تاريخ الاستلام: 2023/01/31 تاريخ القبول: 2024/01/24..

الإرهاب الإلكتروني بين التجريم و آليات مكافحته

Cyberterrorism between criminality and mechanisms to combat it

د. برني كريمة *
جامعة الاخوة منتوري قسنطينة 1(الجزائر)
Karima.berni@umc.edu.dz

د.يولمكاحل أحمد
جامعة الاخوة منتوري قسنطينة1(الجزائر)
ahmed.boulemkahel@umc.edu.dz

ملخص:

تهدف دراسة هذا الموضوع معرفة الإرهاب الرقمي الذي يستمد أهميته من الوضعية الراهنة التي تعيشها جلّ المجتمعات من التحديات الكبيرة في مواجهة ومكافحة جريمة الإرهاب المرتكبة عبر الوسائط الرقمية، نتيجة للتطورات التي شهدها العالم من تكنولوجيا الاتصال و المعلومات ودخول المجتمع عصر الرقمنة، وعولمة الجريمة من حيث أساليبها وتنظيمها، حيث أصبحت جريمة تتميز بسمات خاصة و منظمة تنظيما محكما بواسطة تقنيات جدٌ متطورة، ميزت بينها وبين أنماط الجريمة التقليدية. في ذات الوقت استغلت الجماعات الإرهابية هذا التطور العلمي في احداث الكثير من التطورات الهامة في مجال ارتكاب الجرائم، مع الحرص على طمس معالم الجريمة، وذلك باستخدام التقنيات العالية المتطورة. مما صعب الكشف عنها و الذي أدى إلى ظهور نمط جديد من الإرهاب - الإرهاب الإلكتروني - الذي أخذ أحدث صورة له، باستعمال أسلحة رقمية متطورة.

كلمات مفتاحية: جرائم الانترنت ، الإرهاب الإلكتروني ،. التجريم ، الآليات القانونية ، المكافحة.

Abstract:

As a result of the developments that the world witnessed from the information and communication technology and society's entering the era of digitization, and the globalization of crime in terms of its methods and organization, it has become a crime characterized by special features and a well-organized organization by means of very advanced technologies, which distinguished them from traditional crime patterns. At the same time, terrorist groups have taken advantage of this scientific development to make many important developments in the field of committing crimes, while making sure to obscure the features of crime, by using advanced high technologies. Which made it difficult to detect, which led to the emergence of a new type of terrorism, which is electronic terrorism, which took its latest picture, using advanced digital weapons, unlike conventional terrorism.

.

key words: Cyber-crime, Electronic terrorism ,Criminalization, legal mechanism ,control

*المؤلف المرسل.

. مقدمة:

اعتبر العصر الحالي - عصر الثورة المعلوماتية - الذي ترتب عنها ثورة كبيرة للتقنية و بروز مصطلح الإرهاب الإلكتروني، وهناك من يسميه بالإرهاب الرقمي أو الإرهاب المعلوماتي الذي يشكل جريمة ضد الإنسانية تجاوز مداها ليأخذ صفة العالمية، وأصبح خطرا يهدد ويخيف العالم بأسره.

فالإرهاب الرقمي يستمد أهميته من الوضعية الراهنة التي تعيشها جل المجتمعات من تحديات كبيرة في مواجهة ومكافحة جريمة الإرهاب المرتكبة عبر الوسائط الرقمية، نظرا للأساليب التقنية التي تستخدمها من ناحية، وتنوع أشكالها وتعددها من ناحية أخرى، وخاصة ذلك الإرهاب المصحوب بالعنف الإيديولوجي ومتعدِّد الجنسيات، لا تجمعه قضية وطنية بل عقائد دينية وإيديولوجيات سياسية معتمدا على تنفيذ برنامجا إرهابيا مستعملا في ذلك أسلحة متطورة رقمية[1] عابرة للحدود مستغلا في ذلك مختلف شرائح المجتمع للانخراط في صفوف هذه الجماعات الإرهابية وراء مختلف الدعوات المتطرفة. وهو الأمر الذي أدى إلى توجه أكثر من ثلاثين دولة إلى توقيع اتفاقية دولية أولى لمكافحة الإجرام عبر الإنترنت في بودابست سنة 2001، الذي يعد من أخطر الجرائم التي يرتكبها الإرهاب عبر شبكة الأنترنت[2] ، من خلال جسامة الخسائر التي يمكن أن تسببها عملية ناجحة واحدة تندرج تحت مفهومه.

إذ يعتمد الإرهاب الإلكتروني على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الغير، وإلحاق الضرر بهم، أو تهديدهم ونتيجة لذلك، فقد تغيرت النظرة إلى الإرهاب الإلكتروني التي كانت منحصرة في الأعمال التخريبية وأصبحت تشمل أنشطة أكثر خطورة، إذ أصبحت شبكة الأنترنت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف[3] وثقافة التطرف والتزمت والاتصال ببعضهم البعض والمتعاطفين معهم.

لم تكن الجزائر بمنأى عن هذه المتغيرات والظروف، فقد عاشت ويلات الإرهاب في فترة التسعينات " العشرية السوداء "، إذ واجه المشرع الجزائري ظاهرة الإرهاب بترسانة من النصوص التشريعية ابتداء من المرسوم التشريعي رقم 03/92 ، المتعلق " بمكافحة الإرهاب والتخريب [4]" المعدِّل والمتمم بالمرسوم التشريعي 05/93 ، ثم الأمر11/95 ، المعدّل والمتمم للأمر رقم 195/66 المتضمن قانون العقوبات ولم يكتفي بسياسة ردع الجريمة، بل اعتمد على سياسة المصالحة وبعدها ظهر وجه مستحدث للإرهاب ذو طابع الكتروني، أفرد له المشرع الجزائري نصوص عقابية و إجرائية[5] متعلقة بأنظمة المعالجة الآلية للمعطيات بموجب القانون 15/04، ثم استحدث نصوص تشريعية أخرى تتعلق بالوقاية من جرائم الأنترنت منها : القانون رقم 04/09[6]، والقانون رقم 04/16، المتعلق بجريمة التجنيد الإرهابي في إطار تجسيد السياسة الجنائية للحدّ من الظاهرة الإرهابية المستحدثة ، وآخره المرسوم الرئاسي الذي صدر مؤخرا رقم 21-439 الموافق 7 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته.[7]

تتجلى أهمية هذه الدراسة، في إلقاء الضوء على الدور الذي يجب أن تضطلع به الدول والأفراد للتصدي لهذه الجريمة والوقاية منها. كما تستمد هذه الدراسة أهميتها انطلاقا من أن ظاهرة الجرائم المستحدثة ومنها الإرهاب الإلكتروني، قد غدت تشكل تحدّيا حقيقيا للسياسات الجنائية السائدة و أجهزتها التشريعية والتنفيذية والقضائية .

وقد استفدنا كثيرا مما توصلت إليه الدراسات السابقة، ذلك من خلال اطلاعنا على بعض المؤلفات ، والتي كان في مجملها قليلة بالمقارنة بالرصيد العلمي القانوني في هذا المجال، و هذا راجع لحداثة موضوع الإرهاب المعلوماتي من ناحية - الإطار التشريعي والتنظيمي - الخاص به، فقد تمّ جمع أكبر عدد ممكن من المراجع عبر شبكة الأنترنت، لإعداد هذه الدراسة النظرية للموضوع.

وبناء على ما سبق، فإن الإشكالية التي يتمحور حولها موضوع المقال هي : **ما مدى نجاعة السياسة التشريعية الجنائية للتصدي للجرائم الإرهابية الإلكترونية ؟ و ما هي سبل وآليات المكافحة و الوقاية من جرائم الإرهاب المعلوماتي وفق التشريع الجزائري؟**

وللإجابة على الإشكالية المطروحة أعلاه، اعتمدنا على المنهج الوصفي كونه يقتضي إبراز المعلومات وتوضيح المفاهيم من خلال الوقوف على التحديد الدقيق للمصطلحات ، ثم المنهج التحليلي على اعتبار أهميته في تحليل النصوص القانونية التي يرتكز عليها موضوع الدراسة.

وعليه حاولنا تسليط الضوء على الشكل المستحدث للإرهاب وجرائمه مع إبراز أهم العوامل والاستراتيجيات المتبعة من أجل التصدي لظاهرة الإرهاب المعلوماتي. لذا قسمنا المقال إلى مبحثين اثنين، حيث خصصنا المبحث الأول للإطار المفاهيمي للإرهاب الإلكتروني وإبراز مختلف الصور أو الآليات التي تنفذ بها التنظيمات الإرهابية جرائمها الإلكترونية من خلالها. في حين خصصنا المبحث الثاني لمعالجة أهم الآليات القانونية الدولية والوطنية وسبل الحدّ والمكافحة من ظاهرة الإرهاب الإلكتروني ثم خاتمة تضمنت جملة من النتائج والمقترحات.

1- الاطار المفاهيمي للإرهاب الالكتروني

اعتبر العصر الحالي عصر الفضاء الإلكتروني بامتياز، فقد أصبح هذا الفضاء العمود الفقري لمعظم التفاعلات اليومية، واتجاه معظم الدول والحكومات لتبني الحكومات الذكية. وقد تعدى الأمر إلى بناء مدن ذكية، ومع سهولة الاستخدام ورخص التكلفة، ومع تزايد الاعتماد عليه في مجالات الحياة كافة، سواء كانت سياسية أو اقتصادية أو عسكرية أو قانونية أو غيرها من المجالات المختلفة، ومع تحول مواقع التواصل الاجتماعي لتكون فاعلا غير تقليديا في العلاقات الدولية أصبح الأنترنت سلاحاً ذو حدين[8] ، فكما كان وسيلة لتحقيق الرخاء والتقدم البشري، هناك جانب آخر مظلم يتمثل في تزايد التهديدات والمخاطر الناجمة عن الاعتماد المتزايد عليه في ظل عالم مفتوح تحكمه تفاعلات غير مرئية ، وغياب سلطة قانونية عليا تسيطر عليه ، ليظهر لنا بذلك نوع جديد من الإرهاب عُرف بالإرهاب المرتكب عبر الوسائط الرقمية إنه الإرهاب الإلكتروني[9].

إذ تكمن خطورة هذا النمط الإجرامي على الأمن والسلم العالميين بوجه عام لاسيما مع صعوبة كشف مرتكبيه وتصور حالة التلبس فيه، وتنوع وسائله، وصعوبة حصر وتحديد حجم الدّمار الذي يخلفه في نظم المعلومات .

و من خلال هذا المبحث سنتناول دراسة مفهوم الإرهاب الالكتروني أولا ثم نعرج ثانيا لدراسة صوره و آلياته.

1.1 - مفهوم الإرهاب الإلكتروني

ليس هناك تعريف محدد متفق عليه للإرهاب الالكتروني فحداثة الجريمة وعدم ارتباطها بمكان أو معنى معين يمكن التوافق عليه، أدى إلى وجود تعريفات متعددة وبما أن الإرهاب الالكتروني ما هو إلا نسخة الكترونية للإرهاب التقليدي المادي وأن أول ما يتبادر إلى ذهن المرء عند سماعه لمصطلح الإرهاب المرتكب عبر الوسائط الإلكترونية، أنه جريمة من الجرائم الشاذة غير المألوفة، التي نمت وترعرعت بشكل كبير في الربع الأخير من هذا القرن[10] ، حيث تستهدف المساس بشكل مباشر بكيان وجوهر وجود الدولة، وكذا أمن وطمأنينة الأفراد داخلها.

والجدير بالملاحظة، أنه بالرغم من غياب وجود تعريف متفق عليه للإرهاب على الصعيد الدولي، فقد كانت هناك محاولات عديدة من الجهود الإقليمية والدولية لتعريفه ،كما تضافرت الجهود العربية المبذولة في مجال مكافحة الإرهاب الدولي من خلال إقرار الاتفاقيات العربية[11] لمكافحة الإرهاب التي عقدت في اطار جامعة الدول العربية ،سنحاول إبراز تعريف الإرهاب الالكتروني على ضوء الاتفاقيات الدولية والإقليمية ضمن الفرع الأول، ثم نعرج لدراسة تعريف الإرهاب الإلكتروني على ضوء الجهود العربية في الفرع الثاني.

1.1.1_ تعريف الإرهاب الالكتروني على ضوء الاتفاقيات الدولية و الإقليمية

تعد الاتفاقية الدولية الموقعة في بودابست سنة 2001 هي الأولى من نوعها لمكافحة الاجرام عبر الانترنت حيث عرفت الإرهاب الإلكتروني على أنه " هجمات غير مشروعة أو تهديدات بهجمات ضد الحواسيب أو الشبكات أو المعلومات المخزنة إلكترونيا ، توجه

من أجل الانتقام أو الابتزاز أو الإجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبالتالي لكي ينعت شخص ما بأنه إرهابي على الانترنت وليس مخترقا فلابد أن تؤدي الهجمات التي يشنها على عنف ضد الأشخاص أو الممتلكات أو على الأقل تحدث أذى كافيا من اجل نشر الخوف والرعب[12].

و عرفته الأمم المتحدة سنة 2012 " أن الإرهاب الإلكتروني هو استخدام الأنترنت لنشر أعمال إرهابية .

كما عرف هذا النوع من الإرهاب، بأنه استخدام للحاسوب والوسائل العلمية والتكنولوجية من أجل تنفيذ أعمال إرهابية ليس من السهل تنفيذها على أرض الواقع، ويتم تنفيذها من قبل شخص واحد بشرط أن تتوفر لديه القدرة والكفاءة والخبرة اللازمة في استخدام التقنية المعلوماتية.[13]

ويعرف الفقيه باري كولينلر الإرهاب المعلوماتي بأنه: " سوء استخدام قصدي لنظام المعلومات الرقمية والشبكات أو مكوناتها لتحقيق هدف يدعم أو يسهل حملة إرهابية أو فعل إرهاب."

ويعرف الإرهاب الالكتروني عند دينينج" Dorothy denningg على أنه استخدام عير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر من أجل تحقيق أهداف سياسية واجتماعية، ولكي يعتبر ذلك إرهاب لابد أن يؤدي ترويع واكراه الحكومات والأشخاص والممتلكات أو على أقل التسبب في الضرر والخوف وكذلك إحداث ضحايا وإيذاء بدني وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية.[14]

.وهناك من يعرفها على أساس نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الالكتروني، وبتالي فإن الجريمة الالكترونية هي عبارة عن أفعال غير مشروعة، يكون الحاسب الآلي (الكمبيوتر) محلا لها أو وسيلة لارتكابها[15].

وطبقا لتعريف وكالة المخابرات المركزية الأمريكية فإن الارهاب الالكتروني هو:" أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر وبرامجه، والبيانات والمعلومات والتي تنتج من عنف ضد الاهداف المدنية عن طريق جماعات دون قومية او عملاء سريين". أما مركز حماية البنية التحتية القومية الأمريكية فقد عرف الارهاب الإلكتروني على أن "عمل اجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر وبرامجه، والاتصالات السلكية واللاسلكية ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف، بهدف إرباك وزرع الشك لدى السكان، وذلك بهدف التأثير على الحكومة او السكان لخدمة أجندة سياسية او اجتماعية أو إيديولوجية." [16]

2.1.1 - تعريف الإرهاب الإلكتروني على ضوء الجهود العربية

على الرغم من أن جلّ الدول لم تتضمن في ظل قوانينها الداخلية تعريف مباشرة للإرهاب الإلكتروني إلا أنه بالمقابل أقرت ببعض أشكاله والتي من خلالها يمكن الوصول إلى بعض المفاهيم التي تبنتها بعض الدول منها :

دولة الامارات العربية التي اعتبرت أول دولة عربية أصدرت قانونا مستقلا لمكافحة المعلوماتية، محددة بذلك مفهومه على أنه " العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو عرضه أو عقله أو كاله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى أنواع العدوان.

في حين عرفته المملكة العربية السعودية " أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية أو استخدام التقنيات الرقمية المخالفة لأحكام النظام ومن أنواعه السب والتشهير والابتزاز والإباحة وكذاك الشائعات وما يتعلق بالأمور المالية كالاعتداء على البطاقات البنكية بأشكالها واختلاسها.[17]

من خلال التعاريف السابقة، يجعلنا نقوم بوضع العلاقة بين الجريمة المنظمة والإرهاب فكلاهما يقوم على العنف المنظم، تقوده جماعات دولية ذات قدرات تنظيمية قائمة على التخطيط والتنفيذ، لكن العلاقة تطورت في الآونة الأخيرة، إذ أصبح هناك تعاون بينهم، حيث

عملت الجماعات الإرهابية مع مؤسسات الجريمة المنظمة في شتى الميادين ، كبيع الأسلحة، تهريب وتبيض الأموال وغيرها من الاعمال الاجرامية، بإدخال الوسائل التقنية الحديثة في أعمالهم لتحقيق أغراض غير مشروعة.

2.1- صور الإرهاب الالكتروني

تعمل الجماعات الإرهابية على استخدام تكنولوجيا متطورة لنشر مبادئهم وتصوراتهم، والقيام بعدة أعمال تخريبية عن طريق شبكات الأنترنت للوصول إلى أهدافها المرجوة. و تبرز صور وأشكال عدة للإرهاب الإلكتروني, وإن كان الغرض واحدا. ومن بين صور الإرهاب الإلكتروني نذكر منها:

1.2.1- تدمير واختراق المواقع الإلكترونية والنظم المعلوماتية :

يقصد بالاختراق، الهجوم على شبكة الأنترنت و اختراق المواقع الرسمية والشخصية للأفراد كاختراق البريد الإلكتروني أو الاستيلاء عليه أو إغراقه بالرسائل وقرصنة اشتراكات الآخرين ، من خلال الاستيلاء على أرقامهم السرية.

أ- التجسس الإلكتروني :

في عصر الانفجار الرقمي أصبحت الحدود الجغرافية مستباحة بأقمار التجسس والبث الفضائي الأمر الذي أصبح يهدد سيادة الدول، من خلال عمليات التجسس التي تقوم بها أجهزة الاستخبارات للحصول على الأسرار والمعلومات و إفشائها لدولة معادية لها، أو استغلالها ضد المصلحة الوطنية لتلك الدولة الحساسة للدولة المستهدفة[18]، و قد تم رصد بعض حالات التجسس الدولي من طرف وكالة الأمن القومي، والكشف عن شبكة دولية ضخمة للتجسس بإدارة كندا NSA الأمريكي وبريطانيا وأستراليا ونيوزيلندا لرصد المكالمات الهاتفية والرسائل بمختلف أنواعها.

ب -إنشاء المواقع الإرهابية الرقمية :

أصبحت الجماعات الإرهابية تعتمد على التقنية الإلكترونية لتعليم صناعة المتفجرات وتقديم النصائح والإرشادات لأعضائها حول كيفية اختراق وتدمير المواقع المحجوبة[19]، ونشر الفيروسات ونشر الفكر الضال ولم يقف الأمر عند هذا الحد، بل تجاوز ذلك بإنشاء قسم خاص بالمعلومات وشركات إعلامية نشطة منها " شركة السحاب " الإعلامية ، فأصبحت الجماعات الإرهابية تدير عدة شركات إعلامية عالمية.

ج- تبادل المعلومات الإرهابية :

تتواصل الجماعات الإرهابية مع أعضائها عن طريق شبكة الأنترنت للمراقبة الأمنية من أجل التنسيق لتنفيذ الأعمال الإرهابية، دون الخضوع ودون التقيد بالحدود الجغرافية، ومن أبرز الاستخدامات الإرهابية لشبكة الأنترنت نذكر ما يلي:

2 - الاتصال و التخفي :

عن طريق وضع رسائل مشفرة تمكنه من التواصل دون كشف هويته أو ترك أي أثر جمع المعلومات الإرهابية، تعتمد الجماعات الإرهابية على شبكة الأنترنت من أجل الحصول على المعلومات الاستراتيجية والحساسة للدول، كمواقع المنشآت النووية، مصادر توليد الطاقة، مواعيد الرحلات بالجوية والاطلاع على الإجراءات المقررة لمكافحة الإرهاب لتجنبها[20].

أ-التخطيط والتنسيق للعمليات الإرهابية:

بحيث تضمن لهم الأنترنت السرية وسرعة التنسيق لتنفيذ الهجمات الإرهابية، الحصول على التمويل من خلال استغلال حقل الاستثمار الرقمي والمشاريع الرقمية لجمع الأموال ، وكذا جمعيات العمل التطوعي والخيري لتمويل النشاط الإرهابي.

ب- التدريب الالكتروني للإرهاب:

عن طريق إنتاج ونشر أدلة إرشادية إلكترونية، تتضمن وسائل التدريب والتخطيط والتنفيذ على شبكة الإنترنت لتصبح في متناول الإرهابيين على المستوى العالمي، إلى جانب إنشاء صفحات إلكترونية وهي عبارة عن كل صفحة تشتمل على معلومات مخزنة بشكل صفحات، و معلومات مبينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص. و لأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (HTML) ويقوم بحل رموز و إصدار التعليمات لإظهار الصفحات، سواء بغرض التصريح بتبيينها عمليات فدائية معينة أو لبث تهديدات بتنفيذ هجمات إرهابية أو تصريحات ترتبط بالمشروع الإرهابي.

ج - التهديد و الترويع الإلكتروني :

تستغل الجماعات الإرهابية شبكة الأنترنت العالمية، من أجل بث الرعب والخوف في نفوس الأفراد والدول، من خلال التهديد باغتيال شخصيات سياسية مهمة في الدولة، أو التهديد بتفجير منشآت معينة في الدولة، أو التهديد بتدمير البنية التحتية المعلوماتية عن طريق نشر فيروسات[21] لتدمير الشبكات المعلوماتية والأنظمة الإلكترونية.

2- الآليات والاستراتيجيات الدولية والوطنية في مكافحة الإرهاب الإلكتروني

ساهم التطور العلمي و التكنولوجي في تطور الجريمة بصور مختلفة و مستحدثة و دفعها إلى أرقى مستوياتها و بأحدث الأساليب، فأصبحنا نواجه إجراما غير تقليدي متمثلا في جريمة الإرهاب الإلكتروني، ولقد تباينت الصور الإجرامية لهذه الظاهرة وتشعبت أنواعها، فلم تعد تهدد العديد من المصالح التقليدية التي تحميها القوانين و التشريعات، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات و تكنولوجيا المعلومات، ولقد أصبح تجريم السلوك الإجرامي و ملاحقة الجناة[22] في الجرائم المعلوماتية ، شيئا صعبا لاسيما في ظل التشريعات الجزائية التي تبدو عاجزة عن الحدّ من هذا النوع من الإجرام، سواء من حيث المواكبة في تجريم الأفعال المستحدثة و المرتبطة بالتطور الهائل التكنولوجي، أو من حيث أن أنظمة الملاحقة الإجرائية و طرقها التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة[23] على صعيد الملاحقة الجزائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجزائية الدولي، مما أوجب تطوير البنية التشريعية الجزائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية[24]، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية .

وبناء على ما تقدم، سنتناول بالدراسة الاستراتيجيات والآليات الدولية و الإقليمية في مكافحة الإرهاب الالكتروني في المطلب الأول، ثم نعرج لدراسة الآليات القانونية الوطنية في المطلب الثاني.

2 .1 _ الآليات والاستراتيجيات الدولية و الإقليمية في مكافحة الإرهاب الالكتروني

عمل المجتمع الدولي على اتخاذ عدة استراتيجيات لمكافحة الإرهاب الالكتروني وتحقيق الأمن والاستقرار، ذلك بتظافر الجهود الدولية عبر الاتفاقيات الدولية و الآليات الدولية في مكافحة هذه الظاهرة الإجرامية المستحدثة التي لم تعد تتمركز في دولة معينة بل تتخطى الحدود مستغلة التطور التكنولوجي وبالتالي تعزيز التعاون بينها و أتخاذ تدابير فعالة للتصدي لها ومعاقبة مرتكبيها، فضلا على الجهود العربية من خلال بعض القوانين و المؤتمرات العربية والتعاون فيما بينها في مجال مكافحة هذا النوع من الاجرام المستحدث، من خلال تبادل المعلومات والخبرات المتعلقة بالتنظيمات الإرهابية، وإيجاد أرضية مشتركة لصياغة منظومة قوانين وتشريعات دولية وعربية ووسائل فعالة تتصدى لجذور و امتدادات الظاهرة الإرهابية في الفضاء الرقمي[25]، وقد حذر الخبراء في هذا المجال من خطر أكيد يكمن في تحول الإرهاب من الدعاية والتجنيد إلى شن هجمات إلكترونية على البنية التحتية والأنظمة وسرقة معلومات حساسة كالخطط والخرائط والاستراتيجيات العسكرية.

كما اعتبرت الاتفاقيات الدولية لمكافحة هذا النوع من الإرهاب أهم وسيلة في هذا المجال حيث عملت الأمم المتحدة باعتبارها مركز لتنسيق الجهود بين الدول على ذلك ويظهر ذلك من خلال :

-ا نعقاد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل 1984 حيث تم التوقيع على جملة من الأسس الواجب احترامها لمكافحة الجرائم المتعلقة بالكمبيوتر.

- تم وضع إطار دوليا لمكافحة جرائم الكمبيوتر لقرار هافانا 1991 الناتج عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء.

- اتفاقية بودابست 2001 لمكافحة الجرائم المعلوماتية.

وعلاوة على التعاون الدولي لمكافحة الجريمة الإرهابية عبر الشبكة الإلكترونية، يعتمد التعاون القضائي الدولي كذلك على دعم جهود الشرطة الدولية[26] (الانتربول) في ملاحقة والقبض وتسليم المجرمين والمساعدة القضائية في المواد الجنائية، وقد برزت اتفاقية فيينا سنة 1998 التي دعت لضرورة تعزيز التعاون القضائي المعلوماتي والإداري في الشق الجنائي لحماية البيئة المعلوماتية .

أمام هذا الواقع ونظراً لطبيعة الأنترنت العابرة للحدود، يعتبر التعاون الدولي الفاعل، أحد أهم العناصر، كونه الشرط الأساسي في نجاح الملاحقات و المحاكمات، و قد أصدر مكتب الأمم المتحدة المعني بالمخدرات والجريمة تقريراً عام 2012[27]، أكد على ضرورة التعاون الدولي والإقليمي والوطني لمواجهة استخدام الأنترنت لأغراض إرهابية وقد تم التنبه في هذا المجال، إلى أن غياب الإطار التشريعي الدولي المناسب الذي يحكم موجبات الدول في مجال التعاون لمكافحة الإرهاب الإلكتروني يؤثر سلباً على هذه المواجهة، لاسيما على مستويات التحقيق والتنفيذ .

وهكذا تتكاثف الجهود منذ عام 2014، لإرساء آليات تعاون بين العديد من البلدان، لمواجهة انتشار ظاهرة الدعوات إلى التطرف عبر الأنترنت، حيث أعلنت الولايات المتحدة عن خطة للتحالف المعلوماتي مع الدول الغربية و العربية[28]، لتنسيق الجهود من أجل مواجهة إلكترونية عبر مواقع التواصل الاجتماعي.

وعادت الأمم المتحدة في فبراير 2015، إلى التأكيد خلال قمة مكافحة التطرف والعنف على مخاطر التهديدات الإلكترونية للمجموعات الإرهابية والتي استطاعت في فترة وجيزة تعزيز قبضتها على التواصل الاجتماعي وتوظيفها في الترويج أيديولوجيتها واستقطاب أنصار جدد ، كذلك تنبهت العديد من الدول إلى أن مواجهة الإرهاب الإلكتروني لا يمكن أن تتم إلا بتعزيز الإطار القانوني والتشريعي[29] عبر إصدار قانون خاص، لمكافحة الإرهاب على الأنترنت وإرساء قواعد تعاون فاعل وحقيقي على المستويات الوطنية بين مختلف الإدارات وعلى المستوى الدولي، بالعمل مع بلدان أخرى وتبادل المعلومات بين أجهزة طوارئ الأنترنت، أو إنشاء خلايا مشتركة تعمل على رصد التهديدات السيبرانية وتبادل المعلومات بشأنها .

كما أعلنت الدول الأعضاء عن قلقها إزاء استخدام الإرهابيين تكنولوجيا المعلومات و الاتصالات وبخاصة شبكة الإنترنت من أجل ارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها، وقد برزت نقاط مهمة في تطوير برنامج أمن الفضاء الرقمي التابع للأمم المتحدة لمكافحة الإرهاب، حيث في سنة 2019 نفّذ مكتب الأمم المتحدة لمكافحة الإرهاب المرحلة الأولى من برنامج أمن الفضاء الإلكتروني لجنوب شرق آسيا وبنغلاديش، حيث قدم ورشة عمل ل11 دولة من دول الأعضاء كما نظم ورشة عمل تجريبية متعمقة لتايلاند وبروناي والفلبين وغيرهم من دول، وفي سنة 2020 نفد مكتب الأمم المتحدة لمكافحة الإرهاب[30] المرحلة الأولى من أمن الفضاء الإلكتروني لشرق أفريقيا والوسط الأفريقي والساحل.

ولاشك أن في العالم العربي توجد بعض التشريعات التي تغطي جرائم المعلوماتية الحاسب الآلي بشكل أو بآخر خاصة في تونس والمغرب والمملكة السعودية و الأردن و الإمارات العربية المتحدة و عمان وقطر ولقد حققت دول مجلس التعاون لدول الخليج العربية تقدما ملحوظا في مجال استخدامات تكنولوجيا المعلومات وحظيت دولة الإمارات العربية المتحدة خصوصاً بموقع ريادي في هذا المجال،

وقد استدعى هذا التقدم اتساعاً في الثغرات التي تمّكن "الإرهابيين الإلكترونيين" من شن هجماتهم، وهو الأمر الذي حدا بخبراء دوليين إلى اعتبار أن "حكومات دول الخليج العربي عرضة لمخاطر كبيرة من الإرهاب عبر الإنترنت"، مشيرين إلى أن "هذه المخاطر تتفاقم مع مرور الأيام لأن التقنية وحدها غير قادرة على حماية بيانات الحكومات بشكل كلي من الهجمات المتوقعة.

وتعتبر دولة الإمارات العربية أول دولة عربية تسن قانونا مستقلا لمكافحة الجرائم المعلوماتية، وفي هذا السياق نصت المادة 21 من القانون الاتحادي رقم(02) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على أنَّه :"كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات[31] .

وعليه فقد أطلقت دولة الإمارات العربية المتحدة في شهر مايو 2017 مبادرة دولية تطالب المجتمع الأممي بتجريم الإرهاب الإلكتروني، و وضع الأطر اللازمة تنظيمياً وتشريعياً لتعاون فاعل بين الدول[32]، على المستوى السيبراني يحمي مواطنيها واقتصادها ومجتمعها من أخطار الفضاء الرقمي المفتوح، والجريمة والإرهاب بشكل خاص.

فإلى أي حد ستلتزم الدول بانخراطها في هذه المبادرة بوضعها ضمن دساتيرها من أجل تجريم الإرهاب الإلكتروني في تشريعاتها الوطنية ؟ .

2 .2_الآليات القانونية الوطنية لمكافحة الإرهاب الالكتروني على ضوء التشريع الجزائري

إن جريمة الإرهاب الإلكتروني، تتشابه مع غيرها من الجرائم الأخرى كالجرائم الإلكترونية وجرائم الإرهاب والتجسس و الاحتيال وقرصنة المعلومات، سواء من حيث النشاط الإجرامي المكون للسلوك الإجرامي أو بالنسبة للجناة أو النتيجة الإجرامية، وهو ما أحدث إشكالية في تحديد التكييف القانوني الواضح لهذه الجرائم المستحدثة[33].

ونظرا لذلك، فإن الدول تتبنى مناهج مختلفة عند تصديها للتحديات الناجمة عن استخدام الإرهابيين للوسائل الإلكترونية، فيتمثل الاتجاه الأول بإعمال القوانين الجزائية التقليدية في مكافحة الإرهاب والتي لا تكون متعلقة بجرائم الإرهاب الإلكتروني على وجه خاص، أما الاتجاه الثاني فيتمثل في ملاحقة هذا النوع من الجرائم بموجب القوانين الخاصة بجرائم الأنترنت، أو جرائم التجارة الإلكترونية أو حماية الملكية الفكرية ، ودون أن تكون هذه الجرائم مرتبكة بجرائم الإرهاب .

وأخيرا تتبنى بعض الدول اتجاها متمثلا بتطوير تشريعات وطنية مختصة بتجريم ومعاقبة مرتكبي جرائم الإرهاب الإلكتروني بشكل خاص .

وبالانتقال إلى جهود التشريع الجزائري في مجال مكافحة الإرهاب الإلكتروني فقد تنبهّت الجزائر على خطورة استخدام الإرهابيين للتقنيات الإلكترونية و اضطلعت بدور مهم في مجابهة هذه الجرائم ومكافحتها التي تهدد أمن ومصالح الدولة وسلامة أفرادها[34] ، كما أكد المشرع الجزائري على تعزيز التعاون الدولي من خلال نص المادة 31 من الدستور2016المعدل والمتمم ، وذلك استجابة للالتزامات الدولية في مجال وقاية وقمع الجرائم الإرهابية وتكريسا لمقتضيات مبادئ ميثاق الأمم المتحدة.

لهذا فإنه سيتم تناول أبرز الجهود والآليات القانونية الوطنية المبذولة على مستوى التشريع الجزائري :

بادر المشرع الجزائري إلى استحداث نصوص تجريمية حديثة تتماشى والتطورات التكنولوجيا الرقمية الذي شهدها المجتمع الدولي، لذا لم ينص صراحة على جرائم الإرهاب الإلكتروني، بل أفرد نصوصا عامة يخضع لها كل شخص قام بأفعال من شأنها المساس بأنظمة المعالجة الآلية للمعطيات إذ كيف هذه الأفعال على أنها جرائم معلوماتية وليست إرهابية ، مثل ما جاء بنص القانون رقم 01/05، المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها المعدل والمتمم، والقانون رقم 04/09، المتضمن القواعد الخاصة للوقاية من

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، و القانون رقم 06/15 المؤرخ في 15 فبراير 2015، يعدل ويتمم القانون رقم 01/05، المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها.

وأخيرا قام المشرع الجزائري بتجريم فعل تجنيد الإرهاب الإلكتروني بموجب القانون رقم 02/16 المؤرخ في 19 يونيو سنة 2016[35]، بموجب نص المادة 87 مكرر 12 الواردة ضمن الجزء الثاني بعنوان " التجريم."

ولم يكتفي المشرع الجزائري بالنصوص العامة بقانون العقوبات لقصورها في مواجهة الجريمة سواء تعلق الأمر بقمع الجرائم المعلوماتية، أو تلك المتعلقة بالجريمة الإرهابية العادية الأمر الذي دفعه إلى استحداث ترسانة قانونية جديدة تتعلق بالوقاية من الجرائم الإلكتروني[36] ، كما أكد على هذا من خلال تنصيبه للهيئة الوطنية للوقاية من جرائم الإلكترونية[37] بموجب المرسوم الرئاسي رقم 15/ 261 المؤرخ في 08 /10 / 2015، بهدف المراقبة الإلكترونية للمشتبه فيهم والكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة لقمع وردع هذه الظاهرة الخطيرة[38].

وقد صدر كذلك القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية[39] ومكافحتهما ليشكل تكملة لجملة القوانين والنصوص المتعلقة بمكافحة الإجرام والإجرام الالكتروني يهدف إلى التوصية لإنشاء مرصد وطني للوقاية من التمييز وخطاب الكراهية وينص كذلك على تدابير وعقوبات تمس من يستخدم تكنولوجيا الإعلام والاتصال(شبكات التواصل الاجتماعي)، لكن ما يعاب في هذا الجانب عدم وجود نص صريح يجرم ويعاقب على الإرهاب الالكتروني.

كما قام مؤخرا بإصدار المرسوم رئاسي رقم 21-439 الموافق 7 نوفمبر 2021 [40]يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، السالف الذكر وقد نصت في المادة 04 على "أنه تكلف الهيئة على الخصوص بتحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ وكذلك ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة. ." ، ,إذ كان لازم على المشرع هنا التدخل بقواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها, يمكّن للجهات المكلفة بالبحث والتحري عن الجريمة الالكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى أدلة الاثبات بدقة وسرعة .

نستطيع القول، بأن المشرع قد وُفق إلى حدٌ كبير في تجسيد سياسة المنع والوقاية من جريمة الإرهاب الإلكتروني وهو الأمر الذي يمكن من مكافحة و التصدي لجريمة الإرهاب الإلكتروني.

3_ الخاتمة :

في ختام هذه الدراسة، نستطيع القول أنه لا يمكن وجود طرق مضمونة تماما حماية نظام المعلومات من الاختراق إلى يومنا هذا، ومن بين أهم **النتائج التي توصلنا إليها :**

- ✓ أن جلٌ الدول والمؤسسات سعت إلى اعتماد مجموعة من الإجراءات الالكترونية والتي كانت على شكل مجموعة من الأجهزة والأنظمة والبرامج المتكاملة مع بعضها وفقا لبرنامج موضوع مسبقا للتصدي لأي اختراق في نظم المعلومات بهدف حمايتها تقنيا من الهجمات الإرهابية. اذ سعت العديد من الدول إلى اتخاذ التدابير والإجراءات اللازمة لمواجهة الإرهاب الالكتروني.
- ✓ بالإضافة إلى أن المشرع الجزائري سعى جاهدا إلى إرساء قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تولد مع التطور الحاصل في ارتكاب الجرائم الإرهابية كظاهرة مستحدثة، إذ تقوم هذه القواعد على استعمال أساليب التقنية الحديثة كأحد أهم

دعائم الاستراتيجية للوقاية من خطر هذه الجرائم ومنع حدوثها، تتمثل هذه الأساليب الجديدة في مراقبة الاتصالات الالكترونية وتفتيش النظم المعلوماتية الوارد ذكرها بمقتضى القانون السالف الذكر .

- ✓ خطى المشرع الجزائري خطوات ايجابية في مجال سن تشريعات حديثة لمواجهة الجريمة الإلكترونية ، وبالتالي أصبح للقاضي آليات البث في قضايا الجريمة المعلوماتية، بما يضمن عدم المساس بمبدأ الشرعية الجنائية.

كما اتضح لنا مدى ارتباط هذا النوع من الإرهاب بالتقدم العلمي والتكنولوجي والذي هو في حالة تقدم مستمرة ودون توقف ما دام العقل البشري يعمل. وعليه فهناك علاقة طردية ما بين الاثنين، فكلما حصل تقدم تقني ومعلوماتي صاحبه زيادة في مخاطر الإرهاب الإلكتروني.

إلا أن هذه الجهود محدودة ومازالت بحاجة إلى المزيد من الدراسات والبحوث والتشريع والتنظيم لاحتواء هذه الظاهرة الخطيرة، ومن بين هذه التدابير والإجراءات التي يجب أن تتخذها الدول لمكافحة الإرهاب الإلكتروني والتي نضعها على شكل **مقترحات كما يلي:**

رصد أنشطة الجماعات الإرهابية على الشبكات الاجتماعية وتحليل محتواها وأهدافها والاستراتيجيات المعتمدة فيها.

- ✓ سن القوانين والتشريعات الخاصة لسدّ كافة الثغرات التي تكتشف جريمة الإرهاب الإلكتروني أو سبل التحقيق فيها، القوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية وحفظها.
- ✓ العمل إيجاد منظومة قانونية دولية تحت مظلة الأمم المتحدة، يعهد إليها توثيق وتوحيد جهود الدول لمكافحة ومواجهة الإرهاب الإلكتروني,
- ✓ تعزيز التعاون الدولي والإقليمي من خلال مراقبة كل دولة للأعمال الإجرامية الإلكترونية الواقعة على أراضيها ضد دولة أو جهات أخرى خارج هذه الأراضي، بمساعدة المنظمات الدولية والهيئات المتخصصة بمكافحة الإرهاب الإلكتروني.
- ✓ عقد اتفاقيات الدولية بخصوص جرائم الإرهاب الإلكتروني، وتنظيم كافة الإجراءات المتعلقة بتبادل المعلومات والأدلة التي من شأنها تفعيل اتفاقيات تسليم الجناة في جرائم الإرهاب الإلكتروني.
- ✓ إشراك المجتمع المدني ومؤسساته في التعاون للإبلاغ عن المواقع ذات العلاقة بالإرهاب و الإرهابيين

التهميش وقائمة المراجع:

[1] -- بسمة بركات، سبل محاربة الإرهاب والتطرف في تونس ، ورقة علمية مقدمة في مؤتمر دولي المنعقد بتونس ، تحت شعار" الوقاية من التطرف العنيف " 3/2 يوليو 2018 ، المنشور على الرابط www.Alaraby.co. uk :

[2] - جلال محمد زغبي، أسامة أحمد مناغسة، جرائم تقنية المعلومات الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص 121 و ما يليها

[3] جلال محمد زغبي، أسامة أحمد مناغسة، جرائم تقنية المعلومات الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2006، ص 121 و ما يليها .

[4] - أنظر، نص المرسوم التشريعي رقم 05/93 مؤرخ في 04/19 1993 ، يعدل ويتمم المرسوم التشريعي رقم 03/92 والمتعلق بمكافحة التخريب و الإرهاب ، الجريدة الرسمية ، عدد 25 ، بتاريخ 1993/04/25 .

[5] - أمر رقم 21-11 المؤرخ في 16محرم عام 1443 الموافق 25 أوت 2021 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية العدد65، الصادر بتاريخ 26 أوت 2021.

[6] - أنظر، القانون رقم 04/09 مؤرخ في 14 شعبان عام 1430 ، الموافق 05 جويلية 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها ، الجريدة الرسمية ، الصادرة في 16 أوت 2009 ، العدد 47 . .

[7] - مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبرسنة 2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية، ع86 الصادرة ب 6 ربيع الثاني عام 1443 الموافق 11 نوفمبر سنة 2021

[8] - جلال محمد زغبي، أسامة أحمد مناغسة، المرجع السابق، ص 133.

[9] - ويشير الإرهاب الإلكتروني إلى عنصرين أساسيين هما: الفضاء الافتراضي، أو العالم الإلكتروني، وهو المكان الذي تعمل به أجهزة وبرامج الحاسوب والحواسيب المعلوماتية، وقد استفادت تلك المنظمات الإرهابية من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية، مما زاد من خطورتها، كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، التي تعتمد عليها الحكومات والشركات الاقتصادية الكبرى، أنظر: فريدة بن عمروش، الإرهاب الإلكتروني: دراسة في إشكالات المفهوم والابعاد، المجلة الجزائرية للعلوم الاجتماعية و الإنسانية، م08، ع02، جامعة الجزائر3، الجزائر، 29 /2020/09، ص219.

[10] - ذياب موسى البدانة، الجرائم الالكترونية " مفهوم وأسباب " ورقة علمية مقدمة في ملتقى علمي دولي المعنون، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن، عمان، 2014.

[11] - توفيق مجاهد، جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام2010، مجلة العلوم القانونية والسياسية، م09، ج.ع03، جامعة عبد الحميد بن باديس-مستغانم، الجزائر، ديسمبر2018، ص81

[12] - علي عدنان الفيل، الإرهاب الالكتروني، مقال منشور على الرابط: www.almanhal.com

[13] - جغدم محمد امين، جرائم الإرهاب الالكتروني والجرائم المنظمة، مجلة القانون الدولي والتنمية، جامعة عبد الحميد ابن باديس، مستغانم ، الجزائر، مجلد 06، عدد02

[14] - جدي وفاء، الإرهاب الإلكتروني أسبابه بين النص و التطبيق، مجلة مقاربات، م03، ع05، جامعة سيدي بلعباس، الجزائر، أكتوبر2015، ص45.

[15] - - عادل عبد الرزاق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، مركز الدراسات السياسية الاستراتيجية، عمان، 2014، ص، 102.

[16] - جدي وفاء ، المرجع السابق، ص 48

[17] - ذياب موسى البدانة، المرجع السابق ،ص 145.

[18] -. مرين يوسف، إرهاب الأنترنت عندما تتحول التقنية على وسيلة إجرام، مجلة الدراسات القانونية والسياسية، م04، ع02، جامعة عبد الحميد بن باديس مستغانم، الجزائر، جوان 2018

[19] - عبد الله بن فهد عدلان، الإرهاب الإلكتروني ومسؤولية المجتمع الدولي، مقال منشور على الرابط : / www.al-ain .com article

[20] - زين عابدين، عواد كاظم الكردي، جرائم الإرهاب المعلوماتي، دراسة مقارنة، منشورات حلبي الحقوقية،2018، ص 205.

[21] - مرين يوسف, المرجع السابق، ص 86.

[22] - قصعة خديجة، جمال بن مرزوق، تفعيل آليات الحماية القانونية للحدّ من انتشار الجريمة الالكترونية في العالم والجزائر، مجلة تاريخ العلوم، عدد06، ص74.

[23] - هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر 1998، ص 306 و ما يليها.

[24] - تقرير صحفي حول أعمال اللجنة الثانية في الجلسة التاسعة يوم 22 /04/ 2005 من المؤتمر الحادي عشر للأمم المتحدة: للوقاية من الإجرام والعدالة الجنائية " لدراسة وسائل استدراك عجز الأنظمة القضائية في مواجهة الإجرام المعلوماتي, أنظر الرابط على الموقع : www .un. c OrgleventsL1thcongress/docs

[25] - علي يوسف شكري، الإرهاب الدولي في ظل النظام العالمي الجديد، ط 01، دار السلام الحديثة، القاهرة، 2007، ص174-175

[26] - قسيمة محمد، "الوسائل الفنية للمنظمة الدولية للشرطة الجنائية(الأنتربول) كآلية للتعاون الدولي الشرطي"، حوليات جامعة الجزائر1، م34، ع02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة-الجزائر، جوان 2020، ص126

[27] - عبد الله بن فهد عدلان، الإرهاب الإلكتروني ومسؤولية المجتمع الدولي، مقال منشور على الرابط: www.al-ain .com / article

[28] - مايا حسن ملا خاطر، الاطار القانوني لجريمة الإرهاب الالكتروني، مجلة جامعة الناصر،العدد05، المجلد 01، 2015،ص138

[29] - عبد الله خبابة، الأشكال الجديدة للتجريم على ضوء الاتفاقيات الدولية ،2007/05/31 منشور في المجلة القضائية لوزارة العدل: http://khababa-lawyer.com/dl/nv_crim.pdf

[30] - مكتب مكافحة الإرهاب، أمن الفضاء الإلكتروني، متوفر على الرابط: https://www.un.org، تم الاطلاع عليه يوم 2022/02/01، على الساعة: 15:00.

[31] - قانون رقم (02) المؤرخ في 2006، يتضمن قانون اتحادي لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية لدولة الإمارات العربية المتحدة د.ع، الصادر 30 ذي الحجة 1426 الموافق 30 يناير 2006

[32] - مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، تقرير حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن، فرع منه الإرهاب، نيويورك 2009، ص07-08

[33] - - مايا حسن ملا خاطر، المرجع السابق، ص146.

[34] - - قصعة خديجة، المرجع السابق، ص 49.

[35] -قانون رقم 16-02 مؤرخ 19 جوان يتمم الأمر 66-156، المؤرخ في جوان 1966 والمتضمن قانون العقوبات، والمنشور في الجريدة الرسمية (ع 37)، المؤرخ في 22 جوان 2016 ، ص 4.

[36] -- كما هو الشأن بالنسبة لبعض التشريعات الجنائية المقارنة حيت نصت على أن الإرهاب الإلكتروني ضمن أحكام الجريمة الإلكترونية، ولقد أصبح تجريم السلوك الإجرامي و ملاحقة الجناة من الجرائم المعلوماتية.

[37] - بوعناقة فاطمة الزهراء، المرجع السابق، ص 82.

[38] - تهدف إلى المراقبة الإلكترونية للمشتبه فيهم والكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة لقمع وردع هذه الظاهرة الخطيرة.

[39] - القانون رقم 20-05 المؤرخ في 5رمضان 1441هـ الموافق ل 28/04/ 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والمنشور في الجريدة الرسمية (ع 25) الموافق ل 29 /04/ 2020

[40] - مزيد من التفصيل ، أنظر نص المادة 04 من المرسوم رئاسي رقم 21-439 الموافق 7 نوفمبر 2021.