4.2.5 الحرب الإلكترونية 117
4.3 إجراءات الضبط والتفتيش 120

CHAPTER FIVE / الفصل الخامس نتائج البحث وتوصياته 122
5.1 نتائج البحث والدراسة 122
5.2 التوصيات 126
قائمة المراجع والمصادر REFERENCES 129

Universiti Utara Malaysia

الفصل الأول/ CHAPTER ONE

المقدمة

1.1 خلفية الدراسة/ Background of Study

يشهد الوضع السائد في مجتمعنا تطوراً ملحوظاً بشكل هائل في المجالات التقنية والبرمجية وتسارعاً هائلاً استخدام التكنولوجيا المتطورة في كافة المجالات الاجتماعية والسياسية والاقتصادية[1]، والشك بأن هذا التطور الذي أضحت به الوسائل الحديثة تمثل المحرك الوحيد بين الأشخاص المجتمع وتشارك استخدامه بشكل كبير وفي الوقت عامل بها أصبح لكل شخص الملكيات على الأفعال والتصاريح دون وجود أي مانع من موانع الحدود أو الموانع الجغرافية، هذا بالضافة مع وجود القدرة على تلقي وتقبل المعلومة والاطلاع على المعلومات والبرامج بشكل دقيق وسلسلة وسهولة في الأداء، ومع وجود الايجابيات والمزايا المفيدة الكثيرة التي ساعدت في نشأة تلك الأنواع الذاكرة الحديثة من العوامل المعنوية العلمية[2].

وبالرغم من ذلك الا يمنع من ظهور العديد من الفجوات التي تشكل الشكليات والمورسلية والتي ظهرت على هيئة جرائم جنائية ترتكب بها الأشخاص جراء التكنولوجيا السيما أن هذه الجرائم توصف بالجرائم الخطيرة والتي يتم ارتكابها بسهولة تامة, وبأقل توصف بأنه عابر الحدود, سيما أن متسمى

[1] بلراي محمد وهامي. "العولمة النصية والسياسات الاجتماعية لمواجهة الجريمة الالكترونية في عالم متغير بعض الدول العربية نموذجا." مجلة دراسات في علوم الإنسان والمجتمع 1.01 (2018): 26-08.

[2] احمد بن طيفة & حفوظة الأمير. "الجريمة الالكترونية وآليات التصدي لها". مجلة الباحث للدراسات القانونية والإدارية 1, no. 1 (2017): 148-170. https://www.asjp.cerist.dz/en/article/64136.

بالجريمة المعلوماتية أي الكترونية تكون هناك بغي مجالات التي تغير ملموسة [3]. وكون الجريمة الالكترونية لها زوار يثيرون, الامر الذي أدى إلى ارتكاب الكثير من الجرائم الالكترونية عبر الطرق الحديث من التطبيقات والبرامج المستحدثة عبر شبكات الانترنت, مما أدى هذا الأمر إلى زيادت عدد مرتكبي الجرائم الالكترونية, ومن أكثر الجرائم شيوعاً في الوقت الحاضر "الانترنت أول بديل الالكتروني" والحاسوب, ووسائل التواصل الاجتماعي ومنها الفيس بوك والتويتر والبنت غرام والواتساب"[4].

وتعددت الجريمة الالكترونية الامر الذي حيث أخذت عدة أوجه, وهذا أدى إلى تعدد أنواع الجريمة الالكترونية بحيث نجد بعضها يتصل على الجهاز الكمبيوتر ذاته, واخرى ما يتترابط بالفضاء على المعلومات الموجودة بالجهاز الالكتروني, ونوع أخرى قد يشكل نص بطرق التحايل أو القيام بالتزوير, أو قد يهدف مرتكب الجريمة إلى التطلع على الامور الخاصة والخصوصية, وفي الجريمة اختراق الحواسب الآلية عبر البنوك أو المصارف, وجميع تلك الجرائم في الفضاء الالكتروني[5]. حتى أن بعض الجرائم الالكترونية تصل بحت تمس النساء

---

[3] لطرش فيروز & بن عزوز حكيم. "الجريمة الالكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة." مفاق للعلوم 1.1 (2016). الجيلي الجيلالي. "الجريمة الالكترونية الوطنية والدولية في مكافحة الجرائم السيبرانية". الحوار المتمدن, https://www.ahewar.org/debat/show.art.asp?aid=571423..

[4] مصعب القطاونة، "أهمية الحاجة لنص دورتشريعات خاص قبل الجرائم المعلوماتية", Mohamah.Net, Last modified 2016, https://www.mohamah.net/law. لمزيد من التفصيل انظر: مريس سعيدة بحاش نجيرة بن نجاة زهرة & سعيد شريماء. "أثر استخدام موقع التواصل الاجتماعي في انتشار الجريمة الالكترونية". مذكرة تخرج, جامعة محمد بوضياف المسيلة, 2019.

[5] عادل بن علي بن سالم القبيسي. " Electronic Crime in the Sultanate of Oman: Challenges and legal solutions: الجريمة الالكترونية في سلطنة عمان: التحديات والحلول القانونية." مجلة العلوم الاقتصادية والإدارية والقانونية 3.2 (2019).

وفالهيات خاصة منصات التواصل الاجتماعي الذي أدى الى تطور مجال جديد من العنف إلكتروني يستخدم تقنيات الوسائط كأدوات إلى إيذاء الوسائل وإساءة التحرش الجنسي الإلكتروني قوالب التجسس[6]، هذا النوع من الجرائم التشريع لكبير مؤخراً خاص في أوساط طلبة المدارس والطلبة الجامعيين[7].

ومما الشك فيه أن الأسرة في التشريعات لك الجرائم, ظهر بسبب استعمال الأدوات التقنيات الحديثة الجرائم مرتبط بعض المجرمين التي يصل بحت واضح على المستوى الدولي, ولم تكن موجودة بل ذلك[8].

وتحتوي الجريمة الإلكترونية على شكل الكثير وتنوع صعب جدا في دخل نطاق معين على سبيل الحصر, هذا بالضرورة إلى أن مصل بالتطور الهائل ومن أهول على الأمن بالمتنوعة الارتكاب

Universiti Utara Malaysia

[6] عبد الرازق غزال. "الجرائم الإلكترونية ضد النساء والفتيات: المخاطر وطرق المواجهة." ندى المنظمات الأهلية لمناهضة العنف ضد المرأة، المرأة والعالم وتحديات الثورة الاتصال،)2017(، ص38. لمزيد من التفصيل انظر: شاخ لعيفة& قريشي الحاج العربي بلراهيم. "انتشار الجريمة الإلكترونية المنتشرة الشخاصف في الهيئة الجزائرية دراسة ميدانية على عض مستخدمي مقاهي الإنترنت بمدينة المسيلة". رسالة ماجستير, جامعة محمد بوضياف المسيلة, 2017.

[7] لمزيد من التفصيل انظر: بيرة ليمان. "الجريمة الإلكترونية عبر الإنترنت في أوساط الطلبة الجامعيين". رسالة ماجستير, جامعة محمد بوضياف - المسيلة, 2015. رشيد فارش ونورة قواوش بتأثير موقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية في وسط المراهقين)دراسة ميدانية بثانوية كريم بلقاسم والي الطيبة(. رسالة ماجستير، جامعة الأخوة منتوري ولحاج لخضر الطيبة،)2018(.

[8] أنور المساعدة, "الكفاية الاختصاص في الجرائم الإلكترونية", المجلة الدولية للقانون 2018, (2019), no. 4 doi:10.29117/irl.2018.0043.

للجرائم بحيث تتروح ما بين الكرز عن طريق الاختراقات والتشارات الفيروسات وغيرها والقرصنة والتغيير من الجرائم على وسائل أو الكترونية[9].

وتعد الجريمة على وسائل فئة ذات نطاق دولي وتنتشر في جميع أنحاء العالم وتختلف تماماً عن غيرها من الجرائم التقليدية الأخرى والتي تتصف عامة تعدد المجتمع العالمي, بوصفة خاصة تعدد المجتمع الإماراتي, الأمر الذي يوجب على المشرع عرض نصوص تشريعية تجرم الجرائم على وسائل الكترونية[10].

بحيث تشريع عدالة عامل الأساسي في وضع النصوص القانونية التي يمكن من شأن موضع ضوابط اجرائية تنظم حياة الأفراد في المجتمع وتوقع الجزاء على من يخالف ذلك بما يعني أن القانون وجود بوجود الجماعة يتطور بتطور وضع الحياة مع كل زمان ومكان, لذلك ونظراً لتطور الهائل للأمور الحياتية في مجال الالكترونيات والتقنيات والتكنولوجيا بشكل عام, كان البداً من وجود ضوابط اجرائية تحد من الأمور الأفعال التي يشكل جرائم الكترونية، على يد قدم المشرع في دولة الإمارات العربية المتحدة إلى وضع قانون خاص ينظم ذلك ويحد منه ويقع بعض هذا الجزاء على

---

[9] مقتدى صبرينة & مقدم شيماء، "تأثير الجريمة الالكترونية على المعلومات الرقمية," المجلة الجزائرية للأبحاث والدراسات 3, no. 9 (2019): 137- 159.

[10] عادل دغش العجمي، "المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة," M.A., "جامعة الشرق الأوسط, 2014.

ارتكاب الجرائم وهذا القانون رقم 5 لسنة 2012 بشأن مكافحة الجرائم المعلوماتية وتعديلاته بقرار بقانون رقم 5 لعام 2016[11].

الإمارات كغيرها من الدول التي أصابها ضرر كبير بسبب ارتكاب الجرائم المعلوماتية بجميع أنواعها وصورها بشكل كبير وتعي الحدود بحيث يجب أن يتم وقف تلك الجرائم, وذلك عن طريق فرض وسائل قانونية تحد منها بحيث يجب فرض وضع أمن للفراد بشكل عام وبشكل خاص شركات الإنترنت الموزعة لكل دولة, إلا أن سبب إحالة الجرائم المعلوماتية التي تتسم بالحداثة فهي تتطور بسرعة وكذلك التشريعات المنظمة لمكافحة الجرائم المعلوماتية, الى زال في الفراغ وقصور التشريع في حصر الحماية الجنائية للمجتمعات[12], والذي يوجب معه إلى ضرورة التنبه لقوى الناحية القانونية للجريدة والأمور المرجعية إلى الظاهرة بشكل عام وصريح والتي يكون من شأنها الحد من ارتكاب الجرائم الخطرة بشكل عام, والإلكتروني بشكل خاص[13].

في الإمارات العربية المتحدة أظهرت تقارير رسمية لمديرية الأمن العام أن هناك حالات عديدة للجرائم المتعلقة بين واحد إلى تكون وجه الجريمة خلال العوام الماضية عن طريق مواطنين أجانب

[11] Mohamed Ali, " قانون الجرائم الإلكترونية الإماراتي - قوانين الجرائم الإلكترونية في الإمارات بالتفصيل", Lawyers In Dubai | Legal Consultants In Dubai, Last modified 2020, https://hhslawyers.com/ar/blog/.

[12] "السلامة السيبرانية والأمن الرقمي - البوابة الرسمية لحكومة الإمارات العربية المتحدة", U.Ae, Last modified 2020, https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security.

[13] صباح كنيز & سهير قط, "أثر الجرائم الإلكترونية على أمن واستقرار الدول: قراءة في الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجا", مجلة الناقد للدراسات السياسية, 2018, 119, .doi:10.37136/1999-000-003-006.

وجنسيات أجنبية من دول أخرى وقد استطاعت الجهات المختصة القاء القبض على بعض المتورطين بتلك الأعمال والإحالة للمحاكمة[14].

وقد أصدر المشرع الإماراتي "مرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات والمعدل بقانون اتحادي رقم (12) لعام 2016، والذي أسس لتجريم الأعمال التي تستهدف نظم ووسائط وشبكات المعلومات" ولكن هذا المرسوم غير كافٍ لسد الجرائم المستحدثة والدخيلة في مجال الإثبات الجنائي, وهذا ما أثار الكثير من الإشكاليات من الناحية الموضوعية ومن الناحية الجوانبية بشأن مواجهة الجريمة الإلكترونية, وهذا ما دفع الباحث الى دراسة تلك الإشكاليات في ضوء الفراغ القانوني الذي أضحى يعاني منه المشرع الإماراتي بعد فقدانه صرح التشار ومكافحة الجريمة الإلكترونية[15].

1.2 مشكلة الدراسة/ Problem Statement

الشيك أساس استخدام الجهزة الإلكترونية لكل حساب آلي والمتكون من المورات التي انتشرت بشكل واسع جداً حيث شكل باحث محل النظر والانتباه, لكون مصدر باحث أداة تتداول بين جميع فئات المجتمع سيما أن هناك اضحى استخدامه بشكل كبير في المورات حيث يتم به دفع جمع المال بالنسبة للوضع القتصادي, أو بهدف التجسس وجمع المعلومات بالنسبة للوضع الجتماعي, فالجريمة

[14] المم المتحدة، ورقة العمل الخاصة والجتماعية للغربي لآسيا (الإسكوا)، شرقك لوجيا المعلومات والتصالت المتنوعة في المنطقة العربية، no. 9 ، 2018.

[15] عبد العزيز سالم الدريدي, "الدراسة القانونية لمشرّع الإماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم التحادي رقم 5 لسنة 2102 بشأن مكافحة جرائم تقنية المعلومات ,.M.A "جامعة الإمارات العربية المتحدة, 2018.

عبد المالك صالح. "تشريعات الجريمة الإلكترونية في الهيئة الإماراتية". مجلة الحقوق والعلوم السياسية, العدد 10، ص458 - 474.

الالكتروني تشكل سلباً على الحالة المجتمعية والتي يستحق أن تكون محل حماية اجرائية تكون مشكلة انتهاكاً وخطراً على الظروف الاجتماعية والاقتصادية والسياسية للمجتمعات بشكل عام وتمس الافراد[16].

وتبعاً لذلك فقد أدى التطور التقني إلى تعدد الأساليب وطرق وأدوات ارتكاب الجرائم الالكترونية وخصوصاً الجرائم المرتبطة باستخدام اداة الانترنت بوسيلة الحاسب الآلي وعبر وسائل التواصل الاجتماعي[17]. مما حذا بسلطات إنفاذ القانون أن تتعامل مع مثل هكذا مستحدثة من الجرائم الالكترونية نوع من الاختلاف عما هو المعتاد في الجرائم العادية في مجال الاثبات الجزائي التي يتضمن عدم فإلات ارتكاب هذه الجرائم من الغياب بحجة عدم وجود التنظيم القانوني الالزام لاتخاذ الاجراءات اللازمة[18] لكل ذلك كان على المشرع في أي دولة تعاني من أن تكون الصرامة والمصيرة والمتشرق القانونية تلائم الكيان وقادراً على الوقوف هذا الخضم, وأن الكيان خاسراً ومتأخراً، مما قد ينتج عن ذلك من عواقب وخيمة[19].

تتمثل المشكلة البحثية بتساؤل رئيسي يتعلق بإن مدى الأساليب التي تم بها الفقه الحصول على دليل رقمي الكتروني قبول ذي حجية أمام القضاء الجزائي الماراتي؟

---

[16] عبد اللطيف محمود ربيعة،)"الجرائم الالكترونية" التجريم والمالحقة والإثبات(. المؤتمر الأول للجرائم الالكترونية في فلسطين. نابلس: جامعة النجاح الوطنية, 2016.

[17] يوسف جميل الفقي. "الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة، رسالة ماجستير، الجامعة الاسلامية، غزة)2013(، ص14. حفيظة سليمان& أحمد الدرنشية. الفيسبوك والجرائم الالكترونية في عمان: هل هناك عاقة؟ ", Journal Of Information Studies & Technology (JIS&T) 2019, no. 2 (2019), doi:10.5339/jist.2019.7.

[18] بن قريرة رشيد & بوهوبي يوسف، "التحري الجزائي في مسرح الجريمة الإلكترونية = The Criminal Investigation In Cyber Crime Scene", مجلة جامعة القدس المفتوحة للأبحاث و الدراسات, no. 421 (2017): 52-60, doi:10.12816/0043008.

[19] يلمز عواد. "الإثبات الجريمة الالكتروني قبل الدليل الرقمي", مجلة جامعة كريت للحقوق 3, no. 1 (2017): 476-506.

سيما أن الجرائم الإلكترونية تتسم بالسرعة ومن الصعب الحصول على الدليل المادي, الذي يمثل إثبات الجريمة, هذا بالإضافة إلى أنه من السهل التخلص من هذا الدليل, لذلك فإن معوقات الحصول على هذا الدليل في الجرائم الإلكترونية تضيق نطاق هذا البحث للوصول إلى السبل التي يبنى عليها الحصول على ذلك الدليل.

كما تثور مشكلة أخرى تتعلق بمدى فعالية الضوابط الجوهرية للإجراءات الجزائية في التشريع الجزائري الإماراتي لمواجهة المشكلات الناجمة عن الجرائم الإلكترونية في ظل التطور التقني ألا يتطلب تكاتف الجرائم الإلكترونية؟ كما تثار مشكلة تتعلق بطبيعة المشكلات الموضوعية والجوهرية التي يثيرها هذا النوع من الجرائم, مدى فعالية معالجة المشرع الإماراتي لمواجهة مثل تلك المشكلات[20]. كما تبرز مشكلة مهمة تحتاج إلى باحث للبحث عن الحلول التشريعية لمواجهة المشكلات الناجمة عن الجريمة الإلكترونية كالتكييف والمشرع الإماراتي لتطور التكنولوجي ونص عن انتشار الجرائم الإلكترونية ووضع حد للمجرمين الذين يخترقون القانون عبر شبكات الإنترنت[21]؟.

كما تنتج عبر من المشكلات على المستوى الموضوعية والمستوى الجزائي في الجرائم الإلكترونية صعوبة تتبع آثار الجريمة إن في الغالب لا تترك المجرم أثر فلا يمس فالك أموال والممتلكات فقودة،

[20] جاسم يوسف زيدات, "مدى توفير الضوابط الموضوعية للسرقة الإلكترونية- دراسة مقارنة Rule Of Law And ", Anti-Corruption Center Journal 2019, no. 2 (2019), doi:10.5339/rolacc.2019.9.

[21] إبراهيم الزندي and زكريا هامل, "إجراءات التحقيق في الجرائم الإلكترونية وأحكام الإثبات في القانون الجزائري والمقارن: دراسة شرعية قانونية مقارنة ,"مجلة الدراسات القانونية جامعة أكلي محند أولحاج البويرة, no. 11 (2020): 109-122.

وإنما هي أوقات تغير في السجلات، ومع عظم الجرائم الإلكترونية تربيات الكشف عنها للصرفة، أو بعد وقت طويل من ارتكابها، كما أن الجرائم الإلكترونية تتميز بالقوة لتوقعيد والغباء يتكبت الجرائم يتمتع بالذكاء"[22].

اضف الى ذلك ان العلم يشهد كل يوم نوع جديد من الجرائم الإلكترونية تختلف عن سابق فهو بما الشرعي اي دولة ما يقوم بسن تشريع يحارب فيه الجرائم الإلكترونية الموجودة والمعروفة ينظم اجراءات تشيئ أنواع الجريمة بدءاً من مرحلة التوقيف والبحث التحري حتى المحاكمة نوع وقت قصير يطلع على نوع جديد من الجرائم الإلكترونية يختلف جوهرياً عن الجرائم السابقة مما يحتاج الى اعادة صياغة اوتعديل مواد القانون الموجود ليواكب هذا النوع الجديد من الجرائم بالضرفة الى فحص مدى ملائمة الاجراءات الموجودة ومدى انطباقها على هذا النوع الجديد من الجرائم[23].

إن تطور الجريمة الإلكترونية يشكل تهديدا بمثل رأل كثر المرفق العام والمصالح الخاصة ويقوض الأمن الاجتماعي ويمثل عدوانا على حقوق الأفراد يحيلت على بعض خصوصياتهم اللامية

---

[22] سلوراء جريل العربي, "الجرائم الإلكترونية " الأهداف - الأسباب - طرق الجريمة ومعالجتها" - المركز الديمقراطي العربي", المركز الديمقراطي العربي, .Last modified 2016, https://democraticac.de/?p=35426.يوسف جفال. التحقيق في الجريمة الإلكترونية. رسالة ماجستير، جامعة محمد بوضياف المسيلة, 2017، ص4.

[23] بلتسام غو. "إجراءات المتابعة الجزائية في الجريمة المعلوماتية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي،)2016(، ص1 - 3 بوضياف بلمهان, "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر ,"مجلة الأستاذ الباحث للدراسات القانونية والسياسية.(2018) no. 11 ,بشير حملي. "خصوصية التحقيق في الجريمة الإلكترونية". رسالة ماجستير جامعة محمد بوضياف - المسيلة, 2019، ص26 بتركي, نهى كامل. "التحقيق الجنائي في الجرائم الإلكترونية". Amday55.Blogspot.Com, https://amday55.blogspot.com/2016/04/blog-post.html

وخصوصية مهام التي تشكل التعدي على هيئة الحقوق الخاصة لصيق قبالة الفرد[24]. تورقسم هذه الجرائم بأنها غير ملموسة، كما أنها تحدث من أي مكان وفي الكصوعب فتيب عها، ألنها قد تخرج عن نطاق الدولة، لذا فإن إثبات مثل هذه الجرائم يواجه صعوبة مختلفة، ولها من خصوصية جي تتطلب إجراءات معينة في الإثبات، وهذا شرك لقتواجه الدراسة الحالية؟[25].

وبالتالي جفلما كان موضوع البحث يتعلق بالشرك التالموضوعية والإجرائية متعلقة قبالجرائم الالكترونية في دولة الإمارات العربية المتحدة, فإن ذلك يعني بالضرورة البحث في أهميتها ومركزها القانوني والفقهي الجريمة الالكترونية, مع تحديد التكييف البحثي الإشكالية :

فما هي الجريمة الالكترونية؟ وما هو مركزها القانوني والفقهي ؟ وما هي الصعوبات التي تعرقل عملية الكشف في الجريمة الالكترونية, وما هي الأسباب الجوهرية التي تتسبب في الكشف عن الجرائم الالكترونية, أي إلى أي مدى يمكن أن تؤدي الشرك التالموضوعية والجوهرية في عرقلة الكشف عن الجرائم الالكترونية؟ بالضرفة التي سبق تتمثل شرك لة الدراسة حول معرفة بطبيعة الدليل الالكتروني الذي يساهم في الكشف عن الجرائم الالكترونية، ولكذلك مدى شرعيته؟.

---

[24] زيدان نورالدين. مداخلة بعنوان "معوقات سير التحقيق لعام الإلكتروني الجريمة الإلكترونية أنموذجا." الحقوق جامعة السعودية، (2019).

[25] الهام بولطين. "الإثبات الجنائي في الجرائم الإلكترونية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2018)، ص4 - 5 فيروز عوض الكريم بيرغني. إجراءات التحريز الضبطي الجريمة الإلكترونية، أطروحة دكتوراه، جامعة شندى، السودان. 2017، ص14- 15.

كما يشكل هذا الموضوع مشكلة تدور بشأنها في نفس الباحث سعياً نحو الحصول على الإجابات والحلول التشريعية الموجودة فعلاً وتقييمها ووزنها, وبيان مثالبها ومحاسنها, ومن ثم تقديم الحلول والمقترحات على هيئة إضافة علمية من ناحية وبناء على ما تم من ناحية أخرى.

1.3 أسئلة الدراسة/ Research Questions

تتمثل أسئلة هذه الدراسة من خلال الأسئلة التالية:

1- ما هي المشكلات الموضوعية المتعلقة بالجرائم الالكترونية في دولة الإمارات العربية المتحدة؟

2- ما هي المشكلات الإجرائية المتعلقة بالجرائم الالكترونية في دولة الإمارات العربية المتحدة؟

3- ما الحلول الممكنة لمشكلات الموضوعية والإجرائية المتعلقة بالجرائم الالكترونية في دولة الإمارات العربية المتحدة؟

1.4 أهداف الدراسة/ Research Objectives

يهدف هذا البحث للوصول إلى إجابة واضحة وشاملة للأسئلة السابقة من خلال تحقيق أهداف الدراسة بدءاً من التعريف بمفهوم ماهية الجريمة ذات الطابع الالكتروني, ومعرفة الشكليات التي ترتكز بسببها الجرائم وتعمل الدراسة على المشاركة في وضع القواعد الإجرائية لمساعدة حل الشكليات المتعلقة بالجريمة الالكترونية وتأويل نص دراسة تقييمية تحد من انتشارها وإفادة أدلتها وتوعية المجتمع من أجل التصدي لها.

كما تهدف الدراسة إلى ما سوف تتوصل إليه من نتائج وتوصيات تضع بين يدي المشرع الإماراتي على أمل أن نجد أثراً صائغاً من المشرع الإماراتي في ضرورة التدخل لحل تلك

الشركات, موضوع نصوص قانونية تنظم جرائم الجرائم الإلكترونية والحد منها للحفاظ على حقوق الأشخاص في المجتمع الدولي والوطني على حد سواء لسد الفراغ التشريعي في وجه التطور والانتشار السريع للجرائم الإلكترونية[26] تمثل أهداف الدراسة القانونية الآتية:

ومن أهداف الدراسة الرئيسية تتمثل في: تحليل الشكل الموضوعية والإجرائية لمتطلبات قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة.

يمكن أن تكون الأهداف الفرعية الثالثة:

1 التعرف على الشكل الموضوعي المتعلق قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة.

2 تحديد الشكل الإجرائي المتعلق قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة.

3 اقتراح الحلول الممكنة لمشاكل الموضوعية والإجرائية المتعلقة قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة.

Universiti Utara Malaysia

1.5 أهمية البحث/ Significance of Study

الباحث يعتقد أن الوضع الراهن في مجتمعنا هو عصر السرعة، وهذا ما يفسر الانتشار الكبير لاستخدام الحاسب الآلي والهواتف الذكية سواء في مجال الأعمال أو في الحياة اليومية وبدأت بادر إلى مسامع بعض الفقهاء لتسمية ذلك وهي "الحكومة الإلكترونية"، "المتر الإلكتروني،

[26] حسن الشمري, "القانون الواجب التطبيق على الجرائم الإلكترونية قانون الواجب التطبيق على الجرائم الإلكترونية بتصور مقترح," المجلة العربية للدراسات الأمنية والتدريب 27, no. 35 (2011): 5- 45.

التجارة الإلكترونية[27]، شبكة المعلومات، التوقيع الإلكتروني، الإمضاء الإلكتروني والقرصنة الإلكترونية"[28].

هذه الدراسة تكتسب أهمية بالغة نتيجة لما تحمله من قبل مهارات التخصص والتواصل الحديثة من الشخاص رهن الجرائم الإلكترونية تستهدف الطب مع الجرائم بالضفة إلى الأهمية النظرية والعملية التي تستنتجها هذه الدراسة لكون هات مس لكثير أبلى مصالح الخاص قبل المجتمعات, وتبرز الأهمية من الناحية العلمية في معرفة مصادر الخطر في النظام الإلكتروني شبكات, ومعرفة أنواع الاعتداء على المعلومات وصوره, والنماط المستجدة للجرائم الإلكترونية, كما تظهر أهمية من الناحية العملية الموضوع من خلال معرفة النتائج التشريعي الوطني قانوني قبش أن حماية أمن المعلومات ونظم تكنولوجيا[29].

كما تكمن أهمية هذا الموضوع في محاولة الغور على حل لمشكلات المرتبطة بالجرائم الإلكترونية, في التشريع الإماراتي والتعرف على أهم المشكلات العملية والقانونية التي تثيرها تلك الجرائم بشكل مستمر. ومدى ملائمة الجراءات الضوابط القضائية في قانون الجراءات

---

[27] لمزيد من التفاصيل حول الحماية الجنائية للتجارة الإلكترونية انظر: رزيق قبودودة. "الحماية الجنائية للتجارة الإلكترونية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2015).

[28] "ما هي الجرائم الإلكترونية بدبي والعقوبة المبالغ عنها - عقوبتها - العقوبات المختصة | مايبيوت", مدونة تشمل مواضيع تتعلق بالعقارات و أنماط الحياة المختلفة في الإمارات | مايبيوت, accessed 20 February 2021, https://www.bayut.com/mybayut/ar//.

[29] محمد بن أحمد علي القصودي, "الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً ,"المجلة العربية للدراسات الأمنية و التدريب.2017, doi:10.26735/13191241.2017.004, سيد,سيد طنطاوى محمد. "الجريمة المعلوماتية : التحديات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها". المركز الديمقراطي العربي. https://democraticac.de/?p=54584.

الجنائية" على الجريمة الإلكترونية والصعوبات التي تواجه الدولة وأفراد القانون والقضاء في تطبيق وتنفيذ هذه الإجراءات على هذا النوع من الجرائم[30].

كما تبرز أهمية الدراسة من خلال بحث المشرع الإماراتي على تبني آليات سياسية واضحة لمكافحة الجرائم ذات الطابع الجنائي بحيث تشمل السياسة الجنائية وقائية تهدف بشأن الحد والتصدي للجرائم الإلكترونية فيما أن تم إدخال السياسة العقابية للنجاح والتخطيط السليم والشامل والقدرة على التنفيذ، وتساعد الأدوات التشريعية المتخصصة وأيضاً القضائية على النجاح في مكافحة الجرائم الإلكترونية شتى أنواعها وصورها، رغم حداثتها وانجازاتها[31].

فطالما كانت دولة الإمارات العربية المتحدة تسعى أن تكون واحدة من أكثر الدول أمناً على العالم من خلال استحداث نصوص وقوانين تحمي مصالح الأفراد في جميع أنحاء المجتمع والمجتمعات من الجرائم المتكبة، والتي من بين هذه الجرائم الإلكترونية والتي بدأت تأخذ حيزاً كبيراً على العالم الجديد، وتتطلب قبل التضرر من آثاراً جنائية مادية ومعنوية[32].

---

[30] أسامة بن غانم العبيدي, "التفتيش عن الدليل في الجرائم المعلوماتية", المجلة العربية للدراسات الأمنية والتدريب 29, no. 58 (2013): 85-132, doi:10.12816/0001809. بخيت أطمة الزهراء. "إجراءات التحقيق في الجريمة الإلكترونية". رسالة ماجستير, جامعة المسيلة,2014 ، ص23 -27.

[31] رشا دبشير إبراهيم. "التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبوظبي". مركز الإمارات للدراسات والبحوث الاستراتيجية,العدد313، 2018، ص83 -84.

[32] مصطفى يوسف, "استراتيجية إماراتية لمواجهة الجرائم الإلكترونية", البيان, Last modified 2013, https://www.albayan.ae/across-the-uae/accidents/2013-09-26-1.1967235.

كما أن أهمية الدراسة تبرز في البحث في مدى حجية قواعد النصوص القانونية الجزائية والجوانب المساعدة المتعلقة في مجال أما المطلب الثاني عن الحصول على وسيلة قانونية في مجال الجرائم الالكترونية[33]. كما يمكن أن تظهر أهمية الدراسة عن طريق الاستفادة التي عادت على الباحثين من النتائج والتوصيات لتلك الدراسة والتي يقوض اهتمامها في تقوية الجرائم الالكترونية.

هذا بالإضافة إلى أن هذه الدراسة تعود بالفائدة القانونية والبحثية لعديد من الفئات القانونية والتعليمية داخل المجتمع بما أنه استهدف رجال القانون العاملين في القضاء والنيابة العامة والمحققين في مركز الشرطة, وأيضاً المحامين, وأيضاً تكون هذه الدراسة مرجع ذو قيمة علمية واضافة للمكتبة القانونية في دولة الامارات على المستوى الخاص وللدولة العربية على المستوى العام .

Universiti Utara Malaysia

1.6 منهجية البحث/ Research Methodology

تشير المنهجية المستراجية الدراسة العامة المستخدمة لكي يحدد الطريقة التي يتم بها إجراء البحث, وسوف يستخدم الباحث المنهج الوصفي التحليلي للوصول الى نتائج وتوصيات يبنى على أوجه الفرق التشريعي لدى الشرع الامارتي بخصوص مواجهة تحديات الشرك التقليدية والجوانب المتعلقة قبال الجرائم الالكترونية[34].

[33] لمزيد من التفصيل انظر: شمرزاد حداد. "الدليل الإلكتروني في مجال الإثبات الجنائي". رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2017).

[34] Hamidoush Madani, " Brief in the methodology of legal research (3rd ed), 2015, p.31.

في إطار منهجية البحث تنقسم الدراسة إلى خمسة أجزاء تتضمن مجال البحث، نطاق البحث، أنواع البيانات، طرق جمع البيانات وتحليل البيانات.

وسوف يتم البحث بأدوات التالية:

أ- الاطلاع على مختلف المؤلفات والكتب العلمية والدراسات والبحوث السابقة فيما يتصل بموضوع الدراسة مع الإلمام بالجوانب الأحداث .

ب- الاطلاع على "القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية" بالإضافة إلى "مرسوم قانون الجرائم الإلكترونية في إمارة دبي رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 بشأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة والقوانين ذات الصلة".

ج- الاطلاع على الأحكام والسوابق القضائية المتعلقة والصادرة عن محاكم الإمارات خاصة محكمة النقض ومحاكم الاستئناف بعض القضايا التي تتعلق بموضوع هذه الدراسة وتحليل هذه الأحكام لمعرفة الدور القضائي في تعزيز وتذليل العقبات التي تواجه الجرائم الإلكترونية من خلال تحقيق تنقيح في الشكاوي التي تعرض جميع أفراد القانون في الدولة فإن التصدي مثل هذا النوع من الجرائم.

1.6.1 تصميم البحث/ Research Design

ستشمل الدراسة كلاً من البحث القانوني الفقهي البحث القانوني وعادةً ما يكون البحث القانوني عبارة عن دراسة نظرية قائمة على المكتبات تهتم بتحليل النصوص القانونية والقواعد ذات الصلة

بالدراسة[35]، ويتم اختيار هذه الطريقة نظرًا لوجود العديد من المشكلات المتعلقة بالجرائم الالكترونية في القانون الإماراتي, لذلك البد من تحليلها من خلال المراجعة والتدقيق والتحليل النظري وتسليط الضوء على النصوص القانونية المتعلقة بهذه الدراسة لغرض هذه الورقة البحثية سيقوم الباحث بتحليل النصوص القانونية الحالية، والتشريعات القانونية التي تم مراجعتها وترتيبها من خلال الاستدلال القانوني أو المنهج العقلاني.

على وجه التحديد سيقوم الباحث بتحليل النصوص القانونية والأحكام الخاصة بالقانون الاتحادي رقم (2) لسنة 2006م ومرسوم قانون الجرائم الالكترونية في إمارة دبي رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 بشأن مكافحة جرائم تقنية المعلومات"، مع التركيز بشكل خاص على تلك النصوص التي تشير إلى الجرائم الالكترونية.

يشير البحث القانوني غير العقائدي ،الذي يشار إليه أيضًا بالبحث القانوني الاجتماعي, وعادة ما يكون أكثر اهتمامًا بتقنية المعلومات, لغرض هذه الدراسة يتضمن البحث غير العقائدي المعلومات والآراء جمع البيانات من خلال الوصول إلى هدف غرض يخص يتشكل الدراسة البحثية وتحديد الحلول المحتملة أو الأسئلة التي يثيرها في الدراسة, لسماع الباحث في الحصول على معلومات شاملة فهم مالك البحث[36].

[35] Empirical (non-Doctrinal) Research Method and Its role in Legal Research In-text: (Chakraborty, 2015).

[36] Marshall C & Rossman G, "Designing Qualitative Research (3rd ed)," (California: SAGE Publication .press, 1995): 23

ومن جانب آخر يعتمد الباحث على الجانب العملي كي يتضح مدى تطبيق الجانب النظري على أرض الواقع, هذا بالإضافة إلى إيجاد نموذج التحقيق المطبق على أرض الواقع.

1.6.2 نطاق البحث / Scope of the Study

تهتم هذه الدراسة بموضوع رؤية موضوعية وفق التشريعات الإماراتية :

النطاق الموضوعي للدراسة: تقتصر تلك الدراسة على التشريع الجزائي الإماراتي, مع ذكر بعض التشريعات العربية الأخرى بخصوص وقوفها من معالجة الشركات الموضوعية والجزائية التي تثيرها الجرائم الكترونية.

النطاق الزمني للدراسة: هو يغطي سنوات من عام 2006 إلى عام 2016.

1.6.3 بيانات الدراسة/ Data Collection

سيستخدم الباحث مصدر أساسي لبياناته "مرسوم قانون الجرائم الكترونية في إمارة دبي "رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 بشأن مكافحة جرائم تقنية المعلومات", هذا القانون هو المرجع الأساسي الذي يهتم العتماد عليه الباحث في تلك الدراسة وسيشكل أساس الجانب النظري للبحث.

سوف تتضمن البيانات الأولية كذلك الأحكام والسوابق القضائية المستقاة لصادرة عن المحاكم الجزائية في دولة الإمارات خاصة محكمة النقض ومحاكم الاستئناف كل ذلك بهدف الوصول إلى أكبر قدر من المعلومات حول موضوع هذه الدراسة من جهات مختلفة.

كما تشمل البيانات الباحث على الدراسات الكتابية مثل الكتب والجامعية والأطروحات والمنشورات في المجال التوالتقارير المنشورة على وجه التحديد، وسوف تبين الباحث العديد من القضايا العربية الشرق الأوسطية التي يستخدمها الباحث لتحليل النقدي ومقارنة الآراء المختلفة الواردة في هذه المواد.

بالإضافة إلى ذلك سيقوم الباحث بمراجعة البيانات التي يتم جمعها من خلال الدوات والمؤتمرات والبحوث الموضوعة على نصات تشوبكات المواقع الكترونية والمعلومات التي يتم الوصول إليها من خلال الباحث العلمي في Google وقواعد البيانات عبر الإنترنت تتضمن أبحاث قاعدة البيانات عبر الإنترنت, كما ترجع الباحث إلى قالت ومجالت الرسائل الكترونية تتوجيق أهداف هذه الدراسة.

وذلك نظراً لكثرة الجرائم التي ترتكب بواسطة الجهزة الكترونية سيما وأنه قد بلغ عدد الجرائم التي يتم ارتكابها في السنوات الخيرة في الزيادة نظراً لسهولة ارتكابها بتقنية سهلة ومرنة وسريعة, وقد يتم ارتكابها من منطقة بعيدة, بمعنى دون وجود الجاني في مسرح الجريمة , إلا أن تتوجه الجهزة النيابة في دولة الامارات العربية وخاصة أعضاء النيابة العامة وأجهزة التوجيق الكثير من الصعوبات التي تعرقل عملية الكشف عن الجرائم, سواء في مرحلة جمع الستدلال, أو التوجيق, كونها قد يستغرق وقتاً طويلاً في عملية التقصي والتحري لمعرفة الحقيقة, نظراً لسهولة محو وإخفاء الدليل الجنائي, كون هذا النوع من الجرائم يستخدم بواسطة الجهزة الكترونية الصغيرة والكبيرة

الحواسيب والتي قد يكون من شأنه تعطيل معلومات, أو أموال, فهذا المال يسبب الأمر يسير على الأجهزة الأمنية المختصة, والذي يبدو أن يحتاج إلى كفاءة وخبرة لدى المتهمين القائمين بهذا العمل[37].

بلغت الجرائم الإلكترونية في عام 2020 إلى أكثر من 600000 هجوم في الإمارات العربية المتحدة, وذلك فوق الأرقام التي تم إحصائها, في عام 2021 تلقت الأجهزة الأمنية 1740 بلاغاً عن الابتزاز المالي, وذلك بشرطة مراكز الشرطة وذلك خلال ثلاثة أشهر من عام 2022م, وقد تم استرداد ما يقارب نسبة 80% من الحالات التي تعرض المال إلى الشرطة الأجهزة المحمولة التي تم البلاغ عنها أو أمثلة عن الجرائم التي وقعت في أمام الجرائم بالنص الأمر الصحية وأخبار أنه من قسم الشرطة في الإمارات يطلبون بطاقة الهوية الخاصة بويارات هو تحدث على رابط وهمي أرسله الجاني, وهكذا يكون الضحية وقع في عملية احتيال, وقد تم إعادة إلى ضحايا الجرائم الإلكترونية في عام 2021م ما يقارب 18 مليون درهم نتيجة النصب والتحايل بشرطة الاتصال المحمول قيمتها وأن دولة الإمارات العربية المتحدة قد أحرزت تقدم بشأن مكافحة غسيل الأموال وذلك فوق ما ذكره الرائد/ الريان[38].

إن أنظمة القانون الاتحادي رقم 35 لسنة 1992م بشأن إصدار قانون الإجراءات الجزائية, ومرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة الجرائم تقنية المعلومات, جاء من نظم لجرائم التقنية المرتكبة بشرطة الأجهزة الإلكترونية والمتواجدة بالإمارات وي عد قانون دولة الإمارات العربية المتحدة للجرائم الإلكترونية، أحدث التشريعات في القرن الواحد وعشرين وأشدها وأكثرها تطوراً بحيث

[37] عنوان الجريمة, الجرائم الإلكترونية في دبي, تاريخ النشر 2022/9/4م, تاريخ الدخول 2022/11/14م, https://www.khaleejtimes.com/crime/

[38] الأمم المتحدة يوغوا وبتاريخ النشر 2022/3/14م, https://www.thenationalnews.com/uae/

يبحث هذا القانون الجرائم الإلكترونية في دولة الإمارات العربية المتحدة المجال التالي من ة، الأكثر أهمية، إلا أن القانون لم ينظم أحكام جميع الجرائم الإلكترونية فقد دخلت أحكام ها من يان الجرائم المحمول قبش أن معالجتها, وسبب تزايد الجرائم المرتكبة أصبح فاك رقص في المعرفة بماهية الجرائم الإلكترونية والسرعة التي تتبع عن منعها وذلك بسبب عدد الشركات التي يسببها المخترقون والقرصنة بواسطة الإنترنت, والذي أصبح على تزايد كبير في دولة الإمارات العربية المتحدة.

1.6.4 طرق جمع البيانات/ Data Collection Method

في هذه الدراسة سيقوم الباحث بجمع المعلومات والبيانات من مختلف المراكز المعلومات والمؤسسات القانونية تمثل الجامعات في الدولة العربية والمحاكم المحلية كمصدر أساسي للبيانات, بالإضافة إلى ذلك القوانين الصحفية والأوراق والبيانات البحثية والدوريات والكتب الجامعية المتاحة في مختلف الجامعات.

لن تتسنى هذه الدراسة من جهة القوانين وذلك لوجود القدر الكافي من المعلومات حول هذا الموضوع ولكن هذه الدراسات تختلف عن الدراسات الخرى بغض النظر عن فرة المعلومات حيث انه لتركز على جانب معين وهو الشركات الموضوعية والجرائم المتعلقة قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة وهذا ما يضفي عليه دراسة قيمة بالإضافة إلى ذلك لن تتسنى الدراسة طريقة القوانين الخاصة وصعوبة الوصول إلى الشخاص المستهدفين في الدراسة فقد يتم الوتم عمل القوانين لكون المعلومات التي تتعلق بالشركات الموضوعية والجرائم المتعلقة قبل جرائم الإلكترونية في دولة الإمارات العربية المتحدة سرية ولا يمكن الطلاع عليها.

يبحث الباحث أيضًا من موارد الإنترنت للبحث عن أي معلومات عبر الإنترنت تتعلق بموضوع الدراسة التي تتعلق بمذهب الدراسة.

1.6.5 تحليل البيانات/ Data Analysis

تتعلق البيانات هي مجرد بداية لتبدأ الدراسة في قسم مجرد جمع البيانات نفسها وفي تنظيمها ومراجعتها بعد ذلك يتم تحليل البيانات المستمدة من مختلف المصادر المذكورة سابقاً من قبل الباحث بغرض التحقق من طريقة التحليل والوصف والتحليلية, كما يتم تحليل أدلة من البيانات ومصادر البيانات للتأكد من أن دراسة هذا الموضوع ونتائجه يتم الحصول عليه بشكل شامل وصحيح من مصادره الموثوقة[39]. كما يعتمد الباحث تحليل المحتوى النوعي والتحليل الموضوعي لتحليل مواد القانون وتحديد المعلومات ذات الصلة بقبل دراسة بالإضافة إلى تحليل الوصفي التحليلي والقدي المطبق على البيانات من المصادر القانونية الأولية، بالإضافة لتحليل فوشيرر أحكام المحاكم والسوابق القضائية موضوع هذه الدراسة التي يتم الحصول عليها.

1.7 حدود الدراسة/ Limitation of Study

يوجد في دراستنا هذا الموضوع يتمثل في وجود مصادر محدودة وأحكام يلفقيم القوانين المتعلقة بقبل الإجراءات الإلكترونية، وهذا يحد من النطاق على الوصف والتحليل وهذا هو أساس حاجز كبير في إجراءات هذا البحث بالإضافة إلى ذلك الحد من الوقت الذي يُعطى للباحث إلجراء

[39] محمد, أ. د. باحفوزى, و أ. د باحفوزى. "البيانات ودوره في البحث العلمي." المجلة الدولية للعلوم للمكتبات والمعلومات 9.1)2022(: 21-13.

هذه الدراسة تبحث في الباحث على هذه القيود من خلال البحث في العديد من المصادر والمراجع المتعلقة بموضوع الدراسة سواء المصادر الالكترونية عبر الانترنت والمكتبات والمجلات الالكترونية أو المصادر الجامعية مثل المكتبات والكتب الورقية. بالإضافة إلى الاطلاع على الدراسات السابقة المتعلقة بهذا الموضوع في الدول الأخرى وقارنتها مع الدراسة الحالية للوصول إلى أكبر قدر من المعلومات التي تفيد هذه الدراسة.

1.8 الدراسات السابقة/ Literature Review

تتعبر الدراسات السابقة خاصة في مجال العلوم القانونية من أهم الأجزاء الذي يحتوي له البحث العلمي فالكون الباحث العلمي يبحث خاصة جيدًا بتلك المال اذا لم يتضمن على دراسات سابقة على قبذات الموضوع بناء على ذلك يمكن القول أن الدراسات السابقة عبارة عن عدد من المصادر والموضوعات التي تناول تشكل مسبق ذات موضوع الباحث الذي يقوم الباحث بدراسته ، وهي تمنح الباحث فكرة مجملة لكثير من المعلومات الهامة والقديمة حول موضوع بحثه العلمي.

سيعمل الباحث الدراسات السابقة من خلال طريقة annotated bibliography من خلال قيام الباحث بذكر عنوان الدراسة ثم تقديم ملخص صغير لها وبعد ذلك يعلق على هذه الدراسة والتحليل لها ثم بالنهاية ذكر نتائجها مع الخضوع إلى التعبير الناقد بالكتابة بين الدراسات فإذا وجد الباحث وجود تشابه كبير في دراسات معينة سوف يقوم بذكر هما سوياً وذلك للحرص على عدم تكرار في الأفكار والفهم. كل ذلك لكي تتناسب مع شامل لمشكلات من النواحي الموضوعية من جانب وأخر من النواحي ذات بطبيعة اجرائية والمتعلقة بطرق وجود الحراك الالكتروني, من

الدراسات ذات الصلة بالموضوع منها، هذا أمر بالغ الأهمية إذا كان لهذه الدراسة أن تكون ناجحة في تحقيق أهدافها المرسومة.

من أهم الدراسات السابقة التي وجدها الباحث تحت عنوان موضوع هذه الدراسة دراسة الباحث عبد العزيز سالم السويدي[40]: السياسة الجنائية لمشرّع الإماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، 2018. وكذلك دراسة للباحث سليمان بن مهجع العنزي[41]: وسائل التحقيق في جرائم نظم المعلومات, 2003م".

تحدث الباحث في هذه الدراسة عن "التطورات الجنائية المترتبة على الجرائم المستحدثة عن طريق استخدام وسائل التقنية الحديثة وفقا المرسوم بقانون رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات".

تحدث الباحث عن "القانون رقم 2 لسنة ٢٠٠٦م وهو القانون الأول في دولة الإمارات الذي تناول بعض الجرائم الإلكترونية" التي كانت معروفة آنذاك والتي رافقت إصداره ولكن بمرور الوقت وتقدم وتطور الوسائل التقنية تصل بحر القانون غير مع عصر لما استجد من تطور في مجال التقنية المعلومات، فقام المشرع الإماراتي بإعادة النظر لهذا القانون وأصدر "المرسوم رقم 5 لسنة 2102". تحدث الباحث عن السياسات التي يشكل جزاء الجنائي في "المرسوم رقم 5 لسنة ٢٠١٢م" والعقوبات بالضرورة التي تبادر التي اتخذها المشرع الإماراتي في هذا الصدد كما بين

[40] عبد العزيز سالم السويدي, "السياسة الجنائية لمشرّع الإماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم الاتحادي رقم 5 لسنة 2102 بشأن مكافحة جرائم تقنية المعلومات ,.M.A "جامعة الإمارات العربية المتحدة, 2018.

[41] سليمان بن مهجع العنزي, "وسائل التحقيق في جرائم نظم المعلومات ,.M.A "جامعة نايف العربية للعلوم الأمنية, 2003.

مظ المل س يل س ة ال ق ي ا ي ة س و ا ء ال ت ش د ي و أ ل ت ف خ ي ف ف ى ه ذ ا ل م س و م ب ا ل ض ف ى ة ا ل ى ل ت ت ب ط ي ق ا ل ق ض ا ئ ي ل ه ذ ا ا ل ق ا ن و ن.

و أ ص ى ل ب ا ح ث ف ي ن ا ي ت ر ل س ت ب ع د ت ت ص ي ا ت م ن ه ا إ ع ا د ة ف ي ت ن ظ ر ب ش أ ن ا ل ق ي ب ا ت ا ل غ ل ظ ة ا ل ت ي و ر د ت ف ي ا ل م س و م ب ق ا ن و ن ر ق م 5 ل س ن ة 2012 م ب ح ي ث ت ن ل س ب ا ل ق ي ب ة م ع ا ل ج ي م ة ب ا ل ض ف ة ا ل ى ل ت ح ر ي ح و ل م د ى ت ت ب ط ي ق ا ل ج ه ز ة ا ل ر ق ا ي ة إ ل ا ل ك ت ر و ي ة ك ن و ع م ن ا ل ق ا ي ة م ن و ق و ع ا ل ج ا ئ م و م ا ي ع ر ف ب ا ل ت ا ب ي ر ا ل ا ح ت ر ز ا ي ك ب د ي ل ع ن ا ل ق ي ب ة ا ل ى ل ب ا ق ل ج ي ا ت , و ذ ل ك ف ي ظ ا ل ت ي غ ي ر أ ل خ ي ر ل ق ا ن و ن إ ل ج ر ا ء ا ت ا ل ج ن ا ي ة.

و ت ل ك ا ل د ر ا س ت ت ت ل ف ع ن ا ل د ر ا س ة ا ل ت ي ي ن و ل ى ل ب ا ح ث ا ل ق ي ا م ب ه ا م ن ع د ة ن و ا ح ي أ و ل ه ا أ ل ى ل ب ا ح ث ف ى ر ا س ت ه ا ل س ا ب ق ت ت ح د ث ع ن ف ق ط ع ل ى س ي ا س ة ا ل ق ي ا ي ة ا ل ت ى ا ن ت ه ج ه ا ا ل ش ر ع ا ل م ا ت ي ف ى "م ك ف ح ة ا ل ج ر ا ى ا ل ا ل ك ت ر و ي ة م ن خ ا ل ل ا ل م س و م ر ق م 5 ل س ن ة ٢٠١٢ م" و ل ي ت ح د ث ع ن ا ل ن ا ك ي ا ت ذ ا ت ص ب غ ة م و ض و ع ي ة و ا ج ا ئ ي ة ا ل ت ى و ا ج ه ه ا ا ل ش ر ع ا ل م ا ت ي ب ش أ ن ت ت ب ط ي ق أ ل ح ك ا م ا ل خ ص ق ا ن و ن ا ل ج ر ا ء ا ت ا ل ج ن ا ي ة ع ل ى و ق ا ئ ع ا ل ج ر ا ى ا ل ا ل ك ت ر و ي ة و م ك ي ب ع ه ا م ن ع ض ا ل ت. ك م ا أ ل ى ل ب ا ح ث ل م ت ي ن ا و ل ا ل ف ت ص ي ل م ا ه و ا ل ط ا ر ا ل ق ا ن و ن ي ل ل ج ر ا ى ا ل ا ل ك ت ر و ي ة ك م ا ل ي و ض ح د و ر ا ل م ح ا ك م و ا ل ض ا ف ى م ك ف ح ة ه ذ ا ا ل ن و ع م ن ا ل ج ر ا ئ م و ك ي ف ت ع ا م ل ت م ع ا ج ر ا ء ا ت ا ل ت ح ق ي ق و ا ل ج ر ا ء ا ت ا ل ت ي ت م ت م ق ب ل ج ه ا ت ا ل ت خ ص ا ص و ل ك ف ي ة ل ر ق ا ط ه ذ ه ا ل ج ر ا ء ا ت ا ل ت ت ع ل ق ب ا ل ج ر ا ى ا ل ق ت ي ة ع ل ى ا ل ج ر ا ئ م ا ل ا ل ك ت ر و ي ة.

بين هذان اولان باحثفى الدرلسة الثاني ة عن الوسائل السيتخدم فـي اجراءات التحقيق حول الجرائم الالكترونية العلومات عبراك تشاف جرائم الانترنيت طبالجرائم الالكترونية وذلك بتحديد من اطها وأهدفها بوي ان أضرارها وتحديد نطاق الالي ب والدوات المستعملة مرقبل رتكابي الجرائم الالكترونية, كما هدفت هذه الدرلسة الى شرح طرق الحصول على ألدوات المستخدم فـي رتكاب الجرائم من ظم العلومات داخل المملكة العربية السعودية بوي ان الشرك ال تالتي يتم وضع دوا ستخدام هذه الوسائل وتحديد شكل ال ألدلة المعرف فـي وقوعك الجرائم وكيف يمكن أن تصب طو أين توجد؟! لذلك تحديد إلجراءات ألنهية والدراي ة للوصول ألمن نظم العلومات، وتحديد أهم ألسس لصياغة سياسات ألنهي اقك امل ة لحماية النظمة والعلومات.

أظهرت الدرلسة العديد من الطرق الفنية والإجرائية التي يتس اهف يضبط الجريمة وتحديد نوعها ووقت وقوعها ومصدرها بالضفة الى جميع ألدوات التي يتحدد شخصي وتمك بها الجرائم مثل آثار المتخلفين ومصدر الرسائل الالكترونية والمعلومات المقبولة عبر شل بك انت خلف هذه الدرلسة عن درلسات باحثات التي بحث عن الشرك ال تالموضوعية والجرائية لن اجم قشك ل لدراسي عن الجرائم الالكترونية دوال بحث بتعمق عن وسائل التحقيق فـي هذه الجريمة.

بالضفة الى أن هذه نطاق الدرلسة تختلف عن نطاق درلسات كوال باحث س وفيت حدث عن الشرك ال ت ذات بطبيعة موضوعية وتلك ذات بطبيعة اجرائية للجريمة الالكترونية دخل المارات العربية المتحدة ينما الدرلسة كانت داخل المملكة العربية السعودية وفاك خات الفـبكير فـى القانون المطبق على الجريمة الالكترونية فـى كال الدولتين. بالضفة الى ان منهجية البحث المستخدم فتختلف اتفاقاً عن الن هجية التي ينوى الباحث ستخدام هفـى هذه الدرلسة. بالن هاية سيحاول الباحث الوصول لاى نتائج توصي اتفتي دالوقائع العملى بشك لاكبر من الجدل بالن ظري

تكون المراسلات الدولية متحدة قائمة في الوقت الحالي على نظام معلوماتي كامل في جميع الأمور الحيوية وهذا ما يجعل نطاق الدراسة أكثر تشعباً وشمولاً.

بالإضافة إلى الدراسات السابقة في الباحث "محمد السقي[42] بالبحث عن الحماية الجنائية السرية المعلومات الإلكترونية "دراسة مقارنة"، 2017. وكذلك فقد تناول الباحث ريم سراسي[43] من خلال تناوله موضوع الحماية الجنائية لسرية المعلومات الإلكترونية، 2016م".

تبحث تلك الدراسة مسألة زيادة الضخامة والتفوق والمخزون المراسل المعلومات الإلكترونية وتنوعه وانطوائه عن المواد الخاصة بأسرار الأشخاص وحياتهم الخاصة مثل ذلك المخزون صلب بحثي لما يدار من صلة بمعرفة خصوصية المستخدمين والمجرمين وفي أمثلة هذه الدراسة يقدم مقترح على كل من دول الغرب والدول العربية الأخرى إلى الانضمام "الاتفاقية بودابست" المتعلقة بالجرائم إلى الإلكترونية في عام 2001م وذلك في سبيل عن طريق التعاون الدولي في مكافحة الجرائم القصوى" و وهي تختلف عن دراستي التي تناولت بشكل دقيق وفصل جميع جوانب الجريمة الإلكترونية, سيما أن الدراسة السابقة تناولت الشكليات التي تتطلب الجرائم إلى الإلكترونية في التشريعات الوطنية والدولية.

بينما ركزت الدراسة الثانية على جرائم الجزائرية بشأن المحاولة الدراسة تقديم إطار الفهم لمجرم الجريمة التي تمس سرية المعلومات الإلكترونية من خلال استعراض مفهوم الجريمة

[42] محمد كمال السقي, الحماية الجنائية لسرية المعلومات الإلكترونية "دراسة مقارنة .1st ed ,"المنصورة ، مصر: دار الفكر والقانون, 2017.

[43] ريم سراسي, "الحماية الجنائية لسرية المعلومات الإلكترونية ,.M.A "جامعة أم البواقي, 2016.

المعلومات والخصائص التي يتميز بها الضفة إلى تحديد أهم صفات فئات المجرم المعلوماتي التي يتميز على المجرم التقليدي بالضفة إلى تحديد مفهوم المعلومات والخصائص التي يتميز بها وأنواعها المختلفة كونها المحل الذي ينصب عليه الاعتداء، وفق أقل قاعدة السرية كونها تعد أحد الأهداف الأساسية لأمن المعلومات.

لذلك تحث الباحث في ذات الدراسة عن القصور والسرية بين القانون الجنائي التقليدي والتشريعات الحالية اجرائي قبال الضفة إلى إبراز صور الجريمة التي تمس سرية قانون الجنائي التقليدي و مما الدخول والبقاء غير المصرح به مما و الاعتراض غير القانوني وإيضاح الوضع القانوني في الجرائم المرتكبة أوات خالتبادل من أجل الحد من ارتكاب الجريمة المعلوماتية، كون هذه الجرائم العابرة للحدود لذلك فهي تحت اجتماع الأولى المكافحة هذه الجرائم.

وتوصل الباحث إلى نتيجة مفادها أن الدولة الإمارات العربية المتحدة كانت من وأائل الدول التي تصدت للجرائم المعلوماتية أو المعلوماتية, وذلك من خلال إصدار القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات, كما تم إنشاء دائرة قضائية متخصصة للنظر في الجرائم المعلوماتية والتي تختلف الدراسات السابقة عن الدراسة الحالية حيث أن هذه الدراسة السابقة تناولت في مجمل الأمر طرق الحماية لتقنية المعلومات من الجرائم المعلوماتية قبال الضفة إلى طرق مكافحة الجريمة المتعلقة بتقنيات الكسرية المعلومات سواء كانت تتعلق بفلراد او مؤسسات يتين سواء كون جل تركيز هذه الدراسة على العقوبات التي تواجه تطبيق القانون المختص على الجريمة المعلوماتية من الناحية ذات طبيعة موضوعية وذات طبيعة اجرائية بموجب قبال جرائم المعلوماتية. كما ان الدراسات السابقة لكن تقتصر على كيفية حماية المعلومات والحفاظ على سريتها ودور الشرع في هذه الناحية

بين ما لم يتطرق الباحثون الى المشاكل التي تقف عائقاً في وجه الدولة ومؤسسات القانون في تطبيق هذا القانون.

على ذلك وجد الباحث دراسة قام بها عبد الله دغش العجمي[44] من اول الباحثين هذه الدراسة "موضوع الشكليات ذات الطابع العملي في قانون الإجراءات الجزائية الكويتي دراسة مقارنة (2014م)". نستطيع القول أن هذه الدراسة هي أقرب شيء وجد للباحث الى موضوع هذه الدراسة لكونها ركزت ايضا على الجانب العملي للإجراءات الجزائية الكويتي. كان هدف الدراسة تعريف القصور والمشاكل العملية أثناء الإجراءات الجزائية والقصور بالمشاكل العملية والموضوعية التي تعيق هذه الإجراءات وايجاد حلول لها والتعرف على النصوص لها. الا ان نطاق الدراسة كان دولة الكويت مقارنة بالمملكة الأردنية الهاشمية، حيث ذكر الباحث في دراسته النصوص التي يتكلم بها الجريمة الالكترونية وذلك بموجب قانون الإجراءات نظمة المعلومات الأردني رقم 30 سنة 2010.

تماثل تشارك الباحث هذه الدراسة قام بدراسة الماهية العملية والمسائل الإجرائية والتي تشكل قواعد عائقة في التشريعات الجزائية في دولة الكويت هو مواجهة المشاكل الناتجة عن الجرائم الالكترونية في ظل الفراغ التشريعي بخصوص النظام القانوني لهذا النوع من الإجراءات في الكويت. خرج الباحث بنتائج دراسته بعدة نتائج كان أهمها: سيما أن هذه القواعد فوق التشريعية الكويتية لا تستوعب قواعد كافية على مواجهة الجريمة الالكترونية قبل الضرفة الى ما تنتجه هذه القواعد من شكليات، وحاول الباحث الخروج بتوصيات من خلال دعوة المشرع في دولة الكويت سد الفراغ بنصوص خاصة تبين أن

[44] عبد الله دغش العجمي، "المشكلات العملية لقانون الإجراءات الجزائية الكويتية دراسة مقارنة M.A., "جامعة الشرق الأوسط, 2014.

مكافحة الجريمة المتعلقة بالكترونية واستحداث فصل خاص يعاقب هذه الجرائم داخل قانون العقوبات بالإضافة وجاء الباحث دعوة المشرع في دولة الإمارات لتوحيد مواجهة تصنيف العقوبات الجريمة المتعلقة بالكترونية سواء كانت الموضوعية أم الجنائية.

بعد كل ما قدمناه يجدر بنا القول ان هذه الدراسة تم تقديم شرحاً كافياً ووافياً عن الشرك المتعلقة بالجرائم المتعلقة بالكترونية والتي بسبب ذلك عدم وجود تشريع خاص بالجرائم المتعلقة بالكترونية في دولة الإمارات في ذلك الوقت 2014 الى تلك ان تولي الباحث على قلة الاحاطة قانون تنظيم هذا النوع من الجرائم ولا يستحيل النصوص موجودة لمحاولة تقديم زهاء القانون وضع بها والخروج بتصورات ذات قيمة أعلى حين اي وجد قانون خاص بالجرائم المتعلقة بالكترونية في دولة الامارات العربية المتحدة وبالتالي سيكون تركيز الباحث على نصوص القانون من خلال تحليلها ومحاولة تطبيقها على الوقائع العملية للوصول الى حل للمشاكل التي تتعلق بالجريمة الالكترونية ومحاولة تفسير هذه النصوص والخروج بتوصيات وتلافي ثغرات المشرع الاماراتي.

بالإضافة الى الدراسة اعلاه من قبل الباحث عبد الله محمد الحضرمي[45]: جريمة الدخول غير وجه حق إلى المواقع الالكترونية لنظم المعلومات العام قبل القانون القطري "دراسة تحليلية مقارنة"، 2020. كذلك تحدث الباحث محمد سليمان الخوالدة[46]: دراسة بعنوان جريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات في التشريع الأردني– دراسة مقارنة، 2012".

---

[45] عبد الله محمد الحضرمي, ""جريمة الدخول بغير وجه حق إلى المواقع الالكترونية ونظم المعلومات العام في القانون القطري "دراسة تحليلية مقارنة"،" رسالة ماجستير, جامعة قطر, 2020.

[46] سليمان الخوالدة, "جريمة الدخول غير المشروع إلى موقع الكتروني أو نظام معلومات في التشريع الأردني :دراسة مقارنة" رسالة ماجستير, الجامعة الأردنية, 2012.

تناول الباحثان في هذه الدراسة أحد شكال الجريمة الإلكترونية وهي "جريمة الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلومات يدوي مباشرة، أو عن طريق شبكة المعلومات الدولية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

تحدث الباحث في الدراسة الأولى عن جريمة الاختراق والدخول دون وجه حق الموقع الإلكتروني والنظم المعلوماتية العامة فوق الأمر هو مع مولب في قوانين دولة قطر والقوانين الأخرى المقارنة، وقد قام المشرع في دولة قطر في قانون مكافحة الجرائم الإلكترونية القطري الصادر في سنة ٢٠١٤ بتخصيص المادة الثانية منه لجريمة الدخول دون وجه قانوني إذا وقعت على المواقع الإلكترونية أو الأنظمة المعلوماتية التابعة لأحد أجهزة الحكومة أو المؤسسات التي تتبع الدولة.

عالجت الدراسة الثانية طبيعة الجريمة ذات الطبيعة الإلكترونية من النواحي الجنائية القانونية, من خلال الحديث عن دخول الغير المشروع لمواقع الإلكترونية وشبكة المعلومات حيث عرضت قواعد قانونية تكون بمثابة الحماية هذه الجريمة وتعاقب على عناصرها وأركانها, والأساليب المستخدمة في تلك الجريمة, وحدد الإجراءات التي يتم القيام بها والوقت الذي يجب فيه القرار لهم, وذلك بموجب قانون الجرائم والأنظمة المعلوماتية المطبق في دولة الأردن سنة 2010م وقانون التشريعات الأخرى وانتهت هذه الدراسة إلى العديد من النتائج والتوصيات حيث برز الأهم منها : بوجود تنظيم نظم قانونية خاص بقبائل الجرائم الإلكترونية تهدف إلى حماية مصالح المجتمع ومعاقبة مرتكبيها.

رائي الباحث أن يختار تعاين الدراسين من ضمن الدراسات السابقة لكون مجتمعات عن احد صور الجرائم الالكتروني ة ولكثر ها شيوعاً وانتشار في الوطن العربي خاصة في العالم لفلسطين عتبر هذه الجريمة هي احد اوضح صور الجرائم الالكتروني في العصر الحديث كونها تحيد عن الحديث عبر هذه الدراسة عن نماذج وصور الجرائم الالكتروني ة ومحاولة لمرق اطلن ص القانوني على الشرك التي تص احب الجرائم الالكتروني ة.

تتشابه هذه الدارس في مفرداتها مع دراسة الباحث إلا أنها تختلف عنها الكون مجتمعات عن صورة واحدة او تطبيق عي للجريمة الالكتروني ة في ما دراسة الباحث س وفي عتمد على النواحي المتعلقة بالشكليات الصحابة للجرائم العلومتي ذات بطبيع الكتروني ة من جميع النواحي في ضوء التشريع المارتي.

بالضافة الى الدراسات السابقة أعلاه تحدث الباحث "سيان نصر الثيان[47] عن إثبات الجريمة الالكتروني ة –دراسة تأصيلية تطبيقية- 2012". كذلك تناول الباحث "مصطفى عبد الباقي[48] موضوع "التفتيش في الجريمة الالكتروني ة وإثباتها في فلسطين: دراسة مقارنة"، 2018". علاوة على ذلك تحدث الباحث زبيحة نور الهدى[49] عن "الإثبات الجنائي في الجرائم الالكتروني ة، 2016".

---

[47] سيان ناصر الثيان, "الإثبات الجريمة الالكتروني ة –دراسة تأصيلية تطبيقية" أطروحة ماجستير, جامعة نايف العربية للعلوم الأمنية, 2012.

[48] مصطفى عبد الباقي. "التفتيش في الجريمة الالكتروني ة وإثباتها في فلسطين : دراسة مقارنة". دراسات - علوم الشريعة والقانون, 2018, 284. doi:10.35516/0272-045-986-017.

[49] زبيحة نور الهدى, "الإثبات الجنائي في الجرائم الالكتروني ة" أطروحة ماجستير, جامعة أم البواقي, 2016.

تناول الباحث في هذه الدراسة شرح كل من إثبات الجريمة الإلكترونية في النظام السعودي والشريعة الإسلامية بين الباحث في هذه الدراسة من الهدف الرئيسي حل يلي. خلص الباحث إلى العديد من النتائج أهمها طبيعة الجريمة الإلكترونية التي تستخدم بصفة عامة للأغراض الإلكترونية الرقمية ودعمه من قبل المختصين حيث تتصف الجريمة العلمية بتصنيفها، لكونه طرق التحقيق في إثبات الجريمة الإلكترونية تتطلب إجراءات خاصة لإثبات وقوعها مع الأخذ بعين الاعتبار مراحل وقوعها، وبيئة الجريمة الإلكترونية(، وطرق الإبلاغ عنها [50].

كل ذلك يكون من خلال التحري وجمع الأدلة هو الأساس لكشف الجريمة الإلكترونية ولكن بهدف الوصول إلى الجاني بالرغم من الصعوبات الفنية والتقنية. علاوة على ذلك الخبرة الفنية أهمية كبرى في إثبات الجريمة الإلكترونية يرى الباحث في هذه الدراسة أن عدم وجود دليل مادي فقدان الأثر كما للجرائم التقليدية من أهم الصعوبات في إثبات الجريمة الإلكترونية.

كما تتوصيات الدراسة تركز على تشريعات سياسية أهمها تطوير طرق التحقيق الجنائي بصورة تناسب مع خصوصية الجريمة الإلكترونية بتحديد الجهة الإلكترونية الموجودة في كان معاونة الجريمة الإلكترونية. العمل على تكثيف الهتمام بتطوير الخبراء ودورهم ، كذلك العمل على تنسيق السياسات بين مختلف الجهات الأمنية والقضائية والجهات المختصة في التحقيق لمواكبة التقدم السريع لتكنولوجيا هذا العصر.

---

[50] موسى مسعود ارحومة. "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" في المؤتمر المغاربي الأول. طرابلس: أكاديمية الدراسات العليا, 2009، ص3 -5 .

لذلك الوضع يعتبر مجال دراسة الدراسة حيث تحدد المباحث عن التحقيق في الجرائم الإلكترونية وطرق ضبط الأدلة الرقمية وجمعها بالإضافة إلى بطء عملية الأدلة الرقمية والفنية التي تعامل معها من قبل جهات التحقيق بحيث تعتبر ذات أهمية قانونية وعملية.

ويرى الباحث أن التحقيق في الجرائم الإلكترونية يجب أن يكون من قبل نيابة خاصة تختص في هذا الشأن من الجرائم وفق القواعد والإجراءات محددة وخاصة ويسري هذا العمل للضبطية القضائية والتي يجب أن تكون كذلك تختص في هذا النوع من الجرائم وفق القواعد للتحقيق والمتطلبات النيابة.

وبالتالي الباحث في نهاية بحثه أن يكون هناك طرق تؤدي إلى تحقيق في الجرائم الإلكترونية عبر وضع إجراءات جديدة لقسم التحقيق المختص بهذا النوع من الجرائم للعمل على السيطرة الفعالة على الجرائم الإلكترونية، لذلك وضع مبادئ توجيهية النواع وطرق الحصول على الأدلة الإلكترونية الجنائية وصولاً إلى تحقيق ناجح في الجرائم الإلكترونية.

لذلك الوضع على نسبة قليلة دراسة الثغرات التي تناولت في البحث الجريمة العلمية يمكن أن تتسم بطابع خاص كونها تقع في الفضاء الافتراضي ورتكابها من شخص لديه مواصفات خاصة, و من هنا تبرز صعوبة مالية هؤلاء المجرمين ووضع الذي يدعو إلى إثبات جرائمهم.

عرف الباحث مفهوم الجريمة الالكترونية و وسائل الحصول على الدليل الالكتروني لكذلك بين الغرض و السبب الجنائي الالكتروني. و عالجت الباحثة موضوع اجراءات التحقيق و جمع الادلة في الجريمة الالكترونية , و اهم القواعد الجوهرية التي يمكن الاعتماد عليها لاستخلاص الدليل, بالضرورة الى التدابير الخاصة التي يجب مراعاتها اثناء ضبط الدليل في الحاسوب لينتهي الى تعريف الرابطة القضائية التي اطالت تعاون الدولي لمكافحة الجريمة الالكترونية.

في الناحية يرى الباحث اثبات الجريمة الالكترونية ما هو الجزء من مكونات الجريمة له دور مهم في الوصول الى الجاني بسرعة الطرق على يعتبر الاثبات في الجرائم الالكترونية واحد من المشاكل التي الجوهرية عملي في الجريمة الالكترونية. في هذه الدراسة سوف يتطرق الباحث الى الاثبات الالكتروني للجريمة الالكترونية في قسم مخصص كأحد التطبيقات المشكلة الدراسة ال ان الدراسة سوف تكون على القانون الماتي يجب يتسنى طالب الباحث انينا يجي ديوف ادى التكرار في الكار والنتائج.

في الناحية وجد الباحث عدة دراسات متعلق بالجرائم الالكترونية من هذه الدراسات دراسة الباحث عبد اللطيف محمود ربيعة[51]: الجرائم الالكترونية" التجريم والمالحقة والاثبات، 2016". وكذلك دراسة الباحث نبيل محمود ابو الرب[52]: مفهوم الجرائم على وتمالي وتحديات التشريع في فلسطين، 2018".

[51] عبد اللطيف محمود ربيعة،)"الجرائم الالكترونية" التجريم والمالحقة والاثبات(. المؤتمر الأول للجرائم الالكترونية في فلسطين. نابلس: جامعة النجاح الوطنية, 2016.

[52] نبيل محمود ابو الرب، "مفهوم الجرائم المعلوماتية وتحديات التشريع في فلسطين" أطروحة ماجستير, جامعة النجاح الوطنية, 2018.

كما الولايات المتحدة على المجتمع الفلسطيني السياسي على ظل نشأة العديد من المشاكل التي تصل بحت تشكل جرائم خطيرة يقوم بها الشخص المشترك ولو جي بلا حيث تتميز بمرونته وسرعته وسهولة القيام بواسطتها, الى يمأن هاك مظلن اسباق كونها جريمة عابرة للحدود. هذا يعد الوضع في فلسطين كبقي الدول الخرى حيث كثير من افراد أصابهم ضرر بكبير جراء انتشار الجريمة الالكترونية.

كما الولايات المتحدة هدت إلى السماهم في الحث على الثقافة والفهاهيمية الجتماعية والقانونية وتوعية المجتمع اتبش أن الخطر الذي قد يحدق بسبب الجرائم الالكترونية بقي ين فلأفراد المجتمع فلسطين على يه يرى الباحثان أن هيجب الحد من هذه الجرائم عن طريق الحماية القانونية قبولسلطة الفتاع الجتماعي والذي ضمنته القوانين الجنائية كون هك عدم قبل الوسائل الهام في المجتمع عيس بيل المحافظة والفحاظ على يبة الوطن وحمايته.

خلصت كما الولايات المتحدة إلى وجود نصوص وعبات موضوعية وإجرائي في يتحديد مفهوم الكتشاف لإثبات الجرائم العلومتي التي يقع على بالبيانات لدى تشاقتشريعات المنظمة لمهي لكفلة النواحي القانونية في فلسطين, والي زالي جوهر اغورق صرتشريعي في يتحديد الحماية القانونية من النواحي الجنائية الجنائية، المر الذي يوجب مع هالتشدد الي قظة والى السراع من أجل ايجاد ووضع النظم الجنائية القانونية المشروعة والتي يتفق مع القانون لمكفلحة هذه الجريمة الخطيرة في ظل العتماد على القوانين العاي القديمة (التي التي الحد ألذى حيث طلبات مكفلحتها والحد منها.

Universiti Utara Malaysia

أخيراً تحدث الدكتور "أحمد أسامة حسني[53] في بحث له عن الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية" ،2017". وكذلك الدراسة بالبحث بإسراء جبريل رشمي[54] حيث عالجت موضوع "الجرائم الإلكترونية)الأهداف، الأسباب، طرق الجريمة ومعالجتها"، 2016. أما الدراسة للباحث ذياب البداينة[55] فقد بحث هذا الموضوع عن المفهوم والأسباب للجريمة الحديث في ظل التحولات والتغيرات الداخلية والدولية 2014.

تحدد الباحث في الدراسة الأولى عن ماهيه وخصائص الجريمة الإلكترونية، ومدى تشابكها مع الأركان العامة للجريمة التقليدية والخصوصية، التي تميزه والسمات العامة لمجرمي الجرائم الإلكترونية وأصنافهم إضافةً إلى التحديات والإجراءات والعقبات التي تواجه جهات الإعالة بالضفة إلى طرق الإثبات الجنائي وما يلزم من حلول لتصدي لمواجهة الصعوبات في هذا النوع من الجرائم.

حاول الباحث من خلال هذه الدراسة تبيان الضرر الذي يترتب على الجريمة الإلكترونية والصعوبات التي تواجه المتخصصين في هذا النوع من الجرائم لمواجهة هذا النوع من الجرائم. كذلك أوضحت هذه الدراسة أن المشكلة الأساسية تتمثل في استغلال المجرمين لتبلف في الصعوبة التي تواجه أجهزة الإعالة في القبض عليهم، بسبب ما تسببه تلك الجرائم من عقبات في

---

[53] أحمد أسامة حسني: "الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية". مجلة جامعة الأزهر, سلسلة العلوم الإنسانية 19)2017(: 1-42. http://www.alazhar.edu.ps/journal/detailsr.asp?seqq1=3363.

[54] إسراء جبريل رشمي, "الجرائم الإلكترونية " الأهداف - الأسباب - طرق الجريمة ومعالجتها" - المركز الديمقراطي العربي", المركز الديمقراطي العربي, https://democraticac.de/?p=35426. Last modified 2016.

[55] ذياب البداينة، "الجرائم الإلكترونية: المفهوم والأسباب", in الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية عمان، الأردن: كلية العلوم الاستراتيجية جامعة نايف العربية للعلوم الأمنية, 2014.

التشريعية الجنائية الموضوعية والإجرائية، الأمر الذي تتطلب أن يسارع المشرع في الدول إلى تشريع قانون خاص بمكافحة الجرائم الإلكترونية.

ألمانيا سبقت دول العالم في تشريع قد ركزت على الأمن السيبراني بل الحد من انتشار الجريمة الإلكترونية وطرق التصدي لها والعمل على مكافحتها من خلال إيجاد الأساليب والأدوات التي تختص في مكافحة الجرائم الإلكترونية بالإضافة إلى خلق وإنشاء فرق عمل لدراسة وضع سياسات استراتيجية مناسبة لمواجهة هذا النوع من الجرائم خاصة في الدول العربية، لذلك العمل على سن قانون في جامعة الدول العربية يكون شاملاً لجميع الجرائم الإلكترونية والتصدي لها. بالإضافة إلى ما سبق يمكن القول إن تجريم الاعتداءات الشديدة الرادعة على كل فعل يصوغ لها الأمر من ارتكاب الجريمة الإلكترونية من خلال ضرورة الإسراع في سن قانون الحكومة الإلكترونية بسبب خطورة الجرائم الإلكترونية. والاعتماد على طرق وأساليب بحثية وتطورات تعمل على كشف وإثبات ارتكاب الجرائم الإلكترونية التعرف على هوية المرتكب، بالإضافة إلى نشر الوعي بين أفراد المجتمع في أي خصائص الجرائم الإلكترونية والخطر والضرر المترتب عليها على المدى القريب والبعيد.[56]

أخيراً نستنتج أن الباحث في القانون الجزائي قد وضع الجريمة ذات طابع إلكتروني وأسباب حيث صرفت هذه الأسباب على ثلاثة مستويات من النظام الشخصي والنظام الموسيطي والنظام الكلي فقد

[56] لمزيد من التفاصيل انظر: إيمان بشير محمد&يوسف عثمان يوسف."تنظيم برامج العلاقات العامة لتوعية مخاطر الجرائم الإلكترونية دراسة تحليلية وصفية على الإدارات المسؤولة عن الجرائم الإلكترونية)وزارة العدل، وزارة الداخلية ووزارة الاتصالات وتكنولوجيا المعلومات في الفترة بين 2016-2017م". مجلة العلوم الإنسانية المجلد 19 العدد 2، 156-175.

انطلقت من أن الجرائم الإلكترونية هي أفعال إجرامية ترتكب عن طريق الحواسيب المتصلة بالإنترنت والشبكات. وتشمل الجرائم الإلكترونية كذلك التجسس والسرقة الهوية، والمال والقرصنة والتحرش، إلى رهاب الإلكتروني، ،وبيوت الدافعات، وفلوس روسات، وشم كلمات السر، والإرهاب الإلكتروني"، السرقة الإلكترونية تمات السطو على معلومات وبطاقات الإلكتروني"[57].

ويرى الباحث أن سهولة انتشار الجرائم الإلكترونية تتأتى من خلال سهولة الوصول للمجرمين وانخفاض تكلفة الجريمة ذاتها، وضعف الرقابة والسرعة بالمقارنة التي توظيف الاتصالات والشبكات العالمية في ارتكابها، قلة الخطورة المحتملة التي قد يتعرض لها الجناة، وسرعة الكسب غير المشروع، قلة الوعي بين أفراد المجتمع والتي أتاحت الفرص لارتكابها، العولمة على ضعف الرقابة العامة. كما أسهمت عوامل التحضر السريع، والرغبة في الثراء السريع، وضعف القانون التشريعات وأدوات الحماية، وغياب الرقابة الفنية في انتشار الجرائم الإلكترونية[58].

Universiti Utara Malaysia

1.9 المخطط العريض للدراسة/ Outline of Chapters

ستقسم هذه الدراسة إلى خمسة مباحث على النحو التالي:

الفصل الأول: مقدمة البحث

---

[57] انظر: زيدات, جاسي يوسف. "حدود القانون والعقوبات في السيطرة على السرقة الإلكترونية "اختراق المعلومات والبيانات الإلكتروني"". المؤتمر الدولي المفتوح للجرائم الإلكتروني في فلسطين. بين الواقع. جامعة النجاح الوطنية, 2016.

[58] لمزيد من التفصيل انظر بيزي بن بلراي ماصيق. "العوامل المحددة للجرائم الإلكترونية" أطروحة دكتوراه، جامعة نايف للعلوم الأمنية, 2017.

سيناقش الفصل التمهيدي للدراسة بيان المشكلة ، وأهمية الدراسة ، وأهداف البحث ، وأسئلة البحث المترابطة ، ومنهجية البحث ، والقيود التي تواجه الدراسة ومراجعة الأدبيات.

الفصل الثاني: بيان وتحديد لمشكلات الجريمة والأدلة الناشئة عن الجرائم الالكترونية.

في هذا الفصل سيتطرق الباحث إلى التعريف بمفهوم الجريمة الالكترونية وأنواعها وخصائصها والطبيعة القانونية لتلك الجرائم وأهم خصائصها التي ترتكز عليها وما هي أركان الجريمة الالكترونية ومن هم أطرافها كون أن الفقه قد عرف الجريمة الالكترونية فمنهم من ضيق في مفهومه ومنهم من وسع في مفهومها من خلال هذا المطلب سنتحدث عن تعريف شامل لمفهوم الجريمة الالكتروني وبيان الفرق بين الجرائم الالكترونية والجرائم التقليدية التي تعارف عليها الواقع, وما هي الآليات التي تنفذ به الجريمة الالكترونية.

سيركز الباحث في هذا الفصل على دراسة على الشبكية ذات طبيعة موضوعية التي تنتج عن الجريمة الالكترونية ومن ضمنها الجرائم المتعلقة بالتعدي والاعتداء على الأمور الحياتية الخاصة بالأشخاص ولكذلك الشرك المالي المتعلق بجريمة الاعتداء على الأموال والشرك المتعلق بجريمة التزوير وأيضا الشرك المتعلق بجريمة سرقة المال العلومتي.

كما سيتحدث الباحث في هذا الفصل عن الشبكيات ذات طبيعة اجرائية التي تنتج عن الجرائم الالكترونية من حيث الشبكيات المترابطة بضوابط الجرائم ذات طبيعة الكتروني وانشبكاتها وعن الشبكيات التي تتطلب اجراءات البحث والتحري والتوثيق, وأيضا الشبكيات المترابطة بحيث "القانون المختص والواجب التطبيق في تلك الجرائم".

الفصل الثالث: تحليل النصوص والمواد المرسوم رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 لمكافحة جرائم تقنية المعلومات.

سيتم الطلب الباحث الضوء في دراسته على قانون الجرائم الإلكترونية في إمارة دبي رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016"، من خلال تحليل جميع المواد التي تناول بشكل مباشر تقنية القرصنة والجزاء المقرر له في دولة الإمارات. لمعرفة مدى نجاح أو فشل المشرع الإماراتي في تنظيم ومعالجة الجريمة ذات الطبيعة الإلكترونية.

الفصل الرابع: الحلول العملية والتشريعية لمكافحة الجرائم الإلكترونية والتغلب على المشكلات الناتجة عن هذا النوع من الجرائم.

سوف نناقش الدراسة في هذا الفصل الحلول والأساليب التي يجب اتباعها سبيل مكافحة الجريمة الإلكترونية والتغلب عليها، وذلك من خلال الاطلاع على التشريعات المقارنة في هذا الشأن خاصة الحماية الجنائية من الجرائم الإلكترونية، كما استنطرق الدراسة إلى الدور القانوني والدولي في مواجهة ومكافحة الجريمة الإلكترونية، كذلك دراسة الدور الوطني في سبيل التصدي للجريمة الإلكترونية.

كما يبين الباحث أهم الحلول العملية في شأن مواجهة الجريمة فيتم التغلب على بعض الجزاءات المطلوبة لمكافحة الجرائم الإلكترونية ولكن لا يتم التغلب على الأساليب المستخدمة في تنفيذ الجرائم. كما أنه في هذا الفصل التطرق إلى أهم النتائج الدراسة، كما سنتعرض التوصيات التي من شأنها تحقيق أهداف البحث وتطوير آليات الحد من انتشار ومكافحة الجريمة الإلكترونية.

الفصل الخامس: النتائج والتوصيات للدراسة .

يتناول هذا الفصل أهم النتائج التي توصل إليها الباحث، كما ستتعرض الدراسة التوصيات التي من شأنها تحقيق أهداف البحث في إطار النظام القانوني الإماراتي المتعلقة بالشركات الموضوعية والجزائية المتعلقة بالجرائم المالكترونية.

CHAPTER TWO / الفصل الثاني

بيان تحديد لمشكلات الجزئية والعامة التي ستنشق عن الجرائم المالكترونية

Universiti Utara Malaysia

في هذا الفصل يتطرق الباحث إلى التعريف بمفهوم الجريمة المالكترونية وأنواعها وخصائصها والطبيعة القانونية لتلك الجرائم وأهم خصائصها التي ترتكز عليها وما هي أركان الجريمة المالكترونية ومن هم أطرافها كون أن الفقه قد عرف الجريمة المالكترونية من هم من ضيق في مفهومه ومن هم من وسع في مفهومه من خلال هذا الفصل سنتحدث عن تعريف شامل لمفهوم الجريمة المالكترونية وبيان الفرق بين الجرائم المالكترونية والجرائم التقليدية التي تقع على طبيعة الواقع, وما هي الآليات التي تتبعها الجريمة المالكترونية.

وأيضاً سيركز الباحث في هذا على الشكلية ذات الطبيعة الموضوعية التي تنتج عن الجريمة المالكترونية ومن ضمن هذه الجرائم المتعلقة بالتعدي والاعتداء على الأموال الحياتية الخاصة

بالأشخاص ولكذلك الشركات التي تعلق قبح جريمة الاعتداء على الأموال والشركات التي تعلق قبح جريمة التزوير وأيضا الشركات التي تعلق قبح جريمة سرقة الأموال العمومية.

كما سيتحدث الباحث في هذه الفصل عن الشكليات ذات الطبيعة الإجرائية الناتجة عن الجرائم الإلكترونية من حيث الشكليات المتعلقة بضوابط الجرائم ذات الطبيعة الإلكتروني وإثباتها وعن الشكليات التي تتعلق بإجراءات البحث والتحري الموضوعي, وأيضا الشكليات المتعلقة بحجية "القانون المختص والواجب التطبيق في تلك الجرائم".

في هذا الفصل سوف يتم الإجابة على سؤال البحث الثاني متمثل بمعرفة الشركات ذات الطبيعة موضوعية والإجرائية التي تشكل أسباب ظهور الجرائم الإلكترونية في ظل الوضع الحالي؟ وذلك بهدف تحقيق هدف الدراسة الثاني وهو بيان وتحديد الشركات الجوانب العلمية التي تنبثق عن الجرائم الإلكترونية

Universiti Utara Malaysia

2.1 ماهية الجريمة الإلكترونية

تعد الجرائم الإلكترونية من ضمن الجرائم الأكثر خطرًا في العالم أجمع فهي من ضمن الجرائم المعقدة يعلو من القوانين الخاصة, والتي يفرض الشرع له نظام قانوني خاص جرم من خلاله تلك الجريمة ويبين جميع الطرق التي يمكن من خلال متحقيق الجاني لغاته الجرامية, ولقد تطورت الجرائم الإلكترونية تطورا مأهولا في السنوات الأخيرة, وذلك لما شهده العالم أجمع من تطور بكبير في المجال التكنولوجيا, والذي صاحب تخلل وجود في جميع أنحاء العالم, وإن هذا التطور في مجال التكنولوجيا أدى إلى زيادة تطور البرامج وأجهزة الحاسوب والهواتف وبالأخص شبكات الإنترنت, ذلك صاحب هذا العصر هو عصر التكنولوجيا, وإن الجرائم الإلكترونية تتكتب

بواسطة أجهزة الحواسيب بمختلف أنواعها من غير أو بغير, وذلك بواسطة شبكات الإنترنت, في الحين يشمل عبارة عن ذلك سنبين ما عبارة عن الجريمة الإلكترونية, وبيان أنواعها الجريمة, وتحديد مميزاتها من خصائص, وذلك عبر الجدول:

2.1.1 القصور بالجريمة الإلكترونية

سنتعرض عبر هذا المحور تحديد القصور بالجريمة الإلكترونية من ثم بيان أنواعها, وبيان ما تتمتع بها من خصائص, وذلك عبر التالي.

2.1.2 تعريف الجريمة الإلكترونية

كثرة المسميات والمصطلحات حول فعل الإرتكاب بواسطة أجهزة الحاسوب وشبكات الإنترنت, وتوصل الفقه في نهاية الأمر إلى توحيد تلك المسميات بحيث تطلق على هذا الجرائم الإلكترونية, والذي يشكل ضرراً بالغاً سواء على المستوى الوطني أو الدولي, والتي نجد في البيانات كان من صعب وضع تعريف مخصص لها نظراً لعدم وجود تنظيم قانوني معين, والخلاف سببها, ولكن في ظل الوضع السائد ومع وجود تنظيم قانوني لها استطيع وضع تعريف لها, وعليه فإن الفقه الذي نفي تعريف الجريمة الإلكترونية اختلف وفي وضع تعريف موحداً وذلك بحسب الرؤية التي كان ينظر إليه الفقه الذي نفي تعريفها حيث جانب من الفقه كان يقصر تعريفها على الجانب الفني المتعلق بالفعل الإرتكاب[59], وجانب أخر كان يعرفها بنظر إلى الجانب القانوني أي النظر إلى معين لذلك الفعل الإرتكاب, وأخر كان يرى تعريفها حسب وسيلة ارتكابها أو موضوعها أو وفقاً لمعرفة شخصية الفاعل ومات وبالرغم من صعوبة وضع تعريف شامل لهذه الجريمة وحصر نطاق

[59] كامل فريد السالك: محاضرة ألقيت في مؤتمر الجريمة السورية المعلوماتية في حلب عام 2000-ندوة التنمية ومجتمع المعلوماتية- حلب 21-23 تشرين أول 2000.

محدد، إلا أنه كتب بتقنية المتقدمة في الآلي المتحدة عرفها من خلال تعريف الحاسب الآلي على أنها الجريمة التي تعتمد على بيانات الحاسب الآلي البرامج على وتمثل قبدور رئيسي[60].

كما عرفها كتب بتقنية المتقدمة في رأي أن الجريمة الالكتروني قبل هاشاط جنائي يشمل اعتداءً على برامج بويانات الحاسب إلى الالكتروني ، وعرفت بأنها كالاستخدام في صور فعل أو امتناع غير شرول على تقنية المعلومات، بهدف الاعتداء على أي مصلحة شروعة ،سواء أكانت مادية أو معنوية[61].

وعليه فأنه من جانبنا وفق أقانون لمكافحة جرائم تقنية المعلومات الإماراتي رقم لسنة 2012 وتعديلاته قانون اتحادي رقم 2لسنة 2016, وفي تعريف الجريمة الالكتروني قبأنه هي الجريمة التي تتطلب استخدام جهاز الحاسوب عن طريق الشبكات الانترنت ويكون الهدف منها اختراق الشبكات أو تخريبها أو التجريف أو التزوير أو السرقة والاختلاس أو سرقة حقوق الملكية الفكرية, وتشكل خروجاً عن سلوك الشخص العادي ويعرف بأنه الانحراف الارتكاب جريمة بأركانها المادية والمعنوية بأي أكان الباعث الارتكابها وتعد من الجرائم العابرة للحدود بما أن هذا التعريف جاء مفتقر مطلب يعة الجريمة الالكتروني ومحتوى لجميع عناصر الجريمة شروطها وأركانها, وأيضاً مواكباً مع التطورات والمميزات التي يتمتع بها الجاني في تلك الجريمة, والتي ميزتها عن غيرها من الجرائم "وهي الذكاء والدهاء"[62].

---

[60] بلراهيم رمضان بلراهيم عطيا: الجريمة الالكتروني في الشريعة الإسلامية والأنظمة الدولية, ج2 العدد30, طنطا سنة 2015م, ص370.

[61] كامل مطر: الجريمة الالكتروني, ب ش, ب س, ص7.

[62] شاهين خضر -رضوان سعادة. الجريمة الالكتروني وإجراءات مواجهتها. Diss. جامعة المسيلة, 2021.

2.2 أنواع الجريمة الإلكترونية

فهي تصنف على قبل الجرائم الإلكترونية تصنيفات كثيرة ومتنوعة الحصر لها, وذلك على غرار الجرائم التقليدية الحصورة ضمن نصوص قانونية خاصة, وقد ذهب الفقه والقانون في تصنيف الجريمة الإلكترونية, الأمر الذي ترتب عليه صعوبة حصرها على وجه الدقة وذلك تعدد المعايير في تحديد أنواعها حيث يتم تصنيفها على أساس معيار الأداة المستعملة في ارتكاب الجرم, معنى الحاسوب وإلى بعض الآخر صنفها على معيار أن نماط السلوك المختلفة التي تمثل الجريمة المعلوماتية ومدى اتفاقها أو اختلافها مع القواعد التي تحكم القانون الجنائي وقانون مكافحة الجرائم التقنية المقارنة, وإلى بعض الآخر صنفها عن طريق الاعتماد على محل الجريمة والتي يكون منطها الحاسوب بسبب الاعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة[63].

على أن قانون مكافحة الجرائم التقنية قانون اتحادي رقم لسنة 2012 يتعلق بقانون الاتحادي رقم 2 لسنة 2016 في شأن أنواع الجرائم الإلكترونية على أساس الجرائم الواقعة بواسطة النظام ذاته, والجرائم الواقعة على النظام ذاته وهذه الأنواع من وجهة نظر الفقه بالاعتماد على الرأي الأخير الذي صنفها على أساس محل الجريمة, أما من وجهة نظر القانون فلقد قسم عدة أنواع كون قد نظم القانون المقارن في نظام قانون خاص فرض حماية قانونية لها ووضع جزاء على من يخالف ذلك وسنبين أنواع الجريمة الإلكترونية التي تستخدم بواسطة الحاسوب سواء كان محلها المكونات الصلبة للحاسوب أو البرامج والمعلومات أو شبكات الإنترنت, على مبنى من نظرة الفقه

---

[63] عبد الحكيم موالي إبراهيم: الجرائم الإلكترونية- مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة- الجزائر, المجلد 23, دار المنظومة, سنة 2015م, ص214.

والقانون بشأن أنواع الجرائم فوقاً لمعيار محل الجريمة والأداة المستخدمة, وذلك بيان الجرائم الإلكترونية الواقعة بواسطة النظام ذاته, من شبهة ان الجرائم الإلكترونية الواقعة على النظام ذاته, وذلك عبر الفقرة التالية:

2.2.1 الجرائم الإلكترونية الواقعة على النظام نفسه

تعد الجرائم الإلكترونية سواء كانت حواسيب صغيرة أو كبيرة, الهيوسيلة التي من خلالها يتم تنفيذ الجريمة, ومن هذه الجرائم الواقعة على الأشخاص كتهديد والمضايقة والمراقبة, وذلك عن طريق إرسال رسائل بالبريد الإلكتروني أو التهديد أو عن طريق وسائل التواصل الاجتماعي الأخرى الحديثة التي يسهل استخدامها من الوسائل, هذا بالإضافة لجرائم القذف والسب والتشويه السمعة بهدف الإساءة للغير عن طريق الكتابة والطباعة والنشر وإرسال عن طريق مواقع التواصل الاجتماعي وتعد من أخطر الجرائم الإلكترونية نصوص اعة المحتوى الإباحي بهدف نشره, بالإضافة إلى جرائم انتحال الشخصية بهدف تغرير الناس تدراج, وقد يكون الانتحال على شخصية موقع ما أو على فرد[64], وأيضاً فإن الجرائم الواقعة على الأموال كجريمة إساءة استخدام البطاقات الائتمانية كسحب البطاقات والسحب على المكشوف بالرغم من عدم الأحقية الصريحة دون عرضها للاختراق والسرقة, أو الأمر استخدام البطاقة بعد إلغائها أو انتهاء مدة صلاحيته, أو الأمر استخدامها من قبل الغير بهدف الإساءة والسرقة[65], والأمر الجنسي جل الشاهد صناعة المحتوى الجنسية والمخدرات, واختراق أنظمة الحماية لدى البنوك والمصارف بهدف سرقتها, والقيام بسرقة الإنترنت في موقع الإنترنت .

---

[64] نمطي ريمة: خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة, أعمال المؤتمر الدولي الرابع عشر - الجرائم الإلكترونية , طرابلس 24-25 مارس سنة 2027م, ص9.

[65] يوسف جميل يوسف الفقي: المرجع السابق. ص41.

إلى جانب ذلك فإن الجرائم الواقعة على أمن الدولة قد تهدد سيادتها واستقلالها وتمس بسلامة الأراضي الوطنية, والتي يتعدد من أخطر الجرائم الماسة بالممتلكات الرقمية والتي يتسبب إلى رهاب الممتلكات الرقمية وتستهدف العلوم والمعلومات التي تمس سيادة الدولة, كجرائم التجسس على الممتلكات الرقمية على الدول وذلك بغية الاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتنازعة, هذا وتستخدم موقع الإنترنت في التأثير على الرأي العام الدولي والتأثير على الاقتصاد الدولي والتجارة الدولية مما يسبب في خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وتأثيرها على النظام العام فيها[66].

2.2.2 الجرائم الواقعة على النظام العام

الجرائم الواقعة على النظام العام تعتبر من الجرائم المستقبلية المكونات المادية والمعلومات المدرجة فيها وحتويات الهاتف المنقولة, بغض النظر إلى الجرائم الماسة بالممتلكات الرقمية الواقعة على المكونات المادية للنظام من جهة أخرى تشمل قبل الجرائم الجنائية الجرائم الرقمية كسرقة الكمبيوتر الحاسوب السطوانات وغيرها من الأمور المادية أو حرق الحاسوب أو حرق الحاسوب تشتق من عن طريق فعل مادي يتمثل في إخراج الحاسوب من حيز الاستعمال فهو يطلق على قبل الجريمة الواقعة على المكونات المادية وهي التي تقصد بالأبراج النظام الحاسوب يجب أن يكون هناك معرفة فنية العي في مجال البرمجة, ومن الممكن أن تقع هذه الجريمة على البرامج الشغيلة والتطبيقية التي تعي البرنامج الذي يعد عمل مادي حيث يمكن الوقوف على شكل الحاسوب, كما يمكن الاستحواذ عليه عن طريق تشغيل الحاسوب ويكون ذلك بدفاتر العبابة برنامج لتوغير نظام التشغيل والتالعب والتحت السرفي الحساب[67].

---

[66] نمطي رحيمة: المرجع السابق, ص10.

[67] عبد الحكيم موالي بيراهيم: المرجع السابق, ص217.

2.3 خصائص الجريمة الإلكترونية

سبق أن عرضنا للتشريعات في الجريمة الإلكترونية نتبين من خلالها أن هذه الجريمة هي من الجرائم التي ترتكب بسرعة فائقة وفي الغالب, فيمكن أن نخصر أهم خصائص هذه الجريمة من خلال ما يلي:

2.3.1 جريمة رقمية "ترتكب بواسطة الحواسيب وشبكات الإنترنت"

نظراً لطبيعة الرقمية للجرائم الإلكترونية, نجد أنها تتطلب وجود حاسوب بحيث لا يتصور ارتكاب الجريمة الإلكترونية دون وجود أجهزة حواسيب وأنظمة غير آلية يمكن أن أداءة المساعدة في ارتكاب الجرائم الإلكترونية, وذلك عن طريق توصيل شبكة الإنترنت, حيث يتم الوصول إلى الضحية والذي يعرف بالمجني عليه, ذلك كون تلك الجريمة تسعى إلى النيل من الضحية في بيانات حساباتها أو أجهزة الإلكترونية لكل جوال الأبعاد, عن طريق اختراق نظام الحماية وسرقة المعلومات وتشفيرها أو حذفها أو التعديل بها وبالابتزاز وبذلك يقوم المجرم بدخول إلى نظام البيانات وادخال بعض البيانات التي يمكن أن تساعد في الحصول على المعلومات, والتي من خلالها يستطيع تدمير الجريمة الإلكتروني قبل استخدام الحاسوب, تتولى عبر المكالمات الحاسوب دوراً كبيراً في اتمام الجريمة الإلكتروني فتوجد بعض الثغرات التي تشكل مادة دسمة لتلك المكالمات لما لم يكن المستخدم من الأجهزة الشخصية والمحمولة تخزين المستندات والطباعة وغيرها من الأمور التي قد تستخدم في مجال الحاسب الآلي[68].

[68] بلراهيم رمضان بلراهيم عطية: الجريمة الإلكتروني في الشريعة الإسلامية والأنظمة الدولية, ج2 العدد30, طنطا سنة 2015م.ص373.

والشك في أن أجهزة الحواسيب تكون كافية لوقوع الجريمة الإلكترونية فيما إذا كان الجاني قريب من الحاسوب وقاهر بسرقة بيانات أو معلومات موجودة على الحاسوب, أو قاهر بسرقة مكونات الهاية, كون الجرائم الإلكترونية قد تكون جريمة هاية وغير هاية غير مرئية".

2.3.2 جريمة عابرة للحدود

الجريمة الإلكترونية هي جريمة قد تكون ولي قبل وعي العابر للحدود, وقد تكون وطنية أي داخل حدود الدولة فيما أنه الفيصل دوره على ارتكاب الجريمة الإلكترونية داخل إقليم الدولة القيم فيها الجاني أو المجني عليه حيث قد تطلب الجاني على شخص خارج إقليم الدولة القيم فيها, والمتعلق أيضاً الجريمة الإلكتروني قبل جهاز شخص معين بحيث تم وفاره على المستوى الدولي أيضاً بمعنى قد يرتكبها أجانب, وهذا ما يثيره مشكلة الاختصاص في الجرائم التي ترتكب عبر الإنترنت[69].

2.3.3 جريمة ليس له أثر مادي

كون الجاني في الجرائم الإلكترونية والعامل الأساسي واحد فنية وقدرات عقلية فإن هذه وصفها بالجريمة التي تترك وراءها أثراً مادياً, والجريمة الإلكترونية تكونها اداة لكتب تمثل بأداة فإن عملية الكشف هي كون صعب فيه عض الأحيان إكونها التي ترك أثر مادي لدى ارتكاب الجريمة, يرجع ذلك إلى سهولة في امحاء الجاني بحذف ما تم فعله بسرعة العين في أقل من الثانية, وعدم ترك وراءه أي أثر يدل عليه. لذلك توصف الجريمة الإلكترونية بأنه جريمة هادئة, كون رتكابها الي حتاج إلى

[69] حاجسودي محمد: شكالية الإثبات في الجرائم الإلكترونية, مجلة آفاق علمية- المجلد 11 العدد 1 سنة 2019- رقم العدد التسلسلي 18, جامعة أدرار, ص 279.

العنف أو القوة، والإسفاك الدماء أو وقوع حدث، وإنما يعتمد على السمات الخاطفة السريعة لبرنامج الحاسوب، حيث يتم اختراق المعلومات وتدميرها، سواء بمحوها أو تشويهها، أو تعطيل النظم التي تحتويها دون ترك أي آثار خارجية[70].

2.3.4 خصوصية عملية وقتية

تمتاز الجرائم الإلكترونية بكونها تتم بواسطة الحاسوب عن طريق تواصل شبكات الإنترنت بخبرة العالية لدى الجاني مرتكب الجرم فيه، ليس ترك أي جريمة أخرى تقترفها حيث يكون مرتكب الجريمة الإلكترونية شخص على خبرة فنية وتقنية العالية في مجال الحاسوب وبشبكات الإنترنت، وقد يكون من أصحاب الهواة في هذا المجال الذي يتمتع بالذكاء والدهاء، وعلى دراية بأساليب استخدام الحاسوب، على عكس الجريمة التقليدية الذي قد يكون مرتكبها شخص أمي بسيط متواضع علمه، وقد يكون مرتكب الجريمة الإلكترونية شخص منسجماً اجتماعياً وقادراً مالياً أي ليس بحاجة إلى الأموال ولكن بعثه على ارتكاب الجريمة من أجل رغبته في قهر الغير، وتبتول ذلك الرغبة الحصول على الأموال[71].

ولما كان المرور الحالي لذلك فإن الجاني يلعب دوراً كبيراً في عملية إتمام الجريمة الإلكترونية، أي بمعنى ما يتمتع به من مهارات تؤدي تماماً إلى نجاح هيئته وتحقيق غايته، مع مدى ذلك على الحاسوب، مستغلاً في ذلك التقدم الكبير للحياة الرقمية، وتطور نظم المعلومات، واعتماد الحياة الكبرى من المجتمع على الحاسوب وبشبكات الإنترنت في إنجاز أعمالهم وإتمام صفقاتهم حيث

[70] براهيمي جمال: التحقيق الجنائي في الجرائم الإلكترونية، رسالة مقدمة لنيل شهادة الدكتوراه في القانون العام تخصص قانون جنائي، جامعة مولود معمري تيزي وزو- كلية الحقوق والعلوم السياسية، قسم الحقوق، سنة 2018، ص196.

[71] براهيمي رمضان براهيم عطيا: المرجع السابق، ص375.

صل بالمتاجر التي تقوم بأعمال عن طريق الحاسوب بشبكات الإنترنت, وبدأ المصطلح التجارة عن طريق شبكات الإنترنت, وتخزين المعلومات والبيانات التي تخص أعمال المتاجرة على الحاسوب, أو على الموقع الإلكتروني, كجوجل دايف, ولقد تطور الأمر لكثير لَّ حيث أصبح هناك أعمال تتم عن طريق الإنترنت لقنوات التلفزيونية والتي تكون الموقع المتاجرة والصفحات الإلكترونية التجارية فأصبحت الغالبية الكبرى من المجتمع يعتمد حصد رأس المال اليومي أو الشهري أو السنوي عن طريق العمل على تطبيقات الإنترنت, وهذا ما أدى إلى تزايد الجرائم الإلكترونية بشكل كبير قرن التطور الكبير للحياة اليومية, لذلك فأن الجريمة الإلكترونية تعرف بالجريمة التي تكون متخلفة إختراق أرقام البيانات ومعلومات المقصودة أو سرقتها أو التلاعب بها أو تشويه وتدمير رسائل غير المختلفة من هاتفات وتسهيلية ومن هدف الضرار والإنتقام.

2.4 الطبيعة القانونية وأركان الجريمة الإلكترونية

لكل قاعدة أساس قانوني البدا من تباعها فوق القواعد العامة أن أصل إعمال النص الإمكانية وإلا كان تجريداً ما من مضمونه فحواه, وعليه فأن لكل جريمة نص قانوني يقيد ما يصنفها من ضمن الجرائم الخطرة والشديد خطورة فالجرائم الإلكترونية نظراً لتصنيفها من ضمن الجرائم التي تكاد تكون خطراً نظراً لصعوبة معرفة الجاني فأن لها طبيعة خاصة سنبينها بشكل تفصيلي عبر هذا الأمر, ولكذلك الحال لكل جريمة أركان البد من توفرها سيما أن الأركان تمثل الشرعية الخاصة الدنة الجاني لتوبيخه مما هو مرتبط بالجاني.

2.4.1 الطبيعة القانونية

بعد استعراض ماهية الجرائم الإلكترونية وذلك بتعريفها وخصائصها وصفات مرتكبيها, وأركانها وأنواعها يتضح لنا بأنها تختلف كثيراً عن الجرائم التقليدية وخاصة في الأركان, ولكن يبقى التشابه قائماً وبدأ جوهر الاختلاف يتمثل في الأداة المستخدمة في الجريمة ومحل الجريمة وفي الدليل الذي يكون في الجريمة الإلكترونية في بعض الأحيان غير مرئي, وكما وضحنا سابقاً ترتكب هذه الجريمة بسيط استخدام الحاسوب أو ما يقوم مقامه, عن طريق شبكات الإنترنت فمحل الجريمة هنا هي أشياء قيمية, وعليه ونظراً لاختلاف الجريمة التقليدية عن غيرها من الجرائم الإلكترونية اختلف الفقه في تحديد طبيعة القانونية لها حيث اتجه بعض الفقه إلى أنها اعتداء على أية قيمة, ولطبيعة من نوع خاص, والتي لا يمكن تصنيفها من الأشياء التي يرد عليها الاعتداء, وغيرها من الفقه قال بأنه المعلومات لا تستطيع اعتبارها محلاً للعدوان القانوني, إلا أن تلك الآراء تعرضت لانتقاد حيث التي لا يمكن القول بأن المعلومات الإلكترونية لا تشكل أية قيمة مالية, ذلك كون تلك المعلومات تكون ملكاً للأشخاص وقابلة للبيع والشراء والتنازل بموجب عقود, لذلك تكتسب ملكية خاصة استناداً لخصائص حق الملكية التي تكون محلاً له[72], وذلك ما توصل إليه الفقه الحديث الذي اعتبار المعلومات ببرامج الحاسوب مالاً يقبل النقل والحيازة, ومحله الحقوق المالية, والحديث غير ذلك يصنف على أنه من أشكال القانونية على الصعيد الجزائري والمتمثلة في الجزائري يشكل جرم معاقب عليه القانون استناداً لقانون لمكافحة الجرائم التقنية رقم لسنة 2012 وتعديلات سنة 2016 و 2018, ومن ناحية مدنية تعويض عن الضرر الذي أصاب الضحية, والتي يقوم مقامها التعويض

[72] عبد الحكيم موالي بن براهيم: الجرائم الإلكترونية- مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة- الجزائر, المجلد 23, دار المنظومة, سنة 2015م, ص67.

فوق القواعد القانون المدني العامة, الأمر الذي يترتب عليه زعزعة الثقة بين القانونيين ويربك ون المستفيد الأول والأخير من ارتكاب الجريمة الإلكترونية[73].

2.4.2 أركان الجريمة

لكي يكون أمام جريمة ما مهما كان نوعها لابد من توفر أركانها والتي نص عليها المشرع الإماراتي, بحيث يتأسس فإن مجال البحث عن جريمة ما دون توفر أركانها الثلاثة تتمثل في الركن المادي أي السلوك أو النشاط الجرمي, والركن المعنوي والتي يقصد بها العلم والإرادة لأحداث أمر ضار بالغير, وأخيراً الركن الشرعي أي وجود نص قانوني يجرم الفعل المرتكب ويعتبره جريمة, فالجريمة الإلكترونية فوق القانون لمكافحة الجرائم الإلكترونية الإماراتي رقم 5 سنة 2012م وتعديلات قانون اتحادي رقم 12 سنة 2016 لابد من توفر أركانها الثلاثة والتي سوف نعرضها في هذا المطلب إلى ثلاثة فروع على النحو التالي:

2.4.2.1 الركن المادي للجريمة الإلكترونية

يعتبر الركن المادي من أهم أركان الجريمة لكونه يتضمن ثلاثة عناصر هامة أولها و أهمها السلوك الجرامي الذي يقوم به الجاني, من ثم النتيجة الجرمية التي يبتغي الجاني تحقيقها من وراء السلوك الجرامي والعنصر الثالث والأخير العلاقة السببية بين السلوك والنتيجة وسنبين تلك العناصر عبر النقاط التالية:

[73] يوسف خليل يوسف الشريفي: المرجع السابق, ص46.

أولاً: السلوك:

يعتبر السلوك هو القاسم المشترك بين جميع الجرائم, والعنصر الأول من أركان الجريمة, وهو الذي يقوم به الجاني على شيء محمي بالقانون, والسلوك الجرامي في جريمة الكترونية يتم عن طريق الوسيلة وهي الجهاز الالكتروني أياً كان نوعه وشكله والتصال بشبكة الانترنت, بحيث بدون الوسيلة الي يمكن القول بوجود جريمة الكترونية, والسلوك في جميع الجرائم يشكل عام يتخذ مظهرين اي جابي وسلبي, ففي الجريمة الالكترونية يكون السلوك الاي جابي بصورة أغلب من الجاني وهو أغلب صور الجرائم الالكترونية كالقيام بالاختراق وسرقة البيانات والتهديد والابتزاز وسرقة الأموال القيمية, والسلوك السلبي في جريمة الكترونية يكون عن طريق الامتناع عن فعل كان يجب بتأديته كامتناع موظف الأمن عن حماية البيانات والمعلومات الشركة التي يعمل بها, ومن الجدير بالذكر أن هذا السلوك السلبي نادر الحدوث[74].

ثانياً: النتيجة:

النتيجة تعد العنصر الثاني من عناصر الركن المادي الذي يلي السلوك بحيث يتأسس فيه السلوك يشكل جرم دون وجود نتيجة, وتتخذ النتيجة كعنصر في الركن المادي على أساس يعتد به الشرع ويترتب على هذه النتائج بغض النظر عما يمكن أن يحدثه السلوك الجرامي من نتائج أخرى[75], بحيث يتفق حدف النتيجة الجرمي هو مبين مادي وقانوني بحيث المادي يتمثل في ظاهرة له أثر مبتذل ومحسوس السلوك المجرم, والقانوني يتمثل في الاعتداء على المصالح والحقوق التي يحميها

[74] يوسف خليل يوسف الشرفي: الجرائم الالكترونية, رسالة قدمت لنيل درجة الماجستير, غزة, سنة 2013م, ص50 وما بعدها

[75] صغير يوسف: الجريمة المرتكبة عبر الانترنت, وزارة التعليم العالي والبحث العلمي- جامعة مولود معمري تيزي وزو- كلية الحقوق والعلوم السياسية, رسالة قدمت لنيل شهادة الماجستير في القانون سنة 2013م ص66.

القانون, بغض النظر إلى الجرائم المرتكبة عن طريق الإنترنت وهذا يكون له أثر ملموس إلا أنه لشكل خطورة على المجتمع على الرغم من ضرر يصيب الغير[76].

ثالثاً: العلاقة السببية:

تكون العلاقة السببية العامل المشترك بين السلوك والنتيجة بحيث تنشأ وبدأ يسعى الجاني إلى ارتكاب السلوك الجرامي من أجل تحقيق النتيجة المستهدفة من وراء السلوك، لذلك يقتضي أن يكون هناك علاقة سببية بين السلوك والنتيجة بحيث اذا انتفت العلاقة السببية بين السلوك والنتيجة فلا تكون هناك جريمة نظراً لانتفاء العلاقة السببية. وتجدر أن تكون أمام علاقة سببية في جرائم الإنترنت يجب أن يكون هناك اتصال بالإنترنت من خلال الجهاز الإنترنتي, من ثم اختراق جهاز ما أو موقع ما والوصول إلى بيانات الخاصة بالموقع عبر نشر هذه البيانات من صور أو علوم أو تعبير موقع معد مسبقاً[77].

Universiti Utara Malaysia

2.4.2.2 الركن المعنوي

يعتبر الركن المعنوي للجرائم الإلكتروني بشكل عام أهم الأركان التي يبنى عليها لكن تحديد أن الفعل الارتكاب يشكل جريمة من عدمه، وهو يمثل هذا الركن في الخصوصية الذي كان عليها الجاني وقت ارتكاب الجريمة فهي تكون مرتبط ارتباطاً الوقت التجريم جرائم الجريمة

[76] أدهم سلمان مرب غدادي: وسائل البحث والتحري عن الجرائم الإلكتروني, رسالة قدمت لنيل درجة الماجستير في القانون العام- جامعة النجاح الوطنية, نابلس سنة 2018, ص22.

[77] يوسف خليل يوسف الفقي: المرجع السابق, ص54.

الحالة النفسي أو الذهني أو الشخصي قد يرتكب به[78] فالبد من توفر الإرادة الآثمة لدى الجاني عند إقدامه على فعل السلوك الإجرامي, لذلك يجب أن تكون الفعال إرادية وإلا انتفى الركن المعنوي للجريمة, ويجب أن تكون تلك الفعال مرتبة على مخالفة القواعد القانونية, حتى تكون أما مخالفة فتعترض عقوبة جنائية على قترافها, ويجب أن تكون ارادة الجاني حرة و واعي عن درتكاب جريمتها, كون ها التنسب إلى سلوك اجرامي في حال كان غير مدركاً أو مكرهس بل مكن لديه القدرة على الختيار ألا يتجزع عن ارتكاب الجريمة[79].

في ظل توفر الركن المعنوي في الجرائم الماكترونية فيأن تشترط توفر العلم والإرادة حتى يكون الجاني على علم بالسلوك المقدم عليها, وارادته حرة في ارتكاب هذا السلوك, كون الركن المعنوي للجريمة الماكترونية يقوم على أساس توفر تلك الرادة توجه إلى القيام بعمل غير مشروع جرمه القانون, كأن تكون حال شخصية موظف أمن معلومات أو مزود خدمات, أو سرق أو بطاقات التمان نتيجة, وتكتسب الصفة الجرامية على أساس النتيجة الغير مشروعة المراد من تلك الرادة وهو على علم بجميع الآثار الضارة الناجمة عن عله[80].

على هف أن الجرائم الماكترونية في غالب منها تشكل قصد يخص ونوي ه العام والخاص, ذلك كون الجاني على علم ودراية تام بما يقوم به عمله, ونتائج عمله يسعى إلى تحقيق نتيجة, وفي مجال الجرائم الماكترونية نجد أن النية الجرامية قائمة حتى يتأسس فاك مجال الحديث عن تعتبار

[78] سامر بدر اليم الدليمي: قانون الجراءات الجزائية, ط2, ج2, غزة, سنة 2014, ص141.

[79] يوسف جميل يوسف الفقي: المرجع السابق, ص56 وما بعدها.

[80] مصطفى غدري يوسف: المرجع السابق, ص71.

دخول إلى جهاز مالي يترتب عليه مجرد تحويل أو تحويل أو أي سبب آخر[81]، لذلك فإن هذه الجرائم الإلكترونية هي جرائم عمدية والركن المعنوي فيها يفترض فيها دائماً وبدلاً من مجرد ثبوت الركن المادي بشرط أن تكون إرادة الجاني حرة وعلى علم لفعله يسأل وكيه الجرامي.

لذلك نجد الفقه والقضاء الفرنسي قد قنن مبدأ سوء النية في جرائم الإلكترونية، لكون اشتراط الشرط الشرعي الفرنسي وجود سوء النية في الاعتداء أياً ما كان نوعه سواء كان الاعتداء على برامج الإلكتروني خاصاً أو عاماً مفتوحاً أو مغلقاً فإنه لا يعتبر وجود مبدأ سوء النية[82].

2.4.2.3 الركن الشرعي

نظراً لكون الجريمة الإلكترونية المرتكبة عبر شبكات الإنترنت تختلف كثيراً عن الجرائم التقليدية المادية من حيث الأركان، فإن الجريمة الإلكترونية لها ركن شرعي إلى جانب الركن المادي والمعنوي إلا بد من توفر الركن الشرعي يتمثل الركن الشرعي بوجود نظام قانوني يعين تجريم الجريمة الإلكترونية لكي يكون أمام فعل مجرم يجب أن يتم تجريم الفعل بنص قانوني خاص به.

كون مبدأ الشرعية الجنائية يمنع المشرع الجنائي عند عدم وجود نظام قانوني أي نص قانوني يجرم الفعل فوفقاً لقانون الجزائي المادي الجريمة والعقوبة إلا بنص، وبناء على النص على تجريم تلك الأفعال التي لا يوجد نظام نص وص قانوني لا تعتبر مسؤولين كون أمام قصور

[81] أد مهلس من مرب غدادي: المرجع السابق، ص21.

[82] ولي د طه: التنظيم الشرعي لجرائم الإلكترونية في قوانين, جمهورية مصر العربية بدون نشر أو سنة، ص17.

في مكافحة تلك الجرائم, لذلك وجد مبدأ الشرعية الجريمة والعقوبة إلى نص وتتعبر الآليات المتحدة الأمريكية من ضمن الدول السباقة التي نصت تشريعاً متقدماً بشأن جرائم الكمبيوتر بشكل عام وجرائم الإنترنت بشكل خاص بتوفير الآليات المتحددة وجوانب قدر من التشريع التي تنظم مسائل جرائم الملكية الرقمية[83].

وقد نظم المشرع الماليزي نظاماً خاصاً بشأن مكافحة جرائم تقنية المعلومات وذلك بأصدر قانون اتحادي رقم 5 لسنة 2012, المعدل بقانون اتحادي رقم 2 لسنة 2016م, والذي نص فيه على تجريم جميع الأعمال الغير مشروعة التي يتم استخدام الأجهزة الإلكترونية أياً كان نوع استخدام شبكات الإنترنت, والتي تحدث بشكل فصل عن مهمة الجرائم الإلكترونية وعقوبات الجرائم الإلكترونية[84], كدخول مواقع إلكتروني أو نظام معلومات الإلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح بصورة غير مشروعة, ودخول الموقع الإلكتروني أو وسيلة تقنية المعلومات بقصد الحصول على بيانات حكومية ومعلومات سرية خاصة بمنشأة المالية أو تجارية أو بقصد إيذاء, وغيرها من الأفعال المحددة بـ51 مادة قانونية تبين فيها جميع الجرائم المرتكبة عليه, والظرف المشدد والمخفف منها.

---

[83] يونس عرب: قراءة في الاتجاهات التشريعية لجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان, ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية, المنعقدة بمسقط, سلطنة عمان, 4-2 أبريل 2006م, ص55 مشار إليه لدى صغير يوسف: المرجع السابق, ص61.

[84] الجرائم الإلكترونية بيان الفئة البالغ عن الجرائم الإلكترونية, https://www.bayut.com/mybayut/ar/ بدون تاريخ نشر تاريخ الزيارة 2023/1/1م,

2.5 الفرق بين الجريمة الإلكترونية والتقليدية

الجريمة الإلكترونية والتقليدية هما من الجرائم المعاقب عليها في القانون من حيث أنهما جرماً ويعاقب عليهما القانون, وأيضاً من حيث وجود الأركان الموضوعية والأركان الجزائية, في وجود الجاني والضحية, وهذا يرجع إلى أن الجريمة الإلكترونية هما كان نوعها فأن هناك عدة جريمة ولها أركانها في وجود الجاني والضحية, وهذا تختلف في شتى أنواع الجرائم بشكل عام إلى أن السلوك الإجرامي في الجريمة الإلكترونية الذي أخذ سلوكاً ذهنية وليس سلوك مادي بالفعل والحركة كما في الجريمة التقليدية, ويضاف أن الجاني في الجريمة الإلكترونية هو مجرم إنترنت, وليس كالمجرم العادي في الجريمة التقليدية, وعليه فأن الفوارق بين هما يتم توضيحها من حيث الأداة المستخدمة في الجريمة, ومن حيث مكان وقوع الجريمة, ومن حيث المتهم والتحقيق ومن حيث الدليل, أما من حيث أنواعها سبق وأن بينها سابقاً وفقاً أنواع الجرائم الإلكترونية عبر الرابط التالي:

أولاً: من حيث الأداة المستخدمة في الجريمة

أن الأداة المستخدمة في الجريمة الإلكترونية هي أداة ذات مستوى تقني عالي فائق الجودة بينما أن المستخدم بواسطة الحاسب الآلي عن طريق شبكات الإنترنت وتتأخذ الطابع المادي الملموس أو الغير ملموس, على غرار ما هو في الجريمة التقليدية والتي تكون الدافع مختلفة ذات طابع مادي وملموس تتمثل بالقتل أو بأي وسيلة أخرى عن طريق القوة[85] فهي تلك الجريمة

[85] محمد شرف الدين: الجريمة الإلكترونية والجرائم المعلوماتية, معلومة قانونية تاريخ النشر 8 مارس 2015م https://www.facebook.com/egy.law0 تاريخ الزيارة 2023/1/1.

التي عرفها النظام السعودي بأنها الجرائم الإلكترونية وهي توجد في كل مجتمع لكل سرقة وجريمة القتل والتعدي والسطو والشروع في القتل[86].

ثالثاً: من حيث مكان وقوع الجريمة

الجريمة الإلكترونية تنشأ في بيئة افتراضية وتقع على العلوم والبيانات والأرقام التي تخص الغير, وخطورتها كبير واضرارها كثيرة لكون هذه الشبكة تنشأ بسهولة وتمكن شبكة بعيدة من وقوع الجريمة والذي ينتج عنها سفك الدماء, أما الجريمة التقليدية والتي تقع على الأشياء المادية بسبب استخدام العنف وقد ينتج عن ارتكابها سفك الدماء, والضرر المترتب على هذه الجريمة أقل خطراً قياساً بالجريمة الإلكترونية, والمجهود المستخدم في الجريمة التقليدية كبير ويأخذ وقت كثير, عكس الجريمة الإلكترونية والتي يمكن استخدامها في أقل من الثانية[87].

ثالثاً: من حيث المجرم

يعتبر المجرم في الجرائم الإلكترونية ذو شخصية متعلمة متفوقة على خبرة العاقب أمور التقنية شروبكات الإنترنت يتميز بالذكاء كما وضح من خصائص المجرم الذي يبدع أدق هو مجرم محترف له قدرات فائقة في المهارات التقنية وأن يستغل قدراته ومهاراته في اختراق الشبكات وكسر كلمات المرور أو الثغرات ويتميز بأنه مجرم يعود للإجرام أي تكرار ارتكاب الجريمة لمرات عدة[88], والسرعة في اقتراف الجريمة. أما المتهم في الجريمة التقليدية هو انسان عادي قد يكون متوسط الذكاء

---

[86] أحمد سبلاك الشيخ أحمد تعريف الجريمة التقليدية تعريف كامل بتاريخ النشر 2016, https://specialties.bayt.com/, تاريخ الزيارة 2023/1/1م.

[87] طلال غنيمات: خبراء الجرائم الإلكترونية تأثير خطورة من "التقليدية", 16 سبتمبر 2020, https://alghad.com/ تاريخ الدخول 2023/1/2م

[88] محمد شريف الدين: المرجع السابق نفسه.

أو أمي لا يعرف القراءة أو الكتابة، وقد يكون من أصحاب السوابق، ولا يمكن أن يترك وراءه دليلاً يمكن تتبعه[89].

رابعاً: من حيث إجراءات التحقيق

يكون التحقيق في الجرائم الإلكترونية بواسطة أجهزة متخصصة ذوي خبرة في مجال التقنية وشبكات الإنترنت، أما في الجريمة التقليدية فهي تحتاج إلى متخصصين عاديين، وذلك يرجع إلى أن الجريمة سواء كانت إلكترونية أم ورقية أم مالية أو تقليدية فهي تبقى جريمة في نظر القانون ويعاقب عليها القانون[90].

سادساً: من حيث الدليل الجنائي

في الجرائم الإلكترونية تتمثل الدليل الجنائي في أن هذا الأخير يتكون من بيانات غير مرئية وسهلة محوها وتدميرها في حين الدليل في الجريمة التقليدية يتمثل بأثر مادي ملموس وفهمه دليل عادي يتمثل في سلاح أو أداة عصا أو السلاح الناري وغيرها من الأدوات التي تشكل خطراً، ولما كان الأمر والحال كذلك فإن الجرائم الإلكترونية وإن كانت تتم بواسطة الحاسوب وعبر شبكات الإنترنت، إلا أنه إذا كانت الجريمة تتم فقط بجهاز الحاسوب في مكتوبه المادي تمثل وحدة النظام وشاشة الإظهار ولوحة المفاتيح وإن أرتبط بها عدة أطراف عبر الوسائط وشبكة إظهار أو تخزين بلوحة المفاتيح أو استخدام الحاسوب من غير مالكه أو المرخص له بالاستخدام[91]، أو استخدام مشكل عشوائي من قبل غير المختصين، أو استخدام مشكل غير قانوني، كأن يستخدم طريقة تكاب جريمة معينة،

[89] الطائي جعفر حسن جاسم: جرائم تكنولوجيا المعلومات، دار البداية، ط1 ،سنة 2007, ص157.

[90] أحمد مبارك الشيخ أحمد: المرجع السابق نفسه.

[91] سامر بدر إبراهيم الوليد: المرجع السابق, ص167.

أو استخدامها لغير الغرض المعدة له، كأن يستخدم الموظفين أو العاملين في برامج ألعاب أو بعض الأغراض الشخصية غير المتوافقة مع العمل الرسمي، فيما يمثل هذه الأفعال إختلاس للحاسوب عن غيره من الجرائم الأخرى المتعلقة بالحاسوب, والواقع أن مثل هذه الأفعال وان كان وجودها يتوافق مع وجود الحاسوب ولكن تخرج عن نطاق البحث، والتدخل في مفهوم الجريمة الالكترونية, على اعتبار أن الجريمة الالكترونية تقتصر في الشروعة الغير المشروعة التي تمت بشبكات الانترنت والبرامج المستخدمة من خلال الحاسوب[92].

2.6 المشكلات الموضوعية الناتجة عن الجرائم الالكترونية

لكل جريمة مشكلات وعوائق بسبب التي تمثل تسهيل نواحي الجنائية أو الموضوعية بحيث التي تصور وقوع جريمة دون وجود المجرم, والذي يعرف بمحل الجريمة, بما يعني أن المشكلة الموضوعية التي يبحثها الجرائم الالكترونية تكون حسب نوع الجريمة التي وقعت, بما يعني والحال لكذلك يتم ربط المشكلة بمحل الجريمة, لكل جرائم الالكترونية التي يكون محلها الاعتداء على الأمور الشخصية والحياتية الخاصة بالأشخاص, وأيضاً تظهر المشكلة الموضوعية بسبب في الجرائم التي يكون محلها الاعتداء على الأموال والممتلكات التي تقع على قبل جرائم التزوير والتي يشرع عنها, وأيضاً فالمشكلات الموضوعية تكون في جرائم سرقة الأموال والمعلومات, ومن الجدير بالبيان هاب أن الجرائم الالكترونية ليست محصورة على ما هو رفق طبل هي تتسع فوق المجال هو قبل ون المفاجأة الجرائم التقنية رقم لأسنة 2012 وتعديلات سنة 2016 و 2018 المطبق في الامارات العربية المتحدة, ولكن نظراً لما تشكله تلك الجرائم من طابع خطر وتثير المشكلات من النواحي

[92] كامل فريد السالك: المرجع السابق نفسه.

الموضوعية, سواء تمثلت بتبادل قصاصات النظام المشروع على بعض أحكامها أو صور عبارة قصاصات اشتراف رمتكبها, وهل فالكرقصاصات المشروع يفيد النظام, على رأي الباحث عن هباش يء من الفصل.

2.6.1 جرائم الاعتداء على المراسلات الشخصية "الحياة الخاصة"

تعالج الحياة الخاصة والمراسلات الحياتية حقوق الخصوصية قبل الناس انتهاك حظر المساس بها وذلك وفق الدستور دولة الإمارات العربية المتحدة, ويتبين استشف من المادة 36 والتي تقضي بأن المساكن حرم فلا يجوز دخولها بغير اذن أهلها الا وفق أحكام القانون في الأحوال المحددة فيه" فقد فصل القانون حظراً على دخول المساكن فحاظلًا ذلك على الحقوق الشخصية وعدم التعدي لها دون وجه حق, إلا أنه ونظراً لتسارع رقعة التقنية مع مرور الحضارة قد أدى ذلك إلى قيام الكثير من الأشخاص بخرق أسرارهم وأمورهم الشخصية على الانترنت, ولكن فحظلي حقوق تتسبب انتهاك المعلومات, الأمر الذي أصبحت عليه شبكات الانترنت مصدر لكل جرائم الالكتروني بحيث يسهل على القرصنة أو الهكرز من اختراق والتلاعب بها[93], ونجد أن قانون المكافحة رقم لسنة 2012 الخاص بالجرائم التقنية, قد نظم جريمة الاعتداء على خصوصية الأخرين وذلك وفق النص المادة 21[94] والتي تقضي

---

[93] عادل دغمش العجمي: المشكلات العملية والقانونية للجرائم الالكترونية, قدمة هذه الرسالة لمتطلب الحصول على درجة الماجستير في القانون العام, جامعة الشرق الأوسط, سنة 2014, ص41.

[94] نصت المادة 21 على يعاقب بالحبس مدة التقل عن سنة أشهر والغرامة التي التقل عن مائة وخمسين ألف درهم والتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلومات ، أو نظام معلومات الكتروني ، أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق التالية :

1 - استراق السمع ، أو اعتراض ، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية .

2 - التقاط صور الغير أو إعداد صور الكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها .

3 - نشر أخبار أو صور الكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية .

كما يعاقب بالحبس مدة التقل عن سنة واحدة والغرامة التي التقل عن مائتين وخمسون ألف درهم والتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين ، كل من استخدم نظام معلومات الكتروني ، أو إحدى وسائل تقنية المعلومات ، لإجراء أي

بالحبس أو الغرامة أو كلاهما في حال الاعتداء على خصوصية أي شخص في غير الحالات المصرح بها قانوناً لاستخدام الشبكات والنظم الكترونية.

على من جانب أن المشرع يجرم الاعتداء على معلومات الشخصية التي يتم سرقتها وقت إصدار بطاقة الشخصية بشكل قديم, لمواكبة المشرع الفرنسي الذي نظم أحكام خاصة بمعالجة البيانات والحريات بحيث حظر الاعتداء على الأموال الحياتية وانتهاكها, وذلك في القانون رقم 17 لسنة 1978, لذلك نص المشرع الأماراتي بضرورة نص صريح قانوني يقنن نظم جرائم الاعتداء على المراسلات الحياتية بشأن الجرائم الإلكترونية.

2.6.2 جرائم الاعتداء على الأموال وسرقة المعلومات

تعد جرائم الاعتداء على الأموال في قانون الجراءات الجزائية الإماراتي رقم 35 لسنة 1992 جرائم تتمثل في السرقة أو السلب أو النصب والاحتيال, والتي قد يكون محلها المنقولات أو العقارات, فهذه الجرائم في صورها التقليدية حيث المشرع قد نظمها ونظم الأحكام الخاصة بالعقاب عليها, ولكن في ظل تطور الوسائل العصرية التقنية وتعدد اعتداءات جرائم الأموال بطرق الكترونية, سواء عن طريق حوالات بنكية أو عن طريق سرقة الكترونية ومعرفة بطاقات الائتمان, أدى ذلك إلى انتشار جرائم الاعتداء على الأموال وسرقة المعلومات بشكل الكتروني, وذلك عن طريق الحاسب الآلي باستخدام برامج تتجاوز سلطة الحماية الخاصة بالسرقة, لكن في الفقه

تعديل أو معالجة لبيانات مسجلة أو صورة أو شهادة بقصد التشهير أو الإساءة إلى شخص آخر ، أو الاعتداء على خصوصيته أو انتهاكها(.

حرابات الجمع عالب رعات في قيتها هي عملي قصب والتحيال, أو الي امالص طناع زمص الكترونية لغرض ألعم الت جرايالة الكترونية.

مع زيادة عدد المستخدمين تم اغالق المصرفية لكتشافعملية النصب والتحيال[95], وقد يكون جرائم الاعتداء عن طريق قيام الجاني بسرقة توتحويل مبلغ رة لحرابه الخاص, كم حدثفي الولايات المتحدة عندما قام أحدخبراء الحاسوب باختراق النظام المعلومي ألحالبنوك وقام بتحويل 12 مليون دولار لحرابه الخاصفي مدة التتجاوزثالث قائق, وهذايتم عن طريق ادخال بيانات غير صحيحة "مزيفة", وأيضاً يتم الاعتداء عن طريق التلاعب بالبطاقات الائتمانية الخاصة, ويتم ذلك عن طريق التقاط أرقام الخاصة السرية لبطاقة, ولتخدامها من قبل الجاني, وأيضاً فاك جرائم الحصول والاستيلاء على الأموال الكترونية وهيتلك الأموال المخزنة على المواقع الالكترونية[96].

ونص قانون مكافحة الجرائم المعلوماتية رقم لسنة 2012 على عقوبة كل من ارتكب جرائم الاعتداء على الأموال وسرقة المعلومات وذلك في المادة 11[97] و12[98].

---

[95] عادل الدغمش والعجمي: المرجع السابق, ص51.

[96] بيرل الجنيدي: البنوك الالكترونية, ط1, دار فكر الجامعية, الاسكندرية, سنة 2006, ص39.

[97] نصت المادة 11 على عقوبة السجن بغير حق على المال المنقول او منفعة او على سند بطريقة احتيالية على بالحبس مدة التقل عن سنة واحدة والغرامة التي التقل عن خمسين وخمسين ألف درهم والتجاوز المليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند ، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات(.

[98] جاءت المادة 12 لتنظم جرائم الحصول على أرقام وبيانات بطاقة الائتمان بما يحقق ضبط على بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق ، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات ، إلى أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية ، أو أي وسيلة من وسائل الدفع الكتروني .

2.6.3 جرائم التزوير وما يتفرع عنها

تعد جرائم التزوير من الجرائم الخطرة التي يتعرف كل فعل ينقض تغيير الحقائق والبيانات بأنه تحقيق قصد استعمال ه[99], وقد جرم المشرع الماليزي التزوير وذلك في القانون الاتحادي رقم 3 لسنة 1987 الخاص بقانون العقوبات حيث جرم جريمة التزوير المحرر الرسمي في المادة 217 والتي تنص على أنه "يعاقب على التزوير في محرر رسمي بالسجن مدة لا تزيد على عشر سنوات ويعاقب على التزوير في محرر غير رسمي بالحبس" بينما نصت المادة 211[100] على عقوبة السجن المؤقت في حالة قيام الشخص ذاته أو بواسطة غيره بتقديم أو تزوير ختم من أختام الدولة أو رئيسها أو أحد حكامها وكذلك في حالة استخدام هذا الختم أو الإمضاء مع علمه بتقديمه أو تزويره.

تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم والتي لا تزيد عن مائة ألف درهم أو بإحدى هاتين العقوبتين ، إذا قصد من ذلك استخدام البيانات والأوراق في الحصول على أموال الغير ، أو الاستفادة مما تتيحه من خدمات .

فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين .

يعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني .

[99] سامر بدر العيد, المرجع السابق, ص126.

[100] نصت المادة 211 على يعاقب بالسجن المؤقت مدة لا تقل عن خمس سنوات كل من قلد أو زور بنفسه أو بواسطة غيره خاتم الدولة أو ختم أو إمضاء رئيس الدولة أو أي من حكام الإمارات وأولياء عهودهم ونوابهم أو أحد أقسام أو الطوابع الرسمية أو المالية أو علامات الحكومة ودوائرها أو إداراتها أو إحدى الجهات التي ورد ذكرها في المادة 5 من هذا القانون أو ختم أو إمضاء أو علامات أحد موظفيها أو الدمغات الحكومية للذهب أو الفضة أو غيرها من المعادن الثمينة أو الأحجار الكريمة .

يعاقب بالعقوبة ذاتها كل من استعمل شيئا مما تقدم أو أدخله في الدولة مع علمه بتقليده أو تزويره (.

وقد نظم قانون رقم لسنة 2012 الخاص بمكافحة جرائم التقنية في دولة الإمارات العربية المتحدة جريمة تزوير المستند الكتروني وذلك في المادة 6[101] التي نصت على عقوبة السجن والغرامة في حالة تزوير المستند الحكومي أو غير ذلك حسب الجهة الصادر عنها المحرر أو المستند المزور.

وأيضاً بنفس الجرائم السب والقذف التي تقع عن طريق التزوير أو التقليد في بطاقات الائتمانية فإن المشرع الإماراتي قد جرم ذلك وذلك في المادة 13[102] من ذات القانون.

على هذا نجد أن القوانين الخاصة قد جاءت في بعض منها لتستطيع ولكن هل يوضح المشرع في النص بالجرائم عن تطبيق هل حيث لم يظهر لنا العقوبة الشدة أو المخففة, هذا من جانب أخر, ولم يبين لنا المشرع سواء في القوانين العامة أو الخاصة القوانين تثبتوي المستندات الكترونية أو الحاجية التشريعية له في ظل يبين لنا فقط العقوبة على تزيره ولا اختراقها, لذلك يقتضي الضرورة

---

[101] نصت المادة 6 على يعاقب بالسجن المؤقت والغرامة التي التقل عن مائة وخمسون ألف درهم والتجاوز سبعمائة وخمسون ألف درهم كل من زور مستنداً الكترونياً من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية .

تكون العقوبة السجن والغرامة التي التقل عن مائة ألف درهم والتجاوز الثمانمائة ألف درهم أو إحدى هاتين العقوبتين إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في الفقرة الأولى من هذه المادة .

يعاقب بذات العقوبة المقررة لجريمة التزوير بحسب الأحوال ، من استعمل المستند الإلكتروني المزور مع علمه بتزويره(.

[102] نصت المادة 13 على يعاقب بالحبس والغرامة التي التقل عن خمسمائة ألف درهم والتجاوز المليون درهم أو بإحدى هاتين العقوبتين كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة ، أو أي وسيلة أخرى من وسائل الدفع الإلكتروني ، وذلك باستخدام إحدى وسائل تقنية المعلومات ، أو برنامج معلوماتي .

يعاقب بذات العقوبة كل من :

1 - صنع أو صمم أي وسيلة من وسائل تقنية المعلومات ، أو برنامج معلوماتي بقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة.

2 - استخدم بدون تصريح بطاقة ائتمانية أو إلكترونية أو بطاقة مدينة أو أي وسائل أخرى للدفع الإلكتروني بقصد الحصول لنفسه أو لغيره ، على أموال أو أملاك الغير أو الاستفادة مما تتيحه من خدمات يقدمها الغير.

3 - قبل التعامل بهذه البطاقات المزورة أو المقلدة أو المنسوخة أو غيرها من وسائل الدفع الإلكتروني مع علمه بعدم مشروعيتها(.

تدخل الشريعة لتنظيم هذا الأمر, على هو نص الشريعة لتنظيم الأحكام الخاصة التي تحتويها ضمن نصوص قانونية خاصة.

2.7 المشكلات الجنائية الناتجة عن الجرائم الإلكترونية

تتمثل أهم المشكلات الجنائية القانونية الناتجة عن الجرائم الإلكترونية في ضوابط الجريمة ذاتها من حيث إثباتها وعن المشكلات التي قد تتعلق بإجراءات البحث والتحري والتحقيق, وأيضا المشكلات المتعلقة بتطبيق "القانون الواجب التطبيق على تلك الجرائم".

2.7.1 مشكلة إثبات الجريمة الإلكترونية

وتقصد بمشكلة إثبات الجريمة الإلكترونية, صعوبة الحصول على الدليل الجنائي والكشف عن مرتكب الجريمة, والمترتب على هذا الدليل الجنائي العلمي, الدليل الإلكتروني والذي يتمثل في بيانات مولدة أو مخزنة في شكل رقمي في الحاسوب, بحيث يقوم الفرد بإدخالها يدوياً في جهاز إلكتروني[103] ويتميز هذا الدليل بسهولة محوه وتدميره حيث التي يبقى لها أي أثر يدل على صاحبه, مما يؤدي إلى فلتان الجريمة لأدلة, وأيضاً يؤدي إلى غياب الدليل المرئي المادي, الذي يمكن مقروءة بالقراءة كونه تلك الأدلة تحتاج إلى متخصص يقف عليه ومن ثم يتوجب على الدليل الجنائي قبسب احاطة بوسائل حماية تلك المعلومات السرية لموقع ما, أو شفرة معينة, وأيضاً البعد

[103] مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: جمع وتبادل الأدلة الشبيهة إلكترونية- ورقة معلومات أساسية من إعداد الأمانة فيينا, 27, 28 تشرين الأول أكتوبر 2015, ص2.

الجغرافي ما بين الضحية والجاني يثير صعوبة كبيرة جداً في تقصي الحقائق, وبأقل قدر من التخصص في مجال الجرائم الإلكترونية قد يرتبط بالتطور التكنولوجي الذي يشهده العالم[104].

أما الجاني في الجرائم الإلكترونية يكون شخصاً ليس عادياً بل شخص على معرفة وثقافة عالية وخبرة في مجال الحاسوب والاتصال عبر الأدلة الرقمية وعلى ذلك فإن الجاني يستطيع أن يخترق أي نظام في أي من دولة جغرافيا, دون ترك دليل يدل عليها, الأمر الذي يؤدي إلى صعوبة في تتبعها ومن ثم تتسبب بسرعته في تدمير الدليل الجنائي أو وجوده في دولة أخرى غير الدولة التي ارتكب فيها الجرم, وعدم تركها أي أثر مادي خلفه ويكون ذلك عن طريق الاتصال عبر شبكة الإنترنت بالبرامج في جهاز الحاسوب وإخفاء جرائمهم داخل وحدات تخزين غير مرئية وتكون بالبيانات المكتوبة بلغة رقمية لا يفهمها إلا آلة لا تستطيع أدق على شاشة الكمبيوتر حتى يتمكن الإنسان من فهمها, هذا وأيضاً يقوم الجاني بإخفاء هويته أو يقوم بانتحال شخصية أخرى حتى لا يتسنى التعرف عليه عن طريق ارتكاب الجريمة[105], وقد يقوم شخص مسئول عن حماية نظام المعلومات في شركة ما بإدخال بعض البيانات على برمجة نظام المعلومات في السيرفر الشركة, بهدف نزع أجهزة المالية من المال الجنائية من مال الجناة ضياع الدليل الجنائي, كما حدث في دولة الإمارات العربية المتحدة عندما قام شخص شغل الوظيفة الإلكترونية بتتبع المؤسسة التي يعمل بها, من أجل تتبع قبض المطلوب بمحو الملفات الجنائية

[104] محمد محي الدين عوض: معوقات ملاحقة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية, مجلة جامعة الشارقة- دورية علمية محكمة للعلوم القانونية, المجلد16 العدد1 شوال 1440هـ/ يونيو 2019م, ص636.

[105] صغير يوسف: المرجع السابق, ص119.

المخزن في الجهاز الرئيسي للشركة, وعدم المتسبب الشركة له, قام بالتحاور مسبباً للمؤسسة ضرراً كبيراً في سلسلة الإجراءات التي قام بحفظها[106].

فأظهرت تلك التشافات الدليل الجنائي في الجرائم المالكترونية تتطلب بخبرة العيادة وقدرة اجتهادية فائقة بما أن ذلك يسهل المرفيك التشافات الجنائي, ومعرفة الحقيقة[107].

والمجرى عليه يعتبر الضحية التي يصيبها الضرر من وقوع الجريمة فقد يتخذ المجرى عليه سلوكاً يساعد الجاني القيام بالجريمة دون قصداً فيحدث ذلك, ويؤدي ذلك عن طريق عدم اتخاذ التدابير الوقائية والاحتياطية التي تساعد في عدم وقوع الجريمة, وضعف الجانب الأمني, وقيام الشركة بتسبيط اجراءات التسلسل ثم ارو تسريب التخدام مهلبن ظل تقديم الخدمة وعدم الترتكيز على الجانب الأمنية, وعدم الدراكبش أن خطورة الجرائم المالكترونية مقبل المسؤولين في الشركات والمؤسسات, وعدم نشر الجانب الرشادالذي يهدف إلى توعية المستخدمين لمدى خطورة الجرائم المالكترونية[108], كما وقد يسعى المجرى عليه إلى كتمان وقوع الجريمة التي أصابته, وذلك بعدم الإبلاغ الأجهزة الأمنية خشية من اطلاع عامة الجمهور على المعلومات التي يجب أن يطلع عليها, أو خشية من فقدان الزبائن لها, أو بهدف التستر على الفضيحة إذا ما كانت الجريمة المالكترونية تنال الأبرياء غير الحقيقية[109]. وقد يكون ذلك وعي لدى المسؤول عن حماية نظام المعلومات من أن الفعل الذي حدث يشكل اختراقاً لنظام المعلومات, أو تكون هذه الجريمة ذات أثر محدود, أو قد يغلب

---

[106] حاجسودي محمد: المرجع السابق, ص 272.

[107] عادل الدغمش الجهني: المرجع السابق, ص84.

[108] محمد محي الدين عفاف: المرجع السابق, ص 638.

[109] ص غري يوسف: المرجع السابق, ص121.

طابع ألزامية على الشخص المسئول عن حماية نظام المعلومات في تعمد إلى عدم الإفصاح عن وقوع جريمة بهدف عدم إعطاء نصوص تحصول على تقوية وعالوة. ذلك نرى ضرورة قيام الجهزة الأمنية من خلال دورات ومؤتمرات وورشة عمل تهدف إلى توعية المواطنين بمدى خطورة الجرائم الإلكترونية وكيفية التعامل معها, وضرورة الإبلاغ عنها, حتى لا تفشى الأمور ويكون غير رهم ضحية لمثل ذلك الفعل.

2.7.2 المشكلات المتعلقة بالتحقيق والقانون الواجب التطبيق

يعرف التحقيق في الجرائم الإلكترونية بالتحقيق الرقمي, وهو مجموعة من الأدلة المتتبعة من أجل معرفة وتقديم الدليل الرقمي المخزن في سيرفر الإلكتروني قمم غنطة أمام الجهات القضائية, وهذا يتحقق بها عدة معوقات التي تؤدي إلى عرقلة التحقيق, والذي يدور رمته عكس بطريقة قريبة على فسرية المحققون تجعل من هغير واثق من نفسه, وأيضاً تؤثر على المحتمع بحيث تجعل فقدان الثقة في الجهزة الأمنية, وتؤدي إلى زيادة نطاق المجرم نفسه وتشجيعها على ارتكاب المزيد من الجرائم[110], والمشكلات التي تواجه التحقيق في الجرائم الإلكترونية تكون بسبب نقص المهارة في استخدام الحاسوب وشبكات الإنترنت, وعدم المعرفة بأسباب ارتكاب الجرائم الإلكترونية, وأيضاً بسبب بقاء الخبرة في مجال التحقيق, وضعف المعرفة بالغة الجنائية, السيما أن العاملين في مجال الحاسوب وشبكات الإنترنت لديه مصطلحات علمية خاصة, وأيضاً تنوع المجالات التقنية وتوسعها, الأمر الذي يترتب عليه تحتاج كل نوع من أنواع الجهزة التقنية إلى اجراءات تحقيق

[110] حاجسودي محمد: المرجع السابق, ص276.

جرائم تختلف[111], وأيضاً من ضمن الإشكاليات التي تتقبل ورفي هذا المرتنازع الاختصاص وضعف التعاون الدولي بين الدول والكم الهائل للبيانات يشكل صعوبة في إجراء التحقيق.

2.7.2.1 تنازع الاختصاص بالتحقيق في الجرائم الإلكترونية

وهذا يعني أن كثير من التحقيق في الجرائم الإلكترونية تكون متعلقة بطابع العابر للحدود الدولة, بالإضافة إلى السلوك الجرامي الذي يتجرد من الطابع المادي إلى الطابع الافتراضي الرقمي, وهذا ما يجعل من الجريمة الإلكترونية الرتكب في إقليم دولة أخرى ونتيجته في دولة اخرى تنازع في الاختصاص وتعدد الإقليمية لها, خاصة وقد أجمع الفقه على أنه لا يجوز لأجهزة الأنظمة التابعة للدولة اللجوء إلى التحقيق أو التفتيش العابر للحدود من أجل البحث عن المعلومات أو البيانات المخزنة داخل حاسوب متواجد في إقليم دولة أخرى, كون القول بغير ذلك يشكل انتهاك لسيادة الدول وقوانين الدولي الذي يقضي بعدم التدخل في شؤون الداخلية للدول[112].

2.7.2.2 ضعف التعاون الدولي بين الدول

الشك أن ضعف التعاون الدولي بين الدول في مجال البحث والتحري والتحقيق في الجرائم الإلكترونية, يؤدي إلى زيادة الجرائم الإلكترونية وتشجيع المجرمين على ارتكاب الجرائم العابرة للحدود[113]. وأيضاً يؤدي عدم التعاون الدولي إلى زيادة القيود على تبادل المعلومات عبر الحدود

---

[111] محمد محي الدين عوض: المرجع السابق, ص640.

[112] بلراوي جمال: المرجع السابق. ص182 وما بعدها.

[113] الباغث, جمال, and يوسف."صعوبات التحقيق في الجرائم الإلكترونية." مجلة الرسالة للدراسات والبحوث الإنسانية 6.3)2021(: 70-83.

الدول مما يعطي المجرمين الفرصة الكافية من الوقت وزيادة أنشطتهم الإجرامية فتتعاون الدول فيما بينها في التحقيق والتفتيش من أجل القبض على الجناة والوصول للجناة، لذلك تتضمن اتفاقية بودابست مجموعة من الإجراءات الخاصة بالتحري ومطابقة الاتفاقية العربية، والتي تضمنت نقاط هامة تتمثل في سرعة التحفظ على بيانات الحاسوب المخزنة وواجبات مقدمي الخدمات على التزويد بالمعلومات المطلوبة، وتفتيش وحجز بيانات الحاسوب المخزنة، وأيضاً التجميع الفوري لبيانات الحاسوب[114] وتقديم المعلومات غير المكتملة بالمعلومات، وطلبات المساعدة القانونية المتبادلة وتشكل هذه الاتفاقيات المصدر الأول للقوانين التي تتشمل الحقوق والتزامات الأطراف في الاتفاقيات[115].

إلا أنه وبالرغم من وجود اتفاقيات وضرورة من اداتها هي وجد مثل هذه الاتفاقيات تحول دون ذلك وتجعل من التعاون صعب الحدوث وتتمثل تلك التحديات.

---

[114] فاجي يوسف، الإطار الإجرائي للدليل في مجال البحث عن الجريمة الإلكترونية، مجلة الحقوق والقانون، ص186. أشار إليه لدى أدم بلس من مرب غدادي: وسائل البحث والتحري عن الجرائم الإلكترونية، رسالة مقدمة لنيل درجة الماجستير في القانون العام الخاص، الجامعة الافتراضية الوطنية- نابلس فلسطين، سنة 2018، ص84.

[115] والاتفاقيات الدولية تعطي للدول سهولة في تبادل أدلة الإثبات الإلكترونية، وتشمل شكل التعاون المساعدة القانونية المتبادلة بين الدول، والإجراءات تعجيل المساعدة، وحفظ بيانات الحاسوب، والمساعدة في ضبط البيانات الحاسوبية، والوصول إليها وجمعها والإفصاح عنها، وأيضاً تساعد تلك الاتفاقيات في الوصول إلى البيانات العابرة للحدود ومن شكل التعاون ما يلي:

الأمم المتحدة لبروتوكول الاتجار بالبشر خاصة بالنساء والأطفال يكمل أن يبيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية سنة 2000.

كومنولث الدول المستقلة يتفاق بشأن التعاون في مكافحة الجرائم في مجال المعلومات الحاسوبية سنة 2001.

مجلس أوروبا، اتفاقية الجريمة السيبرانية والبروتوكول الإضافي الاتفاقية الجريمة السيبرانية المتعلق بتجريم أعمال العنصرية وكراهية الأجانب المرتكبة بواسطة النظم الحاسوبية سنة 2001؟

اتفاقية أوروبا بشأن حماية الأطفال من الاستغلال الجنسي والاعتداء الجنسي 2007.

الجامعة القصاية الدول الغربية)الكواس(، مشروع اتفاقية بشأن مكافحة الجريمة السيبرانية داخل إقليم الكواس سنة 2019. جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم التقنية المعلومات سنة 2010. مؤتمر الأطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: المرجع السابق، ص10.

2.7.2.3 عدم وجود نموذج موحد للنشاط الإجرامي يقنن وينظم القانون الجزائية

ويرجع ذلك إلى أن النظم القانونية والقضائية في الدول بشأن مواجهة الجرائم الكترونية الي وجد فيه اتفاق عام تشترك حول نماذج معينة تنص على اساءة استخدام شبكة الانترنت ونظم المعلومات التي يجب تجريمها فيتفق ويكون ما هو مباح في بعض الدول مجرماً في دول اخرى, وهذا يرجع بدوره إلى العادات والتقاليد والديانات السماوية وتوقف كل مجتمع عن الآخر[116].

عدم وجود نماذج موحدة للنشاط الإجرامي يؤدي إلى خلل النظم القانونية الإجرائية حيث طرق التحري والتحقيق ومرحلة المحاكمة التي تكون له فعالية في دولة ما, قد تكون عديمة الفائدة في دولة أخرى, أو قد يكون الدليل مشروعاً وفقاً لقانون دولة ما, كما هو الحال في بعض الدول التي تسمح بالتنصت الالكتروني, وهذه ما يؤدي إلى خيبة أمل جهات التحقيق في نظام الدولة عدم قدرته على تطبيق القانون في دولة أخرى, هذا وأيضاً قد تسمح السلطات القضائية لدى الدولة الثانية من استخدام أدلة إثبات تم جمعها بطرق تراها أنها غير مشروعة, حتى وان كان الحصول عليها بسبب الخصوصية الدولة الأخرى مشروعاً. وتعتبر قضية الدودة الحاسوبية (الفيروس) لوفباغ التي ظهرت في سنة 2000, قد قيل أنها دمرت ملايين الأجهزة الكترونية في مختلف أنحاء العالم, خير مثال على خلل النظم القانونية بين الدول, كون هذا الأخير التحقيق اتسبب بسبب عجز هيكل هذا العمل مجرماً في الملايين[117].

---

[116] حاجسودي محمد: المرجع السابق, ص279.

[117] صغيري يوسف: المرجع السابق, ص134.

2.7.2.4 صعوبة المساعدة القضائية الدولية

أحياناً قد تتعقد إجراءات التحقيق إلى خارج إقليم الوطني بهدف الحصول على أدلة مخزنة في حاسوب تتواجد في إقليم دولة أجنبية, وتحتاج هذه الإجراءات سرعة وقد لا يجدي البدء أن تتم في إطار المساعدة القضائية, وذلك عن طريق إنابة القضائية الدولية ويكون ذلك عن طريق قيام الجهات القضائية بأعطاء إنابة للسلطات القضائية المطلوب منها اتخاذ إجراء معين لتحقيق مصلحة الدولة الطالبة, وقبل ذلك يتم إعمال مثل هذه الإنابة القضائية الدولية بطريق رسمية دبلوماسية, والإنابة القضائية تواجه مشكل التباطؤ من الدولة المطلوب منها في حصل طلب المساعدة والرد عليه, وأيضاً قد تفرض الدولة القضائية في الجرائم السياسية والجرائم التي تمس سيادة الدولة ومصالحها الأساسية[118].

تبرز المساعدة القضائية بسبب وذلك في تنازع الاختصاص في جرائم الإنترنت وعدم وجود قنوات اتصال التسريع لحاجات القائمة على التحقيق بالنص البحث رأي تجمع الأدلة والمعلومات الهامة, وعدم وجود هذا النظم يؤدي إلى عدم القدرة على جمع الأدلة والمعلومات وبشأن تنازع الاختصاص القانوني فيكون ذلك بسبب اختلاف التشريعات والنظم القانونية من دولة أخرى[119].

على صلب من ضروري وجود تعاون دولي من أجل مكافحة الجرائم المالكترونية وتعاد اتفاقية مجلس أوروبا بخصوص الجريمة الإلكترونية التي صدرت في بوابست عام 2001م أول اتفاقية دولية في مجال مكافحة الجرائم المعلوماتية حيث تتقوت بين سياسات التشريعات الوطنية لدول المجلس في ذلك السياق وتحسين تقنيات التحري التالي جنائية حول رتكاب الجريمة المالكترونية وتعزيز التعاون

[118] إبراهيم جمال: المرجع السابق, ص237.

[119] حاجسودي محمد: المرجع السابق, ص280.

بين دول مجلس التعاون الخليجي في مجال المكافحة لهذه الجريمة وتم قرار الاتفاق في فيينا نص على عدة أوجه أهمها إيجاد الفهم الموحد لمصطلحات القانونية الأساسية والتي تقوم عليها إذا التعاون القضائي بين الدول أطراف هذه الاتفاقية, كما مصطلحي الإنابات بين الجهات الحاسوب, تنفيذ الإنابات هناك حق وقال تشرع وجرائم المتعلقة بالحاسوب والتحقيق الذي يستغل المرفق يل أل ظ ال[120].

وكيف يكون تحديد أماكن يل رقمي يستحصل عليه بطريقة شرعية تجيب الباحث نظم القانونية الخاصة بتلك الدول في الجرائم العابرة للحدود, خاصة وأن هذا الذي يصل بحظ امرة جديدة في الجهات الجنائي, البد أخذ بعين الاعتبار, كون القواعد الإجرائية التقليدية لمتعلقة يل حل الشكليات التي تعيق الجرائم المالكترونية فقد جرم المشرع المارتي الجرائم المالكترونية وذلك بفرض قانون خاص به من أجل مكافحة الجرائم المتعلقة بتكنولوجيا وسائل علمية جديدة تساعد في كشف الغموض عن هذه الجرائم وتساعد الجهزة القضائية في الحصول على أدلة[121].

على فأن أبرز المشاكل الجوهرية تمثل في الباحث التحري التحقيق في الجرائم المالكترونية, عندما تكون الجريمة مرتكبة عبر شبكات الإنترنت ووجود الجاني في دولة أخرى عن التي يوجد بها الضحية وهناك تشاف الذي الجنائي في تخيار القانون واجب التطبيق على الجريمة.

---

[120] أيمن سالمة: لمانيا صعب التعاون الدولي في مجال مكافحة الجريمة السيبرانية, مقال منشور بتاريخ الأربعاء 2021م بأبو ظبي, عربية نيوز, www.skynewsarabia.com تاريخ الزيارة 2023/1/4م.

[121] أيمن سالمة: المرجع السابق نفسه.

نوقش هذا الفصل في انوتجيد المشترك التجزئي الفعلي الذي ينبثق عن الجزاءم الكترونية من خلال تعريف القصود بالجريمة الكترونية وأنواعها ولكذلك تبيان خصائص الجريمة الكترونية خصة الوقاعة على النظام ذات هكونها جريمة عابرة للحدود ليس لها أثر مادي كما نوقش هذا الفصل الطبيعة القانونية وأركانها المادي والمعنوي ولكذلك الشرعي، علاوة على ذلك يبين هذا الفصل الفرق بين الجريمة الكترونية والتقليدية والشكل الموضوعية والجزئي للاتجاه عن الجزاءم الكترونية مما يتم الإجابة على سؤال البحث الول ولكذلك تحقيق هدف البحث ألول.

Universiti Utara Malaysia

الفصل الثالث / CHAPTER THREE
تحليل نصوص المرسوم رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 المتعلق بمكافحة جرائم تقنية المعلومات

سيحاول الباحث الضوء في هذا الفصل على قانون الجرائم الإلكترونية في إمارة دبي رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016"، من خلال تحليل جميع المواد التي تناولت بشكل مباشر النصوص المتعلقة بالجرائم الإلكترونية والجزاء المقرر لها في دولة الإمارات. لمعرفة مدى نجاح أو فشل المشرع الإماراتي في تنظيم ومعالجة الجريمة ذات الطبيعة الإلكترونية في هذا الفصل تم الإجابة على سؤال الباحث الثاني وتحقيق هدف الباحث الثاني.

3.1 قانون الجرائم الإلكترونية

من الجدير بالبيان هنا في هذا المقام أن المشرع في دولة الإمارات العربية المتحدة قد فرض نظاماً قانونياً خاصاً تمثل أن مكافحة الجرائم التقنية والمعلومات رقم (5) لسنة 2012 والمعدل بقانون اتحادي رقم (12) لسنة 2016 والذي حدد من خلال الشيء أنواع الجرائم الإلكترونية تمثل العصرياً فرض جزاء على ارتكاب كل نوع منه وذلك بموجب القانون الذي على الأساس المشدد الذي يعاقب أو توقيفها وذلك ضمن نظام قانوني خاص متمثل مشرح مثل الفصل.

في المادة الثانية[122] من مشروع القانون تحدث عن جريمة دخول الموقع الإلكتروني أو نظام المعلومات بدون تصريح بوسيلة غير مشروعة بقصد تفادي العقوبة بالحبس والغرامة على كل شخص قام بالدخول الى موقع إلكتروني او نظام معلومات الكتروني او شبكة معلومات بدون اذن او تصريح وكذلك فرضت عقوبة الحبس أو الغرامة في حال الغاء او حذف او تدمير او افشاء او اتلاف او تغيير او نسخ او نشر او اعادة نشر اي بيانات او معلومات.

يظهر لنا من خلال ذلك النص كل شخص قام بدخول موقع إلكتروني غير مسموح بدخوله, دون الحصول على اذن بذلك أو تخطى صلاحياته أن ولتكب جريمة يعاقب عليها القانون, وشدد القانون في تلك العقوبة اذا ارتكبت من قبل شخص يعمل كمسؤول عن حماية ذلك الموقع وترجع العلة في ذلك بأنه يعلم جيداً أن فعلته هذا غير مسموح به, وهي أيضاً أن فعلته هذا تشكل جريمة ومعاقبة عليها.

Universiti Utara Malaysia

[122] نصت المادة 2 على (1 يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكتروني أو شبكة معلومات ، أو وسيلة تقنية معلومات ، بدون تصريح أو بتجاوز حدود التصريح ، أو بالبقاء فيه بصورة غير مشروعة .

2 تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها في الفقرة 1 من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

3 تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة 2 من هذه المادة شخصية(.

في المادة الرابعة[123] من هذه النظمت أحكام دخول الموقع الإلكتروني لغرض الحصول بيانات حكومية وعلومات سرية قبل منشأة العامة أو تجارية أو بقصد ربحي تفرض عقوبة تتمثل في السجن والغرامة التي العلى كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، بقصد الحصول على بيانات حكومية، أو معلومات سرية قبل منشأة العامة، أو تجارية، أو بقصد ربحية.

وتكون العقوبة السجن مدة التقل عن خمس 5 سنوات والغرامة التي التقل عن خمسمائة ألف درهم والتجاوز 2 مليون درهم، إذا تعرضت هذه البيانات أو المعلومات إلى إلغاء أو الحذف أو إتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر. هذا في ظل أن التجارة الإلكترونية أصبحت عاملاً مؤثراً في نمو اقتصاد البلدان وازدهار تجارتها الداخلية والخارجية، لذلك كان من ضروري أن يتم حماية التجارة الإلكترونية, فرض عقوبة على من يعرقل لها[124].

في المادة الخامسة من نصت على دخول موقع إلكتروني دون تصريح بقصد تغيير تصميمه أو إتلافه أو تعديله أو إلغائه:

بحيث فرضت عقوبة تتمثل في الحبس والغرامة التي التقل عن مائة ألف درهم والتجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه".

---

[123] نصت المادة 2 على يعاقب بالسجن المؤقت والغرامة التي التقل عن مليون وخمسين ألف درهم والتجاوز مليون وخمسمائة ألف درهم كل من دخل بدون تصريح إلى موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، سواء كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية).

[124] مجلة الحقوق للعلوم القانونية والسياسية: معوقات التجارة الإلكترونية ومتطلبات النظام القانوني لمواجهتها (دراسة مقارنة) - العدد الثاني - السنة التاسعة 2017م, ص674.

ويتضح من ذلك النص أن المشرع فرض حماية للموقع من التلاعب غير المشروع الذي يؤدي إلى تدميرها أو حذفها عن طريق الغاء عملها, وفرض عقوبة جنائية على من يقوم بذلك الفعل.

في المادة السادسة نظم أحكام تزوير المستندات الكترونية:

بحيث فرضت على كل من قام بتزوير مستند الكتروني أو قام بتعديله وكان على علم بأنه مزور, حيث يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مئة وخمسون الف درهم ولا تجاوز سبعمائة وخمسون الف درهم كل من زور مستنداً الكترونياً من مستندات الحكومة الاتحادية او المحلية او الهيئات او المؤسسات العامة الاتحادية او المحلية.

في المادة السابعة نصت على فلشاء علوم انفاح وصات بطيبة غير تصريح:

بحيث تعتبر هذا من الجرائم الالكترونية التي تم بفلش المعلومات البطية وتلك الخاصة بالمرضى أو تدعو له أو غيرها أوات الف ملي حيث فرضت عقوبة تمثل في الحبس بالسجن المؤقت كل من حصل او استحوذ او عدل او اتلف او فلش بغير تصريح بيانات اي مستند الكتروني او علوم الكترونية عن طريق الشبكة العلوماتية او موقع الكتروني او نظام المعلوم الالكتروني لوسيلة تقنية علومات وكانت هذه البيانات او المعلومات تتعلق بفحوصات بطية او تشخيص طبي، او علاج او رعاية بطية او سجلات بطية". ويقع ذلك على كل شخص قام بالتلاعب بفلشاء علومات بطية تخص احد المرضى أو قام بأتلافها, وهنا المشرع فرض حماية خاصة لموارد المرضى البطية[125].

[125] سيف تبو مروان: الحكومة الالكترونية ودرها في تحسين أداء إدارات الحكومية, ط1, مكتبة القانون والاقتصاد, الرياض, سنة 1435 هـ 2014م, ص205

في المادة الثامنة جاءت تنظم أحكام التحايل على الوصول الى شبكات المواقع الكتروني و نظام المعلومات الكتروني:

بحيث فرضت جزاء على كل من يقوم بالتحايل على الوصول إلى شبكات المواقع الكترونية بهدف حرمان الغير من الوصول إليها أو بهدف تنفيذ جريمة مما يحيث يُعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تتجاوز الثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من اعاق او عطل الوصول الى شبكة معلومات او مواقع الكتروني او نظام معلومات الكتروني".

المادة التاسعة جاءت تنظم جريمة التحايل على العنوان البروتوكولي للشبكات:

بحيث يعاقب أمام القانون بالحبس على العنوان المواقع الكتروني بهدف ارتكاب جريمة او الحيلولة دون اكتشافها جريمة يعاقب عليه القانون يُعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمس مائة ألف درهم ولا تتجاوز مليوني درهم، أو بإحدى هاتين العقوبتين، كل من تحايل على العنوان البروتوكولي للشبكة المعلومات باستخدام عنوان وهمي أو عنوان لطرف الغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها"وتكون جريمة التحايل عن طريق التحايل على النظام المعالجة الآلي للبيانات, سواء يتفق فيه سبب جريمة الوصول بطريق التحايل, وهذه الجريمة مستحدثة[126].

المادة العاشرة نظمت عقوبة الدخال عمداً وبدون تصريح إلى الشبكة المعلومات احدى وسائل تقنية المعلومات واغراق البريد الالكتروني بالرسائل بقصد التعطيل او الايقاف اوالاتلاف:

[126] بلراهيم رمضان بلراهيم عطيا: المرجع السابق, ص376.

بحيث فوضت عقوبة على كل من يرتكب ذلك تتمثل بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين[127].

المادة الحادية عشرة نصت على عقوبة السعي بغير حق على مال منقول أو منفعة أو على سند:

ويعتبر أن كل من يقوم بجريمة السعي على الأموال المنقولة أو السندات أو المنفعة من المشتراك في الموقع العلوم يتم بطريقة احتيالية يعاقب وفقاً لقانون العقوبات بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مليون وخمسين ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من تحول لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق شبكة المعلومات أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات".

يتضح لنا من خلال هذه المادة أن هدف المشرع من وراء وضع هذا النص هو تجريم الاستعانة بالحاسب الآلي لتحويل الأموال المنقولة, والتي يترتب جزاء على كل من قام بالحصول على الأموال بطريقة غير مشروعة[128].

---

[127] نصت المادة 10 على يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز ثلاثة ملايين درهم أو بإحدى هاتين العقوبتين كل من ادخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات ، وأدى ذلك إلى إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات .

وتكون العقوبة السجن والغرامة التي لا تتجاوز خمسمائة ألف درهم أو إحدى هاتين العقوبتين إذا ما تحقق النتيجة .

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين عن أي فعل عمدي قصد به إعاقة البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته(.

[128] لبراهيم جمال: المرجع السابق, ص115.

المادة الثانية عشرة تحدث عن أحكام استخدام الحاسب الآلي للحصول على معلومات وأرقام بطاقات ائتمانية الكترونية أو حسابات مصرفية:

وتعد هذه من ضمن الجرائم التي تقع على المال حيث فوضت عقوبة على أي شخص الحبس والغرامة أو إحدى تلك العقوبتين لكل من توصل بغير حق، عن طريق استخدام الشبكة العالمية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني[129].

المادة الثالثة عشرة نظمت أحكام تزوير أو تقليد أو نسخ أو استعمال بطاقات الشبكات عبر الإنترنت بسوء استخدام:

سيما أن هذه تعتبر من ضمن الجرائم التي تسبب الأموال والتي يهدف من وراءها الجاني إلى السرقة بسوء استخدام بطاقة ائتمانية شخص أخر أو بطاقة وهمية أو تقليدها أو القيام بعملية نسخ واحدة عنها, فوضت عقوبة مثل الحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم أو إحدى تلك العقوبتين لكل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة،

---

[129] نصت المادة 12 على عقوبة الحبس والغرامة أو إحدى هاتين العقوبتين لكل من توصل بغير حق ، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات ، إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية ، أو أي وسيلة من وسائل الدفع الإلكتروني .

وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم ولا تتجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين ، إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير ، أو الاستفادة مما تتيحه من خدمات .

فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين .

ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني(.

او اوسيلة اخرى من وسائل الفعل الالكتروني، وذلك بسبب استخدام احدى وسائل تقنية المعلومات، او ببرنامج معلوماتي وي عقوبة ذات الغرامة كل من: 1- صنع او صمم اوسيلة من وسائل تقنية المعلومات، اوبرنامج معلوماتي، قصد استعماله اي من الافعال المنصوص عليها في الفقرة الاولى من هذه المادة. 2استخدم بدون تصريح بطاقة ائتمانية الكترونية اوبطاقة مدينة او اي وسائل اخرى للفعل الالكتروني بقصد الحصول لنفسه او لغيره، على اموال او اموال الغير او الاستفادة مما تقدمه من خدمات يقدمها الغير. 3قبل التعامل بهذه البطاقات المزورة او المقلدة او المنسوخة اوغيرها من وسائل الفعل الالكتروني مع علمه بعدم مشروعيتها".

ويظهر لنا من خلال هذا النص أن المشرع الماليزي قد تضمن طوي بطاقات الشيكات عبر الموقع الالكتروني, أي بطاقات الائتمان والصرف الآلي, وذلك بتزويرها أو تقليدها أو نسخها[130].

المادة الرابعة عشر[131] بينت أحكام الحصول على رقم سري او شفرة او كلمة مرور للدخول إلى الموقع الالكتروني، وتعتبر دخول الشخص إلى الموقع الالكتروني عن طريق الكلمات المعلومات بهدف الحصول على البيانات والشفرة الخاصة بذلك الموقع دون الحصول على اذن بذلك جريمة من ضمن الجرائم التي تقع على المعلومات حيث فرضت عقوبة على ذلك تمثلت بالحبس والغرامة

[130] مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة : الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها, سلسلة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية فائز بالمركز الأول في المسابقة, مجلس التعاون لدول الخليج العربية- 2016, ص7.

[131] نصت المادة 14 على يعاقب بالحبس والغرامة التي تقل عن خمسين ألف درهم والتي تزيد على خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من حصل بدون تصريح ، على رقم سري أو شفرة أو كلمة مرور أو أي وسيلة أخرى للدخول إلى وسيلة تقنية معلومات ، أو موقع إلكتروني ، أو نظام معلومات إلكتروني ، أو شبكة معلوماتية ، أو معلومات إلكترونية .
يعاقب بذات العقوبة كل من اعد أو صمم أو انتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات ، أو روج أي طريقة ربط موقع إلكتروني أو برنامج معلوماتي ، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون(.

اوبإحدى تلك الجرائم على كل من حصل عليه دون ترخيص، على رقم سري او شفرة او كلمة مرور او اي وسيلة اخرى للدخول الى وسيلة تقنية تحتوي على معلومات، او موقع أو نظام كمبيوتر، ، للوصول الى بيانات.

المادة الخامسة عشر التقاط او اعتراض النصوص الكترونياً:

هذا وأن المشرع الاماراتي قد اعتبر أن التقاط النصوص الكترونية دون الحصول على اذن مسبق بذلك جريمة معاقب عليها وفقاً للقانون والذي فرض عقوبة تتمثل في الحبس والغرامة التي لا تقل عن مائة وخمسين الف درهم ولا تجاوز خمسمائة الف درهم اوبإحدى تلك العقوبتين كل من التقط او اعترض عمداً وبدون ترخيص اي نص الكتروني عن طريق الشبكة المعلوماتية. فإنقلاشى اي شخص المعلومات التي حصل عليها عن طريق قراءة الرسائل او اعتراض النص الالكتروني بغير وجه حق فإن يعاقب بالحبس مدة لا تقل عن سنة واحدة".

Universiti Utara Malaysia

المادة السادسة عشر والتي تحدثت عن الابتزاز او تهديد شخص لحمله على الفعل او الامتناع عنه:

نجد أن المشرع الاماراتي قد تطرق لسلوك الجرائم التي تحدث تحت الجريمة الالكترونية, ولم يتطرق أيضاً لسلوك الجرائم التي تحدث, كما هو الحال أن يقوم موظف أمن المعلومات عن حماية الذي يتحت حمايته, دون وجه حق أو اذن مسبق, والتي فرضت عقوبة تتمثل أنه يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن مائتين وخمسون الف درهم ولا تجاوز خمسمائة الف درهم او بإحدى تلك العقوبتين كل من ابتز او هدد شخص اخر لحمله على الفعل او الامتناع عنه وذلك بواسطة شبكة المعلومات او وسيلة تقنية المعلومات وتكون العقوبة السجن مدة لا تزيد على عشر سنوات اذا كان الابتزاز مصحوباً بجريمة او بإسناد امور خادشة للشرف او الاعتبار".

ومن خلال ذلك يتضح أن الابتزاز الالكتروني تهدف إلى تدمير بيوت وهدم إلى طرح قيم وانتشار صور أفلام وهمية أو تسريب معلومات سرية لتلك التي تخص الضحية, وقد يصل فعل مبالغ المالية أو استغلال الضحية لتلك التي اهب أعمال غير مشروعة لصالح المبتز[132].

المادة السابعة عشر[133] تطرق الحكام إلى إعداد أو توزيع أو نشر أو إعادة نشر مواد إباحية أو نشاط قمار، ويمكن تصنيف هذا النوع من الجرائم التي تقع على الشخاص والتي تؤدي بهم إلى الانحراف وتشكل مسلسلاً آلداب العامة, فوضت جزاءات مختلفة يلي الحبس كل من أنشأ أو أدار موقع الكتروني أو نشر فعليه أو بث أو أرسل أو نشر أو أعاد نشر عن طريق شبكة المعلومات مواد إباحية أو نشاط قمار، وكل ما من شأنه المس بآداب العامة.

المادة الثامنة عشر والتي نصت على جرائم حيازة مواد إباحية الحداث عمداً:

وتكون هذه الجرائم من ضمن الجرائم التي تقع على الشخاص والتي تشكل أكثر خطورة من الجرائم الواقعة على المال الغير, فرضت جزاءات مختلفة يلي عقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تتجاوز مليون درهم كل من حاز عمداً مواد

---

[132] بالل جراجرة: الابتزاز الالكتروني بدون نشر, سنة 2019, ص14.

[133] نصت المادة 17 يعاقب بالحبس والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقع الكتروني أو نشر فيه أو بث أو أرسل أو نشر أو أعاد نشر عن طريق الشبكة المعلوماتية مواد إباحية أو أنشطة قمار، وكل ما من شأنه المس بآداب العامة.

يعاقب بالعقوبة ذاتها، كل من أنتج أو أعد أو هيأ أو أرسل أو خزن بقصد الاستغلال أو لتوزيع أو لعرض على الغير، عن طريق شبكة معلوماتية، مواد إباحية أو أنشطة قمار، وكل ما من شأنه المس بآداب العام.

فإذا كان موضوع المحتوى الإباحي حيث لا تجاوز الثامنة عشر من عمره، أو كان يشمل هذا المحتوى مصمما لإغراء الحداث فيعاقب الجاني بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن خمسين ألف درهم ولا تتجاوز مائة وخمسين ألف درهم).

إباحية الأحداث بسبب استخدام نظام المعلومات الإلكتروني، أو شبكة المعلومات، او من الإلكتروني، أو إحدى وسائل التقنية المعلومات".

يبين لنا أن المشرع قد نظم سائر الأشكال الاعتداء الجنسي حيث شمل كل من قام بحيازة صور أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو فعلاً جنسية حقيقية أو بالمحاكاة حدث الأحداث أو من عمره يقل عن ثمانية عشر سنة ويعاقب بحبس مدة لا تقل عن عامين.

المادة تسعة عشر نص على جرائم الغواء والتحريض على ارتكاب الدعارة او الفجور:

بحيث أوجبت عقوبة تتمثل في الإعدام بالسجن والغرامة التي لا تقل عن ثلاثين وخمسين ألف درهم والتي تجاوز مليون درهم او بإحدى هاتين العقوبتين كل من حرض او أغوى آخر على ارتكاب الدعارة او الفجور او ساعد على ذلك بسبب استخدام شبكة المعلومات او إحدى وسائل التقنية المعلومات. وتكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تتجاوز مليون درهم إذا كان المجني عليه حدث لم يتم الثامنة عشرة من عمره".

ويعتبر التحريض والغواء بسبب استخدام موقع التواصل الاجتماعي أو عبر الشرعي على الموقع الإلكتروني تو تخصيص له للدعارة والفجور من ضمن الجرائم التي تزعزع استقرار المجتمع والمساس بأمن الدولة الداخلي[135], وفوق ذلك النص سابق الذكر أن كل فعل يقوم به الجاني من عرض مشاهد غير أخلاقية, من خلال اختراق اجهزة الحاسوب يعتبر طائل العقاب كونه يؤثر على المجتمع

[134] عادل الدغمشي العجمي: المرجع السابق, ص92.

[135] شرف الدين وردة وباجراف سامية: الجرائم الماسة بالمصلحة والجريمة المخلة بالمصلحة جريمة المساس بالنظام في التشريع الجزائري, مجلة الدراسات الحقوق والدراسات القانونية والسياسية, العدد الثالث سبتمبر 2017, ص27.

بشكل عام وعلى المرفق بشكل خاص وتعد هذه من الجرائم التي تمس الداب العامة والأمن القومي[136].

المادة غير ونوالتي نصت على سبّ الغير وجعله محالًا للعقاب او الزدراء من قبل الخرين:

وتتعبر هذه الجريمة من ضمن الجرائم الوقاع على الشخاص السب والقذف لآخرين, والتي فوضت جزاءات مثلفي "مع عدم إلخال لبأحكام جريمة القذف المقرر في الشريعة الإلامية، يعاقب بالحبس والغرامة التي الهتقل عن ستين وخمسين الف درهم والتجاوز خمسمائة الف درهم اوبإحدى تهاتين العقوبتين كل من سب الغير اوأسند إليه وقاعة من شأنها انتجعله محالًا للعقاب او الزدراء من قبل آلخرين، وذلك لسبت خدشبك ةمعلومتاية، اوسيل قتقنية عل ومات فإذا قع السب او القذف في حق موظف عام أومكلف بخدمة عام بمناسبة اوبسبب تأدية عمله عد ذلك ظرفا شددالجريمة". وهذا ما فوضت به المحكمة الإتحادية في المغرب بموجب المتهم عن تهمة السب والقذف عبر موقع التواصل الجتماعية, ونظراً لعدم وجود سوابق قضائية لها قضت بمحاكمتها مع وقف التنفيذ[137].

---

[136] بيام محمد لهادي بتعرض لمراقبين الجرائم الالكترونية عبر وسائل الإعلام الرقمي وتأثيرها على ادراك مم لأمن الجتماعي المصري, المجلة العربية للبحوث الإعلام والتصال –العدد 30 يوليو /سبتمبر سنة 2020, الجمعية الدولية لضمان وعية- جامعة قبنها-مصر, ص837.

[137] المحكمة الإتحادية في المغرب: لمفشكاية بمشرة عدد 86/2902/18, حكم عدد 21062, صدر بتاريخ 2018/7/19م.

المادة الحادية والعشرين[138] والتي نصت على جرائم الاعتداء على خصوصية الأشخاص بحيث اعتبرت الاعتداء على خصوصية الأشخاص في غير الأحوال المصرح بها قانوناً من ضمن الجرائم التي يقع على الأشخاص بسبب استخدام موقع التواصل الاجتماعي والمواقع الالكترونية مثل كل عام, فرضت عقوبات مثل الحبس والغرامة على كل من استخدم شبكة معلوماتية، او نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً.

فوفق ذلك فأن المشرع في دولة الامارات العربية المتحدة قد نظم أحكام الخصوصية فرض جزاء على كل من يرتكب الخصوصية فالا يجوز لأي شخص الأي إمام بالتقاط صور لأي غير أو الأي إمام بنشرها, أو الأي إمام نشر أخبار عنه حتى وان كانت حقيقة, إلا بعد الحصول على موافقة كتابية من

Universiti Utara Malaysia

[138] نصت المادة 21 على يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلومات ، أو نظام معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بإحدى الطرق التالية :

1 - استراق السمع ، أو اعتراض ، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية .

2 - التقاط صور للغير أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها .

3 - نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية .

كما يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسون ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين ، كل من استخدم نظام معلومات إلكتروني ، أو إحدى وسائل تقنية المعلومات ، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد بقصد التشهير أو الإساءة إلى شخص آخر ، أو الاعتداء على خصوصيته أو انتهاكها(.

قبل صاحب الشأن[139], وغير ذلك يعتبر تعدي على الحقوق الشخصية لذلك غير ذلك فوق القواعد العام في القانون المدني الماليزي[140].

المادة الثالثة والعشرين تنص على استخدام شبكة معلوماتية والموقع الكتروني أو سيلة تقنية دون الحصول على اذن مسبق:

بحيث يعتبر أن كل من استخدم أو استعمل شبكات المعلومات وموقع الكتروني دون الحصول على اذن مسبق بهدف الكشف عن بيانات تلك الموقع ارتكب جريمة يعاقب عليها القانون فوق الأمان صريح القانون وفي المادة 22 والتي تنص على أنه يُعاقب بالحبس مدة التقل عن ستة أشهر الى غرامة التي التقل عن خمسمائة الف درهم والتجاوز مليون درهم او إحدى تلك العقوبتين كل من استخدم، بدون تصريح، أي شبكة معلوماتية، او موقع الكتروني، او وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله او بسببه".

المادة الثالثة والعشرين تنص على انشاء أو ادارة موقع الكتروني أو نشر معلومات على شبكة معلوماتية تقتضي الاتجار بالبشر او العضاء البشرية:

بحيث فرضت جزاءات مثل في يُعاقب بالسجن المؤقت والغرامة التي التقل عن خمسمائة الف درهم والتجاوز مليون درهم او إحدى تلك العقوبتين كل من أنشأ أو أدار موقع الكتروني او

---

[139] شرف الدين وردة وباجر افسانية, المرجع السابق, ص29.

[140] نص المادة 90 من قانون المعاملات المدنية لدولة الامارات العربية المتحدة المقابل لنص المادة 1 من قانون الاتحادي رقم 5 لسنة 1985م والمعدل بالقانون الاتحادي رقم 1 لسنة 1987م الماليزي والتي تنص على أنه لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق اللازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر).

نشر فيه او نشر معلومات على شبكة معلوماتية او بإحدى وسائل تقنية المعلومات، بقصد الاتجار بالبشر او الأعضاء البشرية، الاستعمال في مصلحة غير مشروعة".

هذا وقد يهدف الجاني إلى تحقيق أرباح ومكاسب مادية, وذلك عن طريق الاتجار بالبشر والأعضاء البشرية, وقد تطور وذلك وأدى إلى تنامي الاتجار إلى مستوى الدافع للاتجار بالبشر[141].

المادة الرابعة والعشرين نصت على أحكام إنشاء او ادارة موقع الكتروني أو نشر معلومات بهدف الترويج او التسهيل ذلك كان من شأنه اثارة الفتنة او الكراهية او الضرر بالوحدة الوطنية والخلل بالآداب العامة:

بحيث تعتبر الشرع الأماراتي هذه الجريمة من ضمن الجرائم التي تمس أمن الدولة المترتبطة بالجرائم الواقعة على النظام المعلوماتي ذاته[142], وذلك وفق ما نص عليه القانون حيث فرضت جزاءات مثل في الحبس بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم والتجاوز مليون درهم لكل من أنشأ او أدار موقع إلكتروني او نشر فيه أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات التي تروج أو تسهل ذلك بما برامج او فكار من شأنه إثارة الفتنة او الكراهية او العنصرية او الطائفية او إلضرار بالوحدة الوطنية او السلم الاجتماعي او إلخلل بالنظام العام او الآداب العامة".

المادة الخامسة والعشرين نصت على عقوبة إنشاء او ادارة موقع الكتروني او نشر معلومات للإتجار والترويج بالأسلحة النارية والذخائر والمفجرات:

---

[141] مجموع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة: المرجع السابق, ص30.

[142] شريف الدين وردة وباجي افسانية, المرجع السابق, ص31.

وحيث تضمن هذه الجريمة من ضمن الجرائم التي تمس أمن الدولة، حيث جاء النص في بأنه يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن خمس مائة ألف درهم ولا تتجاوز مليون درهم، أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات على شبكة معلوماتية أو إحدى وسائل تقنية المعلومات بقصد الاتجار أو الترويج للأسلحة النارية أو الذخائر أو المؤثرات العقلية في غير الأحوال المصرح بها قانونا".

ويظهر لنا من خلال ذلك النص بأن ارتكاب الجرائم على خبرة وسلعة وتحقيق أرباح استطاع أن يطور من نفسه في مجال استخدام وجها من أجل ارتكاب جرائم بطريقة احترافية وخاصة جرائم الاتجار الإلكتروني بحيث يشمل بحث ذلك من يقوم على الترويج للأسلحة النارية إلى جانب المخدرات, كما هو الحال في جرائم الدعارة والترويج للدعارة[143].

المادة السادسة والعشرين[144] نظمت عقوبة إنشاء او ادارة موقع إلكتروني بحيث اعتبرت كل من قام بإنشاء موقع إلكتروني أو عمل على ادارته بطريقة غير مشروعة بقصد الترويج له وتسهيل عمليات ترويجه, وكذلك من نشر معلومات لجماعة إرهابية أرتكاب جريمة من الجرائم المنصوص عليها من الدول, فرض المشرع عقوبة لذلك تتمثل بالسجن والغرامة على كل من أنشأ او أدار موقعاً

[143] أحمد بولحية طيبي: الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي دراسة التجربتين السعودية والقطرية- ألكاديمية للدراسات الاجتماعية والإنسانية قسم العلوم القانونية والسياسية العدد 16- جوان 2016, ص188.

[144] نصت المادة 26 على يعاقب بالسجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مليون درهم ولا تتجاوز مليوني درهم كل من أنشأ أو أدار موقعا إلكترونيا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات ، وكذلك جماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقيادتها أو أعضائها ، أو الترويج لأفكارها ، أو تمويل أنشطتها ، أو تقديم المساعدة الفعلية لها ، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات ، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية(.

الإلكتروني أو الإشراف عليه أو نشر معلومات على شبكة المعلومات العالمية أو وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة تقصد بنشره إلى الناس الترويج لأفكارها أو أغراضها، أو استقطاب عضوية لها أو ترويج أو تبني أفكارها أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب صنع الأجهزة الحارقة أو المفجرات، أو أي أدوات أخرى تستخدم في الأعمال الإرهابية.

المادة السابعة والعشرين: تنظم أحكام نشر وإدارة موقع تدعو فيه إلى جمع تبرعات بدون ترخيص:

لقد جرم المشرع الإماراتي كل من قام بجمع التبرعات بطريقة غير مشروعة حيث يجب أن يكون جمع التبرعات وفق الأصول والطرق المقررة حيث لا بد من الحصول على ترخيص بذلك, ويكثر هذا النوع من الجرائم في الكوارث والحروب, بحيث يسعى المحتالون إلى إنشاء وابتكار الكترونية احتيالية للحصول على أموال بحجة أنها للتبرعات, وقد فرض المشرع عقوبة لكل من يقوم بذلك الأمر بحيث نص على أنه يعاقب بالحبس والغرامة التي لا تقل عن ثلاثين وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على شبكة المعلومات أو وسيلة تقنية معلومات أخرى للدعوة أو الترويج لجمع التبرعات بدون ترخيص مسبق من الجهة المختصة".

المادة الثامنة والعشرين: تنظم أحكام إنشاء موقع إلكتروني ونشر معلومات تمس أمن الدولة:

هذا وأيضاً تعتبر من ضمن الجرائم التي تمس كيان أمن الدولة قيام إنشاء موقع إلكتروني وإدارته ونشر معلومات تمس السيادة وتهدد أمنها وتمس النظام العام والاعتداء على مأموري الضبط

القضائي[145] وحيث نص القانون على كل من يقوم بذلك بالسجن المؤقت والغرامة التي لا تتجاوز مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو استخدم معلومات على شبكة المعلوماتية أو وسيلة تقنية معلومات بقصد الترويج على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام، أو الاعتداء على مأموري الضبط القضائي أو أي من الموظفين المذكورين".

وأيضاً يعاقب كل من قام بنشر معلومات أو أخبار أو إشاعات على موقع إلكتروني أو وسيلة تقنية معلومات أو الشبكة المعلوماتية بقصد السخرية والإضرار بلجنة الدولة ومؤسساتها, أو هاراتك بجريمة تمس أمن الدولة وتثير الفزع بين مواطنيها مما يشكل خطراً على الأوضاع الاجتماعية والثقافية وخاصة السياسية, وذلك وفقاً لنص المادة 29 والتي نصت على أنه "يعاقب بالسجن المؤقت والغرامة التي لا تتجاوز مليون درهم كل من نشر معلومات أو أخبار أو بيانات أو إشاعات على موقع إلكتروني أو الشبكة المعلوماتية أو وسيلة تقنية معلومات بقصد السخرية أو الإضرار بسمعة أو هيبة أو مكانة الدولة أو أي مؤسساتها أو رئيسها أو نائبه أو حكام الإمارات أو أولياء عهودهم أو نواب حكام الإمارات أو علم الدولة أو السلام الوطني أو شعارها أو نشيدها الوطني أو رموزها".

[145] مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: جمع وتبادل أدلة الإثبات الإلكترونية- ورقة معلومات أساسية من إعداد الأمانة في فيينا, 27, 28 تشرين الأول أكتوبر 2015, ص8.

وكذلك الحال في إنشاء المواقع الإلكتروني أو في نشر معلومات تهدف إلى قلب أو تغيير نظام الحكم في الدولة أو تعطيل أحكام الدستور والقانون أو في إفشاء أسرار القانون المعمول بها بموجب أحكام جريمة مس أمن الدولة, وذلك وفق النص المادة 30[146].

المادة الواحد والثلاثون والتي جاءت تنظم أحكام نشر معلومات تهدف إلى تحريض على قوانين الدولة: بحيث تعتبر الجريمة نشر معلومات تسعى من وراءها إلى تحريض الشعب على قوانين الدولة بهدف عدم احترامها أو التحريض على الجرائم التي تمس أمن الدولة, هذا بالرغم من عدم تصنيفها وفقاً لقانون رقم لسنة 2012 وتعديلاته لسنة 2016 و 2018 فإن نشر تلك المعلومات التي تمس قوانين الدولة والتحريض عليه جريمة وفق النص المادة 31 والتي تنص على أنه "يعاقب بالحبس والغرامة التي لا تقل عن خمسين ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من دعا أو حرض عن طريق نشر معلومات على شبكة المعلومات أو وسيلة تقنية معلومات إلى عدم الانقياد إلى القوانين وأنظمة المعمول بها في الدولة".

يلاحظ من نص المادة أن هذه الجريمة من ضمن الجرائم التي تمس أمن الدولة ولا تقبل جرائم الرأي أو الحروب الإلكترونية.

المادة الثانية والثلاثون جاءت من نظمة أحكام الدعوة أو التروج لمظاهرات وسرقة النصوص والتعرض للمقدسات الدينية:

---

[146] نص المادة 30 على "يعاقب بالسجن لمدة لا تقل عن سنة أو بغرامة لا تقل عن خمسين ألف درهم ولا تزيد على مليون درهم كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية أو وسيلة تقنية معلومات بهدف أو بقصد الدعوة إلى قلب أو تغيير نظام الحكم في الدولة أو الاستيلاء عليه أو إلى تعطيل أحكام الدستور أو القوانين السارية في البلاد أو المناهضة للمبادئ الأساسية التي يقوم عليها نظام الحكم في الدولة. ويعاقب بالعقوبة ذاتها كل من روج إلى أو حرض على أي من الأفعال المذكورة أو سهلها للغير".

الحقوق التي تنبع من الرأي العام من أسمى الحقوق الدستورية, التي يفرضها الشرع حماية خاصة, في اطار معين وفق النظام الحكم في الدولة وبطريقة سلمية, وغير ذلك فأن أي عمل يكون من شأنه الدعوة إلى عقد مظاهرات وذلك بقصد إحباط شرعية الممثلين الدستورية, كما هو حال الذي يبذل دان العاهل في الوقت الحاضر دون الحصول على ترخيص مسبق من الجهات المختصة يعتبر أنها ارتكب جريمة يعاقب عليها القانون وفق نص المادة الذي يقضي بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ او ادار مقر للكترونيا او أشرف عليه او استخدم شبكة المعلومات او وسيلة تقنية المعلومات لتنظيم المواجهة او الدعوة لمظاهرات او مسيرات او ملي حكم دون ترخيص من السلطة المختصة".

هذا وأضاف المشرع إحباط إنشاء او ادارة موقع الكتروني أو قام باستخدام شبكة المعلومات او وسيلة تقنية المعلومات لإتجار بالآثار او التحف الفنية دون حق, وذلك وفق النص المادة 33 والتي تنص على أنه يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم او بإحدى هاتين العقوبتين كل من أنشأ او أدار موقع إلكتروني او أشرف عليه او استخدم شبكة المعلومات او وسيلة تقنية المعلومات لإتجار بالآثار او التحف الفنية في غير الأحوال المصرح بها قانوناً".

ويعتبر من ضمن الجرائم الالكترونية التي مس سرقة خدمات الاتصال أو تمكين الغير من الانتفاع بذلك, دون وجه حق, وذلك وفق النص 34 والتي تنص على أنه يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون درهم، او بإحدى

تعاطي المخدرات يعاقب كل من انتفع أو سهل لغيره بغير وجه حق الانتفاع بخدمات المنصات أو قنوات البث المسموعة أو المرئية، وذلك عن طريق شبكة المعلومات أو وسيلة تقنية معلومات".

بالإضافة إلى ذلك فإن الجرائم الإلكترونية قد تمس المقدسات الدينية وذلك عن طريق استخدام وسائل التواصل الاجتماعي في الإساءة, أو عن طريق الشرع على الموقع, وذلك وفق النص المادة 35[147].

يظهر لنا من النص السالف الذكر بأن المشرع نظم الحالات التي يعفى فيها الإساءة إلى المقدسات الدينية جريمة يعاقب عليها القانون وشدد في عقوبة ارتكاب الجرم اذا ما مست الذات الإلهية أو الرسل وهل القانون السالم في أن ذلك يعاقب عليه مسؤولية قانونية توجب العقاب.

المادة السادسة والثلاثون نظمت أحكام الاتجار والتعامل بالمخدرات وارتكاب الأفعال المتعلقة بأموال غير مشروعة:

Universiti Utara Malaysia

[147] نص المادة 35 على)مع عدم الإخلال بأحكام المقرر في الشريعة الإسلامية يعاقب بالحبس والغرامة التي لا تقل عن خمسين ألف درهم ولا تجاوز خمسين درهم أو بإحدى هاتين العقوبتين كل من ارتكب عن طريق الشبكة المعلوماتية أو وسيلة تقنية معلومات أو على موقع إلكتروني ، إحدى الجرائم التالية :

1 - الإساءة إلى أحد المقدسات أو الشعائر الإسلامية.

2 - الإساءة إلى احد المقدسات أو الشعائر المقرر في الأديان الأخرى متى كانت هذه المقدسات والشعائر مصونة وفقاً لأحكام الشريعة الإسلامية.

3 - سب أحد الأديان السماوية المعترف بها.

4 - تحريض المعاصي أو الحض عليها أو التروج لها.

وإذا تضمنت الجريمة الإساءة للذات الإلهية أو لذات الرسل والأنبياء أو كانت مناهضة للدين الإسلامي أو جرحاً لأسس والمبادئ التي يقوم عليها ، أو ناهض أو جرح ما علم من شعائر وأحكام الدين الإسلامي بالضرورة ، أو نال من الدين الإسلامي ، أو بشر بغيره أو دعا إلى مذهب أفكار تنطوي على شيء مما تقدم أو حبذ ذلك أو روجه فيعاقب بالسجن مدة لا تزيد على سبع سنوات(.

بحيث نصت على أنه "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو أدار موقعاً إلكترونياً أو نشر عليه أو نشر معلومات على شبكة المعلوماتية، أو وسيلة تقنية معلومات لتسهيل الاتجار أو الترويج لمخدرات أو المؤثرات العقلية وما في حكمها أو لتسهيل التعامل فيها في غير الأحوال المصرح بها قانوناً".

يعاقب بالحبس مدة لا تزيد على سبع سنوات وبالغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم كل من أنشأ عمداً أو استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، أي من الأفعال الآتية: 1- تحويل الأموال غير المشروعة أو نقلها أو إيداعها لقصد إخفاء أو تمويه المصدر غير المشروع لها. 2- إخفاء أو تمويه حقيقة الأموال غير المشروعة أو مصدرها أو حركتها أو الحقوق المتعلقة بها أو ملكيتها. 3- اكتساب أو حيازة أو استخدام الأموال غير المشروعة مع العلم بعدم مشروعية مصدرها أو يعاقب بذات العقوبة كل من أنشأ أو أدار موقعاً إلكترونياً أو نشر عليه أو نشر معلومات على شبكة المعلوماتية أو وسيلة تقنية معلومات لتسهيل ارتكاب أي من الأفعال المنصوص عليها في الفقرة الأولى من هذه المادة أو للترويج عليها". يتضح من خلال تلك النصوص سالفة الذكر أن المشرع اعتبر كل من قام

ليس استخدام موقع الكتروني وسيلة نشر أو الدارة به دفاً لاتجار في المخدرات والمؤثرات العقلية, أو قد يستهدف عملية ذلك أو قد اقتصر أعمال الدارة تلك الموقع, أنها ارتكب جريمة على يد قانون مكافحة الجرائم التقنية[148].

المادة الثامنة والثلاثون جاءت تنظم أحكام الضرر بمصالح الدولة والإساءة إلى وسائل الموقع الغير قانونية:

وحيث نصت على أن "يعاقب بالسجن المؤقت كل من قدم إلى أي من منظمات او مؤسسات او هيئات او اية كيانات أخرى معلومات غير صحيحة او غير دقيقة او مضللة، وكان من شأنها الإضرار بمصالح الدولة، او الإساءة إلى سمعتها او هيبتها او مكانتها، وذلك بسبب استخدام الشبكة المعلوماتية او إحدى وسائل تقنية المعلومات".

بالضافة إلى أن صراعة المحتوى للكتروني القانوني يتضمن الكه أو صراع فتحت المسائل القانونية وذلك وفق ألن نص المادة 39 والتي نصت على أن "يعاقب بالحبس والغرامة او بإحدى هاتين العقوبتين اي مالك او شغل لموقع الكتروني انشبكة معلوماتية خزن اوأتاحت عمداً اي محتوى غير قانوني، مع علم بذلك، اوليجب ادربزالة او منع الدخول الى هذا المحتوى غير القانوني خلال المهلة المحددة في الشعار الخطي الموجه له من الجهات المختصة والذي يثبت عدم قانونية المحتوى وأن متاح على الموقع الكتروني لشبكة المعلوماتية".

ويظهر لنا أن المشرع الإماراتي قد جعل تلك الجرائم من ضمن الجرائم التي تمس أمن الدولة وتقلل من هيبته في امبإنشاء موقع من شأنه أن تؤدي إلى الحق ضرر بشؤون الدولة الداخلية

[148] بيام محمد لهادي: المرجع السابق, ص847.

وعاقبتها, كالتي تنشر معلومات كاذبة أو تقديم معلومات غير صحيحة بهدف تقويض أحد المؤسسات, أو التي تنشر معلومات تتضمن الدولة بهدف المساس بالسلم الأهلي أو إثارة الفتنة, والتي تمس الكرامة الوطنية وتلك التي تسعى إلى الفجور[149].

وهكذا نجد أن قانون مكافحة الجرائم رقم لسنة 2012 وتعديلاته سنة 2016 و 2018, قد صنف عدد كبير جداً من أنواع الجرائم والتي نرى من خلاله أنه شمل جميع الجرائم الإلكترونية التي قد ترتكب والتي يعاقب عليها مرحلة ارتكاب وقوع الجريمة. ضمن القانون فإن عقوبة التحرش الجنسي تصل إلى السجن المؤقت والغرامة التي تتجاوز مبلغ 2 مليون درهم، فرض عقوبات تكميلية كالمصادرة إلى جانب إدانة الجاني كما يعاقب على الشروع في الجنح المنصوص عليها في المرسوم بقانون بنصف العقوبة المقررة لجريمة التامة, وفي حالة إلى أن تعيد التعدي على القانون تتعرض لغرامة تتضمن عقوبات رادعة على ارتكابها ومنها الجرائم الماسة بأمن الدولة[150].

تلك جميع الحالات التي نص عليها قانون مكافحة الجرائم التقنية والمعلومات رقم لسنة 2012, والتي يفيد اشتمل أنواع الجرائم التي قد ترتكب عبر أجهزة الحاسوب والهواتف الذكية, وعبر شبكات الإنترنت والبرامج وتطبيقات الهواتف يبين العقوبة المقررة لكل جريمة مما يدل التشديد والتخفيف حسب طبيعة الظروف التي ارتكبت فيها الجريمة وبذلك نرى ما توصل إليه المشرع في

[149] عبد اللطيف محمود ربيعة: الجرائم الإلكترونية - التجريم والملاحقة والإثبات, مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين

الواقع في جامعة النجاح الوطنية-نابلس - 7 نيسان 2016م ص9.

[150] مصطفى يوسف: استراتيجية إماراتية لمواجهة الجرائم الإلكترونية, نشر 26 سبتمبر 2013, https://www.albayan.ae/ تاريخ الزيارة 2023/1/6م.

ذلك كان موفقاً في بيان الجرائم المرتكبة عبر الإنترنت, وأيضاً في تقرير العقوبة المقررة نجد هذا الأمر مع ظروف كل جريمة والأمر مع حجم خطورتها, ذلك من حيث تجريم العقوب فقط.

أما من حيث أن هذا القانون جاء شاملاً لشتى أنواع الجرائم نجد أنه قد صيغ بحيث لم ينص على تجريم التسول الإلكتروني والتجريم الحرمان الإلكتروني والتجريم الدعارة الإلكتروني, وأيضاً لم يبين الفقرات غلب على الصعوبات أو الإشكاليات الموضوعية أو الجوانب التي تواجه الجرائم الإلكترونية من حيث إشكال التجريم أو تقرير العقوبة الخوف من الشبهة وبيان القواعد الجوانب الواجبة للإتباع.

3.2 تكييف القانوني للجرائم الإلكترونية

التجريم الإلكتروني هي مقابل الجرائم المعاقب عليه وفقاً للتشريع في دولة الإمارات العربية المتحدة, وقد كان ذلك نتيجة تزايد الجرائم المرتكبة بطريقة إلكترونية السيما أن القانون العقوبات لم يتطرق إلى الجرائم الحديثة التي أصبحت تشكل خطراً جداً فكان البد على المشرع الإماراتي من تنظيم ذلك وفق القانون خاص بحيث سن قانون الجرائم التقنية رقم لسنة 2012 والمعدل بقانون رقم 2 لسنة 2016م يبين من خلال جميع الجرائم الإلكترونية فرض جزءً خاصاً لها بحيث يعتبر هذا القانون خاص بالجرائم الإلكترونية, وقانون العقوبات الإماراتي رقم 3 لسنة 1987م يعتبر قانوناً عاماً لجميع الجرائم التي لم تحظى بتنظيم في قانون الجرائم الإلكترونية.

ومن الجدير بالذكر في هذا المقام أن المشرع الإماراتي جعل من قانون الجرائم الإلكترونية هو القانون المنظم لجميع صور التجريم الإلكتروني, فهو القانون الموضوعي الذي يجرم الأفعال,

وأيضاً هو نفس القانون الجزائي, وذلك على عكس الجرائم القانوني التي ينظم أحكامها الموضوعية قانون الجراءات الجنائية رقم 35 لسنة 1992م, والقواعد الجنائية ينظمها قانون العقوبات رقم 3 لسنة 1987م[151].

على هذا أن الجرائم الإلكترونية هي مرتبطة بالجرائم المعلوماتية التي تشيع الإساءة بالجرائم القديمة, وان صور الجرائم الإلكتروني تمتد عن تشمل الجرائم لأنواع الجرائم التي يقع عليها الفعل الإجرامي. بالنظر إلى قصور المشرع الماليزي حرصاً عدم إنشاء قانون خاص للجرائم الإلكترونية وجعلها مستقلاً عن القانون الجنائي حيث سابقاً ذلك في تحديد وحصر الجرائم الإلكترونية وكذلك الجراءات المتعلقة بها وذلك كي يسهل على المواطنين والمختصين تحديد الجرائم الإلكترونية من عدمه.

في هذا الفصل نناقش الباحث في هذا المبحث النصوص القانونية لنصوص المرسوم رقم)5(لعام 2012 والمعدل بقانون اتحادي رقم)12(لعام 2016م المتعلق مكافحة الجرائم التقنية المعلومات في دولة الإمارات العربية المتحدة حيث تناول المواد القانونية التي تبين أنواع الجرائم الإلكترونية المنصوص وحكم القانون من هذه المواد الضرورة التي يلاحظ في القانون لهذا النوع من الجرائم ، بالنظر تم الإجابة على سؤال البحث الثاني وتحقيق هدف البحث الثاني.

[151] محمد دبراهيم الزغبي في القانون والتشريعات العربي مكافحة الجرائم الإلكترونية, المجلة العربية للنشر العلمي, العدد السابع والثلاثون تاريخ الصدار 2 تشرين الثاني, سنة 2021م, ص 281.

الفصل الرابع / CHAPTER FOUR
الحلول التشريعية لمكافحة الجرائم الإلكترونية التي تقع على الشبكات الناتجة عن هذا النوع من الجرائم

سوف نتناول في هذا الفصل الحلول والأساليب التي يجب اتباعها في سبيل مكافحة الجريمة الإلكترونية ومنع وقوعها، وذلك من خلال الاطلاع على التشريعات المقارنة في هذا الشأن خاصة الحلول الجزائية من الجرائم الإلكترونية، كما استنبطت طرق الدراسة إلى الدور القانوني والدولي في مواجهة ومكافحة الجريمة الإلكترونية، كذلك دراسة الدور الوطني في سبيل التصدي للجريمة الإلكترونية.

كما يأتي الباحث أهم الحلول والعمل في قبيل أن مواجهة تلك الجريمة تقتضي وقوع بعض الإجراءات المطلوبة لمكافحة الجرائم الإلكترونية وكذلك تقتضي وقوع ضوابط وتشريعات الأساليب المستخدمة في تقنين الجرائم. في هذا الفصل تم الإجابة على سؤال البحث الثالث وكذلك تحقيق هدف الدراسة الثالث.

Universiti Utara Malaysia

4.1 الجريمة الإلكترونية في ظل التشريعات المقارنة

4.1.1 القوانين لنظمة الجريمة الإلكترونية

نظم قانون العقوبات الإماراتي رقم (3) سنة 1987م الجرائم الإلكترونية ضمن نص المادة 197" يعاقب بالسجن المؤقت كل من استعمل أي وسيلة من وسائل الاتصال أو وسائل تقنية المعلومات أو أي وسيلة أخرى في نشر معلومات أو أخبار أو تحريض على فعل من شأنه تعريض أمن الدولة للخطر أو المساس بالنظام

العام" ونص المادة المادة 297" يعاقب بالسجن مدة التي تزيد على خمس سنوات كل من عطل عمداً وسيلة من وسائل الخص السلكي والسلكية أو غيرها من الخدمات الخرى المخصصة لمنفعة عامة أو قطع أو تلف شيئاً من أسلاكها أو أجهزتها أو حال عمداً دون إصلاحها وتكون العقوبة السجن مدة التقل عن خمس سنوات إذا ارتكب الجريمة في وقت حرب أو فتنة أو هياج أو استعمال مواد مفرقعة أو منفجرة", وجاء قانون مكافحة الجرائم التقنية رقم 5 لسنة 2012, ناظماً لجرائم الالكترونية التي قد ترتكب, وبشأن ترتيب اجراءات طلب المساعدة شرعية تم اخضاع ذلك لقانون الجراءات الجزائية رقم 35 لسنة 1992 مالمطبق في المارات العربية المتحدة.

4.1.2 لدور القليمي والدولي في مواجهة لجريمة الالكترونية ومكافحتها

فاك عدد كبير من التشريعات الولية والقليمية لمتعرف الجريمة الالكترونية لتفاقية جلس اوروبا بشأن الجرائم الالكترونية واتفاقية جامعة الدول العربية, ومشروع اتفاقية الاتحاد الوربي, إل أن من ظمات تعاون القتصادي والتنمية قد عرفت الجريمة الالكترونية وذلك في اجتماع باريس المنعقد عام 1983 بأنه عبارة عن كل سلوك غير المشروع يصب على فعل غير مصرح به قانوناً يهدف إلى المعالجة آلية للبيانات أو نقلها أو اتلافها[152].

ومن أجل مكافحتها كان البد للتشريعات الوطنية والولية الحد من انتشارها وذلك عن طريق إستراتيجية صارمة وحادة, التركيز على الجانب الجتماعي القليمي والتقني, ونشر الوعي

[152] علي حسين فلية القانون الوطني والدولي في مكافحة الجرائم الالكترونية, قسم القانون في الكاديمية العربية في الدنمارك, ص4.

بين فئة الأفراد والمجتمع والذين يعانون من حجم الخطر الذي قد يلحق بهم بسبب تلك الجرائم، واستمرار العمل المستمر لوضع حلول للتعامل مع الأدوات القانونية والأخلاقية التي قد تنشأ أثناء استخدام هذه التكنولوجيا[153].

4.1.3 التصدي للجريمة الإلكترونية

وكما تطور المجتمع الإنساني عبر التاريخ تطورت أنواع الجرائم التي يرتكبها هذه المجتمعات، الأمر الذي كان يدعو إلى تدخل التشريعات والقوانين التي تحد من آثار الجريمة هذه الجرائم على الفرد والمجتمع، ووضع التشريعات لمكافحة الجرائم الإلكترونية والتصدي لها، ويمكن العلي من صياغة التشريعات لمواجهة الجرائم الإلكترونية من خلال ما يلي:

أولاً: بلورة النصوص الوطنية وضعها موضع التنفيذ، وهذا الغرض أبرمت العديد من الدول الاتفاقيات الوطنية، ومن أبرزها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية (2000) البروتوكول المتعلق بمنع وقمع الاتجار بالأشخاص وبخاصة النساء والأطفال المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، وتشمل هذه الاتفاقيات الأموال والأفراد وتشمل هذه الاتفاقيات على الخصوص التعاون الدولي لمواجهة هذه الظاهرة التي تصل بحث العمومية.

ثانياً: التعاون الدولي لمواجهة الجرائم الإلكترونية، يقتضي في البداية وضع قواعد جديدة للاختصاص خارج الحدود الوطنية، من ثم وضع قواعد جديدة للتعاون الدولي على المستويين

[153] جمال الدين, بدوي. "الأمن السيبراني والتحولات في النظام الدولي." مجلة كلية الاقتصاد والعلوم السياسية 24.1 (2023): 189-230.

القضائي والأمني، والأهم من ذلك تفعيل دور التعاون الدولي وتحقيق التعاون بين الدول العربية لمواجهة الجريمة الإلكترونية.

ثالثاً قيام الدول العربية باتخاذ عدد من التدابير والإجراءات التجريم وعقاب مرتكبي تلك الجريمة وتعزيز الجانب الوقائي لمكافحة أنشطة الجريمة الإلكترونية فقد عمل النظام العربية لمكافحة جرائم تقنية المعلومات وذلك بتاريخ 2010/12/21، كما أدت هذه الاتفاقية لكل من دول مجلس التعاون لدول الخليج العربية لمكافحة ما يسمى بالجرائم الإلكترونية في قطر والأردن والسعودية والإمارات والعراق سلطنة عُمان.

رابعاً تعزيز مؤسسات العدالة الجنائية وزيادة الخبرات الذهنية لدى أفراد الضبطية القضائية في مجال مكافحة الجريمة الإلكترونية من خلال تحديد مجالات تدخل الشرطة لدعم الكشف المبكر عن التهديدات الجديدة والناشئة التي تثيرها الجريمة الإلكترونية، واعتماد تنفيذ سياسات تتكفل التصدي بفعالية لتلك التهديدات.

خامساً تعزيز القوانين الوطنية لمكافحة الجرائم الإلكترونية من خلال نقل معارف المحاكم الجنائية العربية وممارساته والمساهمة في مكافحة الجريمة الإلكترونية.

سادساً إنشاء منصة إتاحة الوصول إلى البحوث المستندة إلى الأدلة لوقوف على أفضل الممارسات الواجب فتحها على قبل الوقاية من الجرائم الإلكترونية، ونشر تلك الممارسات.

سابعاً: بناء القدرات في مجال نوع الجريمة الإلكترونية والعمالة الجنائية، من خلال وضع نماذج تكاملة إدارة المعارف، وتقليل المعارف بسلوب منهجي، بين الشبكات مع المؤسسات الكاديمية والمنظمات الولية وهراك زال بحوث والتوجيه لزيادة فهم تفوق الإنسان ونوع الجريمة الإلكترونية والعمالة الجنائية تبه دفتر يزيادة القدرون.

ثامناً: الدعم السياسي والمؤسسي المرتبط بجيو القتنيذي: ويشمل ذلك الوعي بخطورة التهديدات وضرورة التعامل معه الكولوية وبأعلى قدر من الجدية، مع الهتمام السعداد المسبق بما يشمل الخطط السترايجي والقتنيذية وخطط الطوارئ آليات التنسيق العرضي واعداد الملكوادر التجهيزات التقنية والوجستية.

تاسعاً: وضع الطار التشريعي المئم أمن الفضاء السيبراني ومكافحة الجرائم الإلكترونية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات، وذلك بشراكة عربية من وذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع السترشاد الخبرات والتجارب والبرامج الولية ذات الصلة، واعداد توجيه بالمتخصصين في فيما اذا القرل ورفي الجهات القضائية والشرطية[154].

[154] محمد الزغبي: المرجع السابق, ص292.

4.2 الحلول العملية لمواجهة الجريمة الإلكترونية

4.2.1 صور الجريمة (حالات الجريمة الإلكترونية)

نظراً لتطور العصري الذي تشهده التكنولوجيا في وقتنا الحالي وإلى التطور الكبير المستمر والمتقدم في شتى أنواع المجالات الإلكترونية, نجد أن الجرائم الإلكترونية تأخذ بحالات كثيرة وتتنوع, فمنها ما يقع على الأشخاص في موارده المالية أو في سمعته بهدف الإيذاء والتشهير عن طريق السب والقذف والنشر على المواقع الإلكترونية للإساءة إليهم, أو سرقة الحيز الخاص بهم والشراء من خلالها عن طريق انتحال هويتهم, وقد تقع الجريمة الإلكترونية على الأشخاص دون فرق لسن معين أو ضحية ولكن الشرع المماري يشدد في عقوبة الجريمة التي يضحيتها حدث لم يبلغ الثامنة عشرة من عمره, وأيضاً هناك جريمة التهتز والتهديد. وقد تقع الجريمة الإلكترونية على الدولة بهدف النيل من سيادتها كتشجيع المواطنين على عدم احترام قوانينها وسنوراها ودياناتها السماوية, وشن الحروب الإلكترونية والرهاب الإلكتروني.

والجرائم الإلكترونية ليست نوعاً واحداً، وإنما تختلف حسب الأساس والمعيار الذي يستند إليه الفقهاء فيقسمها بعضهم إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته وبعضهم يضيف إليها أنماطاً أخرى تستند إلى الأساليب المتبعة في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، ويتعدد المحل عندما يقع على مكونات الحاسوب فيقسم إلى جرائم تقع على الأموال بوسائط الحاسوب وتلك التي تقع على الحياة الخاصة[155].

[155] الطائي جهاد محمد: المرجع السابق، ص130 وما بعدها.

في الحديث عن حالات الجريمة الإلكترونية أي صورها والتي تتمثل في تطبيقات على وقوع الجريمة الإلكترونية, سنبين أكثر الجرائم شيوعاً في مختلف دول العالم والتي تتم بإستخدام الحاسوب عن طريق شبكات الإنترنت, وهي الجرائم المالية وبطاقات الإئتمان والتهديد, والحرب الإلكترونية, وإلهاء الإلكتروني, وذلك على النحو التالي:

4.2.2 الجرائم المالية الإلكترونية

ويعد هذا النوع من الجرائم التي يقوم بها أفراد أو هيئات الشخصية أو الهيئات التجارية والمؤسسات الخاصة والحكومية, والتي يسعى مرتكبها إلى جني أموال بطرق غير مشروعة وتقع هذه الجريمة عن طريق القرصنة الفضائية من خلال مواقع التواصل الاجتماعي بحيث يقوم الجاني بإرسال ملف فيروسي على هيئة ملف فيديو أو بمجرد أن يقوم الضحية بفتح هذا الملف فتوجه على جهازه تعمل على اختراق, أو عن طريق الهندسة الاجتماعية التي تستهدف المستخدمين بشكل رئيسي المؤسسات والشركات, وقد يقوم بهذه الجريمة الموظفون الفاسدون الذين يعملون في مؤسسات المالية, عن طريق إدخال البيانات الخاطئة على برامج بهدف السرقة, أو تعديل وحذف البيانات المخزنة, أو كتابة شفرات برمجية أو اعتراض التحويل[156] وتعد سرقة الأموال والمقامرة والتلاعب والعملات

[156] الجزيرة: الجرائم الإلكترونية- احذر حساباتك, تاريخ النشر 2019/7/22 https://www.aljazeera.net/, تاريخ الزيارة 2023/1/20.

الهامة من الخبراء والقراصنة الذين يقومون بالهجمات عن طريق شبكات الإنترنت, من الجرائم التي يصعب اكتشافها, لكون التضرر قد يشمل عدد من الأفراد أو المجتمع بأكمله وإلى سنوات أخرى[157].

وتوازي استخدام الإنترنت والذي يصل لأكثر من 3 مليار استخدام لشبكات الإنترنت, يؤدي إلى تنامي الجرائم الإلكترونية, وهذا ما دفع إلى ضرورة وجود حماية على المستوى الأفراد وتخير فالمتعامل مع الوسيط الإلكتروني, على المستوى الشخصي فيما يستخدم موقع التواصل الاجتماعي المختلفة, وأيضاً القيام بتنفيذ اجراءات وقائية لضمان سلامة أمن المعلومات على صعيد المؤسسات والشركات والبنوك سواء في القطاع العام أو الخاص, وذلك بهدف الحد من المخاطر القضائية التي قد تحدث بسبب قيام الأفراد والشركات والبنوك بالتعامل الكلي على انجاز أعمالهم عن طريق شبكات الإنترنت[158], وقد يتم سرقة الصفحات الشخصي من المالك صفحة الفيس بوك أو الإيميل الت وغيرها من الصفحات المستخدمة عبر الإنترنت, وهذا ما أضطر بالمحكمة نظام القضائي في حكمها في قضية سرقة الفيس بوك "بحبس المتهم سنتان مع الشغل والأشغال خمسة آلاف دينار وغرامة لمئة ألف دينار وبالزام المصاريف القانونية"[159].

على ما قام المشرع الماريني بنص قانوني لفضاء الجرائم الإلكترونية ونص على الجرائم المالية فرض لها عقوبة وذلك في نص المادة 4و11و12و13 من قانون مكافحة الجرائم التقنية والمعلومات رقم لسنة 2012م.

---

[157] بالل جرادة: المرجع السابق, ص9,

[158] حسن الشوبكي: جرائم السرقة والهجمات الإلكترونية, تاريخ النشر 2014/11/18 https://www.ammonnews.net/ تاريخ الزيارة 2023/1/20م

[159] محكمة نظام القضائية الطارئة الرابعة الابتدائية قضية رقم 2019/1190, تاريخ الفصل 2020/1/29م.

4.2.3 جريمة الابتزاز والتهديد الإلكتروني

تنتج التقدم العلمي والتقني في مجال الاتصالات ووجود شبكة الإنترنت تسهل بحر فناك مواقع تواصل اجتماعي مختلفة، مما أدى إلى ظهور أنماط من الجرائم المختلفة، وجريمة الابتزاز والتهديد وغيرها من الجرائم تشكل خطراً على المجتمع المحلي، وتتم هذه الجريمة عن طريق استدراج واصطياد الأشخاص عبر تلك المواقع التواصل الاجتماعي، وعن طريق تطبيقات الهواتف الذكية بغرض إغرائهم بظهور أوضاع غير لائقة يعملي تصويرهم دون علم منهم، من ثم القيام بتهديدهم بنشر الصور المسروقة لهم وقد يطلب منهم[160]، ومن تحقق عملية الابتزاز، والمطالبة بأموال مقابل الامتناع عن نشرهم، أو القيام بتهديدهم من أجل ارتكاب عمال ما أو الامتناع عن عمل، ومن تحقق جريمة التهديد.

علي فأن الجريمة الابتزاز والتهديد الإلكتروني تشكل فئة من فئات العصر، والتي فرزها التطور الكبير في شبكات الإنترنت، ومع أن شبكات الإنترنت له الكثير من الفوائد التي لا حصر لها، إلا أن له أثر سلبي كبيرة، مما أدى بعض دول إلى تدخل الشرعي والقانوني لضبط وقوع هذه الجريمة، والحد من وقوعها وبذلك يمكن القول أن جريمة الابتزاز والتهديد تعني محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعياً أو اعتبارياً إلكترونياً بالتهديد بنشر سر من وقوع إيه الابتزاز والتهديد أثناء ضحية[161].

---

[160] يتنظيم الاتصالات والحكومة الرقمية في الإمارات العربية المتحدة.

[161] دعاء سليمان عبد القادر التميمي: جريمة الابتزاز الإلكتروني، رسالة مقدمة لنيل درجة الماجستير في القانون في فلسطين، سنة 1440 هـ 2019م، ص9 وما بعدها.

وقد تتخذ الجريمة بالابتزاز والتهديد عدة صور, من بينها تعطيل الخدمة حيث يقوم بها الجاني بتعطيل مزود الخدمة لدى الضحية فتشل بكات الإنترنت مما يسمى بالهجوم, أو اعتراض المعلومات المرسلة عن دراسالها من جهة إلى أخرى, وقد يتخذ الجاني أسلوب التجسس طرائق الاحتيال في جهاز الضحية فتحركاً الملفات في جهازه, وقد يتخذ أسلوب التصايل وغالباً ما يستخدم هذه في عمليات السرقة وتختلف الجرائم الإلكترونية, وقد يقوم الجاني بالوصول لمبتغى ألسالك التهويل والتجسس على المعلومات المارة[162].

ويسعى الجاني إلى أسلوب بالابتزاز والتهديد والضحية بهدف الحصول على جانب مادية كالحصول على الأموال, وقد يسعى من وراء ذلك إلى ارتكاب جرائم جنسية وقد احتلت هذه الجريمة المرتبة الأولى في قائمة الدراسة قائمة مرتبها دار المنظومة[163].

وهكذا فأن جريمة بالابتزاز الإلكتروني وتهديد تقع عن طريق أمام الحاسب عرض لمقع الإلكتروني أو خادم يدي الإلكتروني أو نظام حاسوب له جمات متكررة من نوع الحرمان من الخدمة, والتي تؤدي إلى اغراق المقع الإلكتروني بطلبات تعيد تعطل في ناحية الأمر غير قادر على تلبية طلبات الزوار, أو عن طريق تشويه موقع الإلكتروني ومنصات معينة ويلفكون تشويهها إلى بعد أن يضعوا لمصحابها بمبالغ مالية كبيرة, أو عن طريق القيام بهجمات القرصنة والتي أيضاً يطلبون أموالاً حتى يوقفوا الهجمات[164].

---

[162] بالل جاجرة: المرجع السابق, ص13.

[163] سليمان بن عبدالرزاق الغيثان ويحيى بن مبارك خطاطبة و عزالدين بن عبدالكريم: صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين, مجلة البحوث الأمنية- المجلد 27و 69-الهيئة الملكية للأمن الأمنية- مركز البحوث والدراسات,- دار المنظومة,سنة 2018م, ص159.

[164] الجزيرة: الجرائم الإلكترونية- احذر حساباتك,تاريخ النشر 2019/7/22 https://www.aljazeera.net/, تاريخ الزيارة 2023/1/21.

على ما استدعى المشرع المماثل بالتدخل وذلك بفرض نص تشريعي يعاقب فيه كل شخص ارتكب هذه الجريمة, والحد من وقوعها, وذلك وفقاً لنص المادة 8و15و16 من قانون مكافحة الجرائم التقنية رقم لسنة 2012, وهذا ما قضت به محكمة النقض الفلسطينية "فإن استخدام شبكة الكترونية في تهديد شخص حتى ولو كان مشروعاً يعاقب عليه اعتبر فعلاً مجرماً يعاقب عليه القانون"[165].

4.2.4 الجرائم المرتكبة الكترونياً

تعد ظاهرة الإرهاب ظاهرة تقليدية ظل الجرائم التقنية التي كانت تهدد أمن الدول وتمس سيادتها, وهذه الجريمة تثير خوف الكثير من نظراً لكثرة وقوعها في مختلف أنحاء العالم وفقط أصبح الإرهابيين يستخدمون المصادر في نشرات الأخبار عبر وسائل الإعلام التقليدية.

ومع التطور التكنولوجي أخذ الإرهاب بعداً جديداً وذلك بقيام المرتكبين بتنفيذ عملياتهم المرتكبة عن طريق شبكات الإنترنت. وتقصد بالإرهاب إتخاذ مجموع من الأفراد يدعو بالجماعة سواء بشكل فردي أو جماعي, فالأعمال تقوم بها فئة من فئات تختلف عن بعضها دينياً أو سياسياً أو أيديولوجياً, بهدف خلق أجواء من الخوف والزعر في نفوس الفئة المستهدفة, والنيل منها نتيجة ما من ممارسة حقوقها بشكل طبيعي, وكان الإرهاب قديماً عن طريق اختراق موقع رسمي أو حسابات شخصية أو بنكية ولكنه الآن توسع وأصبح يتضمن صور متزايدة من الإرهاب العام الواقعي, فالإرهاب الواقعي يتخذ مظهر مادي, أما عن طريق الوسائل الالكترونية فيقع عن طريق تدمير الأنظمة وتعطيلها

[165] محكمة النقض الفلسطينية قرار النقض رقم 2019/171 بتاريخ 1 يوليو 2019.

مرعياً عن طريق تشويه الشخصيات على العلم الافتراضي بحيث القدرة على ممارسة حق في التبرع عبر الوسائل الالكترونية متنوعة[166].

وتمتد الجرائم الرياضية إلى قصاد الدولة, وذلك عن طريق قيام الرياضيين بالانغماس في الرهاب القتصادي نظراً لتطور وسائل التقنية وجي العلومات الحديثة فيمكن لشبكات الترنت أن تُجمع ألشخاص اصوال خبرات من أجل نظيم عصابة اجرامية فقط وظيفة إلتكنولوجي الحديثة امتبتسهيل جميع أنواع السرقة اتوالتالعبوتخريب العلومات والتجيال, إل أنتلك العصابة الجرامية المتطورة التسطيع العمليات الرياضية دون وجود نشاط قتصادي ودعم المالي لهاويكون ذلك عن طريق الحوالة الالكترونية, وقديقوم الرهاب عن طريق تجارة الالكترونية في المخدرات في القمار[167].

بالمعنى السابق فأن الرهاب يشكلت هديداً أيضاً على المستوى القومي والعركري للدولة, وبين الدول ألخرى المتقدمة, وهذا مافدع إلى عقد اجتماع قمة بين الدول الثنى الاكبر في سرانت بوطس برغ عام 2006 مبشأن مكافحة الرهاب تقض من نفنين ذوتخصصين الطار القانوني الدولي لمكافحة إل رهاب, والتصدي بفعالية لمحاوالت لساءة لستخدام الفضاء الالكتروني أل غراض ارهابية بما في ذلك التحريض على رتكاب أعمال إرهابية, وعلى التواصل مع الرهابيين وصنع الخطط الرهابية وتنجيد وتهريب الرهابيين[168].

---

[166] وليف كري: االرهاب االلكتروني-نوع جديد من االرهاب إلخوراي,نشر 12ابريل 2021 الساعة 18:12ت وقيت أو ظبي https://www.skynewsarabia.com تاريخ الزيارة 2023/2/1م.

[167] أحمد بولحية طيقبو لي: المرجع السابق, ص184 وما بعدها,

[168] مجمع البحوث والدراسات أكاديمية السلطان المرجع السابق, ص68.

وهذا ما دفع المشرع الماليزي إلى التدخل وذلك بسن نصوص تشريعية لتفادي الجرائم الإلكترونية، فرض لها عقوبات وذلك في نص المادة 26 و 44، كما نص المشرع على تشديد عقوبة الإرهاب الإلكتروني وذلك وفقاً لنص المادة 46، من قانون مكافحة الجرائم الإلكترونية رقم 5 لسنة 2012، ويعتبر هذا المشرع من الجرائم الخطرة التي تمس أمن الدولة وتهدد سلامتها سواء على الصعيد الداخلي بين الأفراد داخل المجتمع الواحد، أو على الصعيد الدولي بين الدول وعلاقاتهم مع بعضهم البعض، والذي يعد تماماً وبدايةً يسعى الجاني في ارتكاب جريمته هذه إلى النيل من سيادة الدولة والقضاء على مقوماتها وضرب السياحة، خاصة إن كانت من ضمن الدول التي يعتمد عليها السياحة من جميع الدخل العام، بغض النظر عن إنجازها من أعظم وأكثر دول العالم التي يوجد فيها السياحة.

ولم يستطع المشرع الاعتماد على وسائل الحماية التي تنتهجها الشركات الأمنية، فهي ليست آمنة، والي يمكن الطمئنان لها تماماً، وذلك من الخطورة في ضعف الوسائل الأمنية المستخدمة في حماية شبكات الخاصة بالمؤسسات والهيئات الحكومية، هذا بالإضافة إلى أن الطرق التي يلجأ تجسس العلومات يستكون أكثر الطرق المستخدمة في المنقبل من قبل التنظيمات الإرهابية، نظراً لأهمية العلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياحية والقتصادية وهذه العلومات إذا تعرضت للتجسس لحاصول على فلسوف يسيء استخدامها من اجل الإضرار بمصلحة المجتمع والوطن.

4.2.5 الحرب الإلكترونية

وتعد الحرب الإلكترونية من ضمن الجرائم التي تهدد أمن الدولة من الناحية القومية والاقتصادية كما هو الحال في جرائم الحرب الإلكتروني.

فالحرب الإلكترونية تمثل في صراع مجتمعي يدار عبر شبكات الإنترنت تتضمن طوي على هجمات ذات دوافع سياسية على المعلومات ونظمها, بهدف تعطيل موقع الويب السرية وشل شبكات توتعطيل الخدمات الأساسية, أو القيام بسرقة وتعديل البيانات السرية, وأيضاً تستهدف تخريب أنظمة الحماية, وقد قال الكاتب "فيصري كار" بإمكان أي دولة شن حرب إلكترونية على دولة أخرى بغض النظر عن موارده, ويرجع ذلك إلى أن معظم القوات العسكرية تتوسب شبكات الإلكترونية وتتصل بالإنترنت, مما يجعلها غير آمنة وعرضة للاختراق[169].

والحرب الإلكترونية تتخذ نوعين أول حرب الشبكات حيث تستخدم الشبكة الكهربائية سياسية جزءاً مهماً في تخريب مستويات الجودة التي تتمتع بها المعلومات والبيانات المعلومات, ويتم تدمير تلك عن طريق البحث الشبكي, ونوع الثاني حرب البيانات وتكون بسبب تغلغل البيانات التفق طتنتهي عن تدفق بادل المعلومات بين طرق الاتصال, وذلك دون إلحاق الدمار فيها, وتنوع الحرب الحرب بفمنها القيام بضرب النظمة والوسائل الخاصة بالعدو وتدميرها, والقيام بعمليات السرقة بغرض كشف خطط العدو التي يريد القيام بها, القيام بأعمال المضادة إجراءات الحرب الإلكترونية المعادية, بغرض القيام بتصدي له والوقاية منها والمقابلة للشبكات الكهربائية[170].

---

[169] رماح القدومي: قد تشل دوالب كلها الحرب الإلكترونية, نشر الجزيرة 2020/1/7 https://www.aljazeera.net/ تاريخ الزيارة 2023/2/2م

[170] إيمان الجاري: مفهوم الحرب الإلكترونية, تاريخ النشر 22 أغسطس 2018 أخر تحديث الساعة 21:28, https://mawdoo3.com تاريخ الزيارة 2023/2/2م.

فالحرب الإلكترونية تعمل على السباق الدفاع السياسية من راتلطبه اي رجع إلى أسباب السياسية والتي يتمثل في تهديد استقرار المجتمع سواء على المستوى المحلي أو الدولي, وتهديد الأمن القومي والعسكري كما هو الحال إلى جانت الحرب الإلكترونية التجسس العسكري[171]. وفي الكثير من يرى أن الحرب الإلكترونية قد تصبح القاعدة في الحروب المستقبلية بين الدول حيث تشكل جيوش إلكترونية هذه اختراق الدول الأخرى وتدمير بنيتها التحتية، وقد يكلف القادة العسكريين قيادة مثل هذه الحروب مستقبلا[172].

عليه قد جاء قانون مكافحة الجرائم المعلوماتية للعام وما تضمن نص على معاقبة كافة أو الجرائم الإلكترونية, إلا أنه افتقر إلى وجود نص خاص يجرم عقوبة الحرب الإلكترونية الكشف عن نص المادة 44 والتي تنص على أن يعتبر من الجرائم المرتكبة أمن الدولة، أي جريمة نص وصف عليه في هذا المرسوم بقانون إذا ارتكبت لحساب أو مصلحة دولة أجنبية او اي جماعة إرهابية او مجموعة او جمعية او منظمة او هيئة غير مشروعة(. وكون الحرب الإلكترونية هي من ضمن الجرائم الإرهابية فقد نجد أن هذا النص يتضمن هاولكن بالإضافة لذلك نص المشرع عوض عن صريح نص عقوبة جريمة الحرب الإلكتروني أسوة بجريمة الإرهاب الإلكتروني.

[171] مجموع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة: المرجع السابق, ص30.

[172] الجزيرة: المرجع السابق.

4.3 إجراءات الضبط والتفتيش

ويعد التفتيش في الجرائم الإلكترونية أمراً غير يسير أبداً أن الحصول الأدلة, سيما أن الجرائم الإلكترونية له طبيعة خاصة[173] يبرر الحاجة إلى ضرورة طرق خاصة في جمع الأدلة, لذلك قد حددت التشريعات إجراءات لجمع الأدلة بحيث أوجبت ضرورة توفر ضابطة يعلى المضمون بالبيانات المخزنة تكون نسبية[174], ذلك كون فكرة المعاينة مسرح الجريمة تقتضي إعمال دور في الإفصاح عن الحقائق المؤدية لأدلة المطلوب, ذلك كون الكثير من الأشخاص يترددون على مسرح الجريمة سيما بين وقوع الجريمة والكشف عنها, الأمر الذي يترتب عليه شل الخبط في الأدلة المستقاة من المعاينة, لذلك الحال فأن الخبراء مع عظمة ما يسببه من صعوبة ضبطية الضوئية, وغلبة عن عدم سوابق في مجال الجرائم الإلكترونية حيث تقوم الأجهزة الأمنية بتعيين مكونهم لديهم خبرة في ذلك[175].

والتفتيش يكون هو أكثر الإجراءات أهمية في الجرائم الإلكترونية إلى جانب الخبرة التي يجب أن تتوفر في المحقق عند مباشرته إجراءات التفتيش فأن التفتيش يصب على المكونات المادية والمعنوية للحاسوب.

تفتيش المكونات المادية للحاسوب يعني التفتيش المنصب على المكونات المادية في محور الجرائم الإلكترونية يسهل إجراؤه وتطبق عليه القواعد التقليدية للتفتيش، إذ الخلف على إنما الولوج إلى المكونات المادية للحاسوب بحثاً عن مادية تتطلب الجريمة عملوماتية وقعت فيه لكشف الحقيقة

---

173 عادل الدغمش الاعجمي: المرجع السابق, ص86.

174 زيد طه: المرجع السابق, ص28.

175 صغير يوسف: المرجع السابق, ص132.

عنها وعن رتمك بها يخضع إلى الإجراءات القانونية الخاصة للتسيش، بمعنى أن حكم تسيش تلك الممتلكات الحاية تتوقف على طبيعة المكان الموجود فيه تلك الممتلكات وهل هو من الأماكن العامة أو من الأماكن الخاصة.

إن لصفة المكان بوصفه أمميقة صوى خاص في مجال التسيش فإذا كانت موجودة في مكان خاص كسكن المتهم أو أحد من عائلته كان لها حرمة فلا يجوز تسيشها إلا في الحالات التي يجوز فيها التسيش بموجب الإجراءات المقررة قانونا في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت ممتلكات الحاسوب المراد تسيشها منعزلة عن غيرها من أجهزة الحاسوب الأخرى، أم إنها تتصل بحاسوب آخر أو بشبكة خاصة في مكان آخر كسكن غير المتهم فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة عين مراعاة القيود التي يتلزمها الشرع تسيش هذه الأماكن، أما إذا وجد شخص يحمل ممتلكات الحاسوب الحاية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء كانت بطبيعتها كالطرق العامة والميادين والشوارع، أم كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تسيشها يكون إلا في الحالة التي يجوز فيها تسيش الشخص بموجب القيود المنصوص عليها في هذا النوع[176].

التسيش عن الممتلكات المعنوية للحاسوب يثير تسيش الممتلكات المعنوية للحاسوب جدلا كبيرا في الفقه حيث ذهب جانب من الفقه إلى جواز تسيش ضوابط البيانات المخزنة في الكمبيوتر فتشملها، ويستند هذا الرأي في ذلك إلى القوانين الجزائية عندما تنص على إصدار الإذن بضبط (أي شيء)،

[176] محمد الزغبي: المرجع السابق, ص287.

فإن ذلك يجعل من الصعب على المشرع الماليزي أن يتدخل بتجريم الصور الجنسية وغير الجنسية من جانب آخر ذهب إلى القول بعدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة[177]، على أن يتسنى مواجهة هذا القصور التشريعي في نصوص الشرع الماليزي بنصوص صريحة على جواز تفتيش المكونات المعنوية للحاسب وضبطها وضبط البيانات المخزنة.

CHAPTER FIVE / الفصل الخامس

نتائج البحث وتوصياته

يتناول هذا الفصل إلى أهم النتائج التي توصل إليها الباحث، كما ستتعرض الدراسة التوصيات التي من شأنها تحقيق أهداف البحث في إطار النظام القانوني الماليزي المتعلقة بالشركات الموضوعية والجنائية المتعلقة بالجرائم الإلكترونية.

5.1 نتائج البحث والدراسة

خلصت الدراسة إلى النتائج التالية:

1. الجرائم الإلكترونية من ضمن الجرائم الأكثر خطراً في العالم أجمع وهي من ضمن الجرائم المعاقب عليها ضمن القوانين الخاصة, والتي يفرض المشرع لها نظام قانوني خاص جرم

[177] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط1, دار الفكر الجامعي، الإسكندرية- مصر، 2010م, ص194.

من خلال تفكيك الجريمة إلى جميع الطرق التي يمكن من خلالها تحقيق الجرائم المختلفة الجرائمية, ولقد تطورت الجرائم المالكترونية تطوراً مواكباً لسنوات الثورة الألفية, وذلك لما شهده العالم أجمع من تطور تكنولوجي, والذي صاحبه تخلل وجود في جميع أنحاء العالم.

2. نظم المشرع الماليزي الجرائم المالكترونية ضمن قانون مكافحة الجرائم المالكترونية لسنة 2012 وتبعه القانون الاتحادي رقم 5 لسنة 2012 وتبعه القانون الاتحادي رقم 12 لسنة 2016, في شأن أنواع الجرائم المالكترونية على أساس الجرائم الواقعة بواسطة أنظمة المعلومات, والجرائم الواقعة على أنظمة المعلومات.

3. الجرائم المالكترونية تطرح عدة قضايا قانونية لذلك نجد تطلب وجود حاسوب حيث التي تصور ارتكاب الجريمة المالكترونية دون وجود أجهزة حواسيب والتي يمكن أن تكون أداة الساعدة في ارتكاب الجرائم المالكترونية, وذلك عن طريق تنصيل شبكة الانترنت, حتى يتسنى للوصول إلى الضحية والذي يعرف المجني عليه, وهي من الجرائم العابرة للحدود.

4. الجرائم المالكترونية تكون بواسطة حاسوب عن طريق اتصال شبكات الانترنت فهي تتميز بخبرة العيوب لدى الجاني ارتكاب الجرم فهي ليست كأي جريمة أخرى تتطلب إلى يكون ارتكاب الجريمة المالكترونية شخص على خبرة فنية وتقنية العيوب في مجال الحاسوب وشبكات الانترنت, وقد يكون من أصحاب الهواة في هذا المجال الذي يتمتع بالذكاء والدهاء.

5. الجرائم المالكترونية التي تختلف كثيراً عن الجرائم التقليدية وخاصة في الأركان, لأنها تبقى دائماً وأبداً جوهر الاختلاف يتمثل في الأداة المستخدمة في الجريمة ومحل الجريمة وفي الدليل الذي يكون في الجريمة المالكترونية فيه غامض الأحيان غير مرئي.

6. بشأن المشاكل الموضوعية التي تواجه الجريمة المالكترونية فيتم مواجهته بواسطة القوانين العامة في قانون العقوبات الماليزي وقانون الجراءات الجنائية, والاستعانة بخبراء الفنيين في هذا المجال.

7. تظهر الشكاوي الجوهرية الناتجة عن الجرائم المالكترونية في ضوابط الجريمة ذاته من حيث ثبوتها وعن الشكاوي التي قد تترتب باجراءات البحث والتحري والتحقيق, وبالتالي الشكاوي المترتبة جراء "القانون المختص والواجب التطبيق" لتلك الجرائم.

8. فهناك عدد كبير من التشريعات الوطنية والدولية لم تعرف الجريمة المالكترونية كاتفاقية مجلس اوروبا بشأن الجرائم المالكترونية واتفاقية جامعة الدول العربية, ومشروع اتفاقية الاتحاد الاوروبي, إلا أن من ظاهرة تعاون القصادي والتي تقدم تعريفه.

9. بشأن التصدي للجرائم المالكترونية شوهد الاتجاه البدء من التعاون الدولي لمواجهة الجرائم المالكترونية تتمثل في البداية بوضع قواعد جديدة لتخصص خارج الحدود الوطنية، من ثم وضع قواعد جديدة لتعاون الدولي على المستويين القضائي والأمني، والأهم من ذلك فتح سبل دوال التعاون الدولي بين الدول العربية لمواجهة الجريمة المالكترونية.

10. قيام الدول العربية باتخاذ عدد من التدابير والإجراءات التجريم وعقاب مرتكبي تلك الجريمة وتعزيز الجانب الوقائي لمكافحة أنشطة الجريمة المالكترونية فتقف على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

11. وبشأن التصدي يجب وضع الطار التشريعي الملائم من القضاء السيبراني ومكافحة الجرائم المالكترونية وحماية الخصوصية وحماية الهوية القومية وأمن المعلومات، وذلك بمشاركة العربية من ذوي الخبرة في القطاع الخاص ومؤسسات المجتمع المدني، مع الاستفادة من الخبرات والتجارب والبرامج الوطنية ذات الصلة، واعداد تدريب المتخصصين في مجال اذالقانون وفي الجهات القضائية والشرطية.

12. الجرائم المالكترونية تكتسي قوة متنوعة منها ما يقع على الأشخاص في موارد مهم اللامية أو في سرعة مبهدف الى التشهير لوالتغيير عن طريق السب والقذف والتشهير على الموقع المالكتروني

لإساءة إليهم، أو سرقة الحيازة الخاصة بهم والشراء من خلالها عن طريق انتهاك حقوقهم، وقد تقع الجريمة المالكية الرقمية على الشخص دون فرق بين زمن وآخر ولكن الشرع المارتيشي دفي عقوبة الجريمة التي ضحيتها حدث لم يبلغ الثامنة عشرة من عمره، وأيضاً فإن الجريمة بالابتزاز والتهديد. وقد تقع الجريمة المالكية الرقمية على الدول بقصد الحيلولة من سيادتها لتشجيع المواطنين على عدم احترام قوانينها وتدمير هاوديانتها السماوية، وشن الحروب بالمالكية الرقمية والحرب المالكية الرقمية.

13. الجرائم المالكية الرقمية تختلف بحسب الأساس والمعيار الذي يستند إليه الفقهاء في تقسيمهم لهذه الجرائم فبعضهم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بوساطته، وبعضهم يصنفها إلى أنماط تستند إلى أساس الوسيلة المتبعة في الجريمة، وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء.

14. يعد التشريع في الجرائم المالكية الرقمية أمراً عسيراً لبس أن الحصول الأدلة، سيما أن الجرائم المالكية الرقمية لها طبيعة خاصة، بحيث تحتاج إلى ضرورة طرق خاصة في جمع الأدلة، لذلك قد حددت الاتفاقيات قواعد بسيطة إجراءات لجمع الأدلة بحيث أوجبت ضرورة الحفاظ السريع على المضمون البيانات المخزنة وجعلتها كونها سرية.

15. يثير التشريع المكونات المعنوية للحاسوب جدالاً كبيراً في الفقه، بالإضافة إلى أن التشريع النص على المكونات المادية في محور الجرائم المالكية الرقمية يسهل إجراؤه وتطبيق عليه القواعد القديمة للتشريع.

5.2 التوصيات

هناك عدد من التوصيات التي خلصت إليها هذه الدراسة والتي تفيد المشرع الإماراتي في المستقبل من خلال تفعيل النصوص القانونية الموجودة في قانون الإجراءات الجزائية لدولة الإمارات العربية المتحدة رقم (35) لسنة 1992 وتتبع التوصيات مبينة أن هذه الدراسة أعضاء النيابة العامة وقد أفراد الضبط القضائي وأخيراً تفيد هذه الدراسة المحامين والمواطنين كافة. هذه التوصيات جاءت على النحو التالي:

1- لابد من التعاون القانوني إجراء المزيد من الدراسات حول الجريمة الإلكترونية وبالخص الشركات الموضوعية والجرائم المتعلقة بها, ومدى استخدام الأدلة في مجال الإثبات الجنائي وذلك تسيراً مواكباً للتطور الذي أصبح جزءاً من حياة الفرد أهمية في الكشف عن الجرائم الكشاف الحقيقة التي تركز على القوانين في دولة الإمارات العربية المتحدة.

2- عمل مؤتمرات وندوات تجمع بين رجال الضبط الجنائي في دولة الإمارات العربية المتحدة وهيئة الدولة في النيابة العامة تشكل دوري وإيجاد الحلول المناسبة لمكافحة التشريع الإماراتي.

3- إجراء المزيد من الندوات في الإجراءات الجزائية الإماراتية بموضوع الجريمة الإلكترونية ليس فقط بشأن الكشاف الجرائم بل بسدد جميع الجرائم الخطرة، وبناءً عليه حماية المجتمع من تلك الجرائم وتحقيق الردع العام.

4- ضرورة تركيز المشرع الإماراتي لموضوع تعويض المضرور عن الضرر الذي أصابه من خلال الجريمة التي يمس تشكل مباشر أو بشكل غير مباشر، وذلك إلى جانب المسألة الجزائية, من خلال النصوص المواد المختلفة.

5- الحث على الاهتمام بموضوعات تدريس الجريمة الإلكترونية في الجامعات الإماراتية والعربية والدولية، نظراً لأهمية هذا الموضوع في الكشف عن الجرائم وسرعة وقت على ذلك.

6- نص المشرع الماليزي بفرض نصوص قانونية تنظم جرائم الاعتداء على المسائل الحياتية بشأن الجرائم الالكترونية, كون المشرع عليه نظم جريمة الاعتداء على معلومات الشخصية التي تمس الحق والصفة قبل الشخص بشكل دقيق, لم وعقب المشرع الفرنسي الذي نظم أحكام خاصة بمعالجة البيانات والحريات بحيث حظر الاعتداء على الأمور الحياتية وانتهاكها, وذلك في القانون رقم 17 لسنة 1978.

7- نص المشرع عن تنظيم الأحكام الخاصة التي تحتوي مواضيع من نصوص قانونية خاصة, سيما أن القوانين الخاصة قد جاءت في بعض منها لتنظيم قوانين هي وضوح المعيار في التنظيم بالجرائم عن تنظيم قانوني حيث لم يظهر لنا العقوبة الشدة أو المخففة, هذا من جانب أخر, ولم يبين لنا المشرع سواء في القوانين العامة أو الخاصة القوانين تثبتوي قانونية أو لائحية التشريعية لها في ظل يبين لنا فقط العقوبة على تنزيرها واختراقها, لذلك يقتضي الأمر ضرورة تدخل المشرع عن تنظيم هذا الأمر.

8- نص المشرع الماليزي نص صراحة على جواز تفتيش المكون المعنوي لكمبيوتر وضع عقاب طقانونية لها.

Universiti Utara Malaysia

REFERENCES/قائمة المراجع والمصادر

"السلامة السيبرانية والأمن الرقمي البوابة الرسمية لحكومة الإمارات العربية المتحدة ". U.Ae, Last modified 2020. https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security.

"ما هي الجرائم الإلكترونية بيوت في الإبلاغ عنها - عقوبتها - الجهات المختصة | مايبيوت". مدونة تشمل مواضيع تتعلق بالعقارات و أنماط الحياة المختلفة في الإمارات | مايبيوت. https://www.bayut.com/mybayut/ar/%.

Ali, Mohamed. "قانون الجرائم الإلكترونية الإماراتي - قوانين الجرائم الإلكترونية في الإمارات المحامين في دبي | المستشارين القانونيين في دبي, Last. ". Lawyers In Dubai | Legal Consultants In Dubai https://hhslawyers.com/ar/blog/ .

bin Salem Al, Abdullah bin Ali. "Electronic Crime in the Sultanate of Oman: Challenges and legal solutions: الجريمة الإلكترونية في السلطنة عمان: التحديات والحلول القانونية." مجلة العلوم الاقتصادية والإدارية والقانونية 3.2 (2019)

بلسام بغو. "إجراءات المتابعة الجزائية في الجريمة المعلوماتية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2016)

إبراهيم رمضان إبراهيم عطايا: الجريمة الإلكترونية في الشريعة الإسلامية والأنظمة الوضعية, ج2 العدد30, طنطا سنة 2015م.

إبراهيم رمضان إبراهيم عطايا: الجريمة الإلكترونية في الشريعة الإسلامية والأنظمة الوضعية, ج2 العدد30, طنطا سنة 2015م.

إبراهيم, رشيد شير."التفتيش القانوني في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبوظبي". مركز الإمارات للدراسات والبحوث القانونية العدد313، 2018 .

بلوالربن بيل محمود."مفهوم الجرائم المعلوماتية وتحديات التشريع في فلسطين". أطروحة ماجستير, جامعة النجاح الوطنية, 2018.

أحمد البرندية, فحي ظبي ليم انفب إلى سبوك والجرائم الإلكترونية في عمان: هل هناك علاقة؟ ". Journal Of Information Studies & Technology (JIS&T) 2019, no. 2 (2019). doi:10.5339/jist.2019.7.

أحمد بلبك الشيخ أحمد: تعريف الجريمة الإلكترونية تعريفا كاملا, تواريخ النشر 2016, https://specialties.bayt.com/

أحمد بوطيبة بوعلي: الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي دراسة للتجربتين السعودية والقطرية- الكتيبة في الدراسات الاجتماعية والإنسانية, قسم العلوم القانونية والقانونية العدد 16- جوان 2016.

أدهم بلمن مربغدادي: وسائل البحث والتحري عن الجرائم الإلكترونية, رسالة قدمت لنيل درجة الماجستير في القانون العام- جامعة النجاح الوطنية, نابلس سنة 2018.

ارحومة, موسى مسعود. "إشكاليات الإجراءات التي تثيرها الجريمة المعلوماتية عبر الوطنية". ورقة مقدمة إلى المؤتمر المغاربي الأول. طرابلس: أكاديمية الدراسات العليا, 2009.

رأي جمال حسن سراحنه بشأن قانون الجرائم الإلكترونية الفلسطيني لعام 2018 على المحتوى السياسي في سبوك الصفحتين والمدونين نموذجا. رسالة ماجستير، جامعة القدس، 2019 .

أسامة أحمد المناعسة وآخرون ، جرائم الحاسب الآلي والإنترنت - دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر - عمان - الأردن ، 2000.

بلمهان بوزيان فاطمة. "الجريمة الإلكترونية وإجراءات التشريعية لمواجهتها في الجزائر". مجلة الأستاذ الباحث للدراسات القانونية والسياسية العدد 11، 2018.

آلان شيان ناصر. "إثبات الجريمة الإلكترونية –دراسة تأصيلية تطبيقية". أطروحة ماجستير, جامعة زيان عاشور الجلفة, كلية العلوم الآلية, 2012.

إلهام بوالطمين. "الإثبات الجنائي في الجرائم الإلكترونية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2018).

ايمان الحياري: مفهوم الحرب الإلكترونية بتواي النشر 22 أغسطس 2018 أخر تحديث الساعة 21:28, https://mawdoo3.com/

إيمان, مديرة. "الجريمة الإلكترونية عبر الإنترنت في أوساط الطلبة الجامعيين". رسالة ماجستير, جامعة محمد بوضياف المسيلة, 2015.

أيمن سالمة: لمانظيص على التعاون الدولي في مجال مكافحة الجريمة السيبرانية, قال مرشو ربتوا يخ يوليو 2021 مبأو ظبي, عربية يوز, www.skynewsarabia.com

البداينة ذياب. "الجرائم الإلكترونية المفهوم والأسباب In المنتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية. عمان، الردن كلية العلوم الإستراتيجية جامعة نايف العربية للعلوم الأمنية, 2014.

براهيمي جمال التحقيق الجنائي في الجرائم الإلكترونية, رسالة قدمت لنيل شهادة الدكتوراه في العلوم تخصص القانون, جامعة مولود معمري تيزي وزو كلية الحقوق والعلوم السياسية, قسم

بالسجن أجرة: الإنترنت والابتزاز الإلكتروني، بدون نشر، سنة 2019.

بن مهجع، عن زيس يمان. "وسائل التحقيق في جرائم نظم المعلومات ,.M.A ."جامعة رايف العربية للعلوم الأمنية, 2003.

تركي, نهى كامل."التحقيق الجنائي في الجرائم الإلكترونية ,Amday55.Blogspot.Com ". Last modified 2019. https://amday55.blogspot.com/2016/04/blog-post.html

توهامي بدرالدين. "العولمة الثقافية والسياسات الاجتماعية لمواجهة التحيال والجريمة الإلكترونية في ظل متغيرات عض الدول العربية نموذجا." مجلة دراسات في علوم الإنسان والمجتمع 1.01)2018(: 26-08.

الجرائم الإلكترونية دبي: الشرطة تلقي البلاغ عن الجرائم الإلكترونية, https://www.bayut.com/mybayut/ar/ بدون تواريخ نشر

الجزيرة: الجرائم الإلكترونية- احذر هجوم بك, تواريخ النشر 2019/7/22 https://www.aljazeera.net/

الجنيدي خليل. "الاتفاقيات الدولية والوطنية في مكافحة الجرائم الإلكترونية". الحوار المتمدن, 2017. https://www.ahewar.org/debat/show.art.asp?aid=571423 .

حاج سودي محمد: شكالية تطبيق التفتيش في الجرائم الإلكترونية, مجلة الفقه القانونية- المجلد 11 العدد 1 سنة 2019- رقم العدد التسلسلي 18, جامعة أدرار.

حسن الشوبكي: جرائم السرقة والهجمات الإلكترونية, تواريخ النشر 2014/11/18 https://www.ammonnews.net/

حسنية, أحمد أسامة."الجريمة الإلكترونية بين الشرعية الجنائية والإجرائية". مجلة جامعة الأزهر, سلسلة العلوم الإنسانية 19)2017(: 1-42 . http://www.alazhar.edu.ps/journal/detailsr.asp?seqq1=3363.

الحضري, عبد الله محمد. ""جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية لأنظمة المعلومات في القانون القطري "دراسة تحليلية مقارنة"،". رسالة ماجستير, جامعة قطر, 2020.

الخروق سنة 2018.

حمايشير. "خصوصية التحقيق في الجريمة الإلكترونية". رسالة ماجستير جامعة محمد بوضياف المسيلة, 2019.

خالد ممدوح إبراهيم:فن التحقيق الجنائي في الجرائم الإلكترونية، ط1, دار الفكر الجامعي، الإسكندرية-مصر،2010م, ص194.

Universiti Utara Malaysia

خلفية, احمد and ألمير فخوظة. "الجريمة الإلكترونية وآليات التصدي لها". مجلة التميز للبحوث القتصاد والإدارة 1 (2017): 148-170. 1 , no. https://www.asjp.cerist.dz/en/article/64136.

خلفية, مصطفى. "استراتيجية إماراتية لمواجهة الجرائم الإلكترونية" البيان , Last modified 2013. https://www.albayan.ae/across-the-uae/accidents/2013-09-26-1.1967235.

الخوالدة, ليمان. "جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات في التشريع الأردني :دراسة مقارنة". رسالة ماجستير, الجامعة الأردنية, 2012.

د.جميل عبد الباقي الصغير ،القانون الجنائي والتكنولوجيا الحديثة الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية - القاهرة ، 1992.

د.محمد سامي الشوا ،ثورة المعلومات وانعكاساتها على قانون العقوبات ، الطبعة الثانية ، دار النهضة العربية - القاهرة ، 1998.

د.هلالي عبد اللاه أحمد ،الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء مشروع اتفاقية بودابست الموقع في 23 نوفمبر 2001(،الطبعة الأولى ، دار النهضة العربية - القاهرة ، 2006.

دعاء سليمان عبد القادر التميمي: جريمة الابتزاز الإلكتروني, رسالة مقدمة لنيل درجة الماجستير - القدس فلسطين سنة 1440 هـ 2019م.

ربيع عبد اللطيف محمود. "الجرائم الإلكترونية" التجريم والمكافحة والإثبات(. المؤتمر الأول للجرائم الإلكترونية في فلسطين نابلس: جامعة النجاح الوطنية, 2016.

رزيق قبودودة. "الحماية الجنائية للتجارة الإلكترونية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2015)

رشيد بن فويحة and مهيوبي يوسف."التحريات الجنائية في مسرح الجريمة الإلكترونية = The Criminal Investigation In Cyber Crime Scene". مجلة جامعة القدس المفتوحة للأبحاث والدراسات. doi:10.12816/0043008 .52-60 :(2017) 421 .no ,

رشيد قواريش ونورة قواوش "تأثير موقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية في وسط المراهقين)دراسة ميدانية بثانوية كريم بلقاسم بالي القنيرة(. رسالة ماجستير، جامعة أكلي محند أولحاج البويرة، (2018)

رماح الغلاييني: قد تشل دوالب أكبر اقتصاد العالم بالإلكترونية, نشر الجزيرة 2020/1/7 https://www.aljazeera.net/

زبدة نور الدين. مداخلة بعنوان "معوقات سير المرفق العام الإلكتروني الجريمة الإلكترونية أنموذجا الكلية الحقوق جامعة البليدة، (2019)

الزندي، إبراهيم and زكريا هامل. "إجراءات التفتيش في الجرائم الإلكترونية وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية قانونية". مجلة الدراسات القانونية جامعة أقلي محمد أولحاج البويرة, no. 11 (2020): 109-122.

بن بحة, نور الهدى. "التفتيش في الجرائم الإلكترونية." رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2016)

بن زيدات, لخضر, يوسف. "حدود قانون الإجراءات الجزائية في السيطرة على السرقة الإلكترونية "التجسس الإلكتروني" في ظل المؤتمر الدولي لمكافحة الجرائم الإلكترونية في فلسطين. نابلس: جامعة النجاح الوطنية, 2016.

بن سيريم. "الحماية الجنائية للمعلومات الإلكترونية ,.M.A ". جامعة أبي بكر بلقايد, 2016.

بن مالك, عبد العزيز. "السياسة الجنائية لمشرع الإماراتي في مواجهة الجرائم المعلوماتية في ظل المرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات ,.M.A ". جامعة الإمارات العربية المتحدة, 2018

بن هرماس بلهادي، الهادي: قانون الإجراءات الجزائية, ط2, ج2, غرداية سنة 2014.

بن جيدة, رمسيس, بحاش خيرة, بن نخلة زهرة, و سعيدشيماء. "أثر استخدام موقع التواصل الاجتماعي في انتشار الجريمة الإلكترونية". مذكرة ليسانس, جامعة محمد بوضياف المسيلة, 2019.

بن ليمان بن عبد الرزاق الغيان وبن جيبن مبارك خطبة و عز الدين بن عبد العليم: صور جرائم الإنترنت الإلكتروني ودوافعها وآثارها السلبية المترتبة عليها من وجهة نظر المعلمين ورجال الأمن المستشارين القانونيين, مجلة البحوث الأمنية-المجلد 27و 69 كلية الملك فهد الأمنية- مركز البحوث والدراسات,- دار المنظومة سنة 2018م.

بن مية بو مروان: الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية, ط1, مكتبة القانون والاقتصاد, الرياض سنة 1435 هـ- 2014م.

بن يدس يدطن طاوى محمد. "الجريمة المعلوماتية الصعوبات التي تواجه التعاون الوطني والدولي ولكيفية مكافحتها". المركز الديمقراطي العربي. Last modified 2018. https://democraticac.de/?p=54584.

شرف الدين وردة وباجراف سامية: الجوانب الموضوعية والجزائية لمكافحة جرائم المعلوماتية في التشريع الجزائري, مجلة من الأبحاث والدراسات القانونية والسياسية, العدد الثالث ديسمبر 2017.

شهرزاد حداد. "الدليل الإلكتروني في مجال التفتيش الجزائي". رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، (2017)

الشهري, حسن. "قانون دولي موحد لمكافحة الجرائم الإلكترونية قانون دولي موحد لمكافحة الجرائم الإلكترونية تصور مقترح". المجلة العربية للدراسات الأمنية والتدريب no. 27 , 35 (2011): 5- 45.

صراولي, عبد المالك."تشريعات الجريمة الإلكترونية في البيئة العالمية". مجلة الحقوق والعلوم السياسية.474 -458 :(2018) 10 no. ,

صبرينة, قمراني and ,قدمشيلة."تأثير الجريمة الإلكترونية على المعلومات القيمية". المجلة الجزائرية للأبحاث والدراسات 159.3 -137 :(2019) 9 no. ,

صغيري, يوسف: الجريمة المرتكبة عبر الانترنت, وزارة التعليم العالي البحث العلمي- جامعة مولود معمري تيزي وزو- كلية الحقوق والعلوم السياسية, رسالة مقدمة لنيل شهادة الماجستير في القانون سنة 2013م.

الصيقل, نايف بن إبراهيم. "العوامل المحددة للجرائم الإلكترونية أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية, 2017.

الضويحي, نشر فبن عبد الله. الأمن الفكري الجرائم المعلوماتية وعلاقتها بالاعتداء الشخصي. الطبعة الأولى. السعودية: المعهد العالي للقضاء, 2008.

الطائي, جعفر حسن جاسم: جرائم تكنولوجيا المعلومات، دار البداية، ط1 سنة 2007.

الطائي, جعفر حسن جاسم: جرائم تكنولوجيا المعلومات، دار البداية، ط1 سنة 2007.

عبد الرازق, غزال."الجرائم الإلكترونية ضد النساء والفتيات: المخاطر وطرق المواجهة."نتدى المنظمات الأهلية لمناهضة العنف ضد المرأة، المرأة والعالم وتحديات ثورة الاتصال، (2017)

عبد اللطيف, محمود ربيع: الجرائم الإلكترونية التحريم والمكافحة والإثبات, مقدم إلى المؤتمر الأول للجرائم الإلكترونية في فلسطين المنعقد في جامعة النجاح الوطنية نابلس - 7 نيسان 2016م.

عبد الباقي, مصطفى حسين."التوجه في الجريمة الإلكترونية تشابكات في فلسطين : دراسة مقارنة". دراسات - علوم الشريعة والقانون, 2018, 284-986-045-0272/10.35516:doi . 017.

عبد الحكيم, موالي بهراهيم:الجرائم الإلكترونية- مجلة الحقوق والعلوم الإنسانية- جامعة زيان عاشور بالجلفة-الجزائر, المجلد ع23, دار المنظومة تونس سنة 2015م.

عبد اللا دغمش العجمي: المشكلات العملية والقانونية للجرائم الإلكترونية,مقدمة هذه الرسالة استكمالاً للحصول على درجة الماجستير في القانون العام, جامعة الشرق الأوسط سنة 2014.

العبيدي, أسامة بن غانم. "التفتيش عن الدليل في الجرائم العلوماتية". المجلة العربية للدراسات الأمنية والتدريب 29.. doi:10.12816/0001809. 132-85 :(2013) 58 no. ,

العجمي, عبد الله دغش. "الشركات العملاقة والقانون الجرائم الالكترونية : دراسة مقارنة". رسالة ماجستير, جامعة الشرق الأوسط, 2014.

العربي, نادر جبريل. "الجرائم الالكترونية " الأهداف الأسباب - طرق الجريمة ومعالجتها" - المركز الديمقراطي العربي". المركز الديمقراطي العربي. Last modified 2016. , https://democraticac.de/?p=35426.

عطية عثمان محمد بوحيش. حجية الدليل الرقمي في إثبات جرائم العلوماتية ، رسالة الماجستير، مقدمة إلى أكاديمية الدراسات العليا فرع غازي لعام الجامعي 2009.

الفقي, يوسف خليل يوسف. "الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة، رسالة ماجستير ،الجامعة الاسلامية، غزة،2013.

عمر, محمد أحمد عبد الرحيم. "تطبيق أساليب مواجهة الجريمة الالكترونية في نظام الإدارة العامة للجوازات والهجرة" الكاليوس, جامعة الخرطوم, 2007.

عوادي, نادر. "أثبات الجريمة الالكترونية قبل الدليل العلمي". مجلة جامعة تكريت للحقوق 3 1 no. , (2017): 476-506.

فاطمة الزهراء, بخي. "إجراءات التحقيق في الجريمة الالكترونية". رسالة ماجستير, جامعة الجيلالي, 2014.

فجاج يوسف, الإطار الجزائي الدولي في مجال البحث عن الجريمة الالكترونية, مجلة الفقه والقانون, ص186. شارل يهدى أدهم بلسم نمرب غدادي: وسائل البحث والتحري عن الجرائم الالكترونية, رسالة مقدمة لنيل درجة الماجستير في القانون العام الكلية الدراسات العليا- جامعة النجاح الوطنية نابلس فلسطين سنة 2018.

فيروز عوض الكريم صالح ميرغني. إجراءات التحري والضبط في الجريمة الالكترونية، أطروحة دكتوراه، جامعة شندى السودان. 2017.

القانون الاتحادي رقم)2(لسنة 2016 تعديل المرسوم بقانون اتحادي رقم)5(لسنة 2012 في شأن مكافحة جرائم تقنية العلومات –وزارة العدل.

قانون شرتوب ادل بالإمارات في إمارة دبي المرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية العلومات.

كامل فهمي السالك: محاضرة ألقيت في مؤتمر الجمعية السورية للعلوم في حلب عام 2000- ندوة القانون مية وجتمع العلوماتية-حلب 21-23 تشرين أول 2000

كامل مطر: الجريمة الالكترونية, ب ش, ب س.

Universiti Utara Malaysia

الزيزص باح, & مي رقط. "أثر الجرائم الإلكترونية على أمن واستقرار الدول: قصة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجا". مجلة الزلزال للدراسات السياسية, 2018, 119 . doi:10.37136/1999-000-003-006.

لطرش فيروز & بن عزوز حاتم. "الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة." الفكر القانوني 1.1 (2016)

لطيفة شالخ, ورقية شيالحاج ابراهيم. "التشار الجريمة الإلكترونية المرتكبة ألشخاص في البيئة الجزائرية دراسة ميدانية لعينة من مستخدمي شبكة الفايس بوك". رسالة ماجستير, جامعة محمد بوضياف المسيلة, 2017.

ليلى حسين فالعية القوانين الوضعية والولي في مكافحة الجرائم الإلكترونية, قسم القانون في الكلية الجامعية العربية في الدنمارك.

مجلة المفكر الحلول القانونية والسياسية: معوقات التجارة الإلكترونية ومتطلبات النظام القانوني لمواجهتها)دراسة مقارنة(- العدد الثاني السنة السابعة 2017م.

مجمع البحوث والدراسات الأكاديمية الطالطان قبلوسل علوم الشرطة : الجريمة الإلكترونية في المجتمع الخليجي والكفيلة مواجهتها, مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية فائز بالمركز الأول في المسابقة, مجلس التعاون لدول الخليج العربية- 2016.

محمد شرف الدين: الجريمة الإلكترونية والجرائم العلوماتية, علوم قانونية تواي خالنشر 8 مارس 2015 https://www.facebook.com/egy.law

محمد محي الدين عوض: معوقات مكافحة الجرائم العلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم العلوماتية في الأجهزة الأمنية, مجلة جامعة الشارقة- دورية علمية محكمة في علوم القانوني, المجلد 16 العدد 1 شوال 1440هـ/يونيو 2019م.

محمد مي لبقشير, ويسوف عثمان يوسف "بتوظيف برامج العاقات العام في التوعية بمخاطر الجرائم الإلكترونية دراسة تحليلية وصفية على إدارات المسؤولة عن الجرائم الإلكترونية)وزارة العدل، وزارة الداخلية ووزارة النقل والاتصال السلكي واللاسلكي في الفترة بين 2016-2017م". مجلة العلوم الإنسانية 19 :156-175 (2018) 2 no. ,

مجلة دابراهيم الغبي فعلية القوانين التشريعات العربية في مكافحة الجرائم الإلكترونية, المجلة العربية للنشر العلمي العدد السابع الثلاثون بتواي خالصدار 2 تشرين الثاني سنة 2021م.

السماعدة, أنور. "الكيفية الاختصاص في الجرائم الإلكترونية". المجلة الأردنية القانون 2018 no. , 4 (2019). doi:10.29117/irl.2018.0043.

مصطفى خليفة إستراتيجية إماراتية لمواجهة الجرائم الإلكترونية, نشر 26 سبتمبر 2013, /https://www.albayan.ae

القصودي, محمد بن أحمد علي. "الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً". المجلة العربية للدراسات الأمنية والتدريب, 2017. doi:10.26735/13191241.2017.004.

زين الدين هيثم: الحماية الجنائية للمعاملات الإلكترونية, ط1, دار الفكر الجامعي, الإسكندرية سنة 2006.

مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: جمع وتبادل الأدلة بالطرق الإلكترونية- ورقة معلومات أساسية من إعداد الأمانة, 27, 28 تشرين الأول / أكتوبر 2015.

مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية: جمع وتبادل الأدلة بالطرق الإلكترونية- ورقة معلومات أساسية من إعداد الأمانة, 27, 28 تشرين الأول / أكتوبر 2015.

ميادة عبد الله مصطفى حربي: "التحقيق وجمع الأدلة في الجرائم الإلكترونية وطرق مكافحتها: رسالة ماجستير، جامعة نايف العربية، دراسة مقارنة." (2016)

نهلي رحيمة: خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة, أعمال المؤتمر الدولي الرابع عشر -الجرائم الإلكترونية, طرابلس 24-25 مارس سنة 2027م.

هيام محمد الهادي بتعرض المرقمي للجرائم الإلكترونية عبر وسائل الإعلام المرقمي وتأثيرها على ادراك المسألة من المجتمع المصري, المجلة العربية للبحوث الإعلام والاتصال –العدد 30 يوليو/ أغسطس/ سبتمبر سنة 2020, الجمعية المصرية للعلاقات العامة- جامعة بنها- مصر.

وليد طه بتاني المنظمة الشرعية للجرائم الإلكترونية في القانون الليبي والمقارنة, جامعة مصراتة, بدون نشر أو سنة.

يوسف فيصل التحقيق في الجريمة الإلكترونية. رسالة ماجستير، جامعة محمد بوضياف المسيلة, 2017.

يوسف خليل يوسف الشريفي: الجرائم الإلكترونية, رسالة مقدمة لنيل درجة الماجستير, غزة سنة 2013م.

يوسف فزيدات, د. لجبس. "مدى تأثير عبء الإثبات في الجرائم الإلكترونية- دراسة مقارنة ." Rule Of Law And Anti-Corruption Center Journal 2019, no. 2 (2019). doi:10.5339/rolacc.2019.9.

يونس عرب: قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان, ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية, المنعقدة بمسقط سلطنة عمان, 4-2 يوليو 2006م, ص55 نقلا عن مصطفى يوسف.