مجـــلـة الحـــق للعلوم الشرعية والقانونية
Al-haq Journal for Sharia and Legal Sciences
تصدر عن كلية القانون – جامعة بني وليد – ليبيا
Website: https://www.al-haqjournal.ly/index.php/alhaq/index
المجلد الثالث عشر ــ العدد الثاني 2026 ــ الصفحات (401-420)
ISSN 3005 – 3919 معامل التأثير العربي 1.72 لسنة 2025 2.113 (ISI) لسنة 2025

# Cyber-terrorism under Libyan Criminal Law: A Comparative Analytical Study

**Muna Mohammed Mraga Alagori***
Department of Criminal Law, Faculty of Law, University of Benghazi, Benghazi, Libya
Muna.mahmod@uob.edu.ly

# الإرهاب الإلكتروني في القانون الجنائي الليبي دراسة تحليلية مقارنة

**د. منى محمد مراجع العقوري ***
قسم القانون الجنائي ،كلية القانون ،جامعة بنغازي ، بنغازي ،ليبيا

| Received: 17-07-2026 | Accepted: 22-08-2026 | Published: 27-08-2026 |
|---|---|---|


**الملخص:**
يشهد العالم في العقود الأخيرة تصاعدًا ملحوظًا في استخدام التكنولوجيا لأغراض غير مشروعة، من أبرزها الإرهاب الإلكتروني، الذي يشكّل أحد أخطر التهديدات الأمنية في العصر الرقمي، فقد مكنت التقنيات الحديثة، الجماعات الإرهابية شن هجمات رقمية تستهدف البنية التحتية الحيوية للدول، والترويج لأفكارها المتطرفة، وارتكاب أفعال إجرامية عابرة للحدود دون الحاجة إلى التواجد المادي في مسرح الجريمة.
يهدف هذا البحث إلى تحليل موقف القانون الجنائي الليبي من ظاهرة الإرهاب الإلكتروني، ومدى قدرته على مواجهتها ضمن الإطار التشريعي القائم، وذلك من خلال دراسة تحليلية مقارنة مع بعض القوانين العربية والأجنبية، كالقانون المصري والأمريكي، بهدف الوقوف على أوجه القصور، واقتراح الحلول التشريعية الملاءمة.
وقد توصل البحث إلى أن القانون الجنائي الليبي يفتقر إلى نصوص خاصة صريحة ومحددة تُعرّف الإرهاب الإلكتروني وتجرّمه بشكل واضح، حيث لا تزال النصوص المتعلقة بالإرهاب أو الجرائم الإلكترونية تُعالج الظاهرة بشكل مجتزء أو عام، مما يُضعف من فعالية المواجهة القانونية.

**الكلمات الدالة:** الإرهاب الإلكتروني، الجرائم الإلكترونية، النظم المعلوماتية، القانون الجنائي، ليبيا.

**Abstract:**
In recent decades, the world has witnessed a marked rise in the use of technology for illicit purposes—most notably cyber-terrorism, which constitutes one of the gravest security threats of

the digital age. Modern technologies have enabled terrorist groups to launch digital attacks targeting critical national infrastructure, propagate extremist ideologies, and commit transnational crimes without the need for a physical presence at the scene of the crime. This research aims to analyze the stance of Libyan criminal law regarding the phenomenon of cyber-terrorism and assess its capacity to address this issue within the existing legislative framework. It employs a comparative analytical approach—drawing on examples such as Egyptian and U.S. laws—to identify shortcomings and propose appropriate legislative solutions. The study concludes that Libyan criminal law lacks specific, explicit provisions that clearly define and criminalize cyber-terrorism; existing statutes concerning terrorism or cybercrimes address the phenomenon only in a fragmented or generalized manner, thereby undermining the effectiveness of the legal response.

**Keywords:** Cyber-terrorism, cybercrimes, information systems, criminal law, Libya.

**المُقَدّمَةُ:**

أدى التطور العلمي و التقني الذي شهده العالم إلى ظهور ثورة معلوماتية هائلة شملت معظم جوانب الحياة. بما في ذلك علم الإجرام الذي عرف تطورا كبيرا ببروز مجموعة من الجرائم المستحدثة التي تعتمد على أساليب متطورة، ومن أبرز هذه الجرائم ما اصطلح على تسميته بالإرهاب الإلكتروني أو المعلوماتي الرقمي. حيث يعتبر الإرهاب الإلكتروني من أبشع وأخطر الجرائم التي ترتكب عبر الإنترنت وتهدد العالم بعصره الآلي، حيث يستغل الإرهابيون والمنظمات الإرهابية الساحة المعلوماتية أو الفضاء الإلكتروني من خلال إنشاء حسابات خاصة في مواقع الإنترنت لنشر التطرف والفكر الإرهابي في العالم والتواصل بين أعضائها، وتدمير المواقع ونشر الفيروسات والتجسس على الدول لكشف أسرارها وابتزازها لتحقيق أغراض إرهابية والحصول على تمويل نشاطها الإرهابي، وتدمير البنية التحتية للدول.

ويعتبر هذا النوع من الإرهاب بمثابة النسخة الإلكترونية للإرهاب التقليدي، فمن حيث التنظيم فهو عابر للحدود الإقليمية، متعدد الجنسيات لا تجمعه قضية وطنية أو قومية ولا حتى أيديولوجية سياسية أو دينية، ويهدف إلى تحقيق أكبر الخسائر المادية والبشرية في ظرف وجيز جدا وبسرعة البرق، مستعملا في ذلك أسلحة رقمية متطورة.

وقد كانت أحداث الحادي عشر من أيلول سبتمبر 2001 المنحى الخطير الذي جعل التنظيمات الإرهابية تنقل جزءًا من نشاطها من المجال المادي الواقعي إلى الفضاء السيبراني، فلم تعد تقتصر على المجال الواقعي فقط. وتكمن خطورة الإرهاب الإلكتروني في سهولة استخدام أدواته، التي تقتصر على جهاز حاسوب، وتطبيقات إلكترونية وبرامج معلوماتية، باتت اليوم في متناول جميع مستخدمي شبكة الإنترنت. حيث يمكن للإرهابي أن يشن هجوماً سيبرانياً، أو يجند طاقات جديدة، أو يحصل على تمويل لتنظيمه، وهو جالس في منزله مستخدماً هوية غير حقيقية، خافياً نفسه عن عيون رجال الأمن، ليحقق نشاطه هذا خسائر جسيمة تفوق بقيمتها الأضرار الناجمة عن نسف مبنى أو تدمير جسر أو خطف طائرة أو عن تفجير انتحاري.

**أهمية البحث:** تبرز أهمية بحث موضوع الإرهاب الإلكتروني، كونه يمسّ أحد أبرز التحديات الأمنية المعاصرة التي تواجه المجتمعات والدول على حدٍّ سواء، حيث صاحب التطور المتسارع في تكنولوجيا المعلومات والاتصالات، تطوّراً في الإرهاب التقليدي ليشمل الفضاء الإلكتروني كأداة لتنفيذ هجمات إرهابية، ونشر الدعاية والترويج، والتخطيط للعمليات الإرهابية، مما يستدعي دراسة علمية متخصصة لفهم هذا التحول.

وللبحث أهمية خاصة كونه يساعد على إبراز الحاجة إلى تطوير أطر قانونية وتشريعية تواكب التطورات التقنية، وتتصدى بشكل فعال للأنشطة الإرهابية في الفضاء السيبراني، بما يضمن حماية حقوق وحريات الأفراد ضمن بيئة رقمية آمنة .
كما يسهم البحث في إثراء الأدبيات المتعلقة بالإرهاب الإلكتروني، نظراً لقلة الأبحاث المتخصصة في هذا النوع من الإرهاب، لا سيما في القانون الجنائي الليبي
**إشكالية البحث:** تثير دراسة ظاهرة الإرهاب الإلكتروني إشكالية تمثل مدى ملاءمة القانون الجنائي الليبي لمواجهة الواقع الإجرامي المتطور باستمرار استخدام الإرهابيين والمجموعات الإرهابية لشبكة الإنترنت، ومدى كفاية هذه النصوص لمواجهة الإرهاب المرتكب عبر الوسائط والنظم الإلكترونية .
**أهداف البحث:** يهدف البحث إلى تحديد مفهوم الإرهاب الإلكتروني، وتمييزه عن الجرائم الإلكترونية العادية، وتحليل موقف القانون الجنائي الليبي من هذه الظاهرة.
**منهجية البحث :** لدراسة موضوع البحث اتبعت المنهج الوصفي لوصف الظاهرة من الناحية التقنية والقانونية، مع استخدام المنهج التحليلي لتحليل نصوص القانون الجنائي الليبي، و مقارنته ببعض التشريعات العربية والأجنبية باتباع المنهج المقارن.
وعليه ينقسم البحث إلى مبحثين:
المبحث الأول: ماهية الإرهاب الإلكتروني.
المبحث الثاني : المواجهة القانونية للإرهاب الإلكتروني.

**المبحث الأول: ماهية الإرهاب الإلكتروني**
باتت التكنولوجيا حاجة يومية للأفراد و الدول التي تتجه في غالبيتها الى تبني تقنيات الحوكمة الذكية والعدالة الذكية والأمن الذكي، وأصبحت كذلك وسيلة لارتكاب الجرائم ولا سيما الجرائم الإرهابية.
و للوقوف على تعريف الإرهاب الإلكتروني سنقوم برصد تعريف الإرهاب التقليدي أولا لغوياً وفي قانون مكافحة الإرهاب، تم نتبعه ببيان المقصود بالإرهاب الإلكتروني
**المطلب الأول: التعريف بالإرهاب الإلكتروني**
لا تزال قضية عدم الاتفاق على تعريف محدد للإرهاب إحدى المشاكل المستعصية عن الحل، والسبب في ذلك لا يرجع إلى غموض المصطلح، ولا عجز المعاجم اللغوية عن تقديم المفردات لتعريفه، ولكن يرجع السبب في عدم الرغبة في الاتفاق على تعريف موحد للإرهاب، إلى الاختلاف والتباين الشديدين في وجهات النظر والإرادات السياسية تبعاً لاختلاف الأيديولوجيات والمصالح، فما يراه البعض إرهاباً، يراه آخرون عملاً مشروعاً.
ونتناول فيما يلي بيان المقصود بالإرهاب التقليدي، نتبعه بتعريف الإرهاب الإلكتروني.
**الفرع الأول: المقصود بالإرهاب التقليدي**
إن من أهم القضايا الجدلية على المستوى الدولي، هو عدم الوصول إلى تعريف جامع و مانع متفق عليه للإرهاب بشكل عام ولعل السبب في ذلك يعود إلى تشعب فكرة الإرهاب وتنوع أشكاله ومظاهره وتعدد أسبابه ودوافعه وأنماطه، واختلاف وجهات النظر الدولية والسياسية حوله فما يراه البعض عملا إرهابيا يراه البعض الآخر عملا مشروعا، وعليه كثرت الدراسات حول الإرهاب، وانعقدت العديد من المؤتمرات في شأنه و وقع على العديد من الاتفاقيات الدولية والإقليمية لمكافحته، وتعددت المحاولات لتعريفه.
**1_ تعريف الإرهاب لغوياً :** كلمة إرهاب في اللغة تعني الخوف والرعب، والإرهاب مصدر أرهب، ومادتها رهب، ومصدره رهباً(الصفوي،1950).

والإرهابيون وصف يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم السياسية.
وقد وردت كلمة الإرهاب في أكثر من موضع في القرآن الكريم منها: (وَلَمَّا سَكَتَ عَن مُّوسَى الْغَضَبُ أَخَذَ الْأَلْوَاحَ ۖ وَفِي نُسْخَتِهَا هُدًى وَرَحْمَةٌ لِّلَّذِينَ هُمْ لِرَبِّهِمْ يَرْهَبُون) (الآعراف:154).
(وَاضْمُمْ إِلَيْكَ جَنَاحَكَ مِنَ الرَّهْبِ) (القصص:32) بمعنى الرهبة أي الرعب والخوف.
وفي القاموس السياسي يقصد بها محاولة نشر الذعر والفزع لأغراض سياسية(قاموس الفنون والأداب،1944).
وفي اللغة الفرنسية هو "مجموعة من أعمال العنف التي ترتكب من قبل تنظيم من أجل خلق مناخ غير آمن أو قلب حكومة قائمة ومستقرة" ( Petet larosse).
ويُعرف الإرهاب كذلك بأنه الاستخدام المنظم لوسائل استثنائية للعنف، من أجل تحقيق هدف سياسي كالاستيلاء، أو المحافظة، أو ممارسة السلطة، وعلى وجه الخصوص فهو أعمال العنف واعتداءات فردية أو جماعية أو تخريب تنفذها منظمة سياسية للتأثير في السكان وخلق مناخ غير آمن(Leperit ,1993).
وقد ظهر مصطلح الإرهاب Terror في أول قاموس الأكاديمية الفرنسية عام 1946م، وبحسب هذا القاموس تتكون كلمة إرهاب من عنصرين:
عنصر نفسي ويعني حدوث تخويف، أو إكراه جسيم، أو هياج، أو اضطراب، أو فتنة في النفس، ويكون مبعث هذا الخوف أو ذلك الهياج...الخ وجود خطر حالّ، أو احتمال وقوع خطر في المستقبل.
عنصر بدني يعني قيام الجاني بإحداث مظاهر خارجية بواسطة جسده(صدقي،1949).
وفي اللغة الإنجليزية يقصد بكلمة الإرهاب في قاموس أكسفورد للغة الإنجليزية (استخدام العنف والتخويف بصفة خاصة لتحقيق أغراض سياسية)(Oxford university press,n,d)

**2_ تعريف الإرهاب في الاتفاقيات الدولية:**

تعد اتفاقية جنيف الخاصة بمنع الإرهاب وقمعه الموقعة في عام 1937م، البادرة الأولى للمجتمع الدولي للاتفاق والتعاون حول مكافحة الإرهاب، إلا أنها لم تدخل حيز التنفيذ حتى يومنا هذا_.
وفي تاريخ 1972/12/18 قررت الجمعية العامة للأمم المتحدة تأليف لجنة لدراسة موضوع الإرهاب الدولي وطرق التصدي له وانبثقت عنها لجنة خاصة للتعريف بالإرهاب، لم تتوصل حتى تاريخه إلى وضع تعريف محدد لها(العوجي،2017).
هذا على المستوى الدولي، أما على المستوى العربي، فقد أصدرت جامعة الدول العربية في العام 1998م، الاتفاقية العربية لمكافحة الإرهاب عرفت المادة الأولى منها البند 2 الإرهاب بأنه: "كل فعل من أفعال العنف أو التهديد به أياً كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي يهدف 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 احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر"(الاتفاقية العربية لمكافحة الإرهاب،1998).

**3_ تعريف الإرهاب في القانون رقم 3 لسنة 2014 بشأن مكافحة الإرهاب:**

على المستوى المحلي لم يعرف قانون العقوبات الليبي شأنه شأن كل القوانين التقليدية جريمة الإرهاب، وأن ورد ذكر مصطلح الإرهاب في العديد من النصوص في قانون العقوبات، و في القوانين الخاصة مثل قانون السرقة الحدية، وقانون الجرائم الاقتصادية.
وعندما سن المشرع الليبي قانون مكافحة الإرهاب رقم 3 لسنة2014م، لم يعرف الإرهاب، و أنما عرف العمل الإرهابي في المادة الثانية منه على أنه:" كل استخدام للقوة أو العنف أو التهديد أو الترويع بهدف الإخلال الجسيم بالنظام العام أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر متى كان من شأن هذا

الاستخدام إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالمواد الطبيعية أو بالآثار أو بالأموال أو بالمباني أو بالأملاك العامة أو الخاصة أو استغلالها أو الاستيلاء عليها أو منع أو عرقلة السلطات العامة أو مصالح الحكومة أو الوحدات المحلية أو البعثات الدبلوماسية والقنصلية أو المنظمات والهيئات الإقليمية والدولية في ليبيا من ممارسة كل أو بعض أوجه نشاطها أو منع أو عرقلة قيام مؤسسات أو دور العبادة أو مؤسسات ومعاهد العلم لأعمالها أو تعطيل تطبيق أي من أحكام الدستور أو القوانين واللوائح وكذلك كل سلوك من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية أو بالنظم المالية أو المصرفية أو بالاقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والمواد الغذائية والمياه أو بسلامتها إذا ارتكب بقصد إحدى الجرائم المنصوص عليها في هذا القانون"(قانون الإرهاب،2014، 2).

وعرف المشرع الليبي في المادة الثالثة منه الجريمة الإرهابية بأنها كل جريمة منصوص عليها في قانون مكافحة الإرهاب، وكذلك كل جريمة ترتكب لقصد تحقيق أحد أهداف العمل الإرهابي، أو تمويل الإعمال الإرهابية.

**3_ تعريف الإرهاب في التشريع الجنائي الفرنسي**:

حدد المشرع الفرنسي في قانون العقوبات رقم 86-1020 الصادر في 9 سبتمبر 1986م، والقوانين الصادرة في 1992، 1996 م مجموعة من الجرائم المنصوص عليها مسبقاً وأخضعها لنظام قانوني أكثر صرامة إذا ما ارتكبت في ظروف معينة.

وقد عرفت المادة (42-1) الجرائم الإرهابية على أن "تعد جرائم إرهابية عندما تتعلق بمشروع فردي أو جماعي بقصد الإضرار الجسيم بالنظام العام عن طريق بث الرعب أو الفزع" (أمل،2011).

**4_تعريف الإرهاب في القانون الأمريكي**:

الإرهاب وفق القانون الأمريكي لمكافحة الإرهاب الصادر سنة 1984م، الإرهاب هو"كل نشاط يتضمن عملاً عنيفاً أو خطيراً يهدد الحياة البشرية، ويتضمن انتهاكا للقوانين الجنائية في الولايات المتحدة أو أية دولة أخرى، ويهدف إلى نشر الرعب والقهر بين السكان المدنيين أو التأثير على سياسة دولة ما، بممارسة الرعب أو التأثير على سياسة حكومة ما عن طريق الاغتيال أو الاختطاف"(Lee,2005).

**ثانياً: تعريف الإرهاب الإلكتروني**

يعتمد المختصين عدة مسميات للتعبير عن استخدام التنظيمات، والجماعات الإرهابية للإنترنت لتحقيق أغراضها الإرهابية، منها الإرهاب السيبراني Cyber Terrorism ، الإرهاب الرقمي Digital Terrorism، والإرهاب الشبكي ، والإرهاب الإلكتروني، وذلك للتعبير عن ظاهرة استغلال الجماعات الإرهابية أدوات التقنية الحديثة في اختراق الفضاء السيبراني وتحقيق أهدافها سياسية كانت، أو اقتصادية، أو دينية.

ظهر مصطلح الإرهاب الإلكتروني عقب التطورات الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسيب الآلية والإنترنت في إدارة معظم شؤون الحياة.

إلا أنه لا يوجد تعريف عالمي متفق عليه لهذه الظاهرة، فقد تعددت التعريفات التي تناولته حسب زاوية نظر كل باحث قانونية أو تقنية أو إجرائية.

يتألف مصطلح الإرهاب الإلكتروني .cyber Terrorism كلمتين كلمة

Cyber تعني الإنترنت، و Terrorism وتعني الإرهاب، و يعتبر الغرب أول من أدرك ظاهرة الإرهاب الرقمي أو ما يسمى سيبراني أو المعلوماتي أو الشبكي حيث تعدد تسمياته.

فأول من استخدام كلمة الإرهاب الإلكتروني هو "Collin Barry" في فترة الثمانينات، وفي الوقت الذي يقر فيه بصعوبة إعطاء تعريف شامل للإرهاب التكنولوجي، يرى بأنه عبارة عن: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية وأن هذه الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب."

وجاء في تقرير الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر" نحن بصدد مخاطر متزايدة، بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر، حيث غدا بإمكان الإرهابيين إحداث تدمير كبير بالاعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربر إلكتروني جديد(عبدالصادق،2015)

ولقد ظهر مصطلح الإرهاب الإلكتروني للعلن في الولايات المتحدة الأمريكية عندما قام الرئيس بل كلينتون سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية، التي توصلت إلى أن مصادر الطاقة والاتصالات، وكذا شبكات الكمبيوتر ستكون هدف الأول للهجمات الإرهابية، ولكن هذه الأخيرة لم تعرفه، واكتفت بدراسة الظاهرة ومحاولة فهم سياسة تفكير الإرهابي الإلكتروني والطرق التي يتخذها في تنفيذ عملياته(فايزة،2016)

وقد عرفت وكالة المخابرات المركزية الأمريكية الإرهاب الإلكتروني على أنه: "أي هجوم تحضيري ذو دوافع سياسية موجهة ضد نظم المعلومات، والتي تنتج عن العنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين "(عبدالصادق)

بينما عرفه قاموس Larousse بأنه "مجموعة من الهجمات الخطيرة، فيروسات، قرصنة، ...الخ، على حواسيب، شبكات، وأنظمة الإعلام الآلي لمؤسسة أو هيئة، ترتكب لخلق فوضى عامة بهدف بث الرعب" (Larousse)

-وفي فرنسا عرف الإرهاب الالكتروني على أنه: "كل هجوم الغرض منه الحصول على المعلومات المرتبطة بالغير وامكانياته واستراتيجياته التي يتخذها للدفاع عن نفسه أو تدمير نظم المعلوماتية أو نشر المعلومات الزائفة من أجل تضليله بتوظيف التكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنت " (Petter,2002)

ويعرفه مجمع الفقه الإسلامي: "بالعدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو ماله بغير حق، باستخدام الموارد والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد".(يوسف،20011)

وهناك من يعرف بأنه هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو الابتزاز أو الإكراه أو التأثير على الحكومات والشعوب أو المجتمع الدولي بأسره، لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة(عالية،2020) .

من هذه التعريفات نرى بأنها تتفق جميعها على أن الإرهاب الإلكتروني هو استغلال الفضاء السيبراني كمسرح الجريمة، والوسائل الرقمية كأداة لتحقيق ذات الغايات التدميرية للإرهاب التقليدي، لكن بوسائل أكثر تخفياً، وأقل تكلفة، وأوسع تأثيراً ، وعابراً للحدود.

وهو ظاهرة عالمية تمثل أحد صور الجرائم السيبرانية العابرة للحدود الوطنية، تستخدم الجماعات الإرهابية الإنترنت لاختراق الحواسيب الآلية والنظم الإلكترونية للمؤسسات والمرافق الحيوية والعسكرية والاقتصادية كالبنوك والمطارات والموانئ وغيرها، للاطلاع على بياناتها المخزنة والتجسس عليها، أو تدميرها، أو ابتزاز حكومات الدول للاستجابة لمطالبها، على نحو يهدد أمن الدول العسكري والاقتصادي .

**المطلب الثاني: صور الإرهاب الإلكتروني وتمييزه عن الجرائم الإلكترونية الأخرى**

يعرف الإرهاب الالكتروني بتعدد أشكاله وصوره بحكم انه ينشط في عالم افتراضي غير مرئي لذا يصعب رصده وحصره فلا يتخذ طابعا و نمطا واحد؛ فقد يكون جريمة عادية مستقلة بذاتها ولكن بارتباطها بعناصر

الإرهاب وأساليبه وأهدافه تعد حينها جريمة إرهابية. كما توجد أوجه شبه وتقارب بينه وبين جرائم إلكترونية أخرى.
نتناول في هذا المطلب في فرعين متتالين أهم صور الإرهاب الإلكتروني، ونبحث العناصر التي تمييزه عن غيره من الجرائم الإلكترونية كالحرب السيبرانية، والقرصنة الإلكترونية.

**الفرع الأول: صور الإرهاب الإلكتروني**

وقد أدى عدم وجود تعريف دقيق لمفهوم الإرهاب السيبراني، إلى تداخل بين وجهان مختلفان للتوظيف الإرهابي لتكنولوجيا المعلومات، هما: الاستخدام الإرهابي لأجهزة الكمبيوتر لتسهيل أنشطة التنظيمات الإرهابية من ناحية، والإرهاب الذي ينطوي على تكنولوجيا المعلومات كسلاح و هدف من ناحية ثانية.
حيث ينبغي التمييز بين الإرهاب الإلكتروني، والأعمال الإرهابية التي تمارس على شبكة الإنترنت، فالإرهاب الإلكتروني هو "الأعمال والأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات والشبكة العنكبوتية بقصد إحداث دمار للبنى التحتية المرتبطة، والمدارة بواسطة مثل هذه التكنولوجيا، وشبكات توزيع المياه والكهرباء، أنظمة الخدمات المصرفية، التسجيلات الصحية، الأنظمة العسكرية، وغيرها من البنى التحتية التي من شأن تدميرها أن تحدث أضرار مباشرة وغير مباشرة بالمواطنين والدول"، بينما الأعمال الإرهابية التي تمارس على شبكة الإنترنت هي "الأنشطة التي تقوم بها منظمات أو جماعات إرهابية تقليدية من أجل تدعيم أعمالها على أرض الواقع، وتشمل أنشطة التجنيد، الدعاية، المواد التعليمية الخاصة بالأعمال الإرهابية، التمويل، تبادل الأوامر...الخ"(عدوان،2013) .
ومن ثم، هناك نوعين من الإرهاب السيبراني هما: الإرهاب السيبراني الخالص ( Pure Cyber Terrorism)،والإرهاب السيبراني الهجين (Hybrid Cyber Terrorism).
**الإرهاب السيبراني الخالص:** يقصد به الهجمات المباشرة على البنية التحتية السيبرانية كأجهزة الكمبيوتر، والشبكات، والمعلومات، لتحقيق أهداف سياسية، أو دينية، أو أيديولوجية.
ويمكن تصنيف هذا النوع من الإرهاب إلى نوعين فرعيين؛ الأول يستهدف التلاعب وإفساد وظائف أنظمة المعلومات وإتلاف أو تدمير الأصول الافتراضية والمادية، باستخدام فيروسات الكمبيوتر، و الهجمات الفردية. بينما يشير الثاني إلى القرصنة المصممة لهدم وتدمير المواقع الإلكترونية، وتعطيل الحياة اليومية باستهداف تعطيل الكامل للبنية الأساسية المادية، كشبكة إمدادات الطاقة، والسكك الحديدية، وإمدادات المياه، والأنظمة المالية وغيرها .
**الإرهاب السيبراني الهجين:** ويقصد به استخدام الإنترنت في مختلف الأنشطة الإرهابية مثل: الدعاية، والتجنيد، والتحريض، وجمع الأموال، واستخراج البيانات، والاتصالات، والتدريب، والتخطيط لهجمات إرهابية فعلية، إذ يستخدم الإرهابيون والتنظيمات الإرهابية شبكة الإنترنت لنشر دعايتهم والترويح لأيديولوجياتهم، وشن الحرب النفسية، ونشر التطرف، وتجنيد أعضاء جدد، وذلك من خلال المواقع الإرهابية والمجلات الإلكترونية ومنصات التواصل الاجتماعي المختلفة(البهي،2019).
وسنحاول فيما يلي تسليط الضوء على بعض صور الإرهاب الإلكتروني.

**1-جريمة التجسس الإلكتروني:**

يعد التجسس من أقدم وأخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب.
و عقب الطفرة التي حققتها تكنولوجيا الإعلام، واستخدام الحواسيب الآلية، وشبكات الإنترنت، تطور التجسس وأصبح الهاجس الأكبر للدول .

ويكون التجسس بقيام الإرهابيون المبرمجون الذين يطلق عليهم (الهاكرز أو القراصنة) باختراق المواقع أو الحواسيب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء، بما في ذلك البريد الإلكتروني، واشتراكات المستخدمين والأرقام السرية لبطاقات الإئتمان، وغيرها.

تعد من أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات ولا تكمن خطورته في استخدام الانترنت وحسب، بل في ضعف الوسائل الأمنية المختصة في حماية الشبكات الخاصة بالمؤسسات والهيئات (البشري،2004).

2- **التهديد الإلكتروني:**

تستغل الجماعات الإرهابية شبكة الانترنت العالمية من أجل بث الرعب والخوف في نفوس الأفراد والدول ولقد تعددت الأساليب التي تستعملها في التهديد عبر الانترنت، منها التهديد بقتل الشخصيات السياسية في الدولة أو بتفجير مراكز سياسية، أو تدمير البنية التحتية المعلوماتية عن طريق نشر الفيروسات لإتلاف الأنظمة المعلوماتية(الشهري، ب،ت).

**3- القصف الالكتروني**

هو أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الالكترونية إلى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على استقبال الرسائل من متعاملين معها والذي يؤدي إلى توقف عمل الشبكة، وعادة ما تلجأ هذه المنظمات الإرهابية إلى تدمير البنى التحتية الخاصة بأنظمة المعلومات (الطعاني،2020).

**الفرع الثاني: تمييز الإرهاب الإلكتروني عن غيره من الجرائم الإلكترونية**

مصطلح الإرهاب الإلكتروني يتشابه ويرتبط ببعض المصطلحات كالقرصنة، وحرب المعلومات وسنحاول عرض أهم أوجه التشابه والاختلاف بينهما.

**1- تمييز الإرهاب الإلكتروني عن القرصنة الإلكترونية**

جريمة القرصنة أو الاختراق بشكل عام هو القدرة على الوصول للهدف بطريقة غير مشروعة عن طريق الثغرات في نظام الحماية الخاص بالهدف " (العجلان،2008).

الفارق بينهما في الهدف ففي حين تهدف القرصنة إلى تحقيق المكاسب المادية المحدودة أو التسلية أو الإزعاج، يسعى الإرهاب الإلكتروني إلى استخدام الإمكانيات التقنية والعلمية واستغلال قدرات الحاسوب وشبكات المعلوماتية في العمليات الإرهابية أو ابتزاز الحكومات والدول.

**2- تمييز الإرهاب الإلكتروني عن الحرب السيبرانية:**

ظهر مصطلح الحرب السيبرانية بكثرة في بداية القرن الحادي والعشرين، وتتعدد المصطلحات التي تصف هذه الظاهرة كالحرب الإلكترونية، وحرب الشبكات، يمكننا التميز بينها بين الإرهاب الإلكتروني من خلال التعرض إلى تعريف الحرب السيبرانية، والتي يقصد بها الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وانظمة البيانات بين دولتين أو اكثر، أو بينها وبين جماعة أو جماعات مسلحة منظمة ضمن سياق نزاع مسلح أو سباق للتسلح أو سياسات الردع المتبادل وذلك لأهداف متنوعة من بينها التسلل إلى نظام الحاسوب وجمع البيانات المخزنة به أو سرقتها أو اتلافها أو تبديلها أو التلاعب بها بعد ان تصبح تحت سيطرة مدبر الهجوم(الرشيدي،2021) .

و تنقسم الحرب السيبرانية إلى نوعين: الحرب السيبرانية هجومية: تقوم بها في الغالب الدولة أو أجهزة استخباراتها لأهداف سياسية أو عسكرية أو غيرها، حيث يستحوذ المهاجم على المعلوماتية ونظمها ويقوم بسرقة البرامج الكمبيوترية، أو يقوم بتخريب، أو تعطيل نظم معلوماتية.

أما الحرب السيبرانية الدفاعية: فهي تعمل على حدود الوقاية من أعمال تخريبية التي قد تتعرض لها وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الإضرار التي قد تحدثها (عبدالصادق).
ومن ابرز امثلة الحرب السيبرانية ، هي الحرب الروسية الجورجية عام 2008 ، إذ تزامنت تلك الهجمات مع غزو بري وبحري وجوي من قبل روسيا الاتحادية ضد جورجيا، ردا على هجوم جورجيا ضد جمهورية أوسيتيا الجنوبية، حيث استخدمت حملة سيبرانية مكثفة وشديدة التنسيق ضد مجموعة من الأهداف الجورجية بما فيها مواقع حكومية ذات قيمة استراتيجية، تضمنت سفارتي الولايات المتحدة والمملكة المتحدة.( &shakarian others,2013)
يختلف الإرهاب السيبراني عن الحرب السيبرانية من حيث افتقاده بصورة ضرورية إلى عنصر المشروعية وارتكابه يكون من قبل أفراد، أو جماعات، دون مستوى الدول ؛ وفي ذات الوقت تكون الحرب السيبرانية التي تخوضها الدول في الفضاء السيبراني مشروعة(زهران،2019)، فضلا عن كون هدف الحرب السيبرانية يختلف عن أهداف الإرهاب السيبراني لان نتيجة الهجوم هي من تحدد من يقف وراءه، حيث أن الحرب السيبرانية تقوم به دولة لتحقيق هدف (سياسي أو عسكري ) من اجل مقتضيات الامن القومي ، بينما الإرهاب السيبراني يقوم به الافراد أو الجماعات والتنظيمات الارهابية لتحقيق اهدافهم السياسية والأيديولوجية المتطرفة، وعلى ذلك فإن الهجمات السيبرانية تشمل كل من الحرب السيبرانية، وكذلك الإرهاب السيبراني، إلا أنها تختلف فقط بالأغراض الأساسية لتلك الهجمات.

**المبحث الثاني: المواجهة القانونية للإرهاب الإلكتروني**

بات الإرهاب الإلكتروني يشكل هاجساً يقلق الدول جميعها، وإزاء تزايد خطورة هذا النوع الجديد من الإرهاب، أبرمت العديد من الاتفاقيات الإقليمية والدولية والجهود الدولية والوطنية لمكافحته، ووضع أسس للتعاون الدولي ، وتبادل المعلومات، كما حرصت الدول على سن القوانين لمجابهته ضمن تشريعاتها الداخلية، وإن تباينت مواقفها في هذا الشأن.

**المطلب الأول: المعاهدات الدولية المتعلقة بمكافحة الإرهاب الإلكتروني**

في ظل ازدياد خطورة هذا النوع الجديد من الإرهاب بات من الضروري تضافر الجهود الدولية لمكافحته، عمل المجتمع الدولي للقضاء على الإرهاب الإلكتروني بكافة أشكاله من خلال إبرام اتفاقيات دولية التي أدت دوراً بارزاً في محاربته. عن طريق سن أحكام قانونية تهدف إلى ردع مرتكبي تلك الجرائم، ومن خلال إلزام الدول الأعضاء بتجريم صور الجرائم الإرهابية الإلكترونية، ومن أهم هذه الاتفاقيات:

**الفرع الأول: معاهدة الأمم المتحدة لمكافحة الجريمة الإلكترونية(UNEP)**

هي معاهدة عالمية تهدف إلى مكافحة الجريمة الإلكترونية عالميًا، ووقع عليها في نهاية أكتوبر في فيتنام. وفي الاجتماع، وقّعت 65 دولة على المعاهدة، والتي ستدخل حيز التنفيذ بعد 90 يوماً من تصديق الدولة الموقعة الأربعين عليها، وفقاً للإجراءات القانونية لكل دولة.
تمت الموافقة على الاتفاقية من قبل الجمعية العامة للأمم المتحدة في ديسمبر 2024، بعد خمس سنوات من المفاوضات.
الهدف الرئيسي من الاتفاقية هو جعل الوقاية من الجرائم الإلكترونية، وجعل الاستجابة لها أكثر فعالية من خلال تعزيز التعاون الدولي وتحسين المساعدة التقنية، وتنمية قدرات البلدان الموقعة.
من خلالها تم إنشاء أول إطار قانوني عالمي لجمع الأدلة الإلكترونية المتعلقة بالجرائم الخطيرة ومشاركتها واستخدامها .
وكذلك إنشاء أول شبكة عالمية للاتصال الدائم (24 ساعة في اليوم، 7 أيام في الأسبوع)، مما يسمح بالتعاون السريع بين الدول.

هذه الاتفاقية، تسعى للعمل على تعزيز التعاون الدولي وتبادل المعلومات، بين الدول في مواجهة هذا النوع من الجرائم.
فضلا عن ذلك، تعمل على إرساء أطر قانونية عالمية لمكافحة الجريمة في العالم الرقمي، مما يُتيح للدول سبل التحرك السريع لمواجهة التهديدات الافتراضية. على سبيل المثال التجريم الرسمي للحوادث الإلكترونية، وتقديم المساعدة لضحايا الهجمات الإلكترونية.
بالإضافة إلى ذلك، توفر المعاهدة المساعدة الفنية والموارد الخارجية للدول الأعضاء، لا سيما الدول النامية، لتنفيذ الإجراءات الرامية إلى مكافحة الجرائم الإلكترونية.
وتظهر العلاقة بين هذه الاتفاقية والإرهاب الإلكتروني من خلال مجموعة من الجرائم التي ألزمت الاتفاقية في الفصل الثاني منها الدول الأطراف بتجريمها في تشريعاتها الوطنية، لعل من أهمها:
1 _جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية تُجرّم الاتفاقية الوصول غير المصرح به إلى نظم تكنولوجيا المعلومات والاتصالات (المادة 7). ويُعد هذا النص أساسًا قانونيًا لمواجهة الجماعات الإرهابية التي تخترق الشبكات الحكومية أو العسكرية أو المصرفية بهدف التجسس أو التخريب أو الحصول على معلومات حساسة.
2 - جريمة اعتراض البيانات والاتصالات الإلكترونية وهو ما يشمل عمليات التجسس الإلكتروني التي قد تلجأ إليها الجماعات الإرهابية للحصول على معلومات أمنية واستخباراتية (المادة 8)
3 -جريمة التدخل في البيانات والأنظمة المعلوماتية أو حذفها أو إفسادها أو تحويرها، (المادة 9) وهي من أكثر النصوص ارتباطًا بالإرهاب الإلكتروني، ذلك أن الهجمات الإرهابية السيبرانية غالبًا ما تستهدف البنية التحتية الحيوية مثل شبكات الكهرباء والمطارات والمصارف والمستشفيات. كما تشمل هجمات حجب الخدمة (DDoS)التي تؤدي إلى تعطيل الخدمات العامة.
4- جريمة إساءة استخدام الأدوات التقنية حيث تنص الاتفاقية على العقاب على إنتاج أو حيازة أو توزيع البرمجيات، والأدوات المستخدمة في ارتكاب الجرائم الإلكترونية، مثل البرمجيات الخبيثة وأدوات الاختراق وكلمات المرور غير المشروعة (المادة 11 من الاتفاقية ).
5. جريمة غسل الأموال المتأتية من الجرائم (المادة 17 من الاتفاقية)، وهو جانب وثيق الصلة بتمويل الإرهاب الإلكتروني، خاصة مع استخدام العملات الرقمية والمنصات الإلكترونية لإخفاء مصادر الأموال وتحويلها عبر الحدود.
وقد خصصت الاتفاقية أحكامًا عديدة للتعاون القضائي الدولي، تشمل تبادل الأدلة الإلكترونية، والمساعدة القانونية المتبادلة، وتسليم المطلوبين، وإنشاء شبكات اتصال تعمل على مدار الساعة. وتُعد هذه النصوص ضرورية لمكافحة الإرهاب الإلكتروني؛ بسبب الطبيعة العابرة للحدود للهجمات السيبرانية.
كما أكدت الاتفاقية على ضرورة احترام حقوق الإنسان والحريات الأساسية في أثناء تطبيق التدابير الخاصة بمكافحة الجرائم الإلكترونية، بما في ذلك مبدأ التناسب وحماية الخصوصية وحرية التعبير. لمنع إساءة استخدام قوانين مكافحة الإرهاب الإلكتروني لتقييد الحقوق الرقمية(الأمم المتحدة،2024).
وبذلك يمكن القول إن اتفاقية الأمم المتحدة لمكافحة الجريمة الإلكترونية لسنة 2024 أرست أساسًا قانونيًا دوليًا لمواجهة الإرهاب الإلكتروني، ليس من خلال تعريف مستقل لهذا المصطلح، وإنما عبر تجريم الأفعال التقنية والمالية والتنظيمية التي تعتمد عليها الجماعات الإرهابية في الفضاء السيبراني، مع تعزيز آليات التعاون الدولي وتبادل الأدلة الإلكترونية بين الدول.

وينبغي التأكيد لكي تُحدث هذه الاتفاقية آثاراً عملية ونتائج ملموسة يجب التغلب على بعض التحديات من بينها، ضرورة موافقة كل دولة على المعاهدة داخليًا، وملاءمة تشريعاتها على نحو يضمن الوفاء بالالتزامات الناشئة عنها، وتوفير البنية التحتية اللازمة لتفعيل الإجراءات اللازمة لتنفيذ الاتفاقية.

**الفرع الثاني: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001**

تعتبر اتفاقية بودابست الموقع عليها في 5 نوفمبر 2001 أول اتفاقية تعنى بالجرائم الإلكترونية، وقد وقعت عليها إحدى وعشرون دولة أوروبية، بالإضافة إلى كندا وأمريكا وجنوب أفريقيا، تعد الإطار القانوني الأكثر أهمية، كونها أول معاهدة دولية لمكافحة هذا النوع من الجرائم، وتحدد إجراءات البحث والتحري الرقمية، وتضع أسسا للتعاون الدولي في مجال تبادل المعلومات، وتسليم المجرمين .

ورغم أن اتفاقية بودابست لا تستخدم مصطلح الإرهاب الإلكتروني بشكل صريح ومباشر، إلا أن العديد من نصوصها تُطبق عمليًا على الأفعال الإرهابية المرتكبة عبر الفضاء السيبراني، خاصة الهجمات التي تستهدف البنية التحتية الرقمية أو استخدام الإنترنت في التخطيط أو التحريض أو تمويل العمليات الإرهابية. وتظهر هذه النصوص في مجموعة من المواد التي تجرّم الاعتداء على الأنظمة والمعلومات الإلكترونية، ومن أهم النصوص ذات الصلة:

1. المادة 2 الدخول غير المشروع(Illegal Access)

تجرّم هذه المادة الدخول العمدي غير المصرح به إلى الأنظمة المعلوماتية. ويُعد هذا النص أساسًا قانونيًا لملاحقة الجماعات الإرهابية التي تخترق الأنظمة الحكومية أو الأمنية أو المصرفية لتحقيق أهداف سياسية أو تخريبية.

2 _المادة 4 الإضرار بالبيانات(Data Interference)

إذ تنص على تجريم إتلاف أو حذف أو تعديل البيانات الإلكترونية دون حق. وتبرز أهمية هذه المادة في مواجهة الهجمات الإرهابية التي تستهدف قواعد البيانات الوطنية، أو الأنظمة الحيوية بهدف إحداث الفوضى أو تعطيل الخدمات العامة.

3 _المادة 5 الإضرار بالأنظمة(System Interference)

تجرّم هذه المادة تعطيل عمل الأنظمة المعلوماتية بصورة خطيرة، بما يشمل هجمات حجب الخدمة (DDoS). ويُعتبر هذا النص من أكثر المواد ارتباطًا بالإرهاب الإلكتروني، لأن الجماعات الإرهابية قد تستخدم فعل تعطيل والإضرار بالأنظمة لاستهداف شبكات الكهرباء، أو المطارات، أو المستشفيات، أو المؤسسات المالية.

4 _المادة 6 إساءة استخدام الأدوات الإلكترونية(Misuse of Devices)

هذه المادة تجرم إنتاج أو بيع أو حيازة أدوات وبرمجيات مصممة لارتكاب الجرائم الإلكترونية، مثل البرمجيات الخبيثة وأدوات الاختراق .

كما أفردت هذه الاتفاقية فصلًا كاملًا للتعاون الدولي، بما يشمل تسليم المجرمين وتبادل الأدلة الرقمية، والمساعدة القانونية المتبادلة، وهو أمر بالغ الأهمية في مكافحة الإرهاب الإلكتروني بسبب الطبيعة العابرة للحدود لهذه الجرائم.

وقد أضيفت بروتوكولات لاحقة لهذه الاتفاقية، أهمها البروتوكول الإضافي المتعلق بمكافحة المحتوى العنصري والمتطرف المنشور عبر الأنظمة المعلوماتية، بالإضافة إلى البروتوكول الثاني المتعلق بتعزيز التعاون الدولي والحصول على الأدلة الإلكترونية. الأمر الذي ساهم في تطوير الإطار القانوني لمواجهة الأنشطة المتطرفة والإرهابية عبر الإنترنت(Councl of Europe)

وتعد اتفاقية بودابست وفرت أساساً قانونياً عالميًا للتعامل مع الإرهاب الإلكتروني، لأنها جرّمت الأفعال التقنية التي يعتمد عليها الإرهابيون في تنفيذ الهجمات الرقمية، أو نشر الدعاية، أو تعطيل البنية التحتية الحيوية.

**الفرع الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010**

أبرمت هذه الاتفاقية بتاريخ 21 ديسمبر 2010، بمدينة القاهرة، وتهدف إلى توحيد السياسة الجنائية لحماية المجتمع العربي من خطر جرائم تقنية المعلومات بما فيها جريمة الإرهاب الإلكتروني، و تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، للحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

ألزمت هذه الاتفاقية بموجب المادة 5 منها، جميع الدول الأطراف بأن تجرم في قوانينها الداخلية جميع الأفعال التي نصت عليها في الفصل الثاني منها، بما في ذلك الأفعال المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وقد حصرت الاتفاقية هذه الجرائم في ثلاث صور؛ وهي نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، ونشر طرق صناعة المتفجرات، ونشر الفتن والنعرات والاعتداء على الديانات، وتمويل الأعمال الإرهابية، والتدريب عليها، وتسهيل الاتصال بين المنظمات الإرهابية(الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،2010) .

**المطلب الثاني: مواجهة الإرهاب الإلكتروني في التشريعات الوطنية**

سنعرض فيما يلي لموقف المشرع الليبي من الإرهاب الإلكتروني، تحديداً في القانون رقم 3 لسنة 2014، بشأن مكافحة الإرهاب، والقانون رقم 5 لسنة 2022 بشأن الجرائم الإلكترونية، ونتطرق لبحث مواجهة الإرهاب الإلكتروني في بعض التشريعات المقارنة.

**الفرع الأول: موقف المشرع الليبي من الإرهاب الإلكتروني**

قانون العقوبات الليبي الصادر عام 1953م، لم ينص على جريمة الإرهاب ولا سيما جريمة الإرهاب الإلكتروني، الذي ارتبط ظهوره مع تطور التكنولوجيا ووسائل الاتصال الحديثة.

**أولاً: القانون رقم 3لسنة 2014 بشأن مكافحة الإرهاب**

وجاء القانون رقم 3 لسنة 2014م، بشأن مكافحة الإرهاب، خالياً من نص محدد خاص لجريمة الإرهاب الإلكتروني إلا أنه تضمن عدة تطبيقات للجرائم الإرهابية يمكن أن تقع ضد الاتصالات والنظم الإلكترونية، أو باستخدام الوسائل الإلكترونية والإنترنت، أو عبر المواقع الإلكترونية منها:

-1العمل الإرهابي ضد النظم الإلكترونية

عرف المشرع الليبي العمل الإرهابي في المادة الأولى منه بأنه كل استخدام للقوة أو التهديد أو الترويع بهدف الإخلال الجسيم بالنظام العام أو تعريض سلامة المجتمع أو مصالحه للخطر متى كان من شأن هذا الاستخدام إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو أمنهم للخطر ...، وكل سلوك من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية ...إذا ارتكب بقصد ارتكاب أحد الجرائم المنصوص عليها في هذا القانون .

فالنص هنا يحمي الاتصالات بما تشمله من شبكات ووسائل نقل البيانات وتبادلها، والنظم المعلوماتية التي تتألف من عتاد صلب، وبرمجيات، وشبكات، قواعد بيانات، وإجراءات تعمل على معالجة البيانات وتخزينها ونقلها، واسترجاعها، بهدف تحويلها إلى معلومات ذات قيمة تستخدم في دعم اتخاذ القرارات، وأتمتة العمليات، وتحقيق الأهداف الاستراتيجية للمؤسسة ، وذلك لحماية سلامة البيئة الرقمية، وضمان كفاءتها، واستمرارية عملها(Stair,R, &others,2017)

فأي سلوك ينجم عنه الإضرار بالاتصالات أو بالنظم المعلوماتية إذا ما ارتكب بقصد ارتكاب إحدى الجرائم المنصوص عليها في قانون مكافحة الإرهاب يعد عملاً إرهابياً، وعقوبته هي السجن المؤبد.
فالمشرع الليبي مستعملاً عبارة (كل سلوك) لم يشترط أن يكون السلوك الإجرامي هنا عنيفاً أو باستخدام القوة المادية، وحسن فعل إذ ذلك يتلاءم مع طبيعة الجرائم الإلكترونية اللامادية التي تعتمد على الأثر الرقمي.
تبنى المشرع الليبي صياغة عامة في هذا النص بحيث يشمل التجريم الوسائل التقليدية والمستحدثة، سواء كانت معروفة وقت صدور القانون، أو ظهرت لاحقاً نتيجة للتطور التقني.
كما أن استخدام عبارة (من شأنه الإضرار) تعني أن المشرع الليبي لم يشترط تحقق الضرر الفعلي، وإنما يكفي أن يكون السلوك بطبيعته صالحاً لإحداث الضرر، أو من المحتمل أن يؤدي إليه، وعلى ذلك فأن الجريمة تعد من جرائم الخطر لا جرائم الضرر، ذلك أن مناط التجريم هنا هو تعريض المصلحة المحمية للخطر، وليس الاعتداء عليها بالفعل.
وتطلب المشرع لهذا العمل الإرهابي قصداً جنائياً خاصاً إلى جانب القصد الجنائي العام، وهو أن يكون السلوك قد ارتكب بقصد ارتكاب إحدى الجرائم المنصوص عليها في قانون مكافحة الإرهاب رقم 3 لسنة 2014.
وهذا يعني ضرورة توافر علم الجاني بطبيعة فعله، وأن من شأنه الإضرار بالاتصالات أو النظم المعلوماتية، واتجاه إرادته إلى استخدام هذا الإضرار كوسيلة أو تمهيد لارتكاب جريمة إرهابية أخرى.
وعلى ذلك فإن الإضرار غير المقترن بهذا القصد الخاص لا يكفي لتطبيق هذا النص، وإنما قد يخضع لنصوص جنائية أخرى.
ويعكس هذا الاتجاه سعي المشرع الليبي إلى توفير حماية استباقية للبنية الرقمية، من خلال تبني صياغة مرنة تستوعب التطورات التقنية المتسارعة، الأمر الذي يقتضي ضرورة تفسير هذا النص من قبل القضاء تفسيراً ضيقاً يتفق مع مبدأ الشرعية الجنائية.
-2جريمة الاشتراك في جريمة إرهابية عن طريق وضع خبرات أو كفاءات إلكترونية على ذمة تنظيم إرهابي أو شخص إرهابي.
نصت عليها الفقرة 2 من المادة 11 التي نصت على أن: يعاقب باعتباره شريكاً في الجريمة الإرهابية كل من يتعمد ارتكاب أحد الأفعال ...وضع كفاءات أو خبرات على ذمة تنظيم إرهابي أو أشخاص لهم علاقة بالجرائم الإرهابية المنصوص عليها في هذا القانون، والخبرة في مجال الإنترنت والوسائل الإلكترونية والاتصال تعد من ضمن هذه الخبرات التي إذا ما وظفت لفائدة إرهابي أو تنظيم إرهابي يعد مرتكبها شريكاً في الجريمة الإرهابية.
-3الترويج للقيام بالعمل الإرهابي عبر المواقع الإلكترونية
نصت عليها المادة (15) الخاصة بالترويج للإرهاب والتي نصت على أن: "يعاقب بالسجن مدة لا تقل عن خمس سنوات ولا تزيد عن عشر سنوات كل من قام بالدعاية أو الترويج أو التضليل للقيام بالعمل الإرهابي سواء بالقول أو بالكتابة أو بأي وسيلة من وسائل البث أو النشر أو بواسطة الرسائل أو المواقع الإلكترونية التي يمكن للغير الاطلاع عليها.
-4المساهمة بطريقة مباشرة أو غير مباشرة في صنع أو التدريب على صنع أو استعمال الوسائل الإلكترونية لاستعمالها في ارتكاب عمل إرهابي.
نصت عليها المادة 17 من قانون رقم 3 لسنة 2014 بشأن مكافحة الإرهاب بالقول: يعاقب بالسجن المؤبد كل من ساهم بطريقة مباشرة أو غير مباشرة في صنع أو تدريب على صنع أو استعمال الأسلحة التقليدية أو غير التقليدية والأدوات والمعدات والوسائل السلكية واللاسلكية والوسائل الإلكترونية كذلك أي مادة لها القدرة على

إزهاق الأرواح أو إحداث إصابات بدنية خطيرة أو أضرار مادية جسيمة بأي وسيلة بما في ذلك إطلاق أو نشر المنتجات الكيميائية السامة أو العوامل البيولوجية أو الإشعاعات والمواد المشعة، وذلك لاستعمالها في ارتكاب أي عمل إرهابي مع علمه بذلك .

فتعد جريمة إرهابية بموجب هذا النص المساهمة في صنع، أو التدريب على صنع أو على استعمال الوسائل الإلكترونية، على أن يكون ذلك بقصد جنائي خاص ينبغي توافره لقيام هذه الجريمة إلا وهو قصد استعمالها في ارتكاب عمل إرهابي .

وبذلك يكون المشرع الليبي قد لحظ إمكانية استخدام الإنترنت والوسائل الإلكترونية للقيام بعمل إرهابي باعتباره من الوسائل الإلكترونية.

**ثانياً: قانون مكافحة الجرائم الإلكترونية:**

صدر هذا القانون بتاريخ 2022/9/27، ولم يتضمن نصا خاصاً بجريمة الإرهاب الإلكتروني، إلا أنه جرم بعض أنماط السلوك التي تقع على النظم المعلوماتية أو الشبكة المعلوماتية أو المواقع الإلكترونية بوصفها جرائم إلكترونية، لا بوصفها جرائم إرهابية مثال ذلك الدخول العمدي غير المشروع لأنظمة الحاسب الآلي، أو نظام معلوماتي أو الدخول دون تصريح أو بما يخالف التصريح، وقرر لها عقوبة الحبس مدة لا تزيد عن مئة دينار، ولا تزيد على خمسمائة دينار، أو العقوبتين معاً، وشدد المشرع من العقوبة إذا كان قصد الدخول هو حذف أو إضافة أو تدمير أو نسخ بيانات أو تعطيل عمل نظام معلومات أو إتلاف موقع إلكتروني أو إتلاف محتوياته.

إما إذا نجم عن الدخول تعطيل عمل نظام معلوماتي، فتصبح الجريمة جناية وعقوبتها السجن، والغرامة التي لا تقل عن عشرة ألاف دينار.

هذه النصوص يؤخذ عليها أنها تتعلق بالدخول وإتلاف وتدمير للنظم المعلوماتية عامة، فلم تتطرق للاعتداء على النظم المعلوماتية، والمواقع الإلكترونية الحكومية، أو الخاصة بالجهات الاعتبارية العامة، لما تمثله من أهمية خاصة، لما ينجم عن الاعتداء علي من أضرار جسيمة تشل حركة المرافق العامة، وقدرتها على تقديم خدماتها .

**الفرع الثاني: موقف التشريعات المقارنة**

سنبحث موقف بعض التشريعات المقارنة للوقوف على تجربتها في مكافحة الإرهاب الإلكتروني.

**أولاً: مكافحة الإرهاب الإلكتروني في الولايات المتحدة الأمريكية**

تعد الولايات المتحدة الأمريكية من أولى الدول التي أصدرت قوانين لمكافحة الإرهاب الإلكتروني، ففي أكتوبر 2001 ، أصدرت اتفاقية لمكافحة الإرهاب المعلوماتي وسعت من خلالها سلطات البحث والتحقيق والمراقبة الإلكترونية، وتعمل الحكومة الاتحادية جاهدة على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث تحاول تقنين

استخدام محرك البحث Yahoo - MSN -Google في مجموعة من الشركات .

وهناك خطوات عديدة اتخذتها الولايات المتحدة لمكافحة جريمة الإرهاب الإلكتروني منها:

- إصدار قانون تعزيز أمن المعلومات 2002
- وضع الاستراتيجية الوطنية لتأمين الفضاء الإلكتروني 2003
- أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الإلكتروني.
- إنشاء لجنة حماية البنية التحتية الحساسة في الولايات المتحدة، التي أسست مركز حرب المعلومات الذي يتناول جوانب الإرهاب الإلكتروني.

- إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات، وغيرها من المبادرات (سلطان، 2010).

**ثانياً: مكافحة الإرهاب الإلكتروني في المملكة المتحدة:**

تعد المملكة المتحدة البريطانية هي أخرى من أولى الدول التي سارعت إلى محاربة الإرهاب الإلكتروني، حيث أصدرت قانون إساءة استخدام الحاسب الآلي في عام 1990.

ولقد تبنى القانون البريطاني رقم 2000 لمكافحة الإرهاب والمعروف Act terrorism الذي دخل حيز التنفيذ في فبراير 2001م- تعريفاً موسعاً للإرهاب ليشمل أفعال القرصنة المعلوماتية التي من شأنها إزعاج أو خلق اضطراب داخل النظام الإلكتروني، إذ لا يجرم هذا القانون فقط الأشكال والصور التقليدية للإرهاب بل يجرم كذلك الإرهاب السيبراني ضد نظم المعلومات والاتصالات.

فيشمل مصطلح الإرهاب الاستخدام أو التهديد المصمم للتدخل في نظام إلكتروني أو تعطيله بشكل خطير، بغرض التأثير في الحكومة أو لتخويف الجمهور أو قسم منه تحقيقاً لهدف سياسي أو ديني أو عقائدي(الراشدي) . نتيجة لذلك فإن هجوماً عبر الإنترنت يؤدي إلى أضرار بالغة بالنظم الإلكترونية لم يعد يعامل كجريمة من جرائم الكمبيوتر، ولكن كعمل إرهابي.

**ثالثاً: مواجهة الإرهاب الإلكتروني في فرنسا**

تعتبر التجربة الفرنسية من أهم التجارب في مكافحة الإرهاب، حيث سن المشرع الفرنسي القانون رقم 88/19 المؤرخ في 05 فيفري 1988م، والخاص بالجرائم المعلوماتية والحريات، وجرم مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريقة غير مشروعة المادة 462 /02، كما شدد العقوبة في الأحوال التي ينجم عنها هذا الولوج المحو أو تعديل في معطيات مخزنة آليا، واستعمال المستندات، و عاقب على هذه الجرائم بعقوبة السجن أو الغرامة، وخضع هذا القانون لتعديلات منها عام 1993 م، بحيث وسعت من نطاق السلوكيات محل التجريم إضافة إلى تعديل بعض العقوبات لتحقيق المزيد من الردع (عدوان).

**رابعاً: مكافحة الإرهاب الإلكتروني في مصر**

يوفر كل من القانون المصري رقم 175 لسنة 2018 بشأن جرائم تقنية المعلومات، والقانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب، إطاراً تشريعياً صالحاً لمكافحة هذه الجرائم الإرهابية التي تتم عبر أو بواسطة نظم الحاسوب وشبكة الإنترنت (الراشدي). ومن أبرز هذه النصوص التي يمكن الوقوف عليها:

**1- الدستور المصري**

نص الدستور المصري في المادة 31 منه -وفقًا للتعديلات الدستورية التي أُدخلت عليه في 23 أبريل 2019- على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون".

**2-القانون رقم 94 لسنة 2015 بشأن مكافحة الإرهاب**

**أ- جريمة الإرهاب الإلكتروني:** تصدى المُشَرّع المصري في هذا القانون صراحة لمشكلة الإرهاب الإلكتروني "السيبراني" مواكبة منه للتطورات الحديثة، وهو ما ظهر جلياً في المادة 29 من القانون سالف الذكر حيث. نصت على أنه: "يُعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج.

ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها"(قانون مكافحة الإرهاب المصري،2015، 29).

يتضمن هذا النص صورتان من صور التجريم وهما :

**الأولى:** إنشاء المواقع الإلكترونية أو استخدامها من أجل تحقيق واحد من ثلاثة أغراض هي الترويج للإرهاب، وبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن أي جريمة، وتبادل الرسائل وإصدار التكليفات بين الجماعة الإرهابية أو المنتمين إليها،أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين والجماعات الإرهابية في الداخل والخارج.

**والثانية:** الدخول بغير حق إلى موقع إلكتروني حكومي، ويجب لقيامها فيها توافر عنصرين وهما:

1 _الدخول بغير حق إلى موقع إلكتروني حكومي كالبريد الالكتروني، والاطلاع على ما فيه من معلومات أو بيانات أو تغييرها أو محوها أو إتلافها أو تزوير المحتوى الموجود بها.

2_ وأن يكون الدخول بقصد الحصول على المعلومات والبيانات الموجودة بالموقع من أجل ارتكاب الجريمة الإرهابية الواردة بالفقرة الأولى من المادة 29 أو الإعداد لها(سرور،2019).

ومما تجدر الإشارة إليه أن النص لا يشتمل على تجريم تدمير المواقع، والنظم الإلكترونية والمعلوماتية، وكذلك التجسس الإلكتروني.

ب- مكافحة تمويل الإرهاب

نصت المادة 3 من قانون مكافحة الإرهاب المصري غلى أنه يقصد بتمويل الإرهاب جمع أو تلقي، أو حيازة، أو أمداد، أو نقل، أو توفير أموال، ...أو غيرها، بشكل مباشر أو غير مباشر، وبأية وسيلة كانت بما في ذلك الشكل الرقمي، أو الإلكتروني؛ وذلك بقصد استخدامها كلها أو بعضها في ارتكاب جريمة إرهابية، أو العلم بأنها ستستخدم في ذلك؛؛ فالنص يحظر تمويل الإرهاب بأي شكل، مباشر أو غير مباشر، وبأي وسيلة بما في ذلك الوسائل الرقمية الإلكترونية.

ج- جريمة الإعداد أو التدريب على الإرهاب الإلكتروني:

نص المشرع المصري في المادة 15 من ذات القانون على جريمة التدريب على صنع أو استعمال الاسلحة، أو وسائل الاتصال، أو أية وسيلة تقنية أخرى بقصد ارتكاب جريمة إرهابية(الراشدي).

**3_قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 :**

لم يجرم المشرع المصري صراحة استخدام أدوات تكنولوجيا الاتصالات والمعلومات الحديثة، ووسائلها لأغراض إرهابية، ومع ذلك ضمن القانون رقم 175 لسنة 2018م، بشأن تقنية المعلومات أحكاماً تشدد من عقوبة الاعتداء على الأنظمة الإلكترونية والحاسوبية، وشبكات المعلومات الخاصة بالدولة، ومؤسساتها العامة متى جاء هذا الاعتداء بغرض تعريض أمن الدولة، أو سلامتها للخطر، أو لعرقلة المؤسسات العامة عن أداء مهامها .

1_ جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

جرم المشرع المصري في المادة 20 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 م، الدخول العمدي أو بطريق الخطأ والبقاء دون وجه حق، أو تجاوز الحق المخول للمستخدم من حيث الزمان أو مستوى الدخول، أو اختراق مواقعاً إلكترونياً، أو بريدًا إلكترونيًا، أو حسابًا خاصًا، أو نظامًا معلوماتيًا، يدار بمعرفة الدولة، أو لحسابها، أو أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها .

2 _جريمة الاعتداء على سلامة الشبكة المعلوماتية
جرم المشرع المصري في المادة 21 إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها، والتشويش على شبكة معلوماتية، أو أعاقتها، أو اعتراض عملها، أو إجراء معالجة إلكترونية للبيانات المخزنة عليها بدون وجه حق وغلظ المشرع من العقوبة على هذه الجريمة إذا وقعت على شبكة معلوماتية تخص الدولة، أو أحد الأشخاص الاعتبارية العامة، أو تمتلكها الدولة أو تدار بمعرفتها.

**الخاتمة:**

مع تطور الوسائل التكنولوجية وازدياد الاعتماد على الفضاء السيبراني في مختلف مناحي الحياة، ظهرت تهديدات جديدة أكثر خطورة وتعقيدًا، لعل أبرزها الإرهاب الإلكتروني، الذي لم يعد مجرد تهديد محتمل، بل واقع ملموس تمارسه جهات منظمة وأحيانًا دول ضد البنية التحتية الحيوية للدول والأفراد.
من خلال هذا البحث، تم التطرق إلى الإطار المفاهيمي للإرهاب الإلكتروني، وتحليل موقف التشريع الليبي من هذه الظاهرة، ومقارنته ببعض التجارب القانونية العربية والدولية. وتوصل البحث إلى أن الإطار القانوني الليبي، رغم احتوائه على بعض النصوص ذات الصلة، لا يزال يعاني من نقص في الشمول والدقة فيما يخص هذا النوع المعقّد من الجرائم، سواء من حيث التعريف، أو آليات التجريم، والإثبات.
كما أظهر البحث أن غياب تعريف محدد للإرهاب الإلكتروني، إلى جانب ضعف البنية القانونية والتقنية، يُشكّل عائقًا كبيرًا أمام مكافحته بفعالية، ما يبرز الحاجة الملحّة إلى تطوير المنظومة القانونية برمتها بما يتماشى مع المتغيرات الحديثة.

**التوصيات:**

- إصدار قانون خاص بمكافحة الإرهاب الإلكتروني يتضمن تعريفًا دقيقًا ومفصلًا للمصطلح، مع بيان صوره، وأشكاله، ووسائل ارتكابه، والعقوبات والتدابير الرادعة له.
- تعديل قانون الجرائم الإلكترونية الليبي ليشمل نصوصًا تُجرّم الأفعال الإرهابية التي ترتكب عبر الفضاء السيبراني بشكل صريح، وربطها بمفاهيم الأمن القومي.
- تعزيز التعاون الدولي والإقليمي من خلال الانضمام إلى الاتفاقيات الدولية المتعلقة بالجريمة السيبرانية، وتفعيل التعاون القضائي وتبادل المعلومات.
- إنشاء وحدات ضبطية متخصصة في مكافحة الإرهاب الإلكتروني.

**المراجع**

**أولاً: الكتب**


- البشري، محمد. (2004). الجرائم المعلوماتية. أكاديمية نايف العربية للعلوم الأمنية.
- الشهري، حسن. (د.ت.). الإرهاب الإلكتروني: حرب الشبكات.
- الصفوي، أحمد. (1950). المصباح المنير (الجزء 1). مطبعة مصطفى البابي الحلبي وأولاده.
- الطعاني، سليمان. (2020). الوجيز في التربية الإعلامية (ط. 1). دار الخليج للنشر والتوزيع.
- العوجي، مصطفى. (2017). دروس في العلم الجنائي (الجزء 1: الجريمة والمجرم). منشورات الحلبي الحقوقية.
- الرشيدي، هالة أحمد. (2021). الإرهاب السيبراني: ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية (ط. 1). دار النهضة العربية.
- سرور، أحمد. (2019). الوسيط في قانون العقوبات - القسم الخاص (الكتاب الأول: الجرائم المضرة بالمصلحة العامة). دار النهضة العربية.
- صدقي، عبد الرحيم. (1949). الإرهاب. دار شمس المعرفة للطباعة والنشر.
- عالية، سمير. (2020). الجرائم الإلكترونية (ط. 1). منشورات الحلبي الحقوقية.
- عبد الصادق، عادل. (2015). استخدام الإرهاب الإلكتروني في الصراع الدولي. دار الكتاب الحديث.

- يوسف، أمير. (2011). الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت (ط. 1). مكتبة الوفاء القانونية.

**ثانياً: الدوريات والأوراق البحثية والمؤتمرات**

- العجلان، عبد الله. (2008، 2-4 يونيو). الإرهاب الإلكتروني في عصر المعلومات ،المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، مصر.
- زهران، سحر. (2019). الجوانب القانونية للجرائم الإلكترونية. مجلة كلية السياسة والاقتصاد، (4)
- سلطان، محمد. (2010، 6-7 إبريل). الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب ،المؤتمر السادس لجمعية المكتبات والمعلومات السعودية: المفاهيم والتشريعات والتطبيقات، الرياض، المملكة العربية السعودية.

**ثالثاً: الرسائل العلمية**

- بنرغاي، أمل. (2011). السياسة الجنائية في مواجهة الإرهاب: دراسة مقارنة [رسالة دكتوراه غير منشورة]. كلية الحقوق، جامعة القاهرة.
- نجاري، فايزة. (2016). الآليات القانونية للإرهاب الإلكتروني [رسالة ماجستير غير منشور]. كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.

**رابعاً: المعاجم والموسوعات**

- قاموس الفنون والآداب. (1944). (المجلد 4، ص 467، كلمة.(TERREUR

**خامساً: القوانين والتشريعات والاتفاقيات**

- الأمانة العامة لجامعة الدول العربية. (1998). الاتفاقية العربية لمكافحة الإرهاب.
- قانون الجريمة الإلكترونية رقم 5 لسنة 2022م. (2022). الجريدة الرسمية، السنة الأولى، العدد (1)
- قانون مكافحة الإرهاب رقم 3 لسنة 2014م. (2014). الجريدة الرسمية، السنة الرابعة، العدد (1)

**سادساً: المواقع الإلكترونية والمصادر الرقمية**

- العدوان، رائد. (2013، 23-27 فبراير). المعالجة الدولية لقضايا الإرهاب والإرهاب الإلكتروني ،شبكة السكينة لتقويم الفكر http://www.assakina.com/book/73801.html .
- البهي، رغد. (2019، 30 سبتمبر). الإرهاب السيبراني: المفهوم والسمات والأنماط. المركز المصري للفكر والدراسات الاستراتيجية. استُرجع في 23 أبريل 2026، من https://ecss.com.eg/7141/
- المكتبة الرقمية العالمية. (د.ت.). عناصر المكتبة الرقمية العالمية. استُرجع من https://www.wdl.org/ar/item/11579/
- منظمة شبكة القانون. (2010، 21 ديسمبر). الاتفاقية العربية لمكافحة جرائم تقنية المعلومات. استُرجع في 25 أبريل 2026 https://lawsociety.ly/convention/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%AA%D9%82%D9%86%D9%8A/#

**المراجع باللغة الأجنبية:**

1. Larousse, P. (1910). *Petit Larousse illustré*. Larousse.p974.
2. Lee H. Hamilton, The 9/11 *commission Report, Final Report of The National Commission onTerrorist Attacks upon The United States, Authorized edition, Norton and Company Ltd*, New York, 2005.
3. Robert, P., Rey, A., & Rey-Debove, J. (1993). Le petit robert. -/,p2239.
4. Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Syngress.P24.
5. Stair, R., & Reynolds, G. (2008). *Fundamentals of information systems*. Course Technology Press.
6. *Stevenson, A. (Ed.). (2010). Oxford dictionary of English. Oxford University Press.*

**7.** Pitter BELLEY, Hached attacked*(2002),abused digital crime exposed*, London. Regan Page. p107**.**

**Websites:**

- https://www.unodc.org/unodc/ar/cybercrime/convention/text/convention-full-text.html
- https://www.coe.int/en/web/cybercrime/the-budapest-convention-old?utm_source=chatgpt.com
- https://eur-lex.europa.eu/legal_content/EN/TXT/?uri=LEGISSUM%3A4656911&utm_source=chatgpt.com
- http://www.larousse.fr/dictionnaires/francais/cyberterrorisme

## References

First: Books

- Al-Bashari, Muhammad. (2004). *Information Crimes*. Naif Arab Academy for Security Sciences.
- Al-Shehri, Hassan. (n.d.). *Cyber-Terrorism: Network Warfare*.
- Al-Safawi, Ahmed. (1950). *Al-Misbah Al-Munir* (Part 1). Mustafa Al-Babi Al-Halabi & Sons Press.
- Al-Ta'ani, Sulaiman. (2020). *A Concise Guide to Media Literacy* (1st ed.). Dar Al-Khaleej for Publishing and Distribution.
- Al-Awji, Mustafa. (2017). *Lessons in Criminal Science* (Part 1: Crime and the Criminal). Al-Halabi Legal Publications.
- Al-Rashidi, Hala Ahmed. (2021). *Cyber-Terrorism: Its Nature and Counter-Efforts in Light of National and International Legislation and Law*s (1st ed.). Dar Al-Nahda Al-Arabiya.
- Surour, Ahmed. (2019). *The Intermediate Treatise on Penal Law – Special Section* (Book One: Crimes Harmful to the Public Interest). Dar Al-Nahda Al-Arabiya.
- Sidqi, Abdul Rahim. (1949). *Terrorism*. Dar Shams Al-Ma'rifa for Printing and Publishing.
- Aliya, Samir. (2020). *Cybercrimes* (1st ed.). Al-Halabi Legal Publications.
- Abdul Sadiq, Adel. (2015). *The Use of Cyber-Terrorism in International Conflict*. Dar Al-Kitab Al-Hadith.
- Moussa, A. M. (2026). The Legal Future of Artificial Intelligence Technology: A Study of the Impact of AI Technology on Civil Law. *Al-haq Journal for Sharia and Legal Sciences*, *13*(1), 403-413.
- Ishabaani, M. A. S. M. (2025). Drones Between International Law and the Requirements of National Sovereignty: A Comparative Analytical Study. *Al-haq Journal for Sharia and Legal Sciences*, *12*(2), 162-186.
- Youssef, Amir. (2011). *Cyber and Information Crime and International and Local Efforts to Combat Computer and Internet Crimes* (1st ed.). Al-Wafaa Legal Library. Second: Periodicals, Research Papers, and Conferences
- Jawan, A. F. A. (2026). The legal framework for enforcing arbitration awards issued via electronic media. *Al-haq Journal for Sharia and Legal Sciences*, *13*(1), 497-513.
- Al-Ajlan, Abdullah. (2008, June 2–4). Cyber-terrorism in the Information Age, First International Conference on Information Security and Privacy Protection in Internet Law, Cairo, Egypt.
- Zahran, Sahar. (2019). Legal Aspects of Cybercrimes. Journal of the Faculty of Politics and Economics, (4).
- Elnaas, A. A. (2026). Constitutional and legal protection of personal data: A comparative study between the European General Data Protection Regulation (GDPR) and some comparative legislation. *Al-haq Journal for Sharia and Legal Sciences*, *13*(1), 594-607.
- Sultan, Mohamed. (2010, April 6–7). International and legal protection of the electronic environment against crime and terrorism. The 6th Conference of the Saudi Library and Information Association: Concepts, Legislation, and Applications, Riyadh, Kingdom of Saudi Arabia. Third: Academic Theses
- Banarghai, Amal. (2011). Criminal policy in confronting terrorism: A comparative study [Unpublished doctoral dissertation]. Faculty of Law, Cairo University.

- Najari, Faiza. (2016). Legal mechanisms regarding cyber-terrorism [Unpublished master's thesis]. Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou. Fourth: Dictionaries and Encyclopedias
- Dictionary of Arts and Letters. (1944). (Vol. 4, p. 467, entry: TERREUR). Fifth: Laws, Legislation, and Conventions
- General Secretariat of the League of Arab States. (1998). Arab Convention on the Suppression of Terrorism.
- Cybercrime Law No. 5 of 2022. (2022). Official Gazette, Year 1, Issue (1).
- Counter-Terrorism Law No. 3 of 2014. (2014). Official Gazette, Year 4, Issue (1). Sixth: Websites and Digital Sources
- Al-Adwan, Raed. (2013, February 23–27). International handling of terrorism and cyber-terrorism issues. Al-Sakina Network for Thought Evaluation. http://www.assakina.com/book/73801.html
- Al-Bahi, Raghad. (2019, 30 - (September). Cyber-terrorism: Concept, Characteristics, and Patterns. Egyptian Center for Strategic Studies (ECSS). Retrieved April 23, 2026, from https://ecss.com.eg/7141/
- World Digital Library. (n.d.). Elements of the World Digital Library. Retrieved from https://www.wdl.org/ar/item/11579/
- Law Society Organization. (2010, December 21). Arab Convention on Combating Information Technology Offences. Retrieved April 25, 2026, from https://lawsociety.ly/convention/%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9-%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%AA%D9%82%D9%86%D9%8A/#

  References in foreign languages:

  1. Larousse, P. (1910). Petit Larousse illustré. Larousse. p. 974.
  2. Lee H. Hamilton, The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States, Authorized edition, Norton and Company Ltd, New York, 2005.
  3. Robert, P., Rey, A., & Rey-Debove, J. (1993). Le Petit Robert. ,p2239.
  4. Shakarian, P., Shakarian, J., & Ruef, A. (2013). Introduction to cyber-warfare: A multidisciplinary approach. Syngress.P24.
  5. Stair, R., & Reynolds, G. (2008). Fundamentals of information systems. Course Technology Press.
  6. Stevenson, A. (Ed.). (2010). Oxford dictionary of English. Oxford University Press.
  7. Pitter BELLEY, Hached attacked (2002), abused digital crime exposed, London. Reagan Page. p107. Websites:

  - https://www.unodc.org/unodc/ar/cybercrime/convention/text/convention-full-text.html
  - https://www.coe.int/en/web/cybercrime/the-budapest-convention-old?utm_source=chatgpt.com
  - https://eur-lex.europa.eu/legal content/EN/TXT/?uri=LEGISSUM%3A4656911&utm_source=chatgpt.com
  - http://www.larousse.fr/dictionnaires/francais/cyberterrorisme