جرائم الإرهاب الالكتروني عبر الإنترنت

م.د. عادل محمد على مصطفي
جامعة الاسراء - كلية القانون- بغداد \ العراق

Cyber Terrorism Crimes on the Internet

Lect. Dr. Adel Mohamed Ali Mustafa
Al- Esraa University – College of Law, Baghdad / Iraq
Adel.mohamed@esraa.edu.iq

المستخلص

لقد أصبح الإرهاب الإلكتروني خطراً يهدد العالم بأسره بما ينتج عنه من مخاطر تتفاقم بمرور الزمن، لأن التقنية الحديثة وحدها غير قادرة علي حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة علي الأفراد والمنظمات والدول وخاصة علي المستوي القومي. فلا أحد ينكر أن إرهاب الأمس أصبح مختلف عن الإرهاب اليوم، فالإرهابي بالأمس كان يتسلح ببندقية، أما الإرهابي اليوم فأصبح يتسلح بالتكنولوجيا والمعلومات مستخدما جهاز الحاسب الآلي الذي حول الإنترنت لأداة رئيسية في النشاط الإرهابي الدولي، فقد خدم الإنترنت الخلايا الإرهابية، من حيث تضخيم الصورة الذهنية لقوة وحجم تلك الخلايا التي تمتلك عددا قليلا من الأفراد لديهم خبرة بالإنترنت لبث رسائل إعلامية تخدم أهدافهم الإرهابية. ولقد سعت العديد من الدول إلي اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلي المزيد لمواجهة هذا السلاح الخطير وهو ما سوف نوضحه في هذا البحث.

الكلمات المفتاحية: الارهاب الالكتروني، جرائم، الانترنت

Abstract

Cyber terrorism has become a threat to the entire world, with risks that increase over time , Because modern technology alone is not capable of protecting people from cyber terrorism operations, which It has caused serious damage to individuals, organizations, and countries, especially at the national level. No one can deny that Yesterday's terrorism is different from today's terrorism. Yesterday's terrorist was armed with a rifle, while today's terrorist Today, he is armed with technology and information, using the computer which has turned the internet into a tool A key player in international terrorist activity, the internet has served terrorist cells by amplifying their image. The mindset is that these cells, with their small number of individuals, have internet experience to broadcast media messages that serve their terrorist objectives. Many countries have sought to take measures and precautions to counter cyber terrorism, but these Efforts are limited and more are still needed to counter this dangerous weapon, which we will explain in this research.

Keywords: Cyber terrorism, Crimes, Internet.

مقدمة

اولا:- موضوع البحث

تعتبر الجرائم الإلكترونية أحد أهم ثمار التقدم العلمي السريع في كافة المجالات العلمية التي يتميز بها عصرنا الحاضر، ولقد صاحب التقدم الكبير في مجال العلوم والتكنولوجيا واستخداماتها لخير الإنسانية تقدم آخر وموازي في عالم الجريمة[1].

فعصر الإنترنت أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية أو عصر الاتصالات الحديثة، كل هذه الأوصاف إنما تعبر عن مدي التطور العلمي والتقني المتسارع والقفزات العلمية الضخمة التي تحققت، ومدي تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الفترة الأخيرة، وأصبحت المعلومات في حد ذاتها هي المادة الخام الأساسية للإنتاج التي يعتمد المجتمع علي توفيرها والإستفادة منها، هذا الوجه المشرق للمعلومات يقابله من الجانب الآخر وجة مظلم تمثل في الإجرام المعلوماتي [2].

فالثورة التكنولوجية الحالية في مجال الاتصالات عن بعد قد خلفت وراءها العديد من الجرائم المستحدثة التي لا تعترف بالحدود بين الدول والقارات، كما أتاحت فرص إرتكاب الجرائم التقليدية بطرق غير تقليدية، فيمكن أن يكون الجاني في بلد معين ويرتكب الجريمة في بلد آخر، الأمر الذي ساعد المجرمين علي إرتكاب العديد من الجرائم دون إمكان القبض عليهم[3].

فعلي سبيل المثال نجد أن استخدام البريد الإلكتروني كوسيلة اتصال بين المجرمين، يتعذر معه مراقبتهم علي النحو الذي يحدث في الاتصالات السلكية واللاسلكية.

كذلك فإن عمليات التحويلات المالية الإلكترونية قد تتم بين الجناة والذين قد يكونوا فرادي أو جماعات بغرض تمويل العمليات الإرهابية دون أن يتم إكتشافها.

1- الدكتور / عبدالله عبد الكريم عبد الله، (2007) جرائم المعلوماتية والإنترنت، طبعة أولي، منشورات الحلبي الحقوقية، سوريا، ص15

2- الدكتور/ هلالي عبد الإله أحمد، (2003) الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، ص12

3- الدكتور/ علي محمود علي حمودة، (2003) بحث بعنوان: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية. أكاديمية شرطة دبي، مركز البحوث والدراسات العدد 1 لسنة 2003 من 26- 28 ابريل 2003، دبي، الإمارات العربية المتحدة منشور علي الموقع الإلكتروني.

http://www.f.law.net/law/threads/11333.

والخطير في الأمر أنه يصعب السيطرة علي شبكة الإنترنت وعلي الجرائم التي ترتكب عليها، ومن الصعب اكتشاف هذه الجرائم أو تحديد مصدرها، حيث يستخدم الجاني إسماً مستعاراً، أو يرتكب فعلة من خلال إحدى مقاهي الإنترنت، لذلك فإن جرائم الإرهاب التي ترتكب عبر الإنترنت غالبا ما تقيد ضد مجهول، وفي حالة اكتشاف هذا المجهول، فمن الصعب إقامة الدليل عليه ومحاكمته، فالإرهابيون الذين يستخدمون البريد الإلكتروني في إصدار تكاليفاتهم بارتكاب جرائم الإغتيالات والتخريب وغيرها يكون من الصعب – إن لم يكن من المستحيل – مراقبتهم علي النحو الذي كان يحدث في الاتصالات السلكية واللاسلكية.

وقد تواترت غالبية دول العالم علي إنشاء شبكات للمعلومات لوزارات الدفاع والمؤسسات الاستراتيجية والحيوية الخاصة بها بحيث أدرجت بتلك الشبكات أسرارها المتعلقة بالدفاع وأحاطت تلك الشبكات

بسياج منيع من أساليب التقنية الفنية والتكنولوجية حتي لا يتم اختراقها أو التجسس عليها، إلا أنه قد أمكن اختراق تلك الشبكات والتجسس عليها، وأصبح مألوفا أن تطالعنا وكالات الأنباء العالمية والصحف بجرائم اختراق وتجسس لتلك الشبكات، سواء من جانب الأفراد أو من جانب الدول علي بعضها[1].

ثانيا:- اهمية البحث

تأتي اهمية هذا البحث من خلال عدة نقاط:-

1 – اهمية القضية التي يتناولها وهي الارهاب الالكتروني عبر الانترنت، بما يشكله من خطر نظرا لتنوع واتساع مجال أهدافه.

2 – التأثير البالغ لجريمة الارهاب الالكتروني علي الامن القومي، ومناخ الاستقرار، واثارة مشاعر الخوف والاحباط لدي الراي العام، مما يعطل مسيرة التقدم والتنمية وبرامج الاصلاح الاقتصادي.

3 – اهمية استخدام شبكة الانترنت كوسيلة اتصال عالمية.

4 – اهمية نشر الوعي والثقافة الالكترونية لدي مستخدمي المواقع الالكترونية للحماية من الوقوع ضحية لجرائم الارهاب الالكتروني.

1- الدكتور/ عماد الدين محمد كامل الجمل، الحماية الجنائية لأسرار الدفاع في مواجهة التقدم التكنولوجي الحديث، دراسة مقارنة رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، صـــــ1ـــــــــ.

ثالثا:- اشكالية البحث

تمثلت اشكالية البحث في وجوب تحديد المدي الذي نجح فيه المجتمع الدولي من صياغة تعريف للإرهاب الالكتروني،مما يسهم في مكافحته وتحديد انتشاره،وما يتضمنه من مخاطر علي المجتمع الدولي، فجريمة الارهاب الالكتروني جريمة دولية تشكل تهديدا للمجتمع الدولي بأثره، وللدولة التي يقع فيها علي حد سواء.

رابعا:- منهجية البحث

سوف نتبع في هذه الدراسة المنهج التحليلي والمنهج المقارن لكي يتناسب مع موضوع البحث، فالمنهج التحليلي لتحليل نصوص التشريعات الوطنية للوقوف علي افضل السبل لمواجهة جريمة الارهاب الالكتروني، كما تطرقنا في دراستنا الي المنهج المقارن بين بعض التشريعات والقوانين المقارنة، وذلك للوقوف علي افضل السبل لمواجهة هذه الجريمة.

خامسا:- خطة البحث

لما كان موضوع هذه الدراسة ينصب أساساً علي دراسة جرائم الإرهاب الالكتروني عبر الإنترنت، فإننا لن نعرض للمسائل الفنية إلا عند الضرورة وبالقدر اللازم لفهم المسألة وتقريبها للأذهان حتي نتمكن من اعطائها الوصف القانوني الصحيح.

وفي ضوء ما سبق، فسوف نقسم دراستنا لهذا الموضوع إلي ثلاثة مباحث علي النحو التالي:-

المبحث الأول: مفهوم الإرهاب الإلكتروني وأشكاله ومخاطره.

المبحث الثاني: جرائم الإرهاب الالكتروني عبر الإنترنت في ضوء قانون مكافحة الإرهاب رقم 94 لسنة 2015

المبحث الثالث: نظرية العدول في الجرائم الإرهابية.

المبحث الأول
مفهوم الإرهاب الإلكتروني وأشكالة ومخاطرة

تمهيد وتقسيم:- لقد أصبح الإرهاب الإلكتروني خطراً يهدد العالم بأسره بما ينتج عنه من مخاطر تتفاقم بمرور الزمن، لأن التقنية الحديثة وحدها غير قادرة علي حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة علي الأفراد والمنظمات والدول وخاصة علي المستوي القومي.

ولقد سعت العديد من الدول إلي اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلي المزيد لمواجهة هذا السلاح الخطير وهو ما سوف نوضحة في هذا المبحث من خلال التقسيم التالي:-

المطلب الأول: مفهوم الإرهاب الإلكتروني.

المطلب الثاني: أشكال ومخاطر الإرهاب الإلكتروني.

المطلب الثالث: التجسس الالكتروني علي المؤسسات الرسمية.

المطلب الأول: مفهوم الإرهاب الإلكتروني

قبل التطرق إلي تعريف الإرهاب الإلكتروني لابد أن نشير أولاً إلي تعريف الجريمة الإلكترونية:

أولا:- تعريف الجريمة الإلكترونية

يصعب وضع تعريف عام وشامل لهذه الجرائم، فجرائم الكمبيوتر والإنترنت تعتبر من المسائل الشائكة أمام رجال القانون، بالإضافة إلي أنها أثارت العديد من المشاكل العملية والتي تتمثل في صعوبة تقدير حجم الظاهرة، وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذلك صعوبة توحيد التشريعات وتحقيق التعاون الدولي لمكافحتها[1].

وقد ذهب البعض إلي تعريف الجريمة الإلكترونية بأنها « كل فعل يخالف نص جنائي أرتكب عن طريق الشبكة الإلكترونية» [2].

1- الدكتورة/ نائلة عادل محمد فريد قوره، (2005) جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، صـــــ28ـــــ

2- الدكتور/ نائلة عادل محمد فريد قوره، جرائم الحاسب الآلي الاقتصادية، المرجع السابق، صـــــ21ـــــ

وطبقـا لهـذا التعريـف يجـب أن تتوافـر معرفة كبيـرة بتقنيـات الحاسـوب ليس فقط لارتـكاب الجريمـة، بـل كذلك لملاحقتهـا والتحقيـق فيها، وهـذا التعريف يضيـق بدرجة كبيرة من الجريمة الإلكترونية.

ومن التعريفات المضيقة للجرائم الإلكترونية كذلك ما أورده الفقيه (Merwe) حيث يري أن الجريمة الإلكترونية تتمثل في «الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي»[1]

كما ذهب رأي آخر في الفقه إلي أن الجريمة الإلكترونية هي « أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لدي مرتكب الجريمة»[2]

ومقابل ذلك فإن هناك تعريفات حاولت التوسيع في مفهوم الجريمة الإلكترونية، فعرفها البعض[3] بأنها «كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلي الاعتداء علي الأموال المادية أو المعنوية».

وقد ذهب مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام 2000 إلي تعريف الجريمة الإلكترونية بأنها «أية جريمة يمكن أرتكابها علي نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية»[4].

ولعلنـا نلاحـظ أن هـذا التعريف قد حـاول الإحاطة بجميع الأشـكال الإجراميـة للجريمة الإلكترونيـة، سـواء التي تقع بواسـطة النظام المعلوماتـي، أو داخل هذا النظـام علي المعطيات والبرامـج والمعلومـات، كمـا يشـمل التعريـف جميـع الجرائـم التـي يمكـن أن تقع فـي بيئة إلكترونيـة، فلـم يحصـر الجريمـة المعلوماتيـة في مجـال محدد يتيـح للعديد من صـور هذه الجريمـة الإفـلات مـن دائـرة العقاب، ولعلنـا نؤيد هـذا التعريف نظرا لشـموله لجميع أشـكال الجرائم الإلكترونية.

1- **Merwe (Vander):(1993): computer crimes and other crimes against information technology in south Africa "R.I.D.P, P554.**

2- **Artvr salary,1987 computer relauted Ebejlement, computer and security, vol 6, no 1 , P52.**

3- **حمزه بن عفون، (2012) السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنه، صـــ14ـــ**

4- **الدكتور/ توفيق عبد الله أحمد الخشاشنة، (2016) معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، صـــ31ـــ**

ثانيا:- تعريف الإرهاب الإلكتروني

ذهب البعض إلي تعريف الجريمة الإرهابية الإلكترونية بأنها «أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإرهابي المقصود»[1].

وذهب رأي آخر في تعريفة للإرهاب المعلوماتي الدولي بأنه «هو استخدام الاتصالات الهاتفية ونظم المعلوماتية ومواردها أو التأثير عليها في مجالات المعلوماتية الدولية بهدف القيام بأعمال إرهابية»[2].

ويري رأي آخر أن الإرهاب الإلكتروني هو «العدوان أو التخويف او التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد علي الإنسان في دينة، أو نفسة، أو عرضة، أو عقلة، أو مالة بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتي صنوف العدوان وصور الإفساد، مثل تقديم الوصفات الجاهزة لصناعة القنابل والمفرقعات، ومهاجمة التحكم الوطني في الطيران لإحداث تصادم بين الطائرات"[3].

كما ذهب رأي آخر إلي أن من أشكال الإرهاب الإلكتروني، التجسس الإلكتروني، والأختراقات أو القرصنة علي المواقع الحيوية للمنشآت والمؤسسات الرسمية في المجتمعات المختلفة، والتجنيد الإلكتروني من خلال ما يطلق عليه «التلقين الإلكتروني»، وأخيرا التهديد والترويع الإلكتروني»[4]

ويرى رأي آخر أن الإرهاب السيبراني هو «استخدام الهجمات المستندة إلي الإنترنت في أنشطة إرهابية، بما في ذلك أعمال متعمدة لتعطيل واسع النطاق، في شبكات الكمبيوتر، وخاصة في أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت، عن طريق أدوات مثل فيروسات الكمبيوتر»[5].

1- الدكتور/ عبد الفتاح بيومي حجازي، (2012) الأحداث والإنترنت، أثر الإنترنت في إنحراف الأحداث، دار الفكر العربي، الإسكندرية، صـ17ـ

2- الدكتور/ محمد البخاري طشقند، (2011) الإنترنت ومبادئ الأمن المعلوماتي الدولي «الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول" بحث منشور علي شبكة ضياء للمؤتمرات والدراسات في 2011/7/29 علي الموقع الإلكتروني http://diae.net/4155.

3- الدكتور/ هشام بشير، ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012 بعنوان «مستقبل الإرهاب الإلكتروني» علي الموقع الإلكتروني لجريدة السياسة الدولية التابعة لمؤسسة الأهرام علي الموقع الإلكتروني: http://www.siyassa.org.eg/NewsContent/6/51/2450.

4- Victoria Baranetsky,(2009) What is cyber terrorism? Even experts can't agree, Harvard Law Record, 5 November 2009.

5- Matusitz, Jonathan(2005) "Cyber terrorism" American Foreign Policy Interests2, April 2005, P137 – 147

ويري رأي آخر أن الإرهاب الإلكتروني هو «سلوك غير مشروع يعاقب عليه قانوناً صادر عن إرادة جرمية – مذنبة – ومحله معطيات الحاسب الآلي، لذلك فهي جريمة مستترة تتسم بالسرعة والتطور في أساليب ارتكابها، أقل عنفاً في التنفيذ، وعابرة للحدود ويصعب إثباتها لصعوبة وجود أدلة مادية عليها، ويسهل إتلاف الأدلة الخاصة بها»[1].

وقد ذهب البعض إلي أنها «نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة علي وجدان الأفراد، وإفساد عقائدهم، وإذكاء تمردهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع»[2].

كذلك يمكن النظر إليها علي أنها «استخدام الحاسوب الرقمي بنظمة وبرامجة وملحقاتة ووسائل الاتصال في ارتكاب الجرائم الإرهابية، سواء كانت تلك التقنية هي محل الجريمة أم كانت وسيلة في أرتكابها وسواء كانت عبر شبكة الإنترنت أو بدونها»[3].

وقد ذهب البعض إلى تقسيم الإرهاب الالكتروني إلى ثلاثة مجموعات هي، المجموعة الأولى: الجرائم التي تستهدف النظم والمعلومات كهدف، المجموعة الثانية: الجرائم التي تستخدم وسائل تكنولوجيا المعلومات كوسيلة لارتكاب الجريمة، والمجموعة الثالثة: الجرائم التي ترتبط بمحتوي مواقع المعلومات وبيئاتها»[4].

مما سبق يمكننا تعريف الإرهاب الإلكتروني بأنه «العدوان أو التخويف أو التهديد المادي أو المعنوي باستخدام تقنية المعلومات والوسائل الإلكترونية الصادر عن الدول أو الجماعات أو الأفراد علي الإنسان في دينة أو نفسة أو عرضة أو عقلة أو مالة بشتي صور العدوان والإفساد».

وجدير بالذكر أن المشرع المصري قد عرف العمل الإرهابي في المادة الثانية من القانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب بأنه «كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج، بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو

1- الدكتور/ عبد الفتاح بيومي حجازي، الأحداث والإنترنت، المرجع السابق، صـــ19ـــ.

2- الدكتور/ حسنين المحمدي بوادي، (2006) الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، صـــ54ـــ.

3- الدكتور/ مصطفي موسي، (2005) أساليب إجرامية بالتقنية الرقمية ماهيتها. مكافحتها، دار الكتب القانونية بالمحلة الكبرى،، صـــ74ـــ.

4- الدكتور/ عبد العزيز إبراهيم الشبل، (2007) الجرائم الإلكترونية، ندوة الأمن والمجتمع، الجرائم الإلكترونية، الرياض، 23 ابريل 2007 العدد 14182، النسخة الإلكترونية جريدة الرياض، علي الموقع الإلكتروني:
http://www.alriyadh.com/243897

مصالحة أو أمنه للخطر، أو ايذاء الأفراد أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر،أو غيرها من الحريات والحقوق التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية أو السلام الإجتماعي أو الأمن القومي، أو إلحاق الضرر بالبيئة، أو بالموارد الطبيعية أو بالآثار أو بالأموال أو بالمباني أو بالأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة أو الجهات أو الهيئات القضائية أو مصالح الحكومة أو الوحدات المحلية أو دور العبادة أو المستشفيات أو مؤسسات ومعاهد العلم، أو البعثات الدبلوماسية والقنصلية، أو المنظمات والهيئات الإقليمية والدولية في مصر، من القيام بعملها أو ممارستها لكل أو بعض أوجة نشاطها، أو مقاومتها أو تعطيل تطبيق أي من أحكام الدستور أو القوانين أو اللوائح.

وكذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبنية في الفقرة الأولي من هذه المادة، أو الإعداد لها أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية أو بالنظم المالية أو البنكية، أو بالإقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والمواد الغذائية والمياه، أو بسلامتها أو بالخدمات الطبية من الكوارث والأزمات».

المطلب الثاني: أشكال ومخاطر الإرهاب الالكتروني

لا أحد ينكر أن إرهاب الأمس أصبح مختلف عن الإرهاب اليوم، فالإرهابي بالأمس كان يتسلح ببندقية، أما الإرهابي اليوم فأصبح يتسلح بالتكنولوجيا والمعلومات مستخدما جهاز الحاسب الآلي الذي حول الإنترنت لأداة رئيسية في النشاط الإرهابي الدولي، فقد خدم الإنترنت الخلايا الإرهابية، من حيث تضخيم الصورة الذهنية لقوة وحجم تلك الخلايا التي تمتلك عددا قليلا من الأفراد لديهم خبرة بالإنترنت لبث رسائل إعلامية تخدم أهدافهم الإرهابية.

وقد تعددت أشكال ومخاطر الإرهاب الإلكتروني وذلك على النحو التالي:-

أولا: أشكال الإرهاب الالكتروني

1 – **قيادة الجماعات الإرهابية عن بعد:** حيث يمكن من خلال شبكة الإنترنت بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية، والتي تسيطر علي وجدان الأفراد وتفسد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصلحة المجتمع.

فقد حدث أن وضعت فتاة تنتمي إلي إحدي الجماعات المتطرفة علي موقعها الخاص علي الإنترنت معلومات مفصلة عن كيفية القيام بعمليات التخريب، وكيف يمكن العبث بأسلاك صناديق الاشارات الكهربائية في السكك الحديدية لتعطيل حركة القطارات[1].

2 - **تبادل المعلومات الإرهابية ونشرها من خلال شبكات الإنترنت:**- فعن طريق شبكة الإنترنت يمكن للإرهابيين الالتقاء بسهولة في أي مكان، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين، ويتبادلوا الحديث والاستماع لبعضهم عبر شبكة الإنترنت، بل يمكن أن يجمعوا لهم أتباعا عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية، كذلك أيضا يعتبر البريد الإلكتروني (E-mail) من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدامه في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم[2].

3 - **الحصول علي التمويل:** فمن خلال شبكة الإنترنت وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون علي الشبكة المعلوماتية، من خلال الاستفسارات والاستطلاعات الموجودة علي المواقع الإلكترونية، يقوم الإرهابيون بالتعرف علي الأشخاص ذوي المشاعر الرقيقة، والقلوب الرحيمة، ويتم استجدائهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة وسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية، بطريقة ذكية وأسلوب مخادع، بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية.[3]

4 - **التدريب الإرهابي الإلكتروني:** تحتاج العمليات الإرهابية إلي تدريب خاص، وقد أنشئت معسكرات تدريبية سرية، لكن المشكلة أن هذه المعسكرات دائماً معرضة للخطر، ويمكن

1- الدكتور/ جميل عبد الباقي الصغير،(2002) الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، صـــــ32ـــــــ.

2- للمزيد راجع الدكتور/ عبد الله بن عبد العزيز بن فهد، (2008) بحث بعنوان «الإرهاب الإلكتروني في عصر المعلومات، مقدم إلي المؤتمر الدولي الأول حول «حماية أمن المعلومات والخصوصية في قانون الإنترنت" المنعقد بالقاهرة في الفترة من 2-4 يونيو 2008.

3- الدكتور/ شريف حسين محمد محمد حسن، (2016) القانون الواجب التطبيق علي الجريمة الإلكترونية، رسالة دكتوراه – كلية الحقوق جامعة عين شمس، صـــــ117ـــــــ.

مداهمتها في أي وقت، لذا فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي، كما قامت بعض الجماعات الإرهابية بانتاج أدلة إرشادية للعمليات الإرهابية، تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وهذه الأدلة يمكن نشرها عبر شبكة الإنترنت لتصل إلي الإرهابيين في مختلف أنحاء العالم.[1]

5 – **تدمير المواقع الإلكترونية واتلاف أنظمة المعلومات:**– يقصد بتدمير المواقع الإلكترونية وأنظمة المعلومات، إلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات غالباً ثلاثة أهداف أساسية وهي الأهداف العسكرية، والسياسية والإقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها، ويأتي علي رأسها مراكز القيادة والتحكم العسكري، ثم مؤسسات الخدمات والمنافع كمؤسسات الكهرباء والمياه، ثم تأتي المصارف والأسواق المالية، ذلك لإخضاع إرادة الشعوب والمجتمعات الدولية، والمقصود بالتدمير هو الدخول غير المشروع علي نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي (Server– PC) أو مجموعة نظم مترابطة شبكيا (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

ثانيا:– خصائص الإرهاب الإلكتروني

لا شك أن الإرهاب الإلكتروني ينفرد بعدد من الخصائص، ويتميز بها عن الكثير من الظواهر الإجرامية الأخري ومن أهم هذه الخصائص:–

(1) **مرتكبي جرائم الإرهاب الإلكتروني يكونون من المتخصصين في مجال تقنية المعلومات:**– تتطلب جرائم الإرهاب الإلكتروني مقدرة عقلية وذهنية خاصة لدي الجناة، حيث إن هذه الجرائم لا تتطلب إجراءات تميل إلي العنف بقدر ما تتطلب مقدرة ذهنية وعقلية خاصة لدي الجناه، فالمجرم المعلوماتي ليس مجرماً عادياً، بل يصنف ضمن نوابغ المجرمين، خاصة الأحداث الذين يخشي عليهم من التحول من مجرد الهواية إلي الإحتراف في أفعال اختراق النظم، وقد تتربص بهم منظمات غير مشروعة تعتمد المعلوماتية في جرائمها وتقوم بتجنيدهم الأمر الذي يجعلهم مجرمين معلوماتيين[2].

1– الدكتور/ شريف حسين محمد محمد حسن، المرجع السابق، صـــــ117ـــــــ

2– الدكتور/ عبد الجليل اسماعيل حسن الشيخ زيني (2020) الارهاب الالكتروني في القانون الدولي، الماهيه والجزاء، منشورات الحلبي الحقوقية، الطبعة الاولي،ص156.

ويمكن القول كذلك أن المجرم المعلوماتي متكيف اجتماعياً وليس سلبياً أو منعزلاً عن الآخرين، بل إن بعضهم يلجأ أحيانا إلي ارتكاب هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقه علي الآلة أو علي البرامج المتخصصة لأمن النظم المعلوماتية، وذلك من أجل أن يكون دائماً بعيداً عن الشبهات[1].

ويمكن تصنيف محترفوا الجرائم الإلكترونية إلي طائفتين:-

الطائفة الأولي:- الهواة العابثون

وهو ما اصطلح علي تسميتهم بالهاكرز (HAKERS) [2] وهم بارعون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية، وهذه الطائفة عادة ما تكون من هواة الحاسوب، فيقومون بأعمالهم هذه لمجرد إظهار أنهم قادرون علي اقتحام المواقع الأمنية أحياناً أو مجرد ترك بصماتهم التي تثبت وصولهم إلي تلك المواقع أحياناً أخري.[3]

وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية وهو دافعهم الأول.

الطائفة الثانية:- القراصنة المحترفون (Crackers) [4]

هذه الطائفة تعكس أفعالهم ميول إجرامية خطيرة، تفصح عن رغباتهم في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات، وهم أكثر خطورة من الطائفة الأولي، فهم يستخدمون برامج التقنية في محاولات اختراق الأنظمة والأجهزة للحصول علي المعلومات السرية[5].

1- **Catherine H, Conly:(1989) Organizing for computer crim investigation and prosecution, , P5.**

2- **الهاكرز: هو مصطلح يطلق علي الشخص المتخصص في نظم لمعلومات والبرمجيات، والتعامل مع شبكات الحاسب الآلي والدخول إليها بدون وجه حق. فاروق حسن، معجم مصطلحات الحاسب الآلي، دار الراتب الجامعية، بيروت، 1999.**

3- **الدكتور/ وليد الزبيدي(2003)القراصنة علي الإنترنت والحاسوب، دار أسامة للنشر، عمان، صـــــ40ـــــــــ.**

4- **كراكرز: هو مصطلح في اللغة الإنجليزية، مستمد من الفعل Crack ويعني الكسر والتحطيم، وهم أشخاص يقومون بالتسلل إلي نظم الحاسوب للاطلاع علي المعلومات المخزنة فيها لإلحاق الضرر أو العبث بها أو سرقتها، وذلك بدافع التحدي الإبداعي، وتتراوح أعمارهم ما بين (25 – 40 سنة). الدكتور/ مصطفي محمد موسي، (2003) أساليب اجرامية بالتقنية الرقمية، ماهيتها، مكافحتها، دراسة مقارنة، مطابع الشرطة، صـــــ15ـــــــ.**

5- **الدكتورة/ نهلاء عبد القادر الومني، (2008) الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، صـــــ84ـــــــ.**

(2) الإرهاب الإلكتروني جريمة إرهابية متعدية الحدود

فيمكن أن يكون الجاني في بلد معين ويرتكب الجريمة في بلد آخر، الأمر الذي ساعد المجرمين علي إرتكاب العديد من الجرائم دون إمكان القبض عليهم[1]

(3) صعوبة الإثبات في الإرهاب الإلكتروني

نظراً لسرعة غياب الدليل الرقمي وسهولة إتلافة وتدميرة.

(4) صعوبة إكتشاف جرائم الإرهاب الإلكتروني

وذلك نظراً لنقص الخبرة لدي بعض الأجهزة الأمنية في التعامل مع مثل هذا النوع من الجرائم.

ثالثا:- مخاطر الإرهاب الإلكتروني

يمكن القول بأن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر الحالي والقادم؛ نظرا لتعدد أشكالة وتنوع أساليب ارتكابة واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ وبعيد عن الإزعاج والفوضي، مع توفير قدر كبير من السلامة والأمان للإرهابيين، وسوف نتناول فيما يلي أهم مخاطر الإرهاب الإلكتروني:-

1- تهديد الأمن القومي والعسكري: حيث يمكن من خلال شبكة الإنترنت بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية، والتي تسيطر علي وجدان الأفراد وتفسد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصلحة المجتمع وتهدد الأمن القومي[2].

كما وقع في الآونة الأخيرة عدة جرائم تبين مدي إمكانية تعرض المراكز العسكرية لحوادث قرصنة معلوماتية، بغية الحصول علي معلومات مخزنة في ذاكرة الحاسبات الآلية المستعملة فيها. مثال ذلك، سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها الجيوش التابعة للدول الأعضاء في حلف شمال الأطلنطي (NATO) من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية خلال عام 1994، الأمر الذي أثار حفيظة قيادة أركان الحلف، وحمل السلطات العسكرية الفرنسية علي تصميم برامج جديدة لحماية حاسباتها الآلية[3]

1- الدكتور/ علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المرجع السابق، صـــــ15ـــــ.

2- الدكتور/ جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، المرجع السابق،صـــ32ـــــ.

3- الدكتور/ جميل عبد الباقي الصغير، المرجع السابق، صـــــ33ـــــــ.

كما حدث أن تمكن قرصان أمريكي لم يبلغ الثامنة عشر من عمره من اختراق واحد من أكثر النظم أمانا وهو الخاص بوزارة الدفاع الأمريكية (البنتاجون) وتسلل عبر الجدران النارية Fire Walls والتي وضعت لحماية هذه الشبكة، وكان بإمكانه أن يعرض البشرية كلها لخطر الإبادة لو تمكن من مواصلة عمله بالنفاذ للمخزون النووي الاستراتيجي ومعرفة شفرته، وضبطها بالتالي صوب اتجاه معين لإطلاق آلاف القنابل النووية.

كما ذكر أيضاً أن أحد لصوص الكمبيوتر الهولنديين- إبان غزو العراق للكويت- قد تمكن من سرقة أسرار عسكرية أمريكية بالغة الحساسية، من بينها تحركات القوات الأمريكية ومواقعها وأسلحتها، وتحركات الطائرات المقاتلة، ثم أرسل القرصان هذه المعلومات إلي العراق قبل إندلاع الحرب، إلا أن العراقيين رفضوا الهدية خشية أن يكون في الأمر خدعة.[1]

نذكر أيضاً ما يسمي «بإعصار ويكلس» أو «تسريبات ويكلس»[2] كما يطلق عليه البعض الآخر، ويعد ويكليس واحداً من أقوي منظمات الهاكرز المجهولة التي تحتوي علي كم هائل من الهاكرز، ونال الموقع شهرة كبيرة عام 2010 بعد نشر 90 ألف وثيقة سرية مرتبطة بحرب أفغانستان، ثم نشر 400 ألف وثيقة حول الحرب العراقية، وكان أغلب الوثائق سرية مسربة من مراسلات وزارة الخارجية الأمريكية، وسببت هذه الوثائق الدبلوماسية حرجاً بالغاً للإدارة الأمريكية، وفتح تحقيقاً جنائياً وتوعدت بمحاكمة كل من تبين أنه علي علاقة بالتسريب.

(2) السطو علي أموال البنوك: إن المصارف والبنوك هي الهدف المفضل لقراصنة الإنترنت، فقد تمكن بعض القراصنة من اختراق مجموعة «سيتي جروب» الأمريكية[3]، واستطاعوا سرقة عشرات الملايين من الدولارات، مما أصاب النظام الاقتصادي الأمريكي بخسائر فادحة، وهذا الفعل تبين بعد ذلك أنه تم بالتنسيق بين مجموعة من القراصنة الأمريكيين مع عصابة روسية من خلال شبكة الإنترنت.

1- الدكتور/ جميل عبد الباقي الصغير، المرجع السابق، صـــــ34ـــــــ

2- أ/ مي مجدي، مقال بعنوان: 8 هجمات للهاكرز تنهي أسطورة التفوق الأمريكي...ظهرت علي شكل "فيروسات" عام 1997، القراصنة أغلقوا مضخة مياه إلينوي عام 2011 "بيونج يانج" تصفع "واشنطن" مؤخرا. الهجوم علي وزارة العدل الأشهر، موقع جريدة (فيتو) الإلكترونية في 2014/12/22 علي الموقع الإلكتروني http://www.vetogate.com/1387586.

3- ورقة عمل بعنوان: اختراق حسابات عملاء بنك سيتي جروب الأمريكي، نشر علي صحيفة سبق الإلكترونية في 2011/6/10 علي الموقع الإلكتروني http://sabq.org/MKYede.

كذلك أيضا نجد أن قراصنة الإنترنت يقومون بالتلاعب في كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر، ولعل قضية بنك الباسيفيك الوطني في الولايات المتحدة الأمريكية تعد نموذجا لهذا النوع من الجرائم،فقد كان المواطن الأمريكي «ستانلي مارك» يعمل أخصائياً للحاسبات في هذا البنك، واكتشف مصادفة شفرة تحويل حسابات العملاء بين البنك وغيرة من البنوك التي تتعامل معه، فقام بإصدار أوامر إلكترونية لعدة فروع للبنك بتحويل مبالغ قدرت جملتها بأربعة ملايين دولار لحسابة الذي قام بفتحة في أحد المصارف السويسرية، ثم انتقل إلي جنيف وسحب المبلغ المذكور واشتري به ماساً وأودعة في خزانة خاصة به بأحد البنوك هناك، ومرت شهور دون أن يكتشف أحد حقيقة ما حدث لولا أن المتهم نفسه قد اعترف بالواقعة وهو مخمور[1].

3 – **اتلاف أنظمة المعلومات:** فقد حدث بتاريخ 3 نوفمبر 1988 أن تمكن طالب جامعي أمريكي من إدخال فيروس الدودة إلي شبكة الإنترنت من خلال احدي وسائل الاتصال، وفي مدة لا تتجاوز 24 ساعة كان هذا البرنامج قد انتشر عبر الشبكة وغطي أطرافها كلية.

كما تأثرت به أيضاً شبكات كبيرة ترتبط بشبكة الإنترنت، مثل شبكة «اربانت وميلنت» واكثر من 6000 حاسب في أرجاء الولايات المتحدة الأمريكية، حيث قام هذا الفيروس بملئ ذاكرتها حتي لم يعد بمقدورها القيام بأي عمل أو تنفيذ أي أمر، مما يشكل اتلافاً للمعلومات. وفي أحد القضايا اعتقلت الشرطة في ولاية نيوجيرسي الأمريكية المتهم «ديفيدل سميث» الذي أنشأ فيروس البريد الإلكتروني المعروف باسم «ميلسا» الذي أحدث اضطراباً عالمياً في البريد الإلكتروني بشبكة الإنترنت، وقد وجهت إلي هذا المتهم تهمة التدخل في اتصال عام والتي يعاقب عليها بالسجن لمدة تتراوح بين 5 إلي 10 سنوات وغرامة تصل إلي 150 ألف دولار، كذلك قد يقوم القرصان باتلاف الملفات تماما باستخدام الأمر Format كما قضي القضاء الأمريكي بإدانة موظف سابق– كان يعمل بالخدمات الساحلية الفيدرالية– بالحبس لمدة خمس سنوات، لأنه قام بمحو معلومات تتعلق بترقيات الموظفين ونقلهم، والتي تخص أحد بنوك المعلومات[2].

المطلب الثالث: التجسس الإلكتروني علي المؤسسات الرسمية

تعتبر جريمة التجسس الالكتروني من أخطر جرائم الإرهاب الإلكتروني علي الإطلاق، نظراً لما تحملة من تقنية فائقة وأدوات تكنولوجية عالية الدقة والسرعة، كأقمار التجسس الصناعية،

1- مجلة زهرة الخليج، س 20، العدد 1028 بتاريخ 1998/12/5، صـــــ47ـــــ نقلا عن الدكتور/ جميل عبد الباقي الصغير، المرجع السابق، صـــــ35ـــــ

2- الدكتور/ جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، المرجع السابق، صـــــ49ـــــ

فقد أسفر التقدم العلمي والتكنولوجي الحديث عن وجود طفرة كبيرة في أجهزة التصنت الحديثة ذات القدرة الفائقة والدقة البالغة في الرقابة السمعية والبصرية، فضلاً عن صغر حجمها الذي قد يصل إلي حجم أقل من رأس عود الثقاب، بل إن هناك أجهزة تصنت تخطئ العين المجردة في تبينها لصغر حجمها، بحيث تستطيع تلك الأجهزة والتي تعمل الكترونياً أن تنقل بالصوت والصورة كل ما يجري في المواقع والمنشآت التي تتضمن أسراراً من مسافات بعيدة، وفي ضوء خافت أو حتي في الظلام الدامس.

وسوف نتناول فيما يلي تحديد مفهوم جريمة التجسس الالكتروني، وما هو الدور الذي تقوم به الدولة لمكافحة التجسس الإلكتروني علي مؤسساتها:-

أولا: مفهوم التجسس الإلكتروني

التجسس الإلكتروني يقوم فيه الإرهابيون بالتجسس علي الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية وهي: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي، فحدود الدولة مستباحة بأقمار التجسس والبث الفضائي، ومع توسع التجارة الإلكترونية عبر شبكة الإنترنت، تحولت أيضا مصادر المعلومات التجارية إلي أهداف التجسس الاقتصادي.

وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق، ومن أشهرها البريد الإلكتروني، وكذلك استخدام الفيروسات في الاختراق والتجسس المعلوماتي.

وتجدر الإشارة إلي أن الطرق الفنية للتجسس الإلكتروني سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية، وخصوصا ضد المؤسسات والقطاعات الحكومية، العسكرية والسياسية والاقتصادية، لأن هذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن، وهو ما يهدف إليه الإرهاب في عمومة وعلي سبيل المثال، أعلن أمين مجلس الأمن الروسي (نيكولاي باتروشيف) في 2015/8/26 علي العثور علي برامج تابعة للاستخبارات الأجنبية في نظم المعلومات للمؤسسات الحكومية الروسية وأكد علي تزايد حالات التجسس علي نظم المعلومات الحكومية[1].

1- خبر: مجلس الأمن الروسي يؤكد تزايد حالات التجسس علي نظم المعلومات الحكومية في 2015/8/26 منشور علي الموقع الإلكتروني الإخباري:https://arabic.rt.com/news/

وقد ذهب البعض إلي أن التجسس الإلكتروني هو عبارة عن « عدة طرق لاختراق المواقع الإلكترونية، ومن ثم سرقة بعض المعلومات والتي قد تكون في غاية الأهمية والخطورة للطرف المتلقي والمسروق منه».

أما التجسس الصناعي فهو « نوع من التجسس ينفذ لأغراض تجارية وتقوم به بعض الشركات والمؤسسات التجارية بهدف الحصول علي أسرار صناعية من الشركات المنافسة، وهذا النوع من التجسس غالباً ما يرتبط بالصناعات التقنية، مثل البرمجيات والتقنية الحيوية، وتقنيات الفضاء والاتصالات والمواد والطاقة[1].

ويذكر البعض[2] أن هذه الظاهرة الخطيرة تزداد خطورة يوماً بعد يوم، وهي كما تهدد أمن متصفح الإنترنت بشكل عام، فهي تهدد أيضاً ثقافتنا وهويتنا العربية بشكل أكثر فداحة، ويكفي للتدليل علي ذلك العبث الذي قد يفاجأ به المتصفح إذا ما لجأ إلي البحث عن كلمات ذات مدلول ديني مثلاً، خاصة إذا ما لم يكن ملتزماً بالتركيب الهجائي الشائع لهذه الكلمات باللغة الإنجليزية، حيث يفاجأ عادة بسيل من الإعلانات عن مواقع تتحدث عن عروض مغرية لمواقع هابطة.

ثانيا: دور الدولة في مكافحة التجسس الإلكتروني علي مؤسساتها

إن التصدي لجرائم التجسس الإلكتروني لا يتأتى فقط بالقوانين الوضعية وإنما يكون بوضع تقنيات وآليات فنية عالية التقنية ومتطورة نستطيع من خلالها القضاء علي هذه الظاهرة.

وقد أكد البعض في الإطار التقني علي ضرورة تشفير البيانات وإخفاءها، والاهتمام ببروتوكولات الحماية، ونظم منع المتطفلين، كما يشيروا أيضاً إلي أن أهداف وطرق الحماية تتمثل في «الموثوقية" أي الاحتفاظ بسرية المعلومات عن الجميع، باستثناء الذين لديهم صلاحية للاطلاع عليها، و"تكامل البيانات" بمعني التأكد من أن المعلومات لم تتغير من قبل أشخاص غير مخولين، والتحقق من الشخصية[3].

1- الدكتور/ حسن بن أحمد الشهري، بحث بعنوان الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية وسرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب المجلد 28، العدد 5، صـــ11ـــ علي الموقع الإلكتروني:
http://www.nauss.edu.sa/Ar/CollegesandCenters/ResearchesCenter/studiesmagazine/Archive/1434/Documents/em-dar-56-/.pdf

2- الدكتور/ محمد علي عمران، الدكتور/ فيصل ذكي عبد الواحد، (1999) المدخل لدراسة القانون، الرسالة الدولية للطباعة والكمبيوتر، صـــ52ـــ

3- الدكتور/ مصطفي جاد، (2012): مقال بعنوان «مستقبل الارهاب الالكتروني، في ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012، جريدة السياسة الدولية التابعة لمؤسسة الأهرام، إعداد/ شيريهان نشأت المنيري، علي الموقع الإلكتروني:
http://www.siyassa.org.eg//newsContent/6/51/2450

ويجب علي الدول أن تسارع إلي وضع ضوابط حماية وإنشاء أمن خاص للشبكات، ففي مصر قامت وزارة الداخلية بتشكيل «دوريات أمنية» من خلال الشبكة، تتركز مهامها في العمل علي منع الجريمة قبل وقوعها، وقد استطاعت هذه الدوريات من ضبط «تنظيم الشواذ» يمارس جرائمه عبر الإنترنت، وبعد مداولات استمرت فترة من الزمن، قامت ثلاثون دولة أوروبية بتوقيع معاهدة لتوحيد الجهود في محاربة جرائم الإنترنت[1]. ومطلوب من الأجهزة الأمنية العربية أن تواجه هذا التحدي وتطور قدراتها وتحدث برامجها للقضاء أو للحد من مثل هذه الجرائم.

كما وقعت الجمعية المصرية لمكافحة جرائم الإنترنت[2] بروتوكول تعاون مع كلية الحقوق جامعة عين شمس، بهدف تثقيف وتدريب طلبة وخريجي كليات الحقوق والآداب والإعلام والسياحة والآثار والتجارة والحاسبات والمتخصصين، والسادة القضاة وأعضاء النيابة العامة والسادة المحامين والعاملين في القطاعات القانونية في المؤسسات، وتأهيل وإكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم، ومدي تأثير استخدام تكنولوجيا المعلومات في انجاز مهام أعمالهم، والتعريف بماهية التعامل مع الإشكاليات القانونية في حقل المعاملات الالكترونية، حول موضوعات تشمل كيفية إثبات الشخصية، وكيفية التوقيع الإلكتروني، وأنظمة الدفع النقدي الرقمي، المال الرقمي أو الإلكتروني، سرية وأمن المعلومات من مخاطر إجرام التقنية العالية، خصوصية العميل، المسئولية عن الأخطاء والمخاطر، حجية المراسلات الالكترونية، التعاقدات المصرفية الالكترونية، مسائل الملكية الفكرية لبرمجيات وقواعد معلومات البنك أو المستخدمة من موقع البنك أو المرتبطة بها، علاقات وتعاقدات البنك مع الجهات المزودة للتقنية أو الموردة لخدماتها، مشاريع الاندماج والمشاركة والتعاون المعلوماتي والجريمة الالكترونية، وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية، وعقود التجارة الإلكترونية، وحماية الملكية الفكرية عبر الإنترنت، والتعرف بأشكال وأنماط الجرائم عبر الإنترنت وماهية الدليل الرقمي وحجته في الإثبات، وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم[3].

1- الدكتور/ محمد منير الجهبيني، جرائم الحاسبات ووسائل مكافحتها، المرجع الإلكتروني السابق.

2- موقع الجمعية المصرية لمكافحة جرائم الانترنت والمعلومات www.eapiic.net

3- الدكتور/ عبد الصبور عبد القوي علي، (2015) بحث بعنوان الجرائم الالكترونية، أنواعها وأهدافها وآثارها، المملكة العربية السعودية، مجلة الدراسات المالية والمصرفية، العدد الأول، صـــ16، 17ـــــ

ومن خلال الاطار القانوني لمواجهة ظاهرة التجسس الالكتروني، فقد ذهب البعض إلي ضرورة تخصيص دوائر قضائية معينة للنظر في الجريمة الالكترونية، والاستفادة مما انتهي إليه الاتحاد الأوروبي والدول الأخرى في مجال التشريعات الجنائية[1].

وقد أكد البعض علي ضرورة تعاون واتفاق حكومات الدول علي سن قوانين وعقوبات لمرتكبي الإرهاب الإلكتروني، ودعم الجهود التشريعية والأمنية[2].

ومن جانب الشركات، ضرورة وضع تصميم لبرامج حماية ضد تلك الجرائم التي ترتكب وتهدد أمن المجتمعات، ذلك لا يغني عن أهمية دور الأفراد ودعم وتنمية الوعي الإلكتروني بينهم وحثهم علي استخدام أنظمة الحماية والوقاية لكل الأضرار التي يمكن أن تلحق بأجهزتهم ومؤسساتهم.

وجدير بالذكر أن من أهم الجهود المبذولة في مصر في مجال مكافحة الإرهاب الإلكتروني، هي تفعيل التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المجرمين، كذلك إصدار عدد من القوانين والتشريعات الجديدة لتجريم أي استخدام غير آمن لتكنولوجيا المعلومات مثل (قانون التوقيع الإلكتروني رقم 15 لسنة 2004، وقانون تنظيم الاتصالات رقم 10 لسنة 2003، وقانون حماية الملكية الفكرية رقم 82 لسنة 2002، وقانون مكافحة الإرهاب رقم 94 لسنة 2015) بالإضافة إلي التنسيق والتعاون الدائم مع الانتربول الدولي في مجال تبادل المعلومات والخبرات الأمنية في رصد ومتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي الإلكتروني لتزايده المستمر من خلال العناصر الإجرامية المحترفة والمنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية.

كذلك أنشأت مصر إدارة متخصصة بوزارة الداخلية عام 2002 وهي إدارة مكافحة جرائم الحاسبات وشبكات المعلومات لرصد وتتبع كافة أنواع الاستخدام غير الآمن وغير المشروع لشبكة الإنترنت وضبط مرتكبيها، والعمل علي نشر الوعي المعلوماتي بين أفراد المجتمع بخطورة تلك النوعية من الجرائم علي المجتمع المصري.

كذلك في مبادرة لوزارة الاتصالات وتكنولوجيا المعلومات المصرية فقد أنشأت عام 2008 أول جهاز فني متخصص في حماية وتأمين البلاد من أي هجمات إلكترونية محتملة عبر شبكة الإنترنت والذي يعد من المبادرات المحمودة.

1- الدكتور/ جميل عبد الباقي الصغير، (2012) ورقة عمل مقدمة إلي الندوة التي نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012 بعنوان «مستقبل الإرهاب الإلكتروني» إعداد/ شيريهان نشأت المنيري، جريدة السياسة الدولية التابعة لمؤسسة الأهرام، علي الموقع الإلكتروني: http://www.siyassa.org.eg/NewsContent/6/2450/

2- لواء/ محمود الرشيدي، ورقة عمل في ندوة بعنوان «مستقبل الإرهاب الإلكتروني» المرجع السابق.

وذهب رأي إلي أن دور الدولة يأتي من مفهومها لأسباب اللجوء للإرهاب الإلكتروني والتي لخصها في، ضعف بنية الشبكات المعلوماتية، وقابليتها للاختراق، وغياب الحدود الجغرافية، وتدني مستوي المخاطرة، وسهولة الاستخدام، وقلة التكلفة، وأخيراً صعوبة اكتشاف وإثبات الجريمة في هذا النوع من الإرهاب، وعلي الدول اتخاذ تدابيرها في تقوية البنية التحتية لشبكة المعلومات، ووضع نظم ذات تقنيات عالية لمنع الهاكرز والمخترقين من الولوج إلي هذه الشبكات[1].

المبحث الثاني
جرائم الإرهاب الالكتروني عبر الإنترنت
في ضوء قانون مكافحة الإرهاب رقم 94 لسنة 2015

تمهيد: يعد الإرهاب عبر شبكة الإنترنت واحداً من أخطر أشكال الإرهاب الذي يتمثل في استخدام الموارد المعلوماتية المتمثلة في شبكات المعلومات وأجهزة الكمبيوتر وشبكة الإنترنت لأغراض التخويف أو الإرغام لأهداف سياسية، فقد استغلت الكثير من الجماعات والأفراد المتطرفين استخدام تلك التكنولوجيا، ولا سيما شبكة الإنترنت في ممارسات لتهدد أمن الدولة المعتدي عليها في ارتكاب الجرائم الإرهابية[2].

كما يمكن استخدام الإنترنت والحاسب الآلي في ارتكاب جرائم ماسة بالأمن الفكري، حيث تتوالي عبر الإنترنت الهجمات الثقافية والحضارية التي قد تزعزع الأمن الفكري للشعوب المغلوبة علي أمرها، وتنشر عبرها القوي الغالبة فكرها، ولغتها، وقيمها[3].

كذلك أيضاً نجد أن الإرهاب عبر شبكة الإنترنت يمكن أن يتسبب في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادة، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو اختراق النظام المصرفي، أو ارباك حركة

1- الدكتور/ نشأت الهلالي، ورقة عمل مقدمة إلي الندوة التي نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية، بعنوان «مستقبل الإرهاب الإلكتروني»، المرجع الإلكتروني السابق.

2- الدكتور/ محمد سيد سلطان، (2012) قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني، صـــ13ـــ.

3- الدكتور/ جميل عبد الباقي الصغير، (1992) القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولي، منشورات دار النهضة العربية، صـــ57ـــ.

الطيران المدني، أو شل محطات الطاقة الحرارية والنووية، وتتعدد الأماكن التي تتأثر بالجريمة في آن واحد[1].

ولذا أصبح من الوظائف الأساسية لأي نظام قانوني، الاستجابة السريعة للتطورات الجديدة التي يشهدها المجتمع، وقد تداركت معظم الدول التعامل مع جرائم الكمبيوتر من خلال القوانين. ولا تخلو المواجهة الجنائية لهذه الجرائم من قصور يمكننا ردة إلي عدم وجود نصوص كفيلة بمعالجة هذه المشكلات والتي من بينها الاستخدام غير المشروع لشبكة الإنترنت.

وقد استطاع المشرع المصري مكافحة الاستخدام غير المشروع لشبكة الإنترنت فيما يتعلق بالنشاط الإرهابي الإلكتروني، حيث نص في المادة 29 من القانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب علي أنه « يعاقب بالسجن مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعاً علي شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية، أو لبث ما يهدف إلي تضليل السلطات الأمنية، أو التأثير علي سير العدالة في شأن أية جريمة إرهابية، أو تبادل الرسائل بإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الارهابية في الداخل والخارج».

"ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً الكترونياً تابعاً لأية جهة حكومية، بقصد الحصول علي البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو اتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولي من هذه المادة أو الاعداد لها».

من هذا النص نجد أن المشرع المصري لم يكتف بالنشاط الإجرامي الذي يبتغي الترويج للأفكار والمعتقدات الداعية إلي ارتكاب أعمال إرهابية أو تضليل السلطات الأمنية أو التأثير علي سير العدالة في شأن الجرائم الإرهابية، أو التواصل مع أفراد الجماعة الإرهابية، بل امتدت الحماية الجنائية لتشمل المواقع الإلكترونية الحكومية، طالما قصد الجاني الحصول علي المعلومات، أو العبث بها بقصد ارتكاب جريمة من الجرائم المشار إليها في الفقرة الأولي من المادة، بيد أن

1- Mascala Carinne,(2000) criminalitè et contrat èlectronique, IN: Le contrat èlectronique Travaux de l´association CAPITANT Henri, journèes national, Paris, , P119.‘ ectronique Travaux de lMt

التي تتأثر بالجريمة في آن واحد النظام المصرفي أو ارباك حركة الطيران المدني أو شل محطات الطاقة الحراري

النص المؤثم جاء خاليا من تجريم الفعل الإجرامي الذي يقع من الشخص المعنوي، إذا ما وقعت الجريمة بناء علي أجهزة قدمها أو خبرات فنية وفرها، وهو ما كان يقتضي علي المشرع أن يتناولها ويقرر لها العقوبات بما يكفل المواجهة اللازمة للجريمة في شتي صورها، فضلاً عن أن النص التجريمي جاء خالياً من مواجهة السلوك الإجرامي الذي يتخذ صورة تصميم الموقع، فضلاً عن أنه لم يقرر عقوبات تكميلية للجريمة بشأن الأجهزة المستخدمة في ارتكاب الجريمة، وهو ما سوف نتناول الحديث عنه عند تعرضنا لأركان الجريمة علي النحو التالي:

أركان الجريمة:-

أولا: الركن المادي

يتكون الركن المادي بصفة عامة من عناصر ثلاثة: السلوك الإجرامي والذي يعد بمثابة: نشاط إنساني إرادي في المحيط الخارجي يتم التعبير عنه بحركة من الجسم أو مجرد السكون. والثاني يعرف بالنتيجة الإجرامية ويقصد بها: الأثر المادي الخارجي الناجم عن السلوك الإجرامي والذي يعتد به المشرع في التكوين القانوني للجريمة[1]. ويتصور توافر الركن المادي للجريمة دون توافر النتيجة الإجرامية، فالنتيجة الإجرامية ليست عنصراً ضرورياً في الركن المادي، كما هو الحال في الجرائم السلبية وجرائم الخطر وجرائم المشروع. والثالث والأخير: علاقة السببية والتي يعني بها ذلك الرباط الذي يربط سلوك الجاني بالنتيجة الإجرامية التي يسأل عنها. وهذا العنصر لا وجود له في الجرائم التي لا تشكل النتيجة فيها أحد عناصر الركن المادي، بينما تعد عنصراً ضرورياً من عناصر الركن المادي بالنسبة للجرائم ذات النتيجة[2].

نخلص مما سبق أن عناصر الركن المادي تختلف باختلاف نوعية الجريمة، فالجريمة الشكلية لا يتكون ركنها المادي إلا من عنصر السلوك فقط، بينما في الجرائم ذات النتيجة فإن ركنها المادي يتكون من عناصر ثلاثة: السلوك والنتيجة والسببية، وكي نحدد عناصر الركن المادي في الجريمة الإرهابية عبر الإنترنت ينبغي أن نحدد أولا طبيعة تلك الجريمة، هل هي جريمة شكلية أم جريمة ذات نتيجة؟

طبيعة الجريمة الإرهابية عبر الإنترنت: باستقراء نص المادة 29 من القانون رقم 94 لسنة 2015 الذي جرم الأعمال الإرهابية المرتكبة عبر الإنترنت، نجد أن هذه الجريمة تعد من

1- الدكتور/ محمود نجيب حسني، (1983) علاقة السببية في قانون العقوبات، دار النهضة العربية، صـــ48ـــ

2- الدكتور/ محمد محيي الدين عوض، (1981) مبادئ القانون الجنائي، القسم العام، صـــ176ـــ

طائفة الجرائم الشكلية، أي أنها تقع وتكتمل بمجرد إتيان السلوك المكون لها وهو الدخول أو البقاء دون أن يتطلب المشرع أية نتيجة إجرامية، حيث جرم المشرع بوصفه نشاطاً إجرامياً إرهابياً كل فعل من شأنه الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية، ولا يشترط أن تلقي هذه الأفكار قبولاً أو رفضاً عند متلقيها، ولم يشترط المشرع ترويجاً لطائفة معينة من الناس، بل إن الجريمة تتحقق بمجرد الدخول بذات القصد. ولم يشترط المشرع شكلاً معيناً يتم فيه الترويج، فمن الممكن أن يكون بالكتابة، أو برسم صورة تعبيرية، أو أياً من صور التواصل التي تخترق الحظر الذي فرضه المشرع لمواجهة هذه الطائفة من الجرائم والتي تدعو إلي ارتكاب أعمال إرهابية.

ولا يشترط وقوع هذه الأفعال أو عدم وقوعها، فمناط التأثيم هو الترويج للأفكار أو المعتقدات الداعية للإرهاب.

وإذا ما انتهينا إلي أن هذه الجريمة من الجرائم الشكلية، فإن هذا يعني أن عناصر الركن المادي لها لا يتعدي عنصراً واحداً وهو السلوك الإجرامي دون عنصري النتيجة الإجرامية وعلاقته السببية.

السلوك الإجرامي: يتطلب النشاط أو السلوك الإجرامي في الجرائم الإرهابية التي تقع بواسطة الإنترنت، وجود بيئة رقمية واتصال بالإنترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة ويقوم بتحميل الحاسب ببرامج الاتصال، وكذلك ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه، والتي يستطيع من خلالها الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية، أو لبث ما يهدف إلي تضليل السلطات الأمنية أو التأثير علي سير العدالة في شأن أي جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية سواء كان ذلك في الداخل أو الخارج، وكذلك تمكنه من اختراق المواقع الإلكترونية الحكومية لتحقيق غايته في ارتكاب الجريمة الإرهابية.

ويتمثل النشاط أو السلوك الإجرامي في الجريمة الإرهابية المرتكبة عبر الإنترنت في نشاط اجرامي ايجابي من شأنه أن يبرز إلي العالم الخارجي الجريمة[1].

ولا يتصور أن تقع الجريمة بالسلوك الإجرامي السلبي، فيشترط الدخول ليتحقق الغرض المحدد بالنص المؤثم، سواء ترتب علي هذا الدخول غير المشروع التلاعب بهذه البيانات أو

1- الدكتور/ عمر الفاروق الحسيني، (1991) الحماية الجنائية للحاسب، ورقة بحثية مقدمة إلي الندوة التدريبية باتحاد المصارف العربية خلال الفترة من 7-9 مايو 1991، صـــ3ـــــ

الحصول علي البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغيرها أو محوها أو اتلافها أو تزوير محتواها الموجود بها، ومن هنا فإن النشاط الإجرامي الايجابي هو ما تقوم به الجريمة ولا يتصور وقوعها بالسلوك السلبي.

ويتمثل السلوك الإجرامي في هذه الجريمة في أحد أفعال: الإنشاء أو الاستخدام لأحد المواقع الإلكترونية عبر شبكة الإنترنت بغرض الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية، والدخول غير المشروع لأحد المواقع الإلكترونية الحكومية.

(1) **إنشاء واستخدام مواقع علي الإنترنت:**- يقوم الإرهابيون بإنشاء مواقع لهم علي شبكة الإنترنت، وذلك لنشر أفكارهم ومعتقداتهم الداعية إلي إرتكاب أعمال إرهابية، بل تعليم الطرق والوسائل التي تساعد علي القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول علي المواقع المحجوبة، وطرق نشر الفيروسات وغير ذلك.

والموقع هو: عبارة عن معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل علي معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمي لغة تحديد النص الأفضل (HTML) Hyper text mark up language ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (www Browser) ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة. [1]

وإذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادل الآراء والأفكار والمعلومات صعباً في الواقع فإن الإنترنت سهل هذه العملية كثيراً، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، ويتبادلون الحديث والاستماع لبعضهم عبر الإنترنت. بل يمكن أن يجمعوا لهم أتباعاً وأنصاراً عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الإنترنت ومنتديات الحوار، وما يسمي بغرف الدردشة.

(2) **الدخول والبقاء غير المشروع:**- نصت المادة 29 بقولها «أنشأ أو استخدم..... كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً...» وعلية فإن الصورة البسيطة للجريمة

1- الدكتور/ أيسر محمد عطية، (2014) ورقة عمل بعنوان دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، مقدمة في الملتقي العلمي بعنوان «الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية خلال الفترة من 7 – 9 /1435/11 هـ 2 – 4 /2014/9، كلية العلوم الاستراتيجية – عمان – الأردن، صـ16ـــــ.

تتمثل في مجرد الإنشاء أو الاستخدام، أما الدخول أو البقاء غير المشروع في المواقع الإلكترونية الحكومية فيتحقق به الظرف المشدد للجريمة، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما الحصول علي البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغيرها أو محوها أو اتلافها أو تزوير محتواها الموجود بها، ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلي النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة، ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[1].

(3) **فعل البقاء:**- يقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة علي هذا النظام، وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلاً عن الدخول إلى النظم، وقد يجتمعان، ويكون البقاء معاقباً عليه استقلالاً حين يكون الدخول إلي النظام مشروعاً، ومن أمثلة ذلك إذا تحقق الدخول إلي النظام بالصدفة أو عن طريق الخطأ أو السهو، وكان عليه قطع وجودة وانسحابه فوراً، أو في حالة تجاوزه للمدة المسموح له البقاء فيها بداخل النظام، أو في حالة طبعة لنسخة من المعلومات، في حين سمح له بالرؤية فقط، فإنه يعاقب علي جريمة البقاء غير المشروع، متي توفرت أركانها. وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معاً، وذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلي النظام، ويدخل إليه بالفعل ضد إرادة من له حق السيطرة عليه[2].

وقد اعتبر المشرع ظرفاً مشدداً للجريمة الدخول بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً حكومياً بقصد الحصول علي البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو اتلافها أو تزوير محتواها الموجود بها طالما كان ذلك بغرض ارتكاب جريمة من الجرائم التي تناولتها المادة في فقرتها الأولي أو الإعداد لها.

ولا يشترط تحقق النتيجة الإجرامية الواقعة علي البيانات أو المعلومات، فتتحقق الجريمة وتنعقد المسئولية الجنائية طالما تحقق قصد الدخول بغية تحقيق هذه النتيجة ولو لم تتحقق فعلاً.

بالإضافة إلي ذلك فإن المشرع لم يشترط أن تكون هذه البيانات أو المعلومات من طائفة الأسرار العسكرية أو الماسة بأمن الدولة من جهة الداخل أو الخارج، ولكن يكفي أن تكون هذه

1- الدكتور/ علي عبد القادر القهوجي، (1999) الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة، بيروت، صـــــ121ـــــ.

2- الدكتور/ مصطفي السعداوي، الوسيط في شرح قانون مكافحة الإرهاب رقم 94 لسنة 2015 دراسة نقدية تحليلية مقارنة، دار الكتاب الحديث، صـــ535ـــــ.

البيانات والمعلومات موجودة علي موقع إلكتروني حكومي، فتتحقق النتيجة إذا وقعت علي بيانات الناخبين المقيدين بجداول الانتخابات أو المشمولين برعاية اجتماعية معينة من قبل الدولة، طالما كان هذا الدخول بغرض ارتكاب جريمة من الجرائم المحددة حصراً بالفقرة الأولي من المادة 29 [1].

ثانيا الركن المعنوي:-

لم يكتشف المشرع بالقصد الجنائي العام لتحقيق الركن المعنوي للجريمة، بل تطلب أن يكون للجاني قصد خاص من ارتكابه الجريمة وهو الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية أو لبث ما يهدف إلي تضليل السلطات الأمنية أو التأثير علي سير العدالة في شأن أي جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمية إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج.

ويقوم القصد الجنائي الخاص علي نفس العناصر التي يقوم عليها القصد العام، غير أنه يتميز بإضافة عنصر آخر، فبالإضافة إلي الإرادة والعلم قد يشترط القانون عنصرا إضافيا في القصد الجنائي، وهو اتجاه نية الجاني نحو تحقيق غاية محددة[2]. لذلك فالفرق بين القصد العام والقصد الخاص ليس في الطبيعة إرادة وعلم وإنما في الموضوع الذي يتعلق به العلم والإرادة، فهو أوسع نطاقاً في القصد الخاص منه في القصد العام.

ثالثا العقوبة:-

باستقراء نص المادة 29 من القانون رقم 94 لسنة 2015 المجرمة للواقعة محل البحث يتضح لنا أن الجزاء الجنائي المقرر لمرتكب هذه الجريمة ليس واحداً في جميع الأحوال، فهناك حالات يخفف فيها العقاب، كما أن هناك حالات يشدد فيها العقاب. فقد عاقب المشرع بالسجن مدة لا تقل عن خمس سنين علي الجريمة في صورتها البسيطة غير المقترنة بظرف مشدد.

واتخذ المشرع من محل الجريمة ظرفاً مشدداً إذا وقعت علي أحد المواقع الإلكترونية التابعة لأية جهة حكومية وعاقب بالسجن المشدد مدة لا تقل عن عشر سنين.

1- الدكتور/ مصطفي السعداوي، الوجيز في شرح قانون مكافحة الإرهاب، المرجع السابق، صـ536ـ

2- الدكتور/ يسر أنو علي، (1996) شرح قانون العقوبات، النظرية العامة، صـ331ـ

رابعا تقييم السياسة التشريعية المجرمة للجرائم الإرهابية التي تقع بواسطة الإنترنت:-

يحسب للمشرع المصري تشديده للعقاب، إذ جعل العقوبة السجن وجوبياً، كما أنه شدد العقاب متي كانت الجريمة واقعة علي أحد المواقع الإلكترونية الحكومية. وما نعيبه علي المشرع المصري أن العقوبات التي فرضها جاءت قاصرة، حيث توقف بالعقوبة عند حد العقوبات السالبة للحرية، وقد كان من الواجب علي المشرع أن يفرض عقوبة الغرامة بين حدين أدني وأقصي، وذلك لإصلاح ما تم اتلافة من بيانات علي نفقة الجاني، كما كان يجب علي المشرع أيضاً أن يفرض عقوبة المصادرة والغلق إذا ارتكبت الجريمة في محل مخصص لاستخدام الإنترنت، وهو قصور من المشرع يوجب التدخل لفرض هذه العقوبات.

وهذا هو مسلك بعض التشريعات العربية فنجد مثلاً أن المشرع الأردني قد جرم الإرهاب الإلكتروني بصورة خاصة، حيث أفرد نصاً خاصاً في قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 للإرهاب الإلكتروني، حيث نص في المادة العاشرة من هذا القانون علي ما يلي «كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو أنشأ موقعاً إلكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لاتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة».

كما نص في المادة 12 من ذات القانون علي أنه «(أ) مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكي عليه الشخصية يجوز لموظفي الضبطية العدلية، بعد الحصول علي إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلي أي مكان تشير الدلائل إلي استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم. (ب) مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، باستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضبطية العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ علي المعلومات والبيانات المتعلقة بارتكاب الجريمة»

(جـ) للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها

أو يشملها هذا القانون، ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة علي نفقة مرتكب الجريمة".

كذلك في المملكة العربية السعودية نصت المادة 13 من نظام مكافحة الجرائم المعلوماتية، الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8 هـ علي أنه «مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم باغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متي كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكة»[1].

ولعلنا نري أن النهج الذي اتبعه كلاً من المشرع الأردني والمشرع السعودي في شأن عقوبة المصادرة والإغلاق هو الأولي بالاتباع، وندعو المشرع المصري إلي اتباع ذات النهج بشأن مصادرة الأجهزة المستخدمة في الجريمة دون الإخلال بحقوق الغير حسني النية، ويجب علي المشرع المصري مواجهة هذا القصور في النص بفرض العقوبات التكميلية لتحقيق الردع المناسب بنوعية العام والخاص.

1- لمزيد من التفصيل أنظر الدكتور/ أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة. الإرهاب الإلكتروني وطرق مواجهته، المرجع السابق، صـــ35،36ـــ.

المبحث الثالث
نظرية العدول في الجرائم الإرهابية

الأصل أن من يرتكب جريمة ما تقع عليه عقوبتها، ولكن تقتضي المصلحة العامة أحياناً رفع العقوبة كليا، لذلك نص القانون علي أسباب تعفي من العقاب، لا يسمح للقاضي أن يضيف إليها، أو يمتنع عن تطبيقها عند توافر شروطها، وهذه الأسباب هي الأعذار المعفية من العقوبة[1].

ويترتب علي توافرها رفع العقوبة عن الجاني، رغم بقاء السلوك الإجرامي علي أصلة في الجريمة، ورغم توافر شروط المسئولية الجنائية في الجاني، وهو ما يعد بمثابة تنازل من الهيئة الاجتماعية عن كل أو بعض حقوقها المترتبة علي الجريمة.

وإذا كانت الجرائم الإرهابية تتميز بالحيطة والسرية من ناحية، ومن ناحية أخري تتعاظم آثارها الخطيرة علي المجتمع، لما تسببه من آثار في مختلف مناحي الحياة، ورغبة من المشرع لتلافي ذلك، فقد فتح باب العودة للجاني، شريطة أن يعدل عن سلوكه الإرهابي بأحد الطرق المنصوص عيلها قانونا، ومن هنا لجأت معظم التشريعات العقابية إلي التشجيع علي العدول عن السلوك الإجرامي، لضمان فاعلية المكافحة في مواجهة ظاهرة معقدة كالإرهاب[2]. باعتباره سبباً موجباً للإعفاء من العقاب إذا ما تحققت شروطه.

ويقصد بالعدول الموجب للعفو في مجال الجرائم الإرهابية، ذلك النشاط أو السلوك المضاد للجريمة[3]، والذي يتجسد في أنماط سلوكية ينص عليها المشرع وفق شروط محددة، ويرتب علي توافرها ميزات معينة يكافئ بها الإرهابي. ومن أمثلتها في مجال جرائم الإرهاب، الإخبار عن الجريمة الإرهابية، أو الإخبار عن الجرائم الإرهابية المماثلة، وهو ما يقتضي بطبيعة الحال الانفصال عن العمل الإرهابي.

وقد يكون العدول قبل تحقق النتيجة الإجرامية، بحيث يمنع النتيجة الإجرامية للعمل الإرهابي من الوقوع أصلاً، ويتحقق ذلك الغرض مثلاً في حالة قيام أحد الجناة بالإبلاغ عن وجود قنبلة في مكان عام علي نحو يسهم فيه بالحيلولة دون حدوث التفجير الإرهابي.

1- الدكتور/ أحمد فتحي سرور، (1991) الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، الطبعة الخامسة، رقم 533، صـــ678ـــ.

2- الدكتور/ محمد أبو العلا عقيدة، (2009) تطوير أنظمة العدالة الجنائية في مكافحة الإرهاب علي المستوي الوطني والإقليمي والدولي، جامعة نايف العربية للعلوم الأمنية، الرياض، صـــ124ـــ.

3- F.Palazzo,(1987)Terrorisme et législation anti-terrorismé enItalie, R.S.C., P550.

وقد يكون العدول لاحقا علي إتمام الجريمة، فيعمل علي إزالة النتيجة الإجرامية التي وقعت مسبقاً أو يمنع من تفاقمها بالحد من ضررها ما أمكن.

ويتحقق ذلك مثلاً في الحالة التي تختطف فيها مجموعة إرهابية أحد الأشخاص بهدف قتلة أو تعذيبه، ثم يقوم أحد المختطفين بإبلاغ السلطات المختصة ويسهم في تحرير الرهينة دون أن يلحقه أذي.

والإعفاء من العقاب في الجرائم الإرهابية خطة تشريعية أنتظمها المشرع في التشريعات المعنية بمكافحة الإرهاب في أغلب التشريعات كطريق لمواجهة الجريمة الإرهابية، ولعل من ابرز تلك التشريعات، التشريع الفرنسي، والتشريع الإيطالي، والتشريع المصري، وسوف نتناول كل تشريع من التشريعات السابقة بشيء من الإيجاز فيما يلي:-

أولا:- موقف المشرع الفرنسي:-

لم يغفل المشرع الفرنسي – مثله في ذلك مثل مشرعي الدول الأوروبية الأخري التي عرفت الإرهاب – عن أهمية اسلوب المكافأة في مجال مكافحة الإرهاب، فقد ضمن قانون العقوبات الفرنسي الجديد صوراً من الإعفاءات والتخفيف المتعلقة بالعقوبة بالنسبة للعناصر الإرهابية الذين عادوا إلي صوابهم وأعلنوا توبتهم، أو بعبارة أخري أولئك الذين لعبوا دوراً لا يستهان به في عملية اجهاض الجريمة أو الحد من آثارها، فضلا عن الجانب الأهم وهو دورهم في كشف هوية الجناة والمساعدة في القبض عليهم.

وقد أخذ المشرع الفرنسي بمبدأ الإعفاء من العقاب Absolutoire وتخفيف العقاب Attenuante، ويعتبر هذا المبدأ مكافأة علي الإبلاغ أو الإفشاء عن العناصر الإرهابية، وقد ورد النص علي هذا المبدأ في المواد 422-1، 442-2 من قانون العقوبات الفرنسي الجديد.

1 - الإعفاء من العقاب (L´exemption de pèine):- تنص المادة 1/422 من قانون العقوبات الفرسي الجديد علي أن «كل شخص شرع في ارتكاب عمل إرهابي، يعفي من توقيع العقوبة عليه إذا ما أبلغ السلطات الإدارية أو القضائية بما يسمح بإحباط تنفيذ الجريمة، وعند الاقتضاء الكشف عن هوية المذنبين الآخرين»[1]

1- ورد النص باللغة الفرنسية كالآتي:-

"Toute personne qui a tentè de commettre un acte de terrorisme est exempte de peine, si, ayant averti l´autoritè administrative ou judiciaire, elle a permis d´éviter la réalisation de l´infraction et d´identifier, le cas échéant, les autres coupables".

ويستخلص من هذا النص أن الإعفاء من العقوبة يتضمن ما يلي[1]:-

أ- الشروع في ارتكاب الجريمة الإرهابية: بمعني البدء في تنفيذ الجريمة الذي يعقبة عدول إرادي من جانب الإرهابي، مثال ذلك الإبلاغ عن وجود سيارة ملغومة في مكان لا يوجد به أشخاص الأمر الذي لا يتسبب عنه حدوث خسائر في الأرواح وعليه فالأمر يتعلق بالمعلومات التي يدلي بها الإرهابي عن الانفجار الذي يوضح البرنامج الخاص الذي استهدف قتل واحد أو أكثر من الأشخاص، بما يساعد علي منع حدوث الانفجار أو تحديد أعضاء الجماعة الإرهابية.

ب- مدي فاعلية المعلومات المتحصل عليها لكي يصدر إعفاء من العقاب: فيجب أن تكون المعلومات التي يتم الإدلاء بها إلي السلطة الإدارية أو القضائية منتجة في منع وقوع خسائر، وتحديد المذنبين الآخرين.

وفي الحقيقة إن الاستفادة من الإعفاء ينطوي بلا شك علي فائدة مزدوجة تكمن في فاعلية الإبلاغ من خلال إحباط ارتكاب الجريمة من جانب، ومن جانب آخر كشف هوية الجناة الآخرين إذا ما كان لهم وجود في الواقع.

2 – تخفيض العقوبة: (La diminution de peine):

نصت المادة 442/2 من قانون العقوبات الفرنسي الجديد علي أن «يتم تخفيض عقوبة الحبس إلي النصف للفاعل أو الشريك في جريمة من جرائم الإرهاب إذا أخبر السلطات القضائية أو الإدارية، وأدي ذلك إلي توقف العمل الإجرامي، أو تجنب أن ينجم عن الجريمة موت شخص أو حدوث عاهة مستديمة، وكذلك كشف هوية الجناة الآخرين إذا ما اقتضي الأمر ذلك»[2]

والواقع أن الإرهابي في هذه الحالة إما أن يكون قد أرتكب جريمة تامة أو شرع في ارتكابها، حيث يجري التخفيض في الحالتين، إذا ما أدلي بما لدية من معلومات للسلطات الإدارية أو القضائية.

1- **B. Bouloc, Problémes des repentis, la tradition française relative au statut des repentis, Rev. de. Scien Crim., 1986, P.771.**

- J. Foyer,(1992) Droit et politique dans la répression du terrorisme en France, in Mélanges offerts à G.Levasseur, Litec, , P.409 ets.

- R. Merle,(1986) la penitence et la peine, éd. Cujas, , P.46 ets.

2- **ورد النص باللغة الفرنسية كالتالي:-**

2- Art. 422-2, La peine privative de liberté encourue par l´auteur ou le complice d´un acte de terrorisme est réduitede moitié si, ayant averti les autorités administratives ou judiciaires, il a permis de faire cesser les agissements incriminés ou d´éviter que l´infraction n´entraîne mort d´homme ou infirmité permanente et d´identifier, le cas échéant, les autres coupables. Lorsque la peine encourueest la reclusion criminelle à perpétuité, celle-ci est ramenée à vingt ans de reclusion criminelle.

فإذا كانت المعلومات التي يدلي بها الإرهابي التائب لا تمنع وقوع الجريمة، إلا أنها تسمح إما بإيقاف الأفعال المجرمة (كاحتجاز الرهائن، تغيير مسار الطائرة) وإما يتجنب وقوع حالات وفاة أو جروح خطيرة قد تصل إلي إحداث عاهة مستديمة، وإما الكشف عن هوية الجناة، فلا شك أنه يستفيد من هذا التخفيض.

ومن الملاحظ أن المشرع الفرنسي قد راعي مبدأ التدرج في منح الميزات بحسب أهمية سلوك العائد في الحد من العمل الإرهابي، فالإخبار عن مخطط إرهابي مثلاً لابد أن يكون كفيلاً بمنعة من الحدوث لكي يستحق الجاني الإعفاء من العقاب، أما إذا وقع العمل الإرهابي، فلن يستفيد الجاني إلا من عذر مخفف، وهذا بدورة رهن بمدي إسهامه في الحد من النتائج الضارة للعمل الإرهابي، كما إذا قامت مجموعة إرهابية بخطف شخص بهدف قتلة، ويخبر الجاني عن جريمة الخطف ويسهم في منع وفاة المجني عليه.

ثانيا: موقف المشرع الإيطالي:-

فرق المشرع الإيطالي بين حالة الانفصال عن التنظيم الإرهابي، وحالة الإرهابي الذي يصدر عنه ما يدل علي أنه ندم علي ما اقترفه من أفعال وأتي ما يدل علي عودته للاندماج في السلوك الصحيح للمواطن، وسوف نعرض لحالات الإعفاء من العقاب أو التخفيف منه علي النحو التالي:-

1 - **حالات الانفصال عن الإرهاب:-** يعرف الانفصال عن الإرهاب بأنه الهجر النهائي للتنظيم الإرهابي، الذي يمكن استخلاصه من سلوكيات الإرهابي المنفصل بطريقة موضوعية، مثل الاعتراف بالأنشطة التي قام بها فعلاً، أو انتهاجه سلوكيات لا تتفق موضوعياً وبطريقة واضحة مع استمرار الرابطة الجماعية، أو إنكاره العنف كطريقة ومنهج للكفاح السياسي[1].

وهناك عدة نصوص أوردت الأحكام الخاصة بالانفصال نذكرها فيما يلي:-

أ- المادة 289 مكرر/4 من قانون العقوبات: حيث تقرر هذه الفقرة ظرفاً مخففاً للمساهمة في الجريمة، فالإرهابي الذي ينفصل عن الآخرين ويعمل علي أن يستعيد المجني عليه حريته، يعاقب بعقوبة السجن الذي لا تقل مدته عن سنتين ولا تتجاوز ثماني سنوات. علي أنه إذا مات المجني عليه بعد اخلاء سبيله بسبب ناتج عن الاحتجاز فإن العقوبة تكون السجن الذي لا تقل مدته عن ثماني سنوات ولا تتجاوز ثماني عشر سنة.

1- F.Palazzo, Terrorisme et législation anti-terrorismé en Italie op.cit, P650.

ب- يدخل ضمن حالات الانفصال أيضاً ما نصت عليه المادة 4 من المرسوم بقانون رقم 625 لسنة 1979 والذي أدخلت عليه تعديلات بالقانون رقم 15 الصادر في 6 فبراير 1980، حيث قررت هذه المادة استبدال عقوبة السجن من عشر إلي عشرين سنة بدلاً من عقوبة السجن مدي الحياة للإرهابي الذي ينفصل عن الإرهابيين الآخرين ويعمل علي منع أن يؤدي النشاط الإجرامي إلي نتائج أخطر، أو يساعد بصورة فعالة سلطات الشرطة والقضاء في جمع أدلة حاسمة أو القبض علي المساهمين الآخرين[1].

ويلاحظ أنه لا يلزم أن يؤدي السلوك المعتبر لمنح الإعفاء إلي عدم تحقق النتائج الأخطر، بل يكفي أن يكون سلوكاً ملائماً في حد ذاته لمنع تحقق هذه النتيجة، دون أن يشترط أن يسفر السلوك عن تحقق المنع.

جـ- ويعد من حالات الانفصال عن الإرهاب ما قررته المادة الأولي من القانون رقم 304 لسنة 1982، إذ قررت هذه المادة الإعفاء الكامل من العقاب بالشروط التالية:-

- أن يحل الإرهابي أو يتسبب في حل الجمعية أو العصابة.
- أن يعدل عن الاتفاق أو ينسحب من الجمعية أو العصابة أو يسلم نفسة دون مقاومة أو يلقي السلاح، مقدماً في كل الحالات كل معلومة متعلقة بهيكل وتنظيم الجمعية أو العصابة.

ويشترط لكي يستفيد الإرهابي من الإعفاء الكامل ما يلي:

1 - ضرورة أن يكون الغرض من الاتفاق أو الجمعية أو العصابة التي كان الجاني عضوا بها هو الإرهاب أو قلب نظام الحكم.

2 - يجب أن يسلك الإرهابي التائب ذلك قبل صدور حكم إدانة نهائي بصدد الجرائم السابق الإشارة إليها.

3 - يجب أن يكون سلوك التائب معاصراً لوقوع الجريمة، وواضحاً بطريقة لا تأويل فيها.

وقد أطلق الفقه الإيطالي علي الحالات السابقة حالات الإرهابي النادم Pentto لأن الإرهابي بعد أن ينفصل عن التنظيم الإرهابي يندم علي أفعاله مقدماً يد العون لسلطات التحقيق والعدالة للمساعدة في الكشف عن المساهمين الآخرين وأدوارهم والشهادة ضدهم[2].

1- الدكتور/ محمد أبو الفتح الغنام، (1991) الإرهاب وتشريعات المكافحة في الدول الديمقراطية، مطبعة المعرفة، صـــ86ـــــ

2- الدكتور/ محمد أبو الفتح الغنام، المرجع السابق، صـــ116ـــــ

2 - **حالات تخفيف العقاب:**- نص المشرع الإيطالي في المادة الثانية من القانون رقم 304 لسنة 1982 علي أن «تستبدل عقوبة السجن مدي الحياة بعقوبة السجن من خمس عشر سنة إلي إحدي وعشرين سنة، وتخفض العقوبات الأخرى بمقدار الثلث بحيث لا تتجاوز مدتها بأية حال خمس عشرة سنة، وذلك بالنسبة للمتهمين في جريمة أو أكثر مرتكبة بغرض الإرهاب أو قلب النظام الدستوري وذلك بشرط:-

- أن يحل أو يتسبب في حل الجمعية أو العصابة، أو أن يعدل عن الاتفاق أو ينسحب من الجمعية أو العصابة أو يسلم نفسة دون مقاومة أو يلقي السلاح مقدما في كل الحالات معلومات عن هيكل وتنظيم الجمعية أو العصابة.
- أن يمنع بأية حالة أن يتم تنفيذ الجرائم التي تم تكوين الجمعية أو العصابة بقصد ارتكابها.
- أن يقدم اعترافاً كاملاً بكل الجرائم المرتكبة بأن يعلن المتهم أو يقر بكل ما اقترفه بطريقة كاملة ومفصلة.
- يجب أن يعمل المتهم بصورة فعالة لمحو وتخفيف النتائج الضارة الخطرة للجريمة أو لمنع ارتكاب جرائم مرتبطة[1].

ونلاحظ الفارق بين هذه الحالة وحالة الإعفاء الكامل من العقاب إذ أنه بالرغم من اشتراك السلوك الموضوعي للتائب في الحالتين، وضرورة صدوره قبل النطق بالحكم النهائي بالإدانة في أية حالة كانت عليها الإجراءات، إلا أن الإعفاء الكامل يشترط ألا يكون الإرهابي قد قام بجناية من جنايات الإرهاب فعلاً، ومن ثم فإن محاكمته تكون عن عضويته وانضمامه إلي تنظيم بهدف الإرهاب.

كما نص المشرع الإيطالي في المادة الثالثة من القانون رقم 304 لسنة 1982 علي أن «يستفيد المتهم في إحدى الجرائم بغرض الإرهاب أو قلب النظام الدستوري بتخفيف العقاب بشرط أن:-

- أن يأتي هذا المتهم أحد صور السلوك المنصوص عليها بالفقرتين الأولي والثانية من المادة الأولي، وأن يقدم اعترافاً كاملاً بكافة الجرائم المرتكبة ويساعد سلطة الشرطة أو القضاء في جمع أدلة حاسمة للتعرف أو للقبض علي واحد أو أكثر من الجناة في الجرائم المرتكبة لتحقيق نفس الغرض.

ويكون التخفيف كبيراً إذا كان سلوك التائب ذا قيمة عالية غير عادية، بأن أدي إلي القضاء علي منظمة إرهابية كاملة أو علي قطاع منها ويكون التخفيف في هذه الحالة في حدود نصف العقوبة.

1- الدكتور/ محمد أبو الفتح الغنام، المرجع السابق، صـــ117ـــــ وما بعدها.

وفي هذه الحالة يجوز الإفراج المؤقت عن المتهم. وفي جميع الأحوال يجوز شمول الحكم المخفف بموقف التنفيذ[1].

ثالثا: موقف المشرع المصري:-

لقد أحسن المشرع المصري صنعاً بما أوردة بشأن الإعفاء من العقاب في حالة الإخبار عن مخطط إرهابي حيث نص في المادة 38 من القانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب علي أن «يعفي من العقوبة المقررة للجرائم المشار إليها في هذا القانون كل من بادر من الجناة بإبلاغ السلطات المختصة قبل البدء في تنفيذ الجريمة، ويجوز للمحكمة الإعفاء من العقوبة إذا حصل البلاغ بعد تنفيذ الجريمة وقبل البدء في التحقيق، وذلك إذا مكن الجاني السلطات من القبض علي مرتكبي الجريمة الآخرين، أو علي مرتكبي جريمة أخري مماثلة لها في النوع والخطورة»[2].

ومن الملاحظ أن المشرع المصري قد حصر حالات الإعفاء من العقاب في الجرائم الإرهابية في حالتين، إحداهما وجوبية علي المحكمة، والأخرى جوازيه:-

1 – الحالة الأولي:- الإبلاغ قبل البدء في تنفيذ الجريمة، ويقع الأمر فيها وجوبياً علي المحكمة بالإعفاء من العقاب.

2 – الحالة الثانية:- إذا حصل البلاغ بعد تنفيذ الجريمة وقبل البدء في التحقيق وهي سلطة تقديرية للقاضي بشرط أن يتحقق الآتي:-

أ- التمكين من القبض علي المتهمين الآخرين.

ب- القبض علي مرتكبي جريمة أخري مماثلة لها في النوع والخطورة.

ويخضع الإعفاءات من العقاب لعدول الجاني لنظام خاص قدرة المشرع نظراً لخطورة الجرائم الإرهابية من حيث وقت العدول، وسلوك الإرهابي، وما يمكن أن يحققه هذا العدول من إحداث خلل في بنيان الجماعات الإرهابية.

1- الدكتور/ محمد أبو الفتح الغنام، المرجع السابق، صـــ118ـــــ.

2- تعد هذه المادة لاغية للمادة 88 مكررا (هـــ) حيث تنص علي «يعفي من العقوبات المقررة للجرائم المشار إليها في القسم كل من بادر من الجناة بإبلاغ السلطات الإدارية أو القضائية قبل البدء في تنفيذ الجريمة وقبل البدء في التحقيق، ويجوز للمحكمة الإعفاء من العقوبة إذا حصل البلاغ بعد تمام الجريمة وقبل البدء في التحقيق. ويجوز لها ذلك إذا مكن الجاني في التحقيق السلطات من القبض علي مرتكبي الجريمة الآخرين، أو علي مرتكبي جريمة مماثلة لها في النوع والخطورة».

* **وقت العدول:**- عادة ما يرغب المشرع الجنائي بالإفادة من ميزات العدول بأسرع وقت ممكن، لذلك فهو ينظم مكافأة العدول التي تتمثل في الإعفاء من العقوبة وفق تناسب عكسي مع المرحلة التي تتم فيها، فكلما كان عدول الجاني في مرحلة مبكرة كان جديراً بمكافأة أكبر، وذلك نظراً إلي أثرها المهم في تجنيب المجتمع العمل الإرهابي لذلك تشدد بعض التشريعات في منح العذر المعفي من العقوبة وتشترط أن يكون العدول قبل البدء في تنفيذ العمل الإرهابي كالمشرع المصري، أو تكون علي الأقل في مرحلة الشروع، كالمشرع الفرنسي (المادة 442/1 من قانون العقوبات الجديد).

ولا شك أن السياسة العقابية الحكيمة تقتضي أن يبقي خيار العدول مفتوحاً أمام الجاني في مراحل الجريمة كلها مهما كانت رغبته في العدول متأخرة حتي لو كانت بعد صدور حكم بات، حيث ثبت بالتجربة أن وجود عدد من قيادي وأعضاء الجماعات الإرهابية داخل السجن، قد سمح باستمرار البناء التنظيمي لبعض المنظمات الإرهابية، وأن أعمال التخويف والترهيب داخل السجن قد تكون عائقاً أمام عدول بعض هؤلاء، لذلك لجأت بعض التشريعات إلي تقرير أحكام خاصة بالعدول في أثناء مدة التنفيذ العقابي كمنح الإفراج الشرطي للإرهابيين الموجودين داخل السجن والراغبين في العدول، الأمر الذي يسهم في خلخلة البناء الصلب للمنظمات الإرهابية التي تعمل من داخل السجن، فضلاً عن دورة في الحد من ازدحام السجون، وهذا هو ما فعلة المشرع الإيطالي[1].

* **دور سلوك الإرهابي:**- لاشك أن لسلوك المجرم الإرهابي دوراً هاماً في تحديد درجة المكافأة التي سيحصل عليها، فالمشرع يتغاضى أحياناً عن جسامة الجريمة، ويمنح الإرهابي أعظم مكافأة وهي الإعفاءات من العقاب، عندما يكون لعدولة قيمة غير عادية وأثر مهم في خدمة المجتمع، ومن ذلك علي سبيل المثال حل الجماعة أو المنظمة الإرهابية.

ولقد أدركت معظم التشريعات العقابية أن كفالة الردع الفعال في مواجهة جرائم الإرهاب لا تتأتي من خلال سياسة أحادية الجانب، بل لابد من الجمع بين الأداتين التشديديه والتشجيعية. وقد تم التوصل إلي هذه النتيجة بعد ملاحظة أن التصاعد والتشديد المستمر لعقوبات جرائم الإرهاب لم يحقق النتائج المرجوة منه علي صعيد الردع بشقية، فسياسة المواجهة وحدها لم تفرز إلا مزيداً من النشاطات الإجرامية[2]. فقد ثبت أن فئة الإرهابيين تتسم بضعف الحساسية تجاه

1- **Evans Robert H,(1989)Terrorism & subversion of the state, Italian legal responses, Terrorism and political violence journal, volume 1, No 3, P342.**

نقلا عن الدكتور/ محمد أبو الفتح الغنام، الإرهاب وتشريعات المكافحة في الدول الديمقراطية، المرجع السابق، ص125

2- **الدكتور/ محمد مسعود قيراط، (2001) الإرهاب- دراسة في البرامج الوطنية واستيراتيجيات مكافحتة، جامعة نايف للعلوم الأمنية، الرياض، صـــــ177ـــــــــ.**

سياسة الزجر، فأقصي العقوبات وهي الإعدام لم تكن تخيفهم، بل علي العكس كانت تدفعهم للإستماتة في المقاومة والإمعان في الإجرام، لأن الموت بحسب اعتقادهم كان يحولهم من أفراد عاديين من عامة الشعب إلي أبطال ورموز[1]. أما عن سبب ذلك فمردة إلي أن غالبية المجرمين الذين ينخرطون في العمل الإرهابي هم أشخاص يشعرون بالعزلة والظلم والاضطهاد الاجتماعي أو الاقتصادي أو السياسي[2].

ومن هنا أدرك المشرع المصري ضرورة حث الإرهابيين بفتح أبواب الرجوع لهم، الأمر الذي يشكل حافزاً نفسياً للخروج عن طريق الإرهاب، إذ يعد العدول عن ممارسة الإرهاب بمنزلة ردع خاص ذاتي بالغ القيمة، لأنه نابع من الجاني نفسة، ويدل علي أنه عاد إلي رشدة. وإذا كان المشرع المصري قد قدر خطورة الجرائم الإرهابية بأن توسع في الفقرة الثانية من المادة 38 من القانون رقم 94 لسنة 2015 بأن حفز الجاني بالإبلاغ عن الجرائم الإرهابية دون الجريمة التي اقترفها، فكان أولي به أن يوسع مدة الاستفادة من الإعفاء بجعله حتي تنتهي المحاكمة، وليس كما أوردها باشتراط البلاغ بعد تنفيذ الجريمة وقبل البدء في التحقيق، وهي في جميع الحالات سلطة تقديرية للقاضي.

رابعا:- موقف المشرع العراقي

لقد أحسن المشرع العراقي صنعاً بما أوردة بشأن الإعفاء من العقاب في حالة الإخبار عن مخطط إرهابي حيث نص في المادة الخامسة من القانون رقم 13 لسنة 2005 بشأن مكافحة الإرهاب علي أن

"1 – يعفي من العقوبات الواردة في هذا القانون كل من قام بإخبار السلطات المختصة قبل اكتشاف الجريمة او عند التخطيط لها ويساهم اخباره في القبض علي الجناة او حال دون تنفيذ الفعل.

2 – يعد عذرا مخففا من العقوبة للجرائم المنصوص عليها في المادة الثانية من هذا القانون للشخص اذا قدم معلومات بصورة طواعية للسلطات المختصة قبل وقوع او اكتشاف الجريمة من قبل السلطات وقبل القبض عليه وادت المعلومات الي التمكن من القبض علي المساهمين الآخرين وتكون العقوبة السجن».

1- الدكتور/ محمد أبو الفتح الغنام، الإرهاب وتشريعات المكافحة في الدول الديمقراطية، المرجع السابق، صـــــ310ـــــ.

2- الدكتور/ محمد أبو العلا عقيده، تطوير أنظمة العدالة الجنائية في مكافحة الإرهاب علي المستوي الوطني والإقليمي والدولي، المرجع السابق، صـــ115ـــــ.

نتائج وتوصيات البحث

عرضنا في هذا البحث لموضوع جرائم الإرهاب عبر الإنترنت، وأبرزت الدراسة أن جرائم الإرهاب الإلكتروني تعد واحداً من أخطر أشكال الإرهاب، التي ينتج عنها تدمير المواقع الإلكترونية واتلاف أنظمة المعلومات مما يهدد الأمن القومي والعسكري. وقد توصلت الدراسة إلي النتائج والتوصيات التالية:-

أولا: نتائج البحث

بينا من خلال هذه الدراسة أن الإرهاب الإلكتروني أصبح هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة علي حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة علي الأفراد والمنظمات والدول.

1) كما بينت الدراسة أن من أكثر الوسائل المستخدمة في الإرهاب الإلكتروني هو استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، كما يقوم الإرهابيون أيضاً باختراق البريد الإلكتروني للآخرين وهتك أسرارهم والتجسس علي مراسلاتهم والاستفادة منها في عملياتهم الإرهابية.
2) كما توصلت الدراسة أيضاً إلي أن الجماعات الإرهابية تقوم بتصميم وإنشاء مواقع لهم علي شبكة المعلومات الدولية (الإنترنت) لنشر أفكارهم والدعوة إلي مبادئهم، وتعليم الطرق والوسائل التي تساعد علي القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول علي المواقع المحجوبة، وطرق نشر الفيروسات وغير ذلك.
3) إن أجهزة الأمن تحتاج إلي كثير من العمل لتطوير قدراتها للتعامل مع الجرائم الإلكترونية والوقاية منها، وتطوير إجراءات الكشف عن الجريمة، خاصة في مسرح الحادث، بحيث تتمكن من تقديم الدليل المقبول للجهات القضائية، وأيضاً يلزم نشر الوعي العام بجرائم الإرهاب الإلكتروني، والعقوبات المترتبة عليها، واستحداث الأجهزة الأمنية المختصة القادرة علي التحقيق في جرائم الكمبيوتر، والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

4) يعد من أبرز التحديات القانونية في مجال مكافحة جرائم الإرهاب عبر الإنترنت يتمثل في عدم استيعاب التشريعات والأنظمة للجرائم المستحدثة عبر شبكات المعلومات والوسائط الإلكترونية.

5) كما توصلت الدراسة إلي أن معظم التشريعات العقابية قد لجأت إلي التشجيع علي العدول عن السلوك الإجرامي، لضمان فاعلية المكافحة في مواجهة ظاهرة معقدة كالإرهاب باعتباره سبباً موجباً للإعفاء من العقاب إذا ما تحققت شروطه.

ثانيا: توصيات البحث

توصلت الدراسة إلي مجموعة من التوصيات والمقترحات نوجزها فيما يلي:-

1) نظراً للطبيعة المتعدية الحدود لجرائم الإرهاب الإلكتروني، ولما تثيرة من اشكالات قانونية، يتعين علي الدول التدخل علي محورين، الأول داخلي من خلال ملائمة تشريعاتها مع هذا النمط الجديد من الجرائم، وثانيهما دولي عن طريق تعاون واتفاق حكومات الدول علي سن قوانين وعقوبات لمرتكبي جرائم الإرهاب الإلكتروني وإبرام اتفاقيات دولية جماعية وثنائية علي حد سواء، مع تفعيل اتفاقيات تسليم المجرمين في جرائم الإرهاب الإلكتروني.

2) ضرورة تعديل قوانين الإجراءات الجنائية، بالقدر الذي يسمح ببيان الأحكام اللازم اتباعها حال التفتيش علي الحاسبات، وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتي يستمد الدليل مشروعيته، مع سد كافة الثغرات التي تكتنف جريمة الإرهاب الإلكتروني.

3) ضرورة تضمين المناهج الدراسية بكليات الحقوق مادة عامة عن الجرائم الإلكترونية، بالإضافة إلي ضرورة إدراج الجانب المعلوماتي لكل مادة قانونية، كدراسة الجرائم المعلوماتية ضمن مادة قانون العقوبات، وتدريس آلية عمل المحاكم الإلكترونية ضمن مادة قانون المرافعات، وآلية عمل الحكومة الإلكترونية ضمن مادة القانون الإداري.

4) ضــرورة وضــع مفهوم دولــي موحد للإرهــاب بصفة عامــة، والإرهــاب الإلكتروني بصفة خاصة.

5) تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضد دول أو جهات أخري خارج هذه الأراضي.

6) العمل علي تعزيز إجراءات الأمن والحراسة بأنواعها المختلفة، سواء كانت بشرية أو تكنولوجية علي مراكز ونظم المعلومات التكنولوجية، وفق أحدث تكنولوجيا متقدمة في مجالات التأمين والتشفير بأنواعها المختلفة، مع إنشاء غرفة لإدارة الأزمات التكنولوجية يشارك فيها أخصائيون وخبراء في مختلف التخصصات التكنولوجية والأمنية لإعداد ووضع سيناريوهات لمواجهة أي هجمات إلكترونية محتملة تتعرض لها البلاد والقضاء عليها.

7) ضرورة تحفيز دور المؤسسات الدينية في التوعية وعلي رأسها الأزهر الشريف في رفع الوعي الديني والمبادئ والأخلاقيات بين المجتمع وبذل كل الجهود التي تهدف إلي توعية الشباب في مواجهة دعاوي الجماعات المتطرفة عبر الإنترنت.

8) تفعيل الدور الوقائي الذي يسبق وقوع جرائم الإرهاب عبر الإنترنت، وذلك من خلال تفعيل دور أجهزة الإعلام في مواجهة المواقع التي تروج للفكر المتطرف والإرهاب عبر شبكة الإنترنت، كما نؤكد علي ضرورة التعاون الكامل بين وسائل الإعلام والأجهزة الأمنية في مواجهة الإرهاب الإلكتروني، بأن تزود أجهزة الأمن وسائل الإعلام بكل ما لديها من معلومات في حالة رصد لها لمثل هذه المواقع التي تغذي الفكر المتطرف، كما نؤكد علي أن دور الإعلام يجب أن لا يقتصر علي الإعلام الموجة ضد الجماعات الإرهابية، إنما يجب أن يمتد ليشمل وضع ضوابط خاصة للتغطية الإعلامية للجماعات الإرهابية، ويجب أن تأخذ هذه الضوابط بعين الإعتبار ما يلي:-

(أ) تركيز الإعلام علي ضحايا الإرهاب وفئاتهم واعدادهم وخصوصاً الضحايا من النساء والأطفال وكبار السن، حتي تكون الرسالة الإعلامية قوية وفعالة ومؤثرة في نفوس الجمهور.

(ب) عدم المبالغة في نشر التهديدات الصادرة عن الجماعات الإرهابية من خلال شبكة الإنترنت، نظراً لما يتركه ذلك من آثار سلبية في نفوس المواطنين.

(ج) إبراز دور الأجهزة الأمنية في مكافحة الإرهاب الإلكتروني والتصدي له، مما يولد لدي الجمهور الثقة في قدرات أجهزة الأمن للتصدي للإرهاب والفكر المتطرف عبر الإنترنت.

(د) عدم تسليم وسائل الإعلام بكل ما تنشره الجماعات المتطرفة عبر شبكة الإنترنت، وعدم اعتبارها مصدر من مصادر الإعلام الموثوقة.

(هـ) تعظيم دور المواطن في التصدي لجرائم الإرهاب عبر الإنترنت، وخلق الشعور لدي الجمهور بأن هذا الدور لا يقل أهمية عن دور أجهزة الأمن، بل إن الدور الذي يلعبه المواطن يفوق باقي الأدوار، لأن المواطن من أهم الفئات المستهدفة بالإرهاب الإلكتروني، حيث تسعي الجماعات المتطرفة من وراء استخدام الإنترنت إلي استدراجه وتجنيده لخدمة مصالحها وأهدافها.

وختاماً: أسأل الله عز وجل أن أكون قد وفقت في هذا البحث وأن يرزقني الإخلاص في القول والعمل، وأن يجعل هذا العمل خالصاً لوجهة الكريم، وأدعوه سبحانه أن يغفر لي ما بدر مني من خطأ، وحسبي أني بشر أصيب وأخطئ، وصلي اللهم وسلم على سيدنا محمد وعلي آله وصحبة أجمعين.

مراجع البحث

أولاً: المراجع العربية

(أ) الكتب العامة والمتخصصة

1. الدكتور/ أحمد فتحي سرور،(1991) الوسيط في قانون العقوبات، القسم العام، دار النهضة العربية، الطبعة الخامسة.
2. الدكتور/ جميل عبد الباقي الصغير، (2002) الإنترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية.
3. ـــــــــــــ (1992): القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولي، دار النهضة العربية.
4. الدكتور/ حسنين المحمدي بوادي،(2006): الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي.
5. الدكتور/ عبد الجليل اسماعيل حسن الشيخ زيني (2020) الارهاب الالكتروني في القانون الدولي، الماهية والجزاء، منشورات الحلبي الحقوقية، الطبعة الاولي.
6. الدكتور/ عبد العزيز إبراهيم الشبل،(2007) الجرائم الإلكترونية، ندوة الأمن والمجتمع، الجرائم الإلكترونية، الرياض، 23 ابريل 2007 العدد 14182، النسخة الإلكترونية جريدة الرياض.
7. الدكتور/ عبد الفتاح بيومي حجازي،(2009) الأحداث والإنترنت، أثر الإنترنت في انحراف الأحداث، دار الفكر العربي، الإسكندرية.
8. الدكتور/ علي عبد القادر القهوجي،(1999) الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة، بيروت.
9. الدكتور/ عبدالله عبد الكريم عبد الله،(2007) جرائم المعلوماتية والإنترنت، طبعة أولي، منشورات الحلبي الحقوقية، سوريا.
10. الدكتور/ عمر الفاروق الحسيني،(1991) الحماية الجنائية للحاسب، ورقة بحثية مقدمة إلي الندوة التدريبية باتحاد المصارف العربية مايو 1991.
11. الدكتور/ محمد أبو العلا عقيدة، (2009) تطوير أنظمة العدالة الجنائية في مكافحة الإرهاب علي المستوي الوطني والإقليمي والدولي، جامعة نايف العربية للعلوم الأمنية، الرياض.
12. الدكتور/ محمد أبو الفتح الغنام، (1991) الإرهاب وتشريعات المكافحة في الدول الديمقراطية، مطبعة المعرفة.
13. الدكتور/ محمد سيد سلطان،(2012) قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني.

14. الدكتور/ محمد علي عمران، الدكتور/ فيصل ذكي عبد الواحد، (1999)المدخل لدراسة القانون، الرسالة الدولية للطباعة والكمبيوتر.

15. الدكتور/ محمد محيي الدين عوض، (1981) مبادئ القانون الجنائي، القسم العام.

16. الدكتور/ محمد مسعود قيراط (2001)، الإرهاب- دراسة في البرامج الوطنية واستراتيجيات مكافحته، جامعة نايف للعلوم الأمنية، الرياض.

17. الدكتور/ محمود نجيب حسني،(1983) علاقة السببية في قانون العقوبات، دار النهضة العربية

18. الدكتور/ مصطفي السعداوي، الوسيط في شرح قانون مكافحة الإرهاب رقم 94 لسنة 2015 دراسة نقدية تحليلية مقارنة، دار الكتاب الحديث.

19. الدكتور/ مصطفي موسي، (2005): أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها، دار الكتب القانونية بالمحلة الكبرى.

20. الدكتور/ هلالي عبد الإله أحمد،(2003): الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية.

21. الدكتورة/ نائلة عادل محمد فريد قوره، (2005): جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية.

22. الدكتورة/ نهلاء عبد القادر الومني،(2008): الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع.

23. الدكتور/ يسر أنو علي،(1996): شرح قانون العقوبات، النظرية العامة.

(ب) الرسائل والاطاريح الجامعية

1. الدكتور/ توفيق عبد الله أحمد الخشاشنة،(2016): معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.

2. حمزه بن عفون، (2012): السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير في العلوم القانونية، جامعة الحاج لخضر باتنه، الجزائر.

3. الدكتور/ شريف حسين محمد محمد حسن، (2016): القانون الواجب التطبيق علي الجريمة الإلكترونية، رسالة دكتوراه – كلية الحقوق جامعة عين شمس.

4. الدكتور/ عماد الدين محمد كامل الجمل، الحماية الجنائية لأسرار الدفاع في مواجهة التقدم التكنولوجي الحديث، دراسة مقارنة رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

(ج) الابحاث والمقالات

1. الدكتور/ أيسر محمد عطية، (2014): ورقة عمل بعنوان دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني وطرق مواجهته، مقدمة في الملتقي العلمي بعنوان «الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية خلال الفترة من 7 – 9 /11/ 1435 هـ، 2 – 4 /9/ 2014، كلية العلوم الاستراتيجية، عمان، الأردن.

2. الدكتور/ جميل عبدالباقي الصغير (2012): ورقة عمل مقدمة إلي الندوة التي نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012 بعنوان "مستقبل الإرهاب الإلكتروني".

3. الدكتور/ حسن بن أحمد الشهري، بحث بعنوان الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية وسرية المعلومات من التجسس، المجلة العربية للدراسات الأمنية والتدريب المجلد 28، العدد 5.

4. الدكتور/ عبد الصبور عبد القوي علي،(2015): بحث بعنوان الجرائم الالكترونية، أنواعها وأهدافها وآثارها، المملكة العربية السعودية، مجلة الدراسات المالية والمصرفية، العدد الأول.

5. الدكتور/ عبد الله بن عبد العزيز بن فهد،(2008) بحث بعنوان «الإرهاب الإلكتروني في عصر المعلومات، مقدم إلي المؤتمر الدولي الأول حول «حماية أمن المعلومات والخصوصية في قانون الإنترنت» المنعقد بالقاهرة في الفترة من 2-4 يونيو 2008.

6. الدكتور/ علي محمود علي حمودة، (2003) بحث بعنوان: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية. أكاديمية شرطة دبي، مركز البحوث والدراسات العدد 1 لسنة 2003 من 26- 28 ابريل 2003، دبي، الإمارات العربية المتحدة.

7. الدكتور/ محمد البخاري طشقند، (2011):الإنترنت ومبادئ الأمن المعلوماتي الدولي «الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول» بحث منشور علي شبكة ضياء للمؤتمرات والدراسات في 2011/7/29.

8. الدكتور/ مصطفي جاد، (2012):مقال بعنوان «مستقبل الارهاب الالكتروني، في ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012، جريدة السياسة الدولية التابعة لمؤسسة الأهرام.

9. الدكتور/ هشام بشير، (2012): ندوة نظمها المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 ابريل 2012 بعنوان «مستقبل الإرهاب الإلكتروني» علي الموقع الإلكتروني لجريدة السياسة الدولية التابعة لمؤسسة الأهرام.

ثانيا: المراجع الأجنبية

1. Artvr salary,(1987): computer relauted Ebejlement, computer and security, vol 6, no 1.
2. Bouloc (B),(1986): Problémes des repentis, la tradition française relative au statut des repentis, Rev. de. Scien Crim.,.
3. Catherine (H),(1989): Conly: Organizing for computer crim investigation and prosecution,.
4. Evans Robert (H),(1989):Terrorism & subversion of the state, Italian legal responses, Terrorism and political violence journal, volume 1, No 3,.
5. Foyer (J),(1992): Droit et politique dans la répression du terrorisme en France, in Mélanges offerts à G.Levasseur, Litec,.
6. Mascala Carinne,(2000): criminalitè et contrat èlectronique, IN: Le contrat èlectronique Travaux de l´association CAPITANT Henri, journèes national, Paris,.
7. Matusitz, Jonathan(2005): "Cyber terrorism" American Foreign Policy Interests2, April.
8. Merle (R) (1986): la penitence et la peine, éd. Cujas,.
9. Merwe (Vander)(1993): computer crimes and other crimes against information technology in south Africa "R.I.D.P.
10. Palazzo (F)(1987): Terrorisme et législation anti-terrorismé enItalie, R.S.C.
11. Victoria Baranetsky,(2009): What is cyber terrorism? Even experts can't agree, Harvard Law Record, 5 November.

ثالثا: المواقع الإلكترونية

- http://www.f.law.net/law/threads/11333.
- http://diae.net/4155.
- http://www.siyassa.org.eg/NewsContent/6/51/2450
- http://www.alriyadh.com/243897
- http://sabq.org/MKYede.
- http://www.vetogate.com/1387586.
- https://arabic.rt.com/news/
- http://www.nauss.edu.sa/Ar/CollegesandCenters/ResearchesCenter/studiesmagazine/Archive/1434/Documents/em-dar-56-/.pdf
- http://www.siyassa.org.eg//newsContent/6/51/2450
- www.eapiic.net
- http://www.siyassa.org.eg/NewsContent/6/51/2450/