OPEN ACCESS
Received: 10/11/2024
Accepted: 17/01/2025

مجلة الآداب

Legal procedures in addressing cyber terrorism crimes

Dr. Abdulilah Bin Saeed Ahmed Al-Shahrani*

absahmad@kku.edu.sa

Abstract

This study aims to clarify the concept of cyber terrorism, elucidate the legal procedures preceding the occurrence of cyber terrorism crimes, and outline the legal procedures following such crimes. To achieve these objectives, the descriptive methodology was adopted to analyze and interpret legal texts, judicial rulings, and jurisprudential opinions relevant to the study's subject. The study consists of an introduction and two sections. The introduction discusses the concept of cyber terrorism and some related concepts. The first section addresses the legal procedures prior to combating cyber terrorism. The second section focuses on the legal procedures subsequent to combating cyber terrorism. The study findings indicate that there is no consensus among scholars on the definition of terrorism, with some broadening its scope and others narrowing it. Relevant authorities have taken a range of preemptive measures to prevent such crimes, including issuing numerous regulations and statutes to combat terrorism in all its forms, participating in regional and international agreements on counterterrorism, and establishing specialized bodies, centers, and committees for this purpose.

Keywords: Counterterrorism, Cyber terrorism, Crime Occurrence, Counterterrorism Regulations, International Terrorism.

*Associate Professor of Legal Systems, Department of Jurisprudence Principles, College of Sharia, King Khalid University, Saudi Arabia.

Cite this article as: Al-Shahrani, A. B. S. A. (2025). Legal procedures in addressing cyber terrorism crimes, *Journal of Arts, 13*(1), 548 -563.

© This material is published under the license of Attribution 4.0 International (CC BY 4.0), which allows the user to copy and redistribute the material in any medium or format. It also allows adapting, transforming or adding to the material for any purpose, even commercially, as long as such modifications are highlighted and the material is credited to its author.

(EISSN):2708-5783 ISSN:2707-5508
DOI:https://doi.org/10.35696/joa.v13i1.2447

OPEN ACCESS
تاريخ الاستلام: 10/ 11/ 2024
تاريخ القبول:17/ 01/ 2025

مجلة الآداب

الإجراءات القانونية في التعامل مع جرائم الإرهاب الإلكتروني

د. عبد الإله بن سعيد أحمد الشهراني *

absahmad@kku.edu.sa

الملخص

يهدف البحث إلى بيان مفهوم الإرهاب الإلكتروني، وتوضيح الإجراءات القانونية السابقة على وقوع جريمة الإرهاب الإلكتروني، وذكر الإجراءات القانونية اللاحقة لوقوع جريمة الإرهاب الإلكتروني، واتبع البحث لتحقيق هذه الأهداف المنهج الوصفي، لما يوفره من قدرة على تحليل واستنطاق النصوص النظامية، والأحكام القضائية والآراء الفقهية ذات العاقة بموضوع الدراسة. ويتكون من مقدمة وتمهيد، ومبحثين، تحدث التمهيد عن مفهوم الإرهاب الإلكتروني، وبعض المفاهيم المشابهة، وكان المبحث الأول عن الإجراءات القانونية السابقة لمكافحة الإرهاب الإلكتروني، وكان المبحث الثاني عن الإجراءات القانونية اللاحقة لمكافحة الإرهاب الإلكتروني. وخلص البحث إلى أن مفهوم الإرهاب لم يتم الاتفاق عليه بين الباحثين، فبعضهم يوسع من مدلوله، وبعضهم يختصر، وقد بادرت الجهات المعنية باتخاذ مجموعة من الوسائل السابقة على وقوع الجريمة، ومن ذلك: إصدار عدد من الأنظمة واللوائح لمكافحة الإرهاب بشتى صوره، والدخول في عدد من الاتفاقيات الإقليمية والدولية بشأن مكافحة الإرهاب، وإنشاء الهيئات والمراكز واللجان المختصة بذلك.

الكلمات المفتاحية: مكافحة الإرهاب، الإرهاب الإلكتروني، وقوع الجريمة، لوائح مكافحة الإرهاب، الإرهاب الدولي.

* أستاذ الأنظمة المشارك – قسم الفقه وأصوله – كلية الشريعة - جامعة الملك خالد – المملكة العربية السعودية.

للاقتباس: الشهراني، ع. ب. س. أ. (2025). الإجراءات القانونية في التعامل مع جرائم الإرهاب الإلكتروني، *مجلة الآداب*، *13* (1)، 548-563.

© نُشر هذا البحث وفقًا لشروط الرخصة Attribution 4.0 International (CC BY 4.0)، التي تسمح بنسخ البحث وتوزيعه ونقله بأي شكل من الأشكال، كما تسمح بتكييف البحث أو تحويله أو الإضافة إليه لأي غرض كان، بما في ذلك الأغراض التجارية، شريطة نسبة العمل إلى صاحبه مع بيان أي تعديلات أُجريت عليه.

(EISSN):2708-5783 ISSN:2707-5508
DOI:https://doi.org/10.35696/joa.v13i1.2447

المقدمة

الحمد لله رب العالمين والصلاة والسلام على خير الأنبياء وأشرف المرسلين سيدنا وحبيبنا محمد بن عبد الله، أما بعد:

تعد ظاهرة الإرهاب من أخطر الظواهر التي شهدها العالم، والتي ألمت بواقع العالم العربي والغربي من خلال تعدد الأحداث الإرهابية وتداعياتها، وما خلفته من آثار اقتصادية وسياسية واجتماعية، وقد أصبحت مصطلحات مثل الإرهاب، الإرهاب الدولي الإلكتروني، تعبيرات كثيرة التداول إعلاميا، وأثارت الكثير من الجدل حول أبعادها ومضامينها السياسية والإيديولوجية، وذلك نتيجة تداخل المواقف، واختلاف المصالح السياسية والإستراتيجية والاقتصادية بين الدول، فأصبح الإرهاب فعلا حديث الساعة لدى الشعوب على اختلاف مستوياتها، خاصة بعد أن عرفت التنظيمات الإرهابية زيادة قدراتها واتساع رقعتها وكثرة جرائمها، لتصبح أقوى في الوسائل وأوسع في المدى. (بن عموش، ص 216).

وتتمثل الهجمات الإلكترونية التخريبيَّة التي تهدد المملكة العربية السعوديّة في القرصنة، ونشر الفيروسات، وهجمات تعطيل الخدمات، وتناقش هذه الورقة ماهية الإرهاب الإلكتروني، والإجراءات المبذولة في النظام السعودي لمكافحة هذه الجريمة.

مشكلة الدراسة:

تواجه المملكة العربية السعودية كغيرها من الدول هجمات متعددة في المجال الإلكتروني بهدف الوصول إلى إحداث أضرار في البنية الاقتصادية والسياسية والاجتماعية لها، وتزداد هذه الهجمات وخطورتها مع تطور وسائل التقنية والتكنولوجيا، مما حدا بالمملكة إلى إصدار عدد من الأنظمة في سبيل معالجة ومكافحة هذا الإرهاب، والسؤال الذي نود الإجابة عليه في هذه الدراسة هو:

ما هي الإجراءات القانونية التي اتخذتها المملكة في سبيل محاربة الإرهاب الإلكتروني؟

الدراسات السابقة:

من خلال البحث والاطلاع لم أجد دراسة سبقت بنفس العنوان؛ إلا أن هناك أبحاثا تكلمت حول الموضوع، ومنها:

- وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، دراسة للدكتور عبد الرحمن السند، قدمت في المؤتمر العالمي عن موقف الإسلام من الإرهاب عام 2004م، والدراسة اهتمت بالجانب الشرعي فقط، ولم تتطرق للجانب النظامي؛ حيث إن كثيرا من أنظمة مكافحة الإرهاب صدرت بعد ذلك.
- الإرهاب الإلكتروني دراسة في إشكالات المفهوم والأبعاد، دراسة للباحثة: فريدة بن عموش، منشورة في المجلة الجزائرية للعلوم الاجتماعية والإنسانية، جامعة إبراهيم سلطان، مجلد8، العدد2، 2020م، وقد اهتمت بتحرير مصطلح الإرهاب، وبيان أسبابه وخصائصه، وطرق مكافحته عالمياً، وكل ذلك بعيدا عن الإجراءات القانونية في المملكة العربية السعودية التي سوف نتكلم عنها هنا في دراستنا.

أهداف الدراسة:

تهدف هذه الدراسة لتحقيق ما يلي:

1- بيان مفهوم الإرهاب الإلكتروني.
2- توضيح الإجراءات القانونية السابقة لوقوع جريمة الإرهاب الإلكتروني.

3- ذكر الإجراءات القانونية اللاحقة لوقوع جريمة الإرهاب الإلكتروني.

منهج الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي، لما يوفره من قدرة على تحليل واستنطاق النصوص النظامية، والأحكام القضائية والآراء الفقهية ذات العلاقة بموضوع الدراسة.

خطة البحث:

تتكون من: تمهيد، ومبحثين:

- التمهيد: مفهوم الإرهاب الإلكتروني، وبعض المفاهيم المشابهة.
- المبحث الأول: الإجراءات القانونية السابقة لمكافحة الإرهاب الإلكتروني.
- المبحث الثاني: الإجراءات القانونية اللاحقة لمكافحة الإرهاب الإلكتروني.
- ثم خاتمة اشتملت على أهم النتائج وأبرز التوصيات.

التمهيد

مفهوم الإرهاب الإلكتروني:

يعتبر الإرهاب الإلكتروني من المفاهيم المعقدة والخطيرة، لاعتبارات عدة، منها ما يتصف به هذا النوع من الإرهاب من تعقيدات فنية ناجمة عن ثورة التقنيات والمعلومات، ومنها ما يتصل بقدرة الجماعات الإرهابية على استغلال وسائل الاتصال الرقمي في الوصول إلى شرائح متعددة ومختلفة من البشر، لنشر فكرها المتطرّف. (العذار، 2017، ص222)

ولعلنا نبدأ أولاً بتعريف كلمة الإرهاب، ثم نعرف الإرهاب الإلكتروني:

هناك عدة تعريفات لكلمة (الإرهاب) قبل أن نظيف إليها قيد الإلكتروني، فقد عُرّف الإرهاب بأنه: كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه وأغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم، أو حريتهم، أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد المرافق، أو الأملاك العامة، أو الخاصة، أو اختلاسها، أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر. (الاتفاقية العربية لمكافحة الإرهاب، 1998، م/1).

وعُرف كذلك بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول، بغياً على الإنسان في: دينه، ودمه، وعقله، وماله، وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو المرافق العامة و الأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها. (الإرهاب والعنف، سفر، 1998، ص9).

وفي نظام مكافحة جرائم الإرهاب تم تعريف الجريمة الإرهابية بأنها: كل سلوك يقوم به الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بشكل مباشر أو غير مباشر، يقصد به الإخلال بالنظام العام، أو زعزعة أمن المجتمع واستقرار الدولة أو تعريض وحدتها الوطنية للخطر، أو تعطيل النظام الأساسي للحكم أو بعض أحكامه، أو إلحاق الضرر بأحد مرافق الدولة أو

مواردها الطبيعية أو الاقتصادية، أو محاولة إرغام إحدى سلطاتها على القيام بعمل ما أو الامتناع عنه، أو إيذاء أي شخص أو التسبب في موته، عندما يكون الغرض -بطبيعته أو سياقه- هو ترويع الناس أو إرغام حكومة أو منظمة دولية على القيام بأي عمل أو الامتناع عن القيام به، أو التهديد بتنفيذ أعمال تؤدي إلى المقاصد والأغراض المذكورة أو التحريض عليها.

كما عرف بأنه: أي سلوك يشكل جريمة بموجب التزامات المملكة في أي من الاتفاقيات أو البروتوكولات الدولية المرتبطة بالإرهاب أو تمويله -التي تكون المملكة طرفاً فيها- أو أي من الأفعال المدرجة في ملحق الاتفاقية الدولية لقمع تمويل الإرهاب. (نظام مكافحة جرائم الإرهاب وتمويله، م/1).

أما الإرهاب الإلكتروني فيقصد به: العدوان، أو التخويف، أو التهديد مادياً، أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان فيي: دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض. (السند، 1425، ص 7).

هناك بعض المصطلحات التي تتشابه مع مصطلح الإرهاب الإلكتروني، مثل:

- الجريمة المعلوماتية: فقد نص النظام السعودي على أنها: أي فعل يُرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام. (نظام مكافحة الجرائم المعلوماتية، م/8).

فنلاحظ هنا أن الجريمة الإلكترونية أو المعلوماتية مصطلح عام يشمل الإرهاب الإلكتروني.

أسباب الإرهاب الإلكتروني:

أسباب الإرهاب الإلكتروني تعود للعديد من الأسباب بشكل عام، والتي تتمثل في أسباب اقتصادية، واجتماعية، وفكرية، ولكن الغاية الأساسية من كل تلك الأسباب تتمثل بالأساس في الدوافع ذات الطبيعة السياسية، كما أن كل تلك الأسباب تهدف بالأساس لنشر الخوف والذعر بين الأفراد، واستهداف الأمن العام لجميع الدول لزعزعة الاستقرار وتدمير البنية المعلوماتية لدى الدول. ويشتمل الإرهاب الإلكتروني على العديد من التقنيات التي من خلالها تتم هذه العملية، حيث تستهدف التخطيط، والتحريض، والتجنيد، وزيادة التطرف، والتمويل، والتنفيذ من خلال الهجمات الإلكترونية أو السيبرانية، والتي تستهدف بالأساس: "النظم العسكرية، والبنية التحتية الاقتصادية، ومحطات توليد الطاقة والماء، ونظم الاتصالات، ونظم المواصلات". (وجيه الدسوقي، ص148).

وسائل الإرهاب الإلكتروني:

هناك عدة وسائل تستخدم في الإرهاب الإلكتروني، منها:

1- إنشاء مواقع على الإنترنت: وقد ساعدت المواقع الإلكترونية المنظمات الإرهابية في توسيع أنشطتهم من خلال تبادل الآراء والأفكار والمعلومات، كما ساعدتهم أيضا على جمع أكبر عدد ممكن من الأتباع والأنصار. وتستخدم المنظمات الإرهابية مواقع الإنترنت في: الاتصال والتخفي، وجمع المعلومات، والتخطيط والتنسيق للعمليات الإرهابية، الحصول على التمويل، التعبئة وتجنيد الإرهابيين، التدريب الإرهابي، اختراق وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، والتهديد والترويع الإلكتروني، والتجسس الإلكتروني. (عمير، 2013م، ص35)

2- البريد الإلكتروني: يعد البريد الإلكتروني من أبرز وسائل الإرهاب الإلكتروني، حيث يستخدم في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها. (السند، 2007، ص 8).

3- وسائل التواصل الاجتماعي: وأقدمها الفيس بوك، وتويتر، والإنستغرام، ثم ظهر: السناب شات، والتيك توك، وغيرها من الوسائل السهلة السريعة التواصل والاتصال والتأثير في الناس.

المبحث الأول: الإجراءات القانونية السابقة لمكافحة الإرهاب الإلكتروني

اهتمت المملكة العربية السعودية بمكافحة الإرهاب بكل صوره ومنه الإرهاب الإلكتروني قبل أن يقع، بوضع عدد من الإجراءات الوقائية التي تقي من هذه الجرائم، ونجد أن هناك جهودا بذلت وتبذل قبل وقوع الإرهاب الإلكتروني.

ولعلنا في هذا المبحث نتكلم عن هذه الإجراءات من خلال المطلبين التاليين:

- المطلب الأول: الإجراءات التشريعية لمكافحة الإرهاب الإلكتروني
- المطلب الثاني: الإجراءات الإدارية لمكافحة الإرهاب الإلكتروني

المطلب الأول: الإجراءات التشريعية لمكافحة الإرهاب الإلكتروني

حرصت المملكة من خلال الجهات التشريعية في سن عدد من الأنظمة واللوائح المتعلقة بمكافحة الإرهاب الإلكتروني، ولعلنا نستعرضها فيما يلي:

أولاً: إصدار عدد من الأنظمة واللوائح لمكافحة هذه الجرائم:

سنت العديد من دول العالم قوانين لمكافحة الجرائم الإلكترونية بعد أن ظهر جليا مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها، وأجمعت أغلب هذه القوانين على أن هذه الجرائم الإلكترونية ما هي إلا تعدٍّ على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام الوسائل التقنية، وخصص جزء كبير من هذه القوانين عقوبات رادعة لجرائم الإرهاب الإلكتروني الذي يمتد أثره، ليس إلى دولة معينة بحد ذاتها، بل إنه يمتد ليشمل المجتمع الدولي بأسره. (الشهري، 2015، ص19).

وبالنظر إلى ما قامت به المملكة العربية السعودية نجد أنها قامت بالعديد من الجهود في إصدار الأنظمة واللوائح والقرارات بهذا الشأن، فمن ذلك:

- إصدار نظام مكافحة الجرائم المعلوماتية:

فقد صدر النظام بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / 1428هـ، واشتمل على ست عشرة مادة، وهدف إلى:

1- المساعدة على تحقيق الأمن المعلوماتي.
2- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
3- حماية المصلحة العامة، والأخلاق، والآداب العامة.
4- حماية الاقتصاد الوطني.

وحدد النظام الجهة التي تتولى التحقيق والادعاء في الجرائم المعلوماتية وهي النيابة العامة كما في المادة الخامسة عشرة. وجرّم النظام الإرهاب الإلكتروني في المادة السابعة من النظام حيث أقرَّ: عقوبة السجن لمدة لا تزيد على عشر سنوات وغرامة مالية أو إحداهما ضد كل شخص يرتكب الجرائم التالية:

1- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أداة تستخدم في الأعمال الإرهابية.
2- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

- إصدار نظام مكافحة جرائم الإرهاب:

في عام 1435هـ صدر نظام جرائم الإرهاب وتمويله، بالمرسوم الملكي رقم (م / 16) وتاريخ 1435 / 2 / 24 هـ، اشتمل على 41 مادة في أربعة أبواب. ثم ألغي هذا النظام بإصدار نظام مكافحة جرائم الإرهاب وتمويله مرسوما ملكيا رقم (م 21) بتاريخ 12/2/1439 هـ، حيث اشتمل على 96 مادة موزعة على عشرة فصول. وحدد في المادة الرابعة منه الجهة المختصة بـ: الضبط الجنائي والاستدلال بما في ذلك البحث والتحري والضبط والملاحقة الجنائية والإدارية وجمع الأدلة والقرائن والتحري المالي والعمليات ذات الطابع السري، وكذلك تحديد وتعقب وضبط وتحريز أموال المشتبه به ومتحصلات الجريمة أو وسائطها في الجرائم المنصوص عليها في النظام، وهي (رئاسة أمن الدولة).

وفي المادة الخامسة حدد اختصاص النيابة العامة بأنه: إصدار تكليف بالحضور أو أمر بالقبض والإحضار على من يشتبه في ارتكابه أيًّا من الجرائم المنصوص عليها في النظام.

ثم أصدر مجلس الوزراء اللائحة التنفيذية لنظام مكافحة جرائم الإرهاب وتمويله بقراره رقم (228) بتاريخ 2/5/1440 هـ. حيث جاءت في 26 مادة أوضحت إجراءات ضبط جرائم الإرهاب.

وقد جاء في نظام مكافحة الإرهاب وتمويله: إلزام المؤسسات المالية، والأعمال والمهن غير المالية، والمنظمات غير الهادفة للربح؛ بتحديد و فهم مخاطر تمويل الإرهاب لديها وتقييمها وتوثيقها وتحديثها بشكل مستمر، وتوفير تقييمها للمخاطر، للجهات الرقابية المختصة عند الطلب، مع الأخذ بعين الاعتبار مجموعة واسعة من عوامل الخطر بما فيها تلك المرتبطة بعملائها، أو البلدان أو المناطق الجغرافية، أو المنتجات، أو الخدمات، أو المعاملات أو قنوات التسليم، على أن تتضمّن دراسة تقييم المخاطر وفقاً لهذه المادة تقييماً للمخاطر المرتبطة بمنتجات جديدة، وممارسات العمل والتقنيات قبل استخدامها. (نظام مكافحة الإرهاب، م/63).

ثانياً: الدخول والمصادقة على عدد من الاتفاقيات لمكافحة الإرهاب

صادقت المملكة العربية السعودية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة سنة 2010، والتي تضمّ العديد من الجرائم الإلكترونية مثل سرقة بطاقات الائتمان، وجرائم الإنترنت والإرهاب الإلكتروني، وتصنيع الفيروسات أو نشرها، والقرصنة واختراق الأنظمة، والوصول والاختراق غير المشروع، وغير ذلك. وتهدف هذه الاتفاقيّة إلى تعزيز التعاون بين الدول العربيّة في محاربة الجرائم الإلكترونية، وتؤكد على أهمية تنفيذ قوانين حقوق الملكيّة. وتطبق العقوبات على منتهكي شروط ولوائح الاتفاقيّة.

وقبل ذلك وقعت الدول الأعضاء في مجلس التعاون الخليجي (الاتفاقية العربية لمكافحة الإرهاب) المبرمة في القاهرة سنة 1998م، واتفاقية دول مجلس التعاون لمكافحة الإرهاب الموقعة في الكويت سنة 2004م. وانضمت هذه الدول إلى معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي التي أقرها مؤتمر وزراء خارجية المنظمة في دورته السادسة والعشرين المنعقدة في بوركينا فاسو سنة 1999م. (مكتب الأمم المتحدة، 2009م)

المطلب الثاني: الإجراءات الإدارية لمكافحة الإرهاب الإلكتروني

ثالثاً: إنشاء عدد من الهيئات والمراكز لمكافحة هذا الإرهاب

قبل الحديث عن الهيئات والمراكز التي أنشأتها المملكة نود الحديث عن دور بعض الوزرات في ذلك ومنها:

1- وزارة الاتصالات وتقنية المعلومات: وهي الوزارة المسئولة عن جميع وسائل الاتصال وتقنية المعلومات في المملكة العربية السعودية، وهي الجهة المخول لها اقتراح مشاريع الأنظمة المتعلقة بالاتصالات وتقنية المعلومات ورفعها إلى مجلس الوزراء، وقد قامت الوزارة بإصدار العديد من القرارات المنظمة للتعاملات الإلكترونية منها: القرار رقم 7/ب/ 33181 بتاريخ 2003، المتضمن وضع خطة لتقديم الخدمات والمعاملات الحكومية، والقرار رقم 8189 م/ب/لعام 2005، الخاص بتشكيل لجنة داخل كل جهة حكومية للتعاملات الإلكترونية.

وقد أسهمت الوزارة بصورة كبيرة في الجهود التي تبذلها الدولة لمكافحة جريمة الإرهاب الإلكتروني، من خلال اقتراحها للإستراتيجية الوطنية لأمن المعلومات الخاصة بالمملكة العربية السعودية في عام 2011. وتكونت الإستراتيجية من 90 صفحة، توضح رؤية واضحة للمملكة العربية السعودية، تنص على أن هدفها توفير بيئة رقمية آمنة وقوية، ويمكن القول بأن للإستراتيجية خمسة أهداف رئيسة هي:

- تطوير بنية تحتية لتكنولوجيا المعلومات آمنة ومرنة وموثوق فيها.

- توفير موارد بشرية قادرة على تحقيق الأمن المعلوماتي بأعلى درجاته.

- تهيئة بيئة لأمن المعلومات ملهمة قائمة على الثقة والشفافية والتعاون.

- دعم خدمات الحكومة الإلكترونية ودعم البنية التحتية للمملكة من أجل الإيفاء بأهداف الأمن المعلوماتي وخطط وإستراتيجيات تكنولوجيا المعلومات والاتصالات.

- تعزيز النمو الاقتصادي من خلال البحث والتطوير. (نرمين،2018م، ص207)

2- وزارة الداخلية: تعتبر وزارة الداخلية هي الوزارة المسئولة عن مراقبة شئون الأمن الداخلي، وفي هذا الصدد تسعى الوزارة إلى التصدي للجرائم الإلكترونية، وتقوم بعمل اجتماعات لبحث استعداداتها لمباشرة استقبال بلاغات الجرائم الإلكترونية، وأسلوب تحريز الأدلة الرقمية، وتحديد هوية المجرمين الرقميين، ومراقبة الإنترنت للأغراض الجنائية.

3- وزارة العدل: تختص وزارة العدل بالإشراف على النظام القضائي في المملكة العربية السعودية، كما أنها مسئولة في الوقت نفسه عن ضمان امتثال العاملين لمتطلبات مكافحة غسيل الأموال وتمويل الإرهاب. وقد شهدت المحاكم السعودية زيادة هائلة في البت في أعداد الحالات الخاصة بالجرائم الإلكترونية؛ فبالرغم من أنه كان هناك ما يقرب

من 164 حالة للجرائم الإلكترونية في السعودية في عام 2015، فقد ازداد العدد ليصبح 573 في عام 2016. (موقع وزارة العدل، www.moj.gov.sa).

4- النيابة العامة: لا شك أن النيابة لها الدور البارز في مكافحة الإرهاب، فمنذ صدور الأنظمة التي تجرم الإرهاب والجرائم المعلوماتية نجد أنها نصت على أن المختص في مسائل الضبط والتفتيش والتحقيق والادعاء أمام القضاء هي النيابة العامة. (موقع النيابة، https://www.pp.gov.sa/)

5- رئاسة أمن الدولة: أنشئت بأمر ملكي من خادم الحرمين الشريفين الملك سلمان بن عبد العزيز آل سعود – حفظه الله- في 20 يوليو 2017، وترتبط بمجلس الوزراء وتعنى بكل ما يتعلق بأمن الدولة. وتتبعها كل من المديرية العامة للمباحث وقوات الأمن الخاصة وقوات الطوارئ الخاصة وطيران الأمن والإدارة العامة للشؤون الفنية بالتعاون مع الأجهزة الأمنية التابعة لوزارة الداخلية.

وقد تم إنشاء لجنة في رئاسة أمن الدولة تسمى: اللجنة الدائمة لمكافحة الإرهاب وتمويله، حيث أنشئت بتاريخ 10 /10 /1422هـ الموافق 25 ديسمبر 2001م كنقطة اتصال وطنية لتلقي ودراسة الطلبات المقدمة للمملكة من الدول والمنظمات والهيئات الدولية ذات الصلة بمكافحة الإرهاب وتمويله.

تضم اللجنة الدائمة لمكافحة الإرهاب وتمويله برئاسة أمن الدولة في عضويتها أعضاء دائمين وغير دائمين من جميع الجهات الحكومية ذات الصلة. بموجب نظام مكافحة جرائم الإرهاب وتمويله الصادر بالمرسوم الملكي رقم م/21 وتاريخ 12 /2/ 1439هـ الموافق 1 نوفمبر 2017م. وتُعنى اللجنة الدائمة لمكافحة الإرهاب وتمويله بالآتي:

- تنسيق السياسات الوطنية العامة في مجال مكافحة الإرهاب وتمويله، ومراجعة تلك السياسات وتحديثها دورياً، واتخاذ التدابير اللازمة بشأنها وتطويرها على أساس الالتزامات والمتطلبات والمستجدات الدولية.
- تقييم مخاطر الإرهاب وتمويله بشكل عام وتحديثه دورياً وتطويره على أساس الالتزامات والمتطلبات والمستجدات الدولية، والتنسيق بشأن التقييم مع الجهات ذات العلاقة.
- تلقي الطلبات التي ترد من الدول والهيئات والمنظمات فيما يتعلق بقرارات مجلس الأمن الخاصة بمكافحة الإرهاب أو تمويله.
- وضع الآليات وتحديثها واتخاذ التدابير والإجراءات اللازمة لتنفيذ قرارات مجلس الأمن ذات الصلة، وتشمل قرارات مجلس الأمن 1267(1999)، 1989 (2011)، 2253 (2015)، 1988(2011)، 1373(2001)، والقرارات اللاحقة ذات الصلة.
- تصنيف الأسماء من أفراد وكيانات على القوائم الوطنية بتهمة الإرهاب أو تمويله، واتخاذ الإجراءات حيال تصنيف أسماء الأفراد والكيانات على القائمة الموحدة للجنة مجلس الأمن (2253/1989/1267) والقائمة الموحدة للجنة مجلس الأمن (1988). (موقع اللجنة).

المبحث الثاني: الإجراءات القانونية اللاحقة لمكافحة الإرهاب الإلكتروني

ثمة إجراءات قانونية اتخذتها المملكة العربية السعودية بعد وقوع جريمة الإرهاب الإلكتروني، وذلك بضبط هذه الجرائم، ثم التحقيق فيها، ثم إحالة المتهم للمحاكمة، وبعد ذلك تنفيذ الأحكام القضائية النهائية.

لكن قبل الحديث عن هذه الإجراءات يحسن بنا أن نذكر بعض الصعوبات التي تواجه جهات الضبط حيال ضبط هذه الجرائم، ومنها:

1- التحديات الأمنية: تتمثل في نقص الخبرات الفنية في مجالات تحديد أركان الجريمة الإلكترونية وتقديمها كقضية مكتملة أمام القضاء، بالإضافة إلى صعوبة الرصد والتحقيق ورفع الأدلة الرقمية في كل زمان ومكان، هذه كلها تشكل عوامل تحد من فاعلية المواجهة، فضلاً عن الحدود الفنية والعلاقات بين أطراف أي قضية عبر الإنترنت والتي تتجاوز حدود الدولة الوطنية، وكذلك العدد الهائل من المخالفات والمخالفين على مدار الساعة وهو ما يجعل الضبط والملاحقة من الأمور الصعبة. (فرج، 2015، ص127).

2- التحديات القانونية وغياب جهة السيطرة والرقابة على شبكات الإنترنت: إن التحديات القانونية تتمثل في عدم استيعابها لجرائم الإرهاب الإلكتروني، فالمجرم يستطيع الانطلاق من دولة لا توجد فيها قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق في هذه الجرائم، وكذلك صعوبة وضع معايير واضحة لتحديد الموقع المتطرف والمحرض على العنف والتباس الكثير من المفاهيم وعدم القدرة على تحديد المسؤول المباشر على المحتوى التحريضي أمام القضاء. كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على شبكة الإنترنت، وتسيطر على مدخلاتها، ومخرجاتها يعد سبًبا رئيسًيا في مواجهة ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي شخص الدخول ووضع ما يريد على شبكة الإنترنت وأن كل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة أو إغلاقها وتدميرها بعد قيام المجرم بنشر ما يريده وهذا من شأنه أن يعيق النظر في بعض القضايا.

3- قلة الوعي الأمني: إن معظم مستخدمي شبكة الإنترنت لا يهتم بالإجراءات التي يجب اتخاذها في تأمين معلوماتهم وأجهزتهم أثناء الاتصال بالشبكة حيث يتعامل معظم مستخدمي شبكة الإنترنت باستخفاف ظاهر مع ما يسمعون به يومًيا من اختراقات، وقد أظهرت استطلاعات الرأي أن ثلثي مستخدمي الوصلات عالية السرعة لا يستخدمون جداراً نارياً، أو أنهم يستخدمونها ولكن بشكل خاطئ وهذا ما يساعد العابثين والمجرمين على تحقيق أهدافهم.

4- صعوبة اكتشاف وإثبات الجريمة الإرهابية: في كثير من جرائم الإرهاب الإلكتروني لم يتم العلم بوقوع الجريمة أصلاً، وخاصة في مجال جرائم الاختراق إذ تتعرض الأجهزة يومًيا لمحاولات اختراق دون أن يشعر مستخدموها بذلك، حيث يكتفي بتشغيل برنامج حماية يكشف عن هذه المحاولات، وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، بالإضافة إلى ذلك فإن صعوبة الإثبات تعد من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني لأنها تعطي المجرم أملاً في الإفلات من العقوبة. (حداد، 2018، ص 2).

5- سهولة الاستخدام وقلة التكلفة: إن شبكات الاتصال (الإنترنت) أصبحت زهيدة التكلفة ومتوفرة في جميع دول العالم بخلاف عقد الثمانينات من القرن الماضي، ونظراً لسهولتها وقلة تكلفتها فقد أضحت فرصة مهيئة للإرهابيين في الوصول إلى أهدافهم غير المشروعة والقيام بجرائم الإرهاب الإلكتروني. (الشرفي، 2006م، ص238).

مرحلة ضبط جريمة الإرهاب الإلكتروني والتحقيق فيها ورفع دعوى أمام المحكمة المختصة:

نص نظام مكافحة جرائم الإرهاب وتمويله على أن الجهة المختصة بضبط جرائم الإرهاب وتمويله، وإصدار أوامر الضبط هي جهتان: رئاسة أمن الدولة، والنيابة العامة. وفصل النظام مهام كل جهة على النحو التالي:

1- دوررئاسة أمن الدولة

هناك عدة إجراءات تقوم بها رئاسة أمن الدولة على النحو التالي:

- ضبط الجريمة بما في ذلك البحث والتحري والضبط والملاحقة الجنائية والإدارية وجمع الأدلة والقرائن والتحري المالي والعمليات ذات الطابع السري.
- تحديد وتعقب وضبط وتحريز أموال المشتبه به ومتحصلات الجريمة أو وسائطها في الجرائم المنصوص عليها في النظام. (نظام مكافحة الإرهاب، م/4).
- في مرحلة جمع الاستدلال لها: يُطلب من أي شخص أو من المؤسسات المالية، أو الأعمال والمهن غير المالية المحددة، أو المنظمات غير الهادفة إلى الربح؛ توفير سجلات أو مستندات أو معلومات، وعلى الجهة المطلوب منها ذلك تنفيذه بشكل صحيح ودقيق كما هو محدد في الطلب بصورة عاجلة. وفي حالة كان الطلب موجهاً إلى مؤسسة مالية فيُنفّذ عن طريق الجهة الرقابية المختصّة بالرقابة عليها. وتوضح اللائحة آليات تنفيذ تلك الطلبات. (نظام مكافحة الإرهاب، م/6).
- ولرئيس أمن الدولة -في مرحلة الاستدلال- أن يأمر الجهة المختصة بالحجز التحفظي بصورة عاجلة ودون إبلاغ الطرف المعني على الأموال أو الوسائط أو المتحصلات التي يشتبه ارتباطها بأي من الجرائم المنصوص عليها في النظام أو ستستخدم فيها والتي قد تكون محلاً للمصادرة. (نظام مكافحة الإرهاب، م/9).
- منع المشتبه به من السفر خارج المملكة. (نظام مكافحة الإرهاب، م/10).
- الإفراج المؤقت عن المحكوم عليه في جريمة من الجرائم المنصوص عليها في النظام أثناء تنفيذ العقوبة. (نظام مكافحة الإرهاب، م/13).
- وضع ما يلزم من ضوابط وإجراءات وتدابير لضمان سلامة الوضع الأمني للمفرج عنهم في الجرائم المنصوص عليها في النظام. (نظام مكافحة الإرهاب، م/14).

2- دور النيابة العامة

يتمثل دور النيابة العامة في جرائم الإرهاب في الأمور التالية:

- إصدار تكليف بالحضور أو أمر بالقبض والإحضار على من يشتبه في ارتكابه أيًّا من الجرائم المنصوص عليها في النظام. (نظام مكافحة الإرهاب، م/5).
- إصدار إذن بدخول المساكن أو المكاتب أو المباني وتفتيشها في أي وقت خلال المدة المحددة في إذن التفتيش.
- إصدار إذن بالقبض على الأشخاص وضبط وتحريز الأموال، أو الممتلكات، أو المستندات، أو الأدلة، أو المعلومات، وذلك في أي جريمة من الجرائم المنصوص عليها في النظام. (نظام مكافحة الإرهاب، م/7).
- للنائب العام أن يصدر أمراً مُسبباً بالمراقبة والوصول إلى الأدلة والسجلات والرسائل -بما فيها الخطابات والمطبوعات والطرود وسائر وسائل الاتصال والمعلومات والمستندات المخزنة في الأنظمة الإلكترونية- ذات الصلة بأي من الجرائم المنصوص عليها في النظام، واعتراضها، وضبطها وتسجيلها. (نظام مكافحة الإرهاب، م/8).
- أن تأمر الجهة المختصة بالحجز التحفظي -بصورة عاجلة دون إبلاغ الطرف المعني- على الأموال أو الوسائط أو المتحصلات التي يشتبه ارتباطها بأي من الجرائم المنصوص عليها في النظام أو ستستخدم فيها والتي قد تكون محلاً للمصادرة. (نظام مكافحة الإرهاب، م/9).
- منع المتهم في ارتكاب أي من الجرائم المنصوص عليها في النظام من السفر إلى خارج المملكة. (نظام مكافحة الإرهاب، م/10).

- التحقيق في الجرائم المنصوص عليها في النظام وإقامة الدعوى الجزائية ومباشرتها أمام المحكمة المختصة. (نظام مكافحة الإرهاب، م/18).
- إصدار أمر توقيف أي متهم في جريمة من الجرائم المنصوص عليها في النظام مدة أو مدداً متعاقبة لا يزيد أي منها على (ثلاثين) يوماً ولا تزيد في مجموعها على (اثني عشر) شهراً. (نظام مكافحة الإرهاب، م/19).
- للنيابة العامة أن تأمر بمنع الاتصال بالمتهم أو زيارته مدة لا تزيد على (تسعين) يوماً إذا اقتضت مصلحة التحقيق ذلك. (نظام مكافحة الإرهاب، م/20).
- تتولى النيابة العامة صلاحية تحديد الأموال والوسائط والمتحصلات التي قد تخضع للمصادرة وتعقّبها. (نظام مكافحة الإرهاب، م/22).

ولا بد قبل رفع الدعوى الجزائية أمام المحكمة المختصة من توافر أركان جريمة الإرهاب الإلكتروني، والتي تتمثل في ثلاثة أركان: الركن المادي، والركن المعنوي، والركن الشرعي.

الركن المادي:

ويتمثل الركن المادي في الفعل والسلوك الذي يقوم به المجرم ويمارسه من خلال استخدام وسائل التقنية المعلوماتية، وتتعدد صور هذا الفعل والسلوك حسب ما ورد في نظام مكافحة الإرهاب إلى ما يلي:

- كل من وصف -بصورة مباشرة أو غير مباشرة- الملك أو ولي العهد بأي وصف يطعن في الدين أو العدالة. (نظام مكافحة الإرهاب، م/30).
- من أيّد أي فكر إرهابي، أو دعا له، أو كيان إرهابي، أو جريمة إرهابية، أو منهج مرتكبها، أو أفصح عن تعاطفه معه أو سوَّغ فعله أو جريمته، أو روج لها، أو أشاد بها، أو حاز أو أحرز أي محرر أو مطبوع أو تسجيل -بقصد النشر أو الترويج- أيا كان نوعه ويتضمن تسويغاً، أو ترويجاً لفكر إرهابي، أو لجريمة إرهابية، أو إشادة بذلك. (نظام مكافحة الإرهاب، م/34).
- من حرض آخر على الانضمام إلى أي كيان إرهابي، أو المشاركة في أنشطته، أو جنّده، أو ساهم في تمويل أي من ذلك. (نظام مكافحة الإرهاب، م/35).
- كل من أنشأ أو استخدم موقعاً على الشبكة المعلوماتية أو برنامجاً على أحد أجهزة الحاسب الآلي أو أي من الأجهزة الإلكترونية، أو نَشَر أيًّا منهما؛ لارتكاب أي من الجرائم المنصوص عليها في النظام، أو لتسهيل الاتصال بأحد قيادات أو أفراد أي كيان إرهابي، أو لترويج أفكاره، أو لتمويله، أو لنشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة لاستخدامها في جريمة إرهابية. (نظام مكافحة الإرهاب، م/43).
- من أذاع أو نشر بأي وسيلة خبراً، أو بياناً، أو إشاعة كاذبة، أو مغرضة، أو نحو ذلك، بقصد تنفيذ جريمة إرهابية. (نظام مكافحة الإرهاب، م/44).

الركن المعنوي:

إذا كانت الجريمة بشكل عام تقوم على الركن المعنوي القائم على عنصري العلم والإرادة فإن الإرهاب الإلكتروني لا يكفي فيه القصد العام، بل لا بد أن يعلم الفاعل بالسلوك الإجرامي الذي يرتكبه وإرادة ارتكاب هذا السلوك لقيام الجريمة، أي أن يتوفر ثبوت القصد الخاص بالإضافة إلى القصد العام في نية الفاعل وهو يقوم باستخدام تقنية نظم المعلومات، وأن يهدد بإيقاع أحد الأغراض المعلنة في الجريمة. (هادي، 2019م، ص288)

الركن الشرعي:

يجب العلم بأنه لا جريمة ولا عقوبة إلا بنص النظام، ومن هنا فوجود أي جريمة وفرض العقوبة عليها يعود إلى وجود نص قانوني ثم وجود نظام يقنن العقوبات ويجرم الفعل ويفرض العقوبة المُناسبة على الجاني، ووجود الركن القانوني مُهم جداً وبصورة كبيرة في أي جريمة، وبدونه لا وجود لأي جريمة ولا عقاب على أي جريمة إلا بوجود الركن القانوني أي الشرعي.

ويتمثل الركن الشرعي أو القانوني في الأنظمة التالية:

- نظام مكافحة الإرهاب وتمويله، ولائحته التنفيذية.
- نظام مكافحة الجرائم المعلوماتية.
- نظام مكافحة غسل الأموال.

المحكمة المختصة بقضايا الإرهاب وتمويله:

المحكمة المختصة بقضايا الإرهاب وتمويله هي المحكمة الجزائية المتخصصة التي مقرها الرياض كما نصت على ذلك المادة الأولى من نظام مكافحة الإرهاب.

وقد حدد النظام اختصاصات المحكمة المتخصصة بالفصل فيما يلي:

1- الجرائم المنصوص عليها في النظام.

2- دعاوى إلغاء القرارات ودعاوى التعويض المتعلقة بتطبيق أحكام النظام.

3-طلبات تنفيذ الأحكام الأجنبية النهائية المتعلقة بأي جريمة إرهابية أو جريمة تمويل إرهاب بما فيها الأحكام المتعلقة بمصادرة الأموال أو المتحصلات أو الوسائط المرتبطة بأي من تلك الجرائم.

كما وسع النظام من الاختصاص النوعي للمحكمة الجزائية المتخصصة بشمول النظر فيما إذا: وقعت عدة جرائم يرتبط بعضها ببعض، وكانت إحداها جريمة من الجرائم المنصوص عليها في النظام، فتتولى المحكمة المختصة الفصل في جميع الجرائم الموجهة إلى المتهم، ما لم تفصل أوراق مستقلة لهذه الجرائم قبل رفعها إلى المحكمة. (نظام مكافحة الإرهاب، م/26).

وبالنسبة للعقوبات التي توقعها المحكمة على من ثبتت عليه التهمة، فقد حددها النظام وفصَّلها، وجعل لها حداً أعلى وحداً أدنى. فأقل مدة للسجن ذكرها النظام (سنة) وأعلى حد (30 سنة)؛ وذلك في تفصيل ليس هذا مقام ذكره، لكننا نكتفي بذكر ما يتعلق بالإرهاب الإلكتروني – كمثال وبدون حصر- ومن ذلك:

أن كل من أنشأ أو استخدم موقعاً على الشبكة المعلوماتية أو برنامجاً على أحد أجهزة الحاسب الآلي أو أي من الأجهزة الإلكترونية، أو نَشَر أيًّا منهما؛ لارتكاب أي من الجرائم المنصوص عليها في النظام، أو لتسهيل الاتصال بأحد قيادات أو أفراد أي كيان إرهابي، أو لترويج أفكاره، أو لتمويله، أو لنشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة لاستخدامها في جريمة إرهابية.

فإنه يعاقب بالسجن مدة لا تزيد عن (عشرين سنة) ولا تقل عن (خمس) سنوات. (نظام مكافحة الإرهاب، م/43).

النتائج:

بعد هذا العرض الموجز للإجراءات التي اتخذتها المملكة العربية السعودية في مواجهة الإرهاب الإلكتروني نخلص إلى النتائج التالية:

- أن مفهوم الإرهاب لم يتم الاتفاق عليه بين الباحثين، فبعضهم يوسع من مدلوله، وبعضهم يختصره، وتوصلنا إلى أن النظام السعودي فصّل في التعريفات، فعرّف الجريمة الإرهابية، ثم عرّف الإرهابي، ثم عرّف الكيان الإرهابي.
- لم تقف المملكة مكتوفة الأيدي وتنتظر وقوع جريمة الإرهاب الإلكتروني؛ بل بادرت باتخاذ مجموعة من الوسائل السابقة على وقوع الجريمة، ومن ذلك: إصدار عدد من الأنظمة واللوائح لمكافحة الإرهاب بشتى صوره، والدخول في عدد من الاتفاقيات الإقليمية والدولية بشأن مكافحة الإرهاب، وإنشاء الهيئات والمراكز واللجان المختصة بذلك.
- أن المملكة قد ألغت نظام مكافحة الإرهاب القديم وأصدرت نظاماً جديداً أدخلت فيه مهام واختصاصات رئاسة أمن الدولة.
- أن النظام حاول ذكر صور متعددة لأفعال تعتبر من جرائم الإرهاب، ولا يمنع هذا من دخول صور جديدة مع تقدم الزمن.

ومن أهم التوصيات التي نوصي بها:

- ضرورة زيادة رفع الوعي القانوني لدى المواطن والمقيم حول خطورة جريمة الإرهاب الإلكتروني، وما يترتب على ذلك من عقوبات.
- هناك تداخل بين عمل النيابة العامة ورئاسة أمن الدولة، يحتاج إلى مزيد توضيح وتفصيل في اللائحة التنفيذية.
- إدخال مواد دراسية أو مفردات دراسية في مناهج التعليم توضح الجانب القانوني لجرائم الإرهاب الإلكتروني والآثار المترتبة على ذلك.

المراجع

الاتفاقية العربية لمكافحة الإرهاب. (1998).

حداد، ر. (2018). الإرهاب الإلكتروني وتحديات مواجهته، *مجلة الأمن السيبراني*، (394)، 20-29.

سفر، ح. (1998). الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، بحث مقدم لمجمع الفقه الإسلامي الدولي.

سليمان، ن. (2018). *أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من 2006 إلى 2016* [أطروحة دكتوراه غير منشورة]، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

السند، ع. ع. (2004). *وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها*، بحث مقدم للمؤتمر العالمي عن موقف الإسلام من الإرهاب.

الشرفي، ع. ح. (2006). *الإرهاب والقرصنة البحرية*، جامعة نايف العربية للعلوم الأمنية.

الشهري، ح. (2015). الإرهاب الإلكتروني، *المجلة العربية الدولية للمعلوماتية*، *4*(8)، 22-39.

العذار، أ. ع. (2017). الإرهاب الإلكتروني، *مجلة العلوم القانونية*، *3*(5)، 11-32.

بن عموش، ف. (2020). الإرهاب الإلكتروني دراسة في إشكالات المفهوم والأبعاد، *المجلة الجزائرية للعلوم الاجتماعية والإنسانية*، *8*(2)، 215-232.

عمير، ح. ت. وعبدالله، س. ج. (2013). الإرهاب الإلكتروني ومخاطره في العصر الراهن، *مجلة العلوم القانونية والعلوم السياسية، جامعة ديالي، 2*(1)، 346-318.

اللائحة التنفيذية لنظام مكافحة جرائم الإرهاب وتمويله، الصادرة بقرار قرار مجلس الوزراء رقم (228) بتاريخ 2/5/1440 هـ

المرسي، و. ا. (د.ت)، *الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية*، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (2009). *دراسة حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن.*

موقع اللجنة الدائمة لمكافحة الإرهاب وتمويله. (2024). https://pctc.pss.gov./

موقع النيابة العامة. (2024). https://www.pp.gov.sa/

موقع وزارة العدل. (2024). www.moj.gov.sa.

نظام مكافحة الجرائم المعلوماتية، الصادر بالمرسوم الملكي رقم م/17 بتاريخ 8 / 3 / (1428).

نظام مكافحة جرائم الإرهاب وتمويله، الصادر بالمرسوم الملكي رقم (م 21) بتاريخ 12/2/1439.

هادي، هـ. ط. (2019). المواجهة القانونية والأمنية لجرائم الإرهاب الإلكتروني، مجلة الجامعة العراقية، *مركز البحوث والدراسات الإسلامية، 2*(45)، 20-43.

يوسف، أ. (2015). *جريمة مكافحة الإرهاب الإلكتروني* (ط.1). دار الكتب والدراسات العربية.

Arabic References

al-Ittifāqīyah al-ʿArabīyah li-mukāfaḥat al-irhāb.(1998) .

Ḥaddād, R. (2018). al-irhāb al-iliktrūnī wa-taḥaddiyāt muwājahatih, *Majallat al-amn alsybrāny*, (394), 20-29.

Sifr, Ḥ. (1998). *al-irhāb wa-al-ʿunf fī mīzān al-sharīʿah al-Islāmīyah wa-al-qānūn al-dawlī,* baḥth muqaddam li-Majmaʿ al-fiqh al-Islāmī al-dawlī.

Sulaymān, N. (2018). *Athar al-jarāʾim al-iliktrūnīyah ʿalá al-abʿād al-dākhilīyah lil-amn al-Qawmī : dirāsah ḥālat al-Mamlakah al-ʿArabīyah al-Saʿūdīyah khilāl al-fatrah min 2006 ilá 2016* [uṭrūḥat duktūrāh ghayr manshūrah], Kullīyat al-iqtiṣād wa-al-ʿUlūm al-siyāsīyah, Jāmiʿat al-Qāhirah.

al-Sanad, ʿA. ʿA. (2004). *wasāʾil al-irhāb al-iliktrūnī ḥukmuhā fī al-Islām wa-ṭuruq mukāfaḥatihā,* baḥth muqaddam lil-Muʾtamar al-ʿĀlamī ʿan Mawqif al-Islām min al-irhāb.

al-Sharafi, ʿA. Ḥ. (2006). *al-irhāb wa-al-qarṣanah al-baḥrīyah,* Jāmiʿat Nāyif al-ʿArabīyah lil-ʿUlūm al-Amnīyah.

al-Shahrī, Ḥ. (2015). al-irhāb al-iliktrūnī, *al-Majallah al-ʿArabīyah al-Dawlīyah lil-Maʿlūmātīyah, 4* (8), 22-39.

Alʿdhār, U. ʿA. (2017). *al-irhāb al-iliktrūnī, Majallat al-ʿUlūm al-qānūnīyah, 3* (5), 11-32.

Ibn ʿAmūsh, F. (2020). al-irhāb al-iliktrūnī dirāsah fī Ishkālāt al-mafhūm wa-al-abʿād, *al-Majallah al-Jazāʾirīyah lil-ʿUlūm al-ijtimāʿīyah wa-al-insānīyah, 8* (2), 215-232.

ʿUmayr, Ḥ. t. wʿbdāllh, S. J. (2013). al-irhāb al-iliktrūnī wa-makhāṭiruhu fī al-ʿaṣr al-rāhin, *Majallat al-ʿUlūm al-qānūnīyah wa-al-ʿUlūm al-sīyāsīyah, Jāmiʿat dyāly, 2* (1), 318-346.

al-Lāʾiḥah al-tanfīdhīyah li-niẓām Mukāfaḥat Jarāʾim al-irhāb wa-tamwīluhu, al-ṣādirah bi-qarār qarār Majlis al-Wuzarāʾ raqm (228) bi-tārīkh 1440/5 / 2 H.

al-Mursī, wa. A. (D. t), *al-asālīb al-iliktrūnīyah al-ḥadīthah allatī tstkhdmhā al-Tanẓīmāt al-irhābīyah,* Nadwat Dawr Muʾassasāt al-mujtamaʿ al-madanī fī al-taṣaddī lil-irhāb, Markaz al-Dirāsāt wa-al-Buḥūth, Jāmiʿat Nāyif al-ʿArabīyah lil-ʿUlūm.

Maktab al-Umam al-Muttaḥidah al-Maʿnī bi-al-mukhaddirāt wa-al-jarīmah. (2009). *dirāsah ḥawla Tashrīʿāt Mukāfaḥat al-irhāb fī duwal al-Khalīj al-ʿArabīyah wa-al-Yaman*.

Mawqiʿ al-Lajnah al-dāʾimah li-mukāfaḥat al-irhāb wa-tamwīluhu. (2024). https://pctc.pss.gov

Mawqiʿ al-Niyābah al-ʿĀmmah. (2024). https://www.pp.gov.sa

Mawqiʿ Wizārat al-ʿAdl. (2024). www.moj.gov.sa

Niẓām Mukāfaḥat al-jarāʾim al-maʿlūmātīyah, al-ṣādir bi-al-marsūm al-Malakī raqm M / 17 bi-tārīkh 8/3.(1428) /

Niẓām Mukāfaḥat Jarāʾim al-irhāb wa-tamwīluhu, al-ṣādir bi-al-marsūm al-Malakī raqm (M 21) bi-tārīkh 1439/2 / 12.

Hādī, H. Ṭ. (2019). al-muwājahah al-qānūnīyah wa-al-amnīyah li-jarāʾim al-irhāb al-iliktrūnī, *Majallat al-Jāmiʿah al-ʿIrāqīyah, Markaz al-Buḥūth wa-al-Dirāsāt al-Islāmīyah, 2* (45), 20-43.

Yūsuf, U. (2015). *Jarīmat Mukāfaḥat al-irhāb al-iliktrūnī* (Ṭ. 1). Dār al-Kutub wa-al-Dirāsāt al-ʿArabīyah.