وزارة التعليم العالي والبحث العلمي
جامعة العربي التبسي –تبسة-
كلية الحقوق والعلوم السياسية
قسم: الحقوق

مُذكرة مقدمة ضمن متطلبات نيل شهادة الماستر

تخصص: جريمة وأمن عمومي

بعنوان:

جريمة الإرهاب الالكتروني

إعداد الطالب:

- توات عبد الحكيم

إشراف الأستاذة:

- كردي نبيلة

الاسم واللقب	الرتبة العلمية	الصفة في البحث
السايح بوساحية	أستاذ محاضر قسم "أ"	رئيسا
كردي نبيلة	أستاذة محاضر قسم "أ"	مشرفا ومقررا
شعنبي صابرة	أستاذة محاضر قسم "ب"	ممتحنا

السنة الجامعية: 2021 –2022

" الكلية لا تتحمل أي مسؤولية على ما يرد في هذه المذكرة من آراء "


بسم الله الرحمن الرحيم

بسم الله الرحمان الرحيم

﴿ قَالَ أَلْقُوا فَلَمَّا
أَلْقَوْا سَحَرُوا أَعْيُنَ
النَّاسِ وَاسْتَرْهَبُوهُمْ
وَجَاءُوا بِسِحْرٍ عَظِيمٍ ﴾

صدق الله العظيم

سورة الاعراف –الآية 116.

شكر وعرفان

ربي لك الشكر ولك الحمد ولك الثناء الحسن كما يليق بجلال وجهك وعظيم سلطانك لتوفيقك لنا في إتمام هذا العمل.

إن الحروف لتتهادى بكلماتها لتجسد لكم أجمل عبارات الشكر والثناء.

فنتقدم بجزيل الشكر والعرفان إلى:

الأستاذة كردي نبيلة التي تفضلت بالإشراف على هذا العمل وكانت لنا السند والعون في كل خطوات إعداد هذه الرسالة.

كل التقدير والاحترام لأساتذة كلية الحقوق والعلوم السياسية.

إهـدا ء

إلـى الـوالـد رحمـه الله
إلـى أمـي الـغـالـيـة حفـظهـا الله
إلـى كـل إخـوتـي وأخـواتـي
إلـى كـل الاصـدقـاء والـزمـلاء
إلـى كـل مـن كـان لـهـم فـي هـذا الـدرب نـورا وعـلـمـا وخـلـقـا

عبـد الـحـكـيـم تـوات

قائمة المختصرات:

I.باللغة العربية:

1- ج ر: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

2- د. ت.ن: دون تاريخ نشر.

3- ط: طبعة

4- د.ط: دون طبعة.

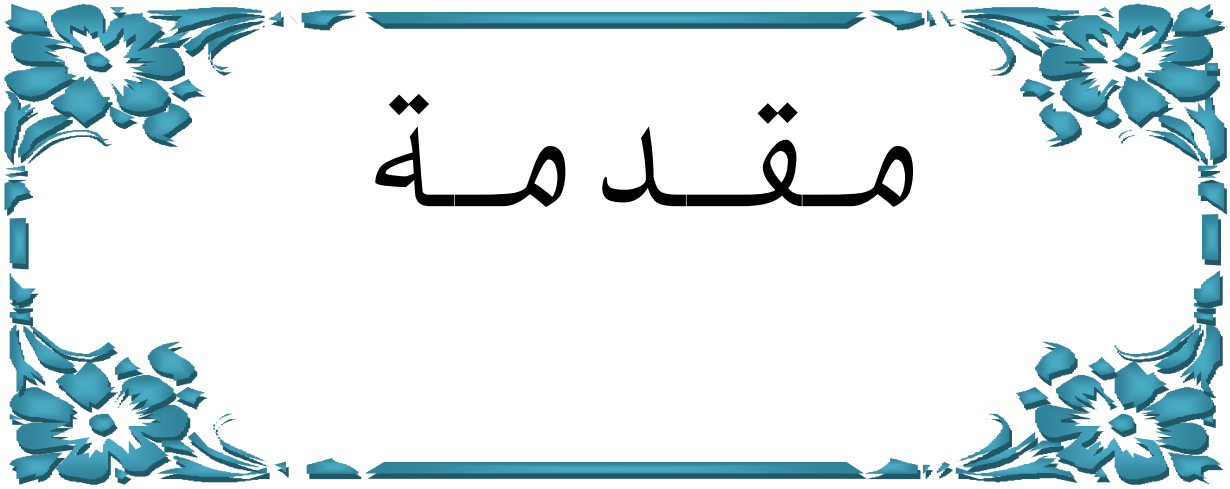
5- ص: الصفحة.

6- ص ص: من الصفحة إلى الصفحة

7- د.د.ن: دون دار نشر

II.باللغة الفرنسية:

- Ed: Edition.
- N°: Numéro
- P: page


مـقــد مــة

شهدت البشرية مرحلة تطور متميزة ارتبطت بتطور التكنولوجيا الهائل ومعالمه الكبرى في الرقمنة المتزايدة والفضاء الافتراضي، كما ظهر مجتمع المعلومات والمعرفة والذي أدى إلى هيمنة وسائل الإعلام والاتصال. فهذه الثورة التكنولوجية برزت كطفرة تطورية غير مسبوقة في فترة زمنية قصيرة، والتي أثرت على التكنولوجيا وهي تتباين من مجتمع لأخر.

وأدت هذه التحولات التكنولوجية والرقمية الهائلة التي عرفها العالم إلى إحداث تغيرات جذرية داخل وبين المجتمعات وخلفت أثارا وانعكاسات كبرى، إذ أصبحت المعلومات والمعرفة مظهرا ومؤشرا ومصدرا هاما للقوة في الآونة الأخيرة، فاستخدام هذه التكنولوجيا وشبكة الانترنت لم يقتصر فقط على جانب ايجابي بل له مظاهر خطيرة سلبية أثرت على المجتمعات والدول ويظهر ذلك من استخدام ولجوء الكثير من الفواعل (أفراد، منظمات إجرامية وإرهابية) لهذه المزايا في أغراض أكثر خطورة مما عكس الجانب السلبي للتطور الالكتروني وأدى إلى بروز مجموعة من الجرائم المستحدثة التي تعتمد على أساليب متطورة، ومن أبرز هذه الجرائم ما اصطلح عليه بالإرهاب الالكتروني الذي ظهر نتيجة تزايد وتصاعد استغلال الجماعات الإرهابية للتكنولوجيا الحديثة إذ ساهمت أدوات الفضاء الالكتروني في تفعيل وتعزيز عمليات الجماعات الإرهابية وتحقيق أهدافها وتنفيذ استراتيجياتها.

فالإرهاب الالكتروني هو الوجه الجديد للعمل الإرهابي الناتج عن اتساع استخدام الفاعلين للعالم الافتراضي والذي نشأ عن الترابط بين الحواسب الآلية وأجهزة الاتصال وغيرها من مكونات البنية التحتية للانترنت واقتحام تكنولوجيا المعلوماتية في إدارة الشؤون المختلفة وتزايد استغلال هذه التكنولوجيا على المستوى الميداني وعلى الصعيد الإعلامي والتواصل.

وقد برزت عدة محاولات لتعريف الإرهاب الالكتروني وتفصيله على الرغم من عدم وجود إجماع في الآراء بشأن نطاقه ومعناه، إلا انه متفق على استخدام الجماعات الإرهابية لأدوات الفضاء الالكتروني لتحقيق وتنفيذ أهدافه فهو حالة اندماج بين العالم الواقعي والافتراضي. إذ تسفر أفعال على الشبكات والوسائط التقنية أي العالم الافتراضي أثرا ملموسا على الواقع الحقيقي لأجل تحقيق أهداف ضد المصالح العامة وبرزت أول محاولات في تقديم إطار مفاهيمي للإرهاب الالكتروني وعرّف بأنه شكل من أشكال الإرهاب الفعلي أو الحقيقي لتوفره على عناصر أساسية في الظاهرة الإرهابية وهي البعد البنيوي للإرهاب ومبدأ الضرر والعناصر المرتبطة بالبعد السياسي والوسائل الإرهابية وهو يحدث عبر الفضاء الالكتروني. فهو هجمات

مقصودة ضد المعطيات بأنواعها ونظم وبرامج الكومبيوتر والاتصالات تحقيقا لأغراض إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم وإثارة الفوضى[1] .

بالرجوع إلى اعتبار الإرهاب جريمة الكترونية منظمة تمتاز هذه الجماعات الإرهابية بتنظيم وتنسيق متواصل بين الأعضاء والتخطيط والتنفيذ للهجمات الالكترونية باستخدام كل الوسائل والتقنيات الحديثة لخدمة العمليات الإرهابية سواء كان ذلك عن طريق الاتصال بشبكة الانترنت لتجنيد عدد من الإرهابيين والتواصل معهم وتدريبهم، أو من خلال الاتصالات بالشبكات السلكية واللاسلكية أو عبر الأقمار الاصطناعية وما يتبعه من عمليات تجسس، فالإرهاب أصبح خطر دولي يؤرق كل المجتمعات لذلك وجب على المجتمعات الدولية التكاثف من اجل مواجهة الإرهاب[2] لذلك أصبحت مواجهة ظاهرة الإرهاب الالكتروني ومخاطره من أهم المشاكل التي تواجه الحكومات المعاصرة، وذلك ومن خلال ابتكار وسائل وتقنيات معلوماتية حديثة هدفها الحد من حركة الإرهاب وجعل تنقلاته الافتراضية أكثر صرامة وتشددا.

- **أهمية الموضوع:**

تتجلى أهمية دراسة الإرهاب الالكتروني في خطورة هذه الظاهرة المستحدثة على البنى التحتية لأنظمة تقنية المعلومات والاتصالات، وتحديد طبيعة الاختراقات والهجومات المستمرة في شتى المجالات وذلك لأنه يتميز عن غيره من أنواع الإرهاب وبطريقة عصرية متمثلة في استخدام الموارد المعلوماتية والوسائل الالكترونية والبنية التحتية للمعلوماتية، فهي جرائم تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها.

ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود، وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود أي أنها ذات طبيعة عالمية.

[1] - نسيب نجيب، **التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب**، مركز الكتاب الأكاديمي، ط1، عمان، 2017،ص:52

[2] - غادة نصار، **الإرهاب و الجريمة الالكترونية**،العربي للنشر و التوزيع ط1،القاهرة ،2017،ص: 132

و تكمن دراسة موضوع الإرهاب الالكتروني في التطرق إلى أهم المفاهيم للإرهاب الالكتروني في مختلف الأبعاد ودوافعه وتحديد ما يميزه عن المفاهيم المشابهة له والاختلافات بين الإرهاب التقليدي، الجريمة الالكترونية والجريمة المنظمة.

وبما أن الإرهاب الالكتروني فعل مجرم لا يقوم إلا بتحقيق كافة الأركان(الركن الشرعي المادي، المعنوي) التي تحدد نطاق الجريمة وتفصلها عن غيرها من الجرائم لأنّها فعل إجرامي يعاقب عليها القانون يهدف إلى نشر الخوف والرعب ويكون لها تأثيرها بجميع أشكاله تهديدا وخطرا للسلم والأمن الدوليين نظرا لما له من أثار وخيمة على امن المواطنين واستقرارهم وعلى الإمكانيات الاقتصادية والهيبة السياسية للدولة في محيطها الإقليمي والدولي وتبيان آليات المكافحة والوقاية منه على الصعيد الدولي أو الإقليمي، حيث يعتبر من أخطر أشكال الإرهاب وأكثرها انتشارا في ظل التطور التكنولوجي وتنامي استخدام شبكة الانترنت.

- **دوافع اختيار الموضوع**

دوافع شخصية تتمثل في الميول الشخصي لدارسة مثل هذه المواضيع وكذلك عدم التطرق باستفاضة لدراسة هذا الموضوع في المسار الدراسي الجامعي.

أما الدوافع الموضوعية فهي تتجلى في الأهمية العلمية لموضوع جريمة الإرهاب الالكتروني وما يترتب عنها من آثار، والآليات القانونية لمكافحة هذه الجريمة على المستوى الدولي والوطني.

و حداثة الموضوع، خاصة بما يتعلق توضيح كونه من الجرائم المستحدثة والتي هي محل اهتمام للدراسة في مختلف المجالات ويعكس آثارا سلبية على الأفراد والدول مما يجعل من المهم والمفيد التطرق إليه بالدراسة والتحقيق والتدقيق.

- **إشكالية الدراسة:** لدراسة هذا الموضوع نطرح الإشكالية التالية:

ما مفهوم الإرهاب الالكتروني ؟ وما مدى فعالية آليات وطرق مكافحة ؟

ونطرح بجانب هذه الإشكالية الرئيسية جملة من الإشكاليات الفرعية التالية:

- ما مفهوم الإرهاب الالكتروني، وما دوافعه؟ وما هي الأغراض التي يسعى إليها؟ فيما تتمثل خصائصه؟ وماهي آثاره وانعكاساته على مستوى الأمن والسلم والعلاقات الدولية؟

– ماهي السبل والأساليب المعتمدة لدى الهيئات والمنظمات الدولية لمواجهة هذه الظاهرة بكل صورها وأشكالها؟

- **المنهج المتبع:**

اعتمدنا في دراستنا هذه على:

– المنهج التحليلي وذالك من أجل الإجابة عن التساؤلات المطروحة من خلال تحليل أحكام قانون العقوبات، والاتفاقيات والمعاهدات.

– المنهج الوصفي للبحث والتعمق في مفهوم الإرهاب الإلكتروني من خلال التطرق إلى الاجتهادات والتطبيقات والمفاهيم المتعددة لجريمة الإرهاب الإلكتروني وما عمل به المشرع وما تناوله الفقه في مؤلفاته.

- **أهداف الدراسة:**

تهدف هذه الدراسة إلى توضيح مفهوم الإرهاب الإلكتروني، وإبراز أهم دوافع وأغراض الإرهاب الالكتروني، وتحديد خصائصه والمفاهيم التي تميزه عن باقي جرائم الإرهاب الأخرى التي ترتكب في العالم المادي، وتبيان أركان جريمة الإرهاب الالكتروني والآثار المترتبة عنه، ونطاق تجريمه على المستوى الوطني والدولي والتعرف على أهم الوسائل والأساليب المعتمدة لدى الهيئات والمنظمات الدولية لمكافحة جرائم الإرهاب الالكتروني وتقنية المعلومات، والآليات التي نصت عليها لمكافحة هذه الجريمة الخطيرة.

- **الدراسات السابقة:**

حظى بالعديد من الدراسات سواء كانت في المؤلفات و الكتب و التي نذكر من بينها " الإرهاب الالكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة" للمؤلف عادل عبد الصادق الذي تطرق فيه إلى دراسة موضوع الإرهاب الالكتروني دراسة تحليلية و مقارنة مع مختلف القوانين محاولا فيها إبراز أهم مفاهيم الإرهاب الالكتروني و أنواعه و كذلك تحديات العلاقات الدولية و تأثيراتها.

و لا نغفل عن اختيار هذا الموضوع و لو اختلفت العناوين في جعله عنوان بحث لرسائل مذكرات عديدة نذكر منها أطروحة الدكتوراه لشعنبي صابرة في " الجهود الدولية في مكافحة الإرهاب الالكتروني –دراسة مقارنة " و رسالة الماجستير لـ: نجاري علي فايزة كريم في " الآليات القانونية لمكافحة الإرهاب الالكتروني "، و أيضا أدرج هذا الموضوع في عدة ندوات و

ملتقيات وطنية سجل فيها العديد من الأساتذة مداخلاتهم و أرائهم حول هذا الموضوع ، من بينهم : وداعي عز الدين" في تطور الجريمة الإرهابية من الجريمة التقليدية إلى الجريمة المعلوماتية" ، مداخلة ملقاة في الملتقى الوطني حول الجريمة المعاصرة.

- **صعوبات الدراسة:**

واجهتنا العديد من الصعوبات كنقص المراجع العامة والمتخصصة بجريمة الإرهاب الالكتروني في المكاتب الجزائرية، وصعوبة حصولنا على المعلومات المتعلقة به وعدم تمكننا من دراسات تتعلق بجوانب هذا الموضوع.

-عدم تمكيننا من الحصول على المعلومات والتطبيقات الخاصة بجريمة الإرهاب الالكتروني نظرا للتداول نفس الموضوع وبطرح متشابه الأفكار.

- قلة وجود النصوص القانونية المتخصصة في جرائم الإرهاب الإلكتروني بالأخص في التشريع الجزائري ويتمثل في الفراغ والقصور التشريعي.

وفي ظل هذه الصعوبات حاولنا الإلمام بموضوع جريمة الإرهاب الالكتروني وإزالة الغموض عنه.

- **التصريح بالخطة:**

وللإجابة عن الإشكالية المطروحة ارتأينا تقسيم موضوع دراستنا إلى فصلين حيث سنتناول في الفصل الأول الإطار المفاهيمي لجريمة الإرهاب الالكتروني والذي ينقسم إلى مبحثين تطرقنا في المبحث الأول إلى ماهية لجريمة الإرهاب الالكتروني أما المبحث الثاني فخصصناه لدراسة قيام جريمة الإرهاب الالكتروني وآثارها.

والفصل الثاني تحت عنوان آليات مكافحة جريمة الإرهاب الالكتروني والذي ينقسم بدوره إلى مبحثين سنتطرق في المبحث الأول إلى الجهود المبذولة لمكافحة جريمة الإرهاب الالكتروني إقليميا ودوليا أما المبحث الثاني سنتناول فيه الجهود المبذولة لمكافحة جريمة الإرهاب الالكتروني وطنيا.

الفصل الأول: الإطار المفاهيمي لجريمة الإرهاب الالكتروني

المبحث الأول: ماهية جريمة الإرهاب الالكتروني

المبحث الثاني: قيام جريمة الإرهاب الالكتروني

يعد الإرهاب ظاهرة قديمة قدم الحياة البشرية ووجوده لا يرتبط بشعب من الشعوب وإنما يتعداه إلى عموم البشر، ولا بدولة معينة بل يتعداه لكل دول العالم، وهو بذلك يمثل تهديدا وخطرا مباشرا للأمن الوطني والدولي وما يتركه من أثر على الواقع. ومما زاد من مخاطر الإرهاب هو التطور الكبير في وسائل الاتصالات وثورة المعلومات –الانترنت– التي حولت العالم إلى قرية صغيرة وجعلت المعلومات في متناول الجميع يستخدمونها في اتصالاتهم أو تنفيذ وظائفهم أو القيام بتنفيذ أنشطة إرهابية مثل التجسس وتدمير الفعاليات الالكترونية للدول والمؤسسات ليظهر ما يعرف بالإرهاب الالكتروني.

كما يعرف الإرهاب الإلكتروني من الجرائم التي استغلت الجانب السلبي للتطور الهائل في وسائل الاتصال وثورة الانترنت وتكنولوجيا المعلوماتية مما أدى إلى انتشاره وارتفاع ضحاياه وكذا الأثر الناتج عنه ممّا ساهم في تميّزه عن غيره من أنواع الإرهاب في استخدامه للموارد والوسائل الإلكترونية وكذا طبيعته ونطاقه ووسائله وحتى في خصوصية متركبيه.

من خلال ما سبق سنتطرق في هذا الفصل إلى ماهية جريمة الإرهاب الإلكتروني **(المبحث الأول)** ، ثم نبيّن أسس قيام جريمة الإرهاب الإلكتروني **(المبحث الثاني)** .

المبحث الأول: ماهية جريمة الإرهاب الإلكتروني

يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب في العصر الحاضر، نظرا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم،كما أن مصطلح الإرهاب الإلكتروني شاع استخدامه بشكل كبير مع الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الآلية والانترنت تحديدا في إدارة معظم الأنشطة.

وتعد جريمة الإرهاب الإلكتروني من أنواع الإرهاب في العصر الحديث، لذا من الأهمية معرفة ماهية الإرهاب الإلكتروني **(مطلب أول)**، وكذا تسليط الضوء على الآثار المترتبة عن جريمة الإرهاب الالكتروني **(مطلب ثاني)**.

المطلب الأول: مفهوم جريمة الإرهاب الإلكتروني

إن الخوض في مسألة البحث عن تحديد المقصود بجريمة الإرهاب الإلكتروني يقتضي علينا الوقوف إلى تعريف هذه الجريمة والأسباب المؤدية للإرهاب الإلكتروني وكذا الوسائل التي يستخدمها الإرهابي المعلوماتي والأهداف التي يسعى إليها.

الفرع+

الأول: تعريف جريمة الإرهاب الإلكتروني

يعد الإرهاب الإلكتروني من أخطر وأبشع الجرائم التي تطال الدول والحكومات وهذا ما جعل التشريعات تتغاضى عن تعريف الإرهاب الإلكتروني فاختلفت توجهات ونظرة الفقه للفعل الإرهابي فالبعض يراه عملا مشروعا من أجل الحرية والتحرر وآخر يراه أنه فعل سالب للحريات،ذلك هو السبب في عدم تحديد تعريف جامع ومانع له[1].

أولا: تعريف الإرهاب

لقد أثار تعريف الإرهاب بشكل عام جدلا كبيرا في الفقه القانوني والتشريعات الجنائية الوطنية والاتفاقيات والمؤتمرات الدولية، ويرجع ذلك إلى عدة أسباب، لعل أهمها نعت البعض لأعمال العنف التي تقع من طرف حركات التحرر ضد العدو الأجنبي بالأعمال الإرهابية، ويكفي أن نستدل في هذا المقام بالموقف السلبي للولايات المتحدة الأمريكية التي ترى أن تعريف الإرهاب يجب أن يشمل جميع أعمال العنف الإرهابي الفردي، وصورا أخرى من العنف بما فيها أعمال العنف التي تمارسها المقاومة المسلحة من أجل تحرير أراضيها ونيل استقلاله. وعليه سنتطرق إلى تبيان المدلول اللغوي لكلمة إرهاب في المعاجم وكذا في الشريعة الإسلامية وفي التعاريف الاصطلاحية وبما جاءت به الاتفاقيات من مفاهيم.

1-الإرهاب لغة:

وردت كلمة الإرهاب في معجم الرائد: إرهاب "أرهب" التي بمعنى نشر الرعب والخوف والفزع في البشر[2]، وكلمة إرهابي هي صفة تطلق على الشخص الذي يلجأ إلى الإرهاب بالقتل أو التخريب لإقامة سلطة أو تفويض.و حسب ما جاء في معجم الوجيز أن الإرهابيين هو

[1] - مصطفى يوسف كافي، **جرائم الفساد ،غسيل الأموال،السياحة،الإرهاب الالكتروني المعلوماتي**، مكتب المجتمع العربي للنشر و التوزيع ،ط1، عمان، 2014، ص: 111

[2] - جبران مسعود، **معجم الرائد الفبائي في اللغة العربية و الإعلام**، دار العلم للملايين،ط3، بيروت، 2005، ص:59

وصف يطلق على الذين يسلكون سبل العنف والإرهاب لتحقيق أهدافهم السياسية [1]. ويتضح بذلك أن كلمة إرهاب في اللغة العربية يدور معناها حول الخوف والفزع والرعب والخشية[2].

وأن كلمة رهبة تنحدر من أصل لاتيني وانتقلت إلى لغات أخرى لدرجة أصبحت مشتقاتها (الإرهابي، الإرهاب، الأعمال الإرهابية، الإرهاب المضاد، الإرهاب السياسي...) وهي مصطلحات واسعة الانتشار[3]. والإرهاب هو السلوك الذي يقوم على ارتكاب العنف لتحقيق أهداف سياسية[4].

2- الإرهاب في اللغة الإسلامية

حرّمت الشريعة الإسلامية فعل الإرهاب بجميع سلوكياته وصوره المختلفة واعتبرته شكل من أشكال الفساد، وأنّ مرادفه هو القتل لا أساس له من الصحة، وذكر مصطلح الإرهاب في القرآن على أنّه إثارة للرّعب والخوف في قوله تعالى:" **وإيّاي فارهبون**" [5]، وقوله تعالى: "**قَالَ أَلْقُوا فَلَمَّا أَلْقَوْا سَحَرُوا أَعْيُنَ النَّاسِ وَاسْتَرْهَبُوهُمْ وَجَاءُوا بِسِحْرٍ عَظِيمٍ** "[6] فكلمة الإرهاب في القرآن الكريم وردت بدلالات الرعب في قلوب الناس وهي صفات مذمومة.

انطلاقا من هذا البعد نلاحظ أن الدين الإسلامي الحنيف أحكامه تنبذ شتّى أصناف الترهيب وإخافة الناس حتى على سبيل المزاح كما عبر عنه بأنّه ظاهرة خطيرة ترتكب ضد الأشخاص والأموال التي تخلّف أثارا في نفوس الناس وتهدد استقرار المجتمع[7].

3-اصطلاحا

---

[1] - سلوى أحمد ميدان، **الإرهاب و الجهود الدولية لمكافحته** ،(العراق، مجلة كلية القانون للعلوم القانونية والسياسية،جامعة كركوك ،العدد05،2006)،ص:54

[2] - شعنبي صابرة، **الجهود الدولية في مكافحة الإرهاب الالكتروني(،أطروحة دكتوراه ،العلوم في الحقوق)**، قانون جنائي،جامعة العربي التبسي، تبسة،2019 ،ص:11

[3] - محمد حسن عمر بروارى، **غسيل الأموال وعلاقته بالمصارف والبنوك-دراسة مقارنة**، دار قنديل للنشر والتوزيع،ط1، عمان، 2013، ص:182

[4] - أمير فرج يوسف، **مكافحة جريمة الإرهاب الإلكتروني-في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب**، دار الكتب و الدراسات العربية، الاسكندرية، د.ط، 2015، ص:45

[5] - الآية 40 من سورة البقرة

[6] - الآية 116 سورة الأعراف

[7] - سعد صالح كشطي، **موقف الشريعة الإسلامية من الإرهاب (مجلة الرافدين للحقوق، العراق مجلد 12 العدد 44)**، ،كلية الحقوق جامعة الموصل، ،2010، ص:404

الإرهاب علم إجرامي يتم عن طريق استخدام أجهزة الكومبيوتر والاتصالات السلكية واللاسلكية وينتج عنه تدمير وتعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك وذلك بهدف التأثير على الحكومة أو السكان لخدمة سياسة أو اجتماعية أو إيديولوجية [1].

ومن المعروف أن الدول لم تتفق على وضع تعريف محدد للإرهاب إلّا أنّه في الوقت نفسه نجد أنّ كل دولة أو منظمة إقليمية أعطت تعريفا للإرهاب انطلاقا من وضعها ومصالحها والزاوية التي تنظر منها[2]. واختلفت تبعا لعدة اعتبارات بالنظر إلى المنفذ للعمل أو الغاية أو الهدف منه، والنتائج المترتبة عليه والأدوات المستخدمة في تنفيذه[3].

وأدّت هذه الاختلافات في وجهات النظر إلى انقسام فقهاء القانون في مسألة تعريف الإرهاب إلى اتجاهين مستندين في ذلك على عدة حجج، فالإرهاب أمر حتمي لتمييزه عن باقي ظواهر العنف المشابهة له سواء كانت مشروعة أم غير مشروعة وهو غير قابل للتعريف وحجتهم في ذلك أنّ أي محاولة لتعريفه لن تكون ملمّة بجميع أشكاله وأساليبه فهو يحتاج إلى عدّة تفسيرات ويشمل مجموعة من الجرائم الإرهابية فيكون بذلك جامدا لا يواكب التطوّر المستمر لأشكال وأساليب الإرهاب[4].

كما رفض آخرون تعريف الإرهاب على اختلاف وجهات النظر الفكرية والسياسية والعقائدية للمهتمين بدراسة هذه الظاهرة التي أصبح تفسيرها كل حسب الجهة التي تخدم مصالحه[5]، ويعتبر من المسائل غير المجدية في الفقه القانوني ما دام مفهومه مستقرا في الأذهان [6].

---

[1] - عادل عبد الصادق، **الإرهاب الالكتروني وتأثيره على الدول** ،دار الأهرام للنشر والتوزيع ،ط1، القاهرة، مصر ،2014، ص:86

[2] - أمير فرج يوسف، **مكافحة الإرهاب**، مكتبة الوفاء القانونية،ط1، الإسكندرية، 2011، ص:10

[3] - محمود عبد العزيز محمد، **الإرهاب النفق المظلم في تاريخ البشرية وعلاقته بالأديان السماوية**، دار الكتب االقانونية، د.ط، القاهرة، 2013، ص:19

[4] - نادية شرايرية، **إشكالية تعريف الإرهاب في القانون الدولي** ،(مجلة التواصل في العلوم الانسانية والاجتماعية المجلد 19 العدد 02،2013)، جامعة باجي مختار،عنابة-الجزائر- م، ص:154

[5] - عبد السلام محمد، **مفهوم الارهاب في الشريعة الاسلامية**،دار الكتب العلمية،ط1،بيروت،2005، ص:23

[6] - أسامة حسين محي الدين، **جرائم الإرهاب على المستوى الدولي** ،المكتب العربي الحديث،د.ط، الإسكندرية، 2009 ،ص: 57.

ويرى في هذا الصدد الفقيه ولتر لكور Walter Laqueur أنّه لا يوجد حاليا تعريف للإرهاب ولا يمكن تعريفه في المستقبل، كما قال في هذا الشأن الفقيه دانيال ستيفنDaniel Stephen:" انّني لن أحاول تعريف الإرهاب لإعتقادي بأنّ مناقشة التعريف لن تحقق تقدما في دراسة المشكلة التي نتعامل معها "[1]. وهو ما أقرّ عليه مجلس الشيوخ الفرنسي سنة 1984 [2] بسبب تعدّد أشكال الإرهاب وأساليبه واتّساع نطاقه وغموض مفهومه.

حسب رأي أصحاب الحجج الرافضة لتعريف الإرهاب فقد أشاروا إلى ضرورة تعريف الإرهاب لوضع الحد الفاصل بينه وبين ظواهر العنف الأخرى ووقعوا في نفس المشكلة على عدم اتّفاقهم على تعريف موحد[3]، فهناك من يقول بأنه الاستعمال المنسق للعنف أو التهديد به من أجل بلوغ أهداف سياسية وهو حسب قول توم مالكيسون Tom Malikson [4] فتعريف الإرهاب بالاستخدام غير المشروع للعنف والتهديد بواسطة فرد أو مجموعة او دولة ضد فرد أو مجموعة أو دولة والذي ينتج عنه رعبا يعرض الأرواح البشرية للخطر ويهدد حريات أساسية [5] الغرض منه الضغط على الجماعة لكي يتغير سلوكها[6].

كما عرّفه الأستاذ محمود شريف بسيوني[7] على أنّه إستراتيجية عنف محرم دوليا تحفز بواعث عقائدية، وتتوخّى أحداث عنف مرعبة داخل شريحة خاصة من المجتمع لتحقيق الوصول

---

[1] - يوسف كوران، **جريمة الإرهاب والمسؤولية المترتبةعنها في القانون الجنائي الداخلي والدولي** ،مركز كرديستان للدراسات الاستراتيجية ،د.ط ،السليمانية، 2007، ص:12

[2] - عثمان علي الحسن ويسي، **الارهاب الدولي ومظاهره القانونية والسياسية في ضوءأحكام القانون الدولي العام** ،دار الكتب القانونية،د.ط ،مصر،2011، ص:65

[3] - توفيق مجاهد،طاهر عباسة، **جريمة الإرهاب الإلكتروني في ضوء أحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ،(مجلة العلوم القانونية والسياسية، المجلد 09–العدد 03 ديسمبر 2018)**، ص:80

[4] - سامي علي حامد عياد، **تمويل الارهاب** ،دار الفكرالجامعي،ط1، الإسكندرية،2008،ص:26

[5] - عبد الله نورشعت، **التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي**،مكتبة الوفاء القانونية ،ط1،الإسكندرية،2017، ص:51

[6] – منتصر سعيد حمودة، **الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام و الفقه الاسلامي** ،دار الفكر الجامعي،ط1، الإسكندرية،2008،ص:38

[7] – توفيق مجاهد، طاهر عباسة ،مرجع سابق ص:80

إلى السلطة أو القيام بدعاية لمطلب أو لمظلمة بغض النظر عن مقترف العنف سواء يعملون لأنفسهم أو نيابة عن دولة من الدول[1].

ولقد تم الأخذ بهذا التعريف من طرف لجنة الخبراء الإقليميين التي نظمت اجتماعاتها في الأمم المتحدة في فيينا من 14 إلى غاية 18 مارس 1988 [2]. إلّا أنّه تعرّض أيضا للنقد باعتباره يركز فقط على الدوافع السياسية للإرهاب فقط.

ويتضح من التعريفات السابقة أن جوهر الإرهاب هو حالة الرعب التي يتمكن فاعلها من فرض سيطرته لتحقيق هدف ما[3].

4-التعريف السياسي

يعرفه المعجم السياسي بأنه:"محاولة نشر الذعر والفزع لأغراض سياسية، وهو وسيلة تستخدمها حكومة استبدادية أو دكتاتورية لإجبار وإرغام الشعب على الاستسلام لها[4].

وتعرف الموسوعة السياسية الإرهاب: "استخدام العنف غير القانوني، أو التهديد به بأشكاله المختلفة كالاغتيال والتشويه والتعذيب والتخريب والنسف، بغية تحقيق هدف سياسي معين مثل كسر روح المقاومة والالتزام عند الأفراد وهدم المعنويات عند الهيئات والمؤسسات،أو كوسيلة من وسائل الحصول على المعلومات أو مال، وبشكل عام هو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية[5] ".

5-تعريف الإرهاب في الاتفاقيات والتشريعات الوطنية

من أهم النقاط المثارة للنقاش من خلال التعاريف الواردة في الاتفاقيات هو انعدام اتفاق جامع ومانع لمصطلح للإرهاب يعتمد عليه دوليا.

أ- في التشريع الدولي

[1] – جمال بوازدية، **الإستراتيجيات المغاربية لمكافحة الإرهاب ،(اطروحة دكتوراه، الدراسات الدولية)**، قسم الحقوق،جامعة الجزائر 2012،03-2013،ص:40

[2] – محمد فتحي عيد، **واقع الإرهاب في الوطن العربي** ،أكاديمية نايف للعلوم الأمنية،الرياض،د.ط ،1999،ص:24

[3] – أحمد فتحي سرور، **مواجهة الارهاب الإلكتروني** دار النهضة العربية،ط 03، القاهرة،مصر ،2011،ص:31

[4] – وضاح زيتون، **المعجم السياسي**.، دار أسامة المشرق الثقافي، ط1، الأردن، 2006، ص: 21.

[5]–الكيالي عبد الوهاب ،**الموسوعة السياسية،الجزء السابع**، المؤسسة العربية للدراسات والنشر، بيروت، د.ط،1994، ص153.

عرفت اتفاقية جنيف لسنة 1937 لقمع الإرهاب على ان: "الأعمال الإرهابية هي الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف، أو يقصد بها خلق حالة من الرعب في أذهان أشخاص معنيين أو مجموعة من الأشخاص، أو عامة الجمهور"[1]. حيث نرى من خلال ما ورد في اتفاقية جنيف لتعريفها للإرهاب استعمالها لعبارات عامة، ولم تحدد بدقة الفعل الإجرامي المشكل للإرهاب.

بينما تعرف الاتفاقية العربية لمكافحة الإرهاب الصادرة من مجلس وزراء الداخلية العرب بالقاهرة في سنة 1997 بأنّه كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه وأغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر"[2].

يعتبر تعريف الاتفاقية العربية كأول خطوة ساهمت في تحديد معنى الإرهاب بعبارات مختصرة دقيقة ومفصلة تشرح الإرهاب، ولم تقف عند هذا الحد بل بادرت بإعطاء تعريف للجريمة الإرهابية.

ب- التشريع الجزائري

اتجهت تشريعات الدول إلى تقديم تعريف الإرهاب في قوانينها الداخلية استجابة للاتفاقيات الدولية، وعلى رأسهم المشرع الجزائري الذي عالج الظاهرة الإرهابية بإصدار المرسوم التشريعي رقم92-03 المؤرخ في 30سبتمبر 1992يتضمن مكافحة الإرهاب والتخريب وعرف العمل الإرهابي من خلال المادة الأولى منه:"**يعتبر عملا تخريبيا أو إرهابيا في مفهوم هذا المرسوم التشريعي كل مخالفة تستهدف أمن الدولة والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي:**

[1]-ولد الصديق ميلود ،**مكافحة الارهاب بين مشكلة المفهوم و اختلاف المعايير** ،مركز الكتاب الاكاديمي، ج1، ط1،عمان، 2018، ص ص:17-18.

[2]- عبد القادر الشيخلي ،**طبيعة الارهاب الالكتروني**، رابطة العرب الاسلامي،ط1، السعودية، 2015، ص: 05.

بثّ الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء على الأشخاص أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو المساس بممتلكاتهم..." [1]

إلا أنه قام بإلغاء هذه المادة وأدخل تعديلات بموجب الأمر 95-11 المؤرخ في 25 فيفري 1995 [2] المتضمن قانون العقوبات تحت عنوان" الجرائم الموصوفة بأفعال إرهابية أو تخريبية " في القسم الرابع بموجب المواد 87 مكرر إلى المادة 87 مكرر 10.

ولقد أدخل المشرع الجزائر الجريمة الإرهابية في قانون العقوبات على أنها جريمة جديدة مستقلة وقائمة بذاتها وبين بدقة في المادة 87 مكرر الركن المادي للجريمة الإرهابية. [3]

ومن خلال استعراض التعريفات السابقة فالإرهاب عدوان غير مبرر على الأبرياء، وقد يكون مدفوعا بأهداف شخصية أو تخريبية أو سياسية أو دينية بهدف ترويع الآمنين وتخويفهم وقتلهم وتعريض سلامة المجتمع للخطر [4].

ثانيا: تعريف الإرهاب الالكتروني

في ظل غياب تعريف موحد للإرهاب تعددت التعاريف للإرهاب الإلكتروني وهو مجموعة من الهجمات الخطيرة وفيروسات قرصنة على حواسيب شبكات وأنظمة الإعلام الآلي لمؤسسة أو هيئة ترتكب لخلق فوضى عامة بهدف بثّ الرعب. فالإرهاب الالكتروني لا يختلف عن الإرهاب عامة إلا من حيث الطريقة التي يلجأ إليها الجاني في ارتكاب جريمته والتي أخذت منحى يتماشى مع التطور التقني والتطور التكنولوجي.

---

[1]-مرسوم تشريعي رقم92-03 ،**يتضمن مكافحة الارهاب و التخريب،** المؤرخ في 30سبتمبر 1992،ج.ر، عدد 70 الصادرة بتاريخ01أكتوبر 1992.

[2]-انظر جريدة رسمية عدد.11 سنة 1995

[3]-بواب بن عامر،**المواجهة التشريعية للإرهاب الإلكتروني**،(**مجلة البحوث العلمية العدد 09،ديسمبر2017**)،ص:282

[4]-هيثم فالح شهاب ،**جريمة الإرهاب و سبل مكافحتها في التشريعات الجزائية المقارنة** ،دار الثقافة للنشر و التوزيع، ط1 ،عمان، 2010،ص:40.

ويستنبط تعريف الإرهاب الإلكتروني من التعريفات السابقة للإرهاب العام. حيث أن نلاحظ أنّ مبدأ تجريم الإرهاب واحد وهو العنف والتهديد.

1-المقصود بالإرهاب الإلكتروني

مع أن الإرهاب الإلكتروني أصبح شائعا في السنوات الأخيرة، وبات خطرا كبيرا على الصعيد الدولي ولا سيما مع التطور السريع لتقنيات الاتصال واعتماد البشر على الانترنت والذي أصبح بصفة متزايدة، كما أنه لم يحظى بدوره على تعريف متفق عليه من قبل المجتمع الدولي، حيث استغل التكنولوجيا الحديثة في تطوير وسائل ارتكاب الجريمة باستغلال البيئة الافتراضية لغرض تنفيذ هجماته، وهو ما ادّى إلى إبرام المعاهدات والاتفاقيات لمحاربة ومكافحة الإجرام الإلكتروني لاسيما معاهدة بودابست سنة 2001 التي تضمنت مكافحة الإجرام عبر الانترنت[1]. غير أنّه لا يوجد لحدّ الآن تعريف عالمي متفق عليه فقد تعددت التعاريف الذي تناولته، ومن أهم التعاريف التي سيقت بصدد جريمة الإرهاب الالكتروني من بينها:

باري كولين من أول مستعملي مصطلح الإرهاب الإلكتروني في الثمانيات وعرفه على أنه:"هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وأنّ الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"[2]

وفي بداية التسعينات صدر تقرير عن الأكاديمية الوطنية الأمريكية عندما قام الرئيس بيل كلينتون سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية التي توصلت إلى أنّ مصادر الطاقة والإتصالات وكذا شبكات الكومبيوتر ستكون الهدف الأول للهجمات الإرهابية ولكن هذه الأخيرة لم تعرفه بل اكتفت بدراسة الظاهرة ومحاولة فهم سياسة تفكير الإرهاب الإلكتروني والطرق التي يتخذها في تنفيذ عملياته الإرهابية واستخدام الانترنت والبراعة في التفوق على أيّ تقنية مستخدمة.

---

[1]-خذيري عفاف ،**الحماية الجنائية للمعطيات الرقمية، (أطروحة دكتوراه ،علوم في القانون الجنائي)**، قسم الحقوق،كلية الحقوق والعلوم السياسية جامعة تبسة ،2017-2018، ص:102

[2]-بوحادة سارة، **أثر الإرهاب الالكتروني على أمن واستقرار الدول**، مداخلة ،د.ط،د.س،ص"04.

إن ما يتميز به الإرهاب الالكتروني عن الإرهاب التقليدي بالطريقة المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات، فالأنظمة الالكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين[1].

وتجدر الإشارة إلى أن خطورة الإرهاب الالكتروني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية مما يجعلها هدفا سهل المنال. وتأسيسا على ما سبق يمكننا القول إن الإرهاب الالكتروني هو الخطر القادم نظرا لتعدد أشكاله وأساليبه واتساع مجال الأهداف التي يمكن مهاجمتها من خلال وسائل الاتصالات وتقنية المعلومات[2].

2- دوافع الإرهاب الالكتروني:

تختلف دوافع الإرهاب الالكتروني تبعا لاختلاف الجهات السياسية والظروف الاقتصادية والأحوال الاجتماعية والاختلاف الديني والعقائدي.

أ- الدوافع الشخصية:

تتعدد الدوافع الشخصية المؤدية للإرهاب، ويمكن بيان أبرزها فيمايلي:

- افتقاد الشخص لأهمية دوره في الأسرة والمجتمع وفشله في الحياة الأسرية مما يؤدي إلى اكتساب بعض الصفات السيئة ومن ضمنها عدم الشعور بالانتماء والولاء للوطن.
- الرغبة في الظهور وحب الشهرة بحيث لا يكون الشخص مؤهلا فيبحث عما يؤهله باطلا فيشعر ولو بالعدوان والتخريب والتدمير.
- نقمة الشخص على المجتمع الذي يعيش فيه نتيجة للظلم وإهدار الحقوق.
- الإحباط في تحقيق بعض الرغبات أو الوصول إلى المكانة المنشودة وإحساس الشخص بأنه أقل من غيره وينظر إليه نظرة متدنية فيلجأ للإرهاب للخروج عن النظام.

ب-الدوافع الفكرية:

[1] - مصطفى يوسف كافي، ماهر عودة الشمايلة،محمود عزت اللحام،**الإعلام و الارهاب الالكتروني**،دار الاعصار العلمي للنشر و التوزيع، ط1 ،الاردن،2015،ص:147

[2] - حسنين شفيق، **الإعلام الجديد و الجرائم الالكترونية –التسريبات ..التجسس الالكتروني..الإرهاب**، ،دار فكر وفن للطباعة والنشر و التوزيع ،ط1، مدينة 6اكتوبر، 2015،ص:21

تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها فيمايلي:

- الجهل بمقاصد الشريعة الإسلامية المتمثل بالظن لا باليقين والتثبت، والفهم الخاطئ للدين، وتفسيره تفسير خاطئ، والجهل بقواعد الدين الحنيف وآدابه وسلوكه.
- الانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة.
- التطرف وهو أمر بالغ الخطورة في أي مجال من المجالات وخاصة المجالات الفكرية.

جـ- الدوافع السياسية:

من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب ما يأتي:

- غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق العامة والتقصير في أمور الرعية.
- معاناة بعض المجتمعات والشعوب الدولية من الظلم والاضطهاد والسيطرة الاستعمارية وسلب الأموال وخرق القوانين والمواثيق الدولية مما يدفع الشعوب إلى التشدد والتطرف.

دوافع اقتصادية:

- تفاقم الأزمات الاقتصادية في المجتمعات الدولية بالإضافة إلى المتغيرات الاقتصادية العالمية.
- التقدم التقني للأنظمة المصرفية العالمية وما أدى إليه من سهولة انتقال الأموال وتحويلها بين جميع أرجاء العالم عن طريق شبكة الانترنت ساعد المنظمات الإرهابية على استغلال الفرصة من اجل تحقيق أهدافهم غير المشروعة [1].

3- أغراض الإرهاب الالكتروني:

- أغراض إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم وإثارة الفوضى ونشر الخوف والرعب بين الأشخاص والدول[2].
- تعطيل الأداء الطبيعي لنظم السيطرة والرقابة الالكترونية وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الإستراتيجية في الدولة.

[1] – مصطفى يوسف كافي، ماهر عودة الشمايلة،محمود عزت اللحام ،مرجع سابق ،ص: 151

[2] – مصطفى يوسف كافي ،**الإدارة الإلكترونية** ،دار ومؤسسة راسلان للنشر والطباعة والتوزيع،ط1،دمشق،2011،ص: 440

- الإخلال بالنظام العام والأمن المعلوماتي وزعزعة الطمأنينة وتعريض سلامة المجتمع وأمنه للخطر وإثارة الرأي العام.
- إلحاق الضرر بالبنى التحتية وتدميرها والأضرار بوسائل الاتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة.
- تهديد السلطات العامة والمنظمات الدولية وابتزازها[1]
- يلجأ الإرهابيون إلى جمع البيانات الإحصائية التي يتم استخلاصها من البيانات الشخصية التي يقوم المستخدمون بإدراجها على شبكة الانترنت بالإضافة إلى الاستفسارات والاستطلاعات المتوفرة على المواقع الالكترونية.

الفرع الثاني: خصائص الإرهاب الالكتروني

أحدثت الثورة التكنولوجية في الاتصالات والمعلومات ثورة فكرية في مفاهيم الحرب والعدوان وفي مضامين القانون الدولي والوسائل أيضا، فلم يعد هناك مجال لإعلان الحرب بين الدول أو بين الجماعات والدول حيث الاعتماد على الضربات الاستباقية، بل شملت الحرب الدخول لأنظمة المعلومات وتدميرها أو التأثير في كيفية عملها مما يكون له الأثر الكبير في ظل الاعتماد المتزايد للدول على التكنولوجيا في الاقتصاد والسياسة وفي شتى مجالات الحياة2.

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم وأصبح الاعتماد على وسائل تقنية المعلومات يزداد يوما بعد يوم سواء في المؤسسات المالية أو المرافق العامة أو المجال التعليمي أو الأمني، وإن أكثر الأنظمة التقنية تقدما وأسرعها تطورا هي الأنظمة الأمنية ورغم تطورها إلا أنها اقل الأنظمة استقرارا وموثوقية نظرا لتسارع وتيرة الجرائم الالكترونية وأدواتها والثغرات الأمنية التي لايمكن أن يتم الحد منها على المدى الطويل[3]. اذ يتميز الإرهاب الالكتروني بعدة خصائص وسمات:

- الإرهاب الالكتروني لا يحتاج عند ارتكابه إلى العنف والقوة بل يتطلب حاسب إلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

[1] – عبد القادر الشيخلي ،مرجع سابق ،ص ص:9-10.

[2] – عادل عبد الصادق، **الإرهاب الالكتروني-القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة**، مطبوعات مركز الدراسات السياسية و الإستراتيجية،ط1 ،القاهرة ،2009،ص: 118

[3] – مصطفى يوسف كافي، ماهر عودة الشمايلة،محمود عزت اللحام ،مرجع سابق ،ص: 147-148

- صعوبة اكتشاف جرائم الإرهاب الالكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مثل هذه الجرائم.
- صعوبة الإثبات في الإرهاب الالكتروني نظرا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره.
- مرتكب جريمة الإرهاب الالكتروني يكون من ذوي الاختصاص في مجال تقنية المعلومات، فالإرهاب الإلكتروني يعتمد على المهارة في التعامل مع الحاسب والذكاء الفردي أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية. وفي أقل الإمكانيات التي تتمثل في الحاسب ووصلة الانترنت دون الحاجة إلى السفر أميالا للتنفيذ مع وجود درجة عالية من الأمان وسهولة الوصول للهدف الذي يتمثل في البنية التحتية الكونية في معظم الدول[1].
- استعمال الأسلحة الناعمة: يستخدم الإرهابيين في جريمة الإرهاب الالكتروني السلاح التقني المتمثل في جهاز الانترنت أو أي جهاز آخر من أجهزة التقدم التكنولوجي للقيام بأغراض إرهابية ويقومون بشن حرب معلوماتية نفسية دون الحاجة إلى استعمال القوة والعنف فانتقال الجريمة من الميدان المحسوس إلى البيئة الافتراضية التي تعد أضرارها الناتجة اخطر من الإرهاب التقليدي[2] .
- جريمة عابرة للحدود: يتسم بكونه جريمة متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق إقليمي محدد[3]، فهي بذلك يمكن أن تمتد آثارها عبر القارات فالمجرم في دولة وضحاياه من عدة جلسات مختلفة، حيث اندثرت الحدود بين الدول وأصبح العالم قرية واحدة بسبب ما أتاحه العصر التكنولوجي من تطور غير خاضع لنطاق إقليمي محدود.
- صعوبة اكتشاف واثبات الجريمة: تمتاز جريمة الإرهاب الالكتروني بصعوبة اكتشافها ويعود ذلك إلى نقص الخبرة والكفاءة لدى أجهزة الضبط والتحقيق للتعامل مع هذا النوع من

[1] – عادل عبد الصادق **الارهاب الالكتروني–القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة** ،مرجع سابق ،ص: 119

[2] - بن صويلح أمال، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام**،(الملتقى الدولي حول الاجرام السيبراني المفاهيم والتحديات خطوة عامة نحو مكافحة الارهاب الالكتروني في الجزائر)،جامعة 8ماي قالمة ،يومي 11-12 أفريل 2017، ص:03

[3] – امير فرج يوسف، **مكافحة الإرهاب**،مرجع سابق، ص:229.

الإجرام الذي يضفي عليها الكثير من التعقيد في الإثبات وإقامة الدليل على مرتكبها وسهولة إتلاف الدليل من قبل المجرم المعلوماتي.

- ارتكابه من طرف فردي أو جماعة: جريمة الإرهاب الالكتروني يمكن أن يرتكبها شخص واحد، كما يمكن أن يرتكبها مجموعة من الأفراد ويبقى القائمون على الجريمة بعيدون عن الخطر فالمواجهة غير مرئية لهم يتميز الإرهاب الالكتروني بأنه يتم بتعاون أكثر من شخص على ارتكابه. [1]
- خصوصية المجرم الإرهابي في جريمة الإرهاب الالكتروني: يمتاز مرتكبها بخبرة عالية وكفاءة كافية في التعامل مع أجهزة الحاسب الآلي وشبكة الانترنت وكذا التعامل مع الناس في مواقع التواصل الاجتماعي التي أصبحت المنبر الالكتروني الأكثر شهرة واستعمالا منهم[2].
- جريمة من الجرائم المتجددة: جرائم الإرهاب الالكتروني من الأنماط الإجرامية المستحدثة وهذا نظرا للأشكال المتعددة التي تأخذها في وقتنا الحاضر ما صعب مواكبتها وكشفها[3].

المطلب الثاني: تمييز جريمة الإرهاب الالكتروني عما يشبهها

هناك عدة جرائم تتشابه مع جريمة الإرهاب الالكتروني وهذا لا يمنع من وجود بعض الاختلافات التي تتميز بها كل جريمة على حدى، وفي هذا الصدد نخص بالذكر جريمة الإرهاب التقليدي،الجريمة المنظمة والجريمة المعلوماتية.

الفرع الأول: تمييزها عن جريمة الإرهاب التقليدي

[1] – مصطفى يوسف كافي، ماهر عودة الشمايلة،محمود عزت اللحام مرجع سابق ،ص: 152

[2] - وداعي عز الدين، **تطور الجريمة الارهابية من الجريمة التقليدية الى الجريمة المعلوماتية**، ملتقى وطني حول الجريمة المعاصرة – كلية الاداب والعلوم الانسانية والعلوم الاجتماعية،جامعة باجي مختار عنابة، يومي 13-17 ديسمبر 2017،ص03

[3] – محمد خميخم، **موقف التشريع الجزائري من جريمة الإرهاب الالكتروني** ،مجلة حوليات جامعة الجزائر 1، المجلد 34،العدد02-2020 ،جوان 2020،ص:34

إن الفكرة الأساسية في تجريم الإرهاب ثابتة تتمثل في الخوف المترتب على استخدام العنف وأن الهدف من كل أنواع الإرهاب التقليدي نشر الخوف والفزع داخل المجتمع وبما أن الإرهاب الالكتروني يعتمد على العنف باستخدام تطبيقات الانترنت والخدمات المتصلة بها فان الإرهاب التقليدي هو نفسه الإرهاب الالكتروني إلا انه يستخدم الحاسب الآلي كمصدر للهجمات[1].
وسنحدد أوجه التشابه والاختلاف بين النوعين وفق مايلي:

أولا: أوجه التشابه: سنبينها في النقاط التالية:

- يتداخل الإرهاب التقليدي والإرهاب الالكتروني باعتبارهما من الأعمال غير المشروعة التي جرمتها التشريعات والاتفاقيات الدولية.
- تتفقان من حيث الغاية التي يسعيان إليها وهي نشر الرعب والخوف وابتزاز الدول ومحاولة السيطرة على نظامها الداخلي وتمويل الأنشطة من خلال الاستيلاء على ممتلكات الناس والسعي لتجنيد أعضاء جدد للانخراط إلى صفوف الجماعات الإرهابية.
- كلتا الجريمتان ترتكبان لأجل المساس بالنظام العام وتعريض سلامة المجتمع للخطر وعلى اختلاف الدوافع سياسية اقتصادية اجتماعية أو فردية[2].

ثانيا: أوجه الاختلاف:

بالرغم من التداخل الكبير بين الجريمتين إلا أن هذا لا يمنع وجود اختلافات بينهما:

- الوسيلة المستخدمة في ارتكاب الجريمتين: تختلف الوسيلة المستخدمة في ارتكاب جريمة الإرهاب التقليدي عن نظيرتها الواقعة عبر الانترنت، فأما الأولى فيلجأ الإرهابيون إلى استعمال الوسائل التقليدية العادية في تنفيذ عملياتهم الإرهابية كاستخدام السلاح أو القنابل على عكس الإرهاب الالكتروني اذ يعتمد على التقنية الرقمية العالية من حاسب وانترنت.

[1] – نور الله تلة، **الارهاب بالوسائل الالكترونية ،(مذكرة ماجستير، القانون الجزائي)** كلية الحقوق، جامعة دمشق،2015–2016، ص ص:26–27

[2] – هروال هبة نبيلة،**جرائم الانترنت دراسة مقارنة، (اطروحة دكتوراه،قانون)** قسم الحقوق، كلية الحقوق والعلوم السياسية ابي بكر بلقايد،تلمسان،2013–2014،ص:337

– المكان الذي ترتكب منه وفيه الجريمتين: فالإرهاب التقليدي يرتكب في مكان مادي ملموس ومرئي أين تسهل فيه معاينة مسرح الجريمة، مثل وضع إرهابي لمتفجرات أو تفجير نفسه أو خطف طائرة، أما الإرهاب عبر الانترنت فيرتكب في العالم الافتراضي الانترنت، فهنا يصعب اكتشاف مدبرها ومنفذها[1].

– يختلف الإرهاب التقليدي عن الإرهاب الالكتروني بأن الأول يسهل كشف آثاره من قبل أجهزة الأمن على عكس الثاني الذي يصعب التيقن بها لنقص خبرة أجهزة الشرطة في التعامل مع العالم السيبرياني[2].

– محل الجريمتين: يقع الاعتداء والعنف في الإرهاب التقليدي على الأشخاص سواء كانوا طبيعيين أو معنويين كالدول أو الممتلكات الخاصة أو العامة، ولكن الشأن يختلف في الإرهاب عبر الانترنت فهو يعتمد على وسائل ناعمة لا تحدث أضرارا مادية كونه مرتبط بالانترنت الذي يقع في البيئة الافتراضية من اختراق للمواقع الالكترونية وتدميرها عن طريق نشر الفيروسات واستخدام برامج للتجسس على الدول وتخريب البيانات ومحوها وغيره من الأنشطة التخريبية[3].

– يختلف الإرهاب الالكتروني عن الإرهاب التقليدي من حيث أن الأول لا يلجأ إلى العنف والقوة للوصول إلى أهدافه على عكس الإرهاب التقليدي الذي يستعملها في تحقيق أغراضه وهو الفارق الجوهري بين الجريمتين.

الفرع الثاني: تمييز الإرهاب الالكتروني عن الجريمة المعلوماتية

أدى التطور الحاصل في مختلف المجالات والاستخدام المتتالي للحاسب الآلي والانترنت إلى ظهور جرائم ذات طبيعة الكترونية أطلق عليها عدة تسميات منها جرائم المعلوماتية، جرائم الكترونية جرائم التقنية العالية. ...الخ. ومفهوم الجرائم المعلوماتية يكون بطريقتين جرائم تقع باستخدام الوسيلة المعلوماتية وجرائم تقع على الوسيلة المعلوماتية[4].

---

[1] – هروال هبة نبيلة، مرجع سابق،ص:337–338

[2] – علي جاسم التميمي، **الإرهاب الالكتروني وأثره على المجتمع** –المجلة السياسية والدولية،جامعة المستنصرية العراق،د.س،ص:491.

[3] – جعفر حسن جاسم الطائي، **جرائم التكنولوجيا المعلومات جديدة للجريمة الحديثة** ،دار البداية،ط1، عمان ،2007،ص:494.

[4] - هيثم عبد الرحمن البقلي ،**الجرائم الإلكترونية الواقعة على العرض بين الشريعة والقانون المقارن** ،دار العلوم للنشر والتوزيع،ط1 ،القاهرة، 2010، ص:15

فالجريمة المعلوماتية هي عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرد لها عقاب وهي سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر [1] ولقد خصص لها المشرع الجزائري القسم السابع من قانون العقوبات بعنوان المساس بأنظمة المعالجة الآلية للمعطيات من خلال إضافة المواد 394 مكرر إلى المادة 394 مكرر 8 [2].

كما انه واكب التطورات الحاصلة وقام بتعديل قانون العقوبات بموجب القانون رقم 15 -04 ولقد عبر المشرع الجزائري عن الجريمة المعلوماتية بالجرائم المتصلة في مرحله اللاحقة لاستحداثه القانون رقم 09-04 الذي يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتعرفها بموجب المادة الثانية فقرة أ:" **يقصد بها مفهوم هذا القانون بما يأتي جرائم المساس بأنظمة المعالج الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكبها عن طريق منظومة المعلوماتية أو نظام الاتصالات الالكترونية** [3].

أولا: أوجه التشابه

- أن الجريمة المعلوماتية من الجرائم المتصلة بالانترنت فهي بذلك تتداخل مع جريمة الإرهاب الالكتروني.
- كلتا الجريمتين تتشابهان في الوسيلة المستعملة في ارتكابهما وهي ضرورة استعمال التكنولوجيا الحديثة إضافة لذلك هما من الجرائم ذات الطبيعة خاصة.

[1] - عبد العال الديربي، محمد صادق اسماعيل، **الجرائم الالكترونية دراسة قانونية قضائية مقارنة**، المركز القومي للإصدارات القانونية،ط1،القاهرة، 2012 ،ص:41

[2] - الامر رقم 66- 156 ،المؤرخ بثمانية جوان 1966 **والمتضمن قانون العقوبات** الجريدة الرسمية عدد 49 الصادرة في 19 جوان 1966

[3] - القانون رقم 09 -04 ،المؤرخ في 05 اوت 2009 **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال** جريده رسمية عدد: 47

- من الجرائم المستحدثة في العالم وكلتاهما من الجرائم العابرة للحدود التي تهدم القيم الأخلاقية لا تتطلبان في ارتكابهما العنف والقوة. [1]
- يسهل ارتكابهما بالنظر إلى طبيعة شبكة الانترنت مع قله تكلفتها
- خصوصية المجرم الذي يمتاز بذكائه وفطنته في أسلوب ارتكابه للجريمة فهو لا يعرض نفسه للخطر كما يتصف بتكيفه مع محيطه فلا يبين عدوانيته وكراهيته وخطورته الإجرامية
- إظهار القدرات والبراعة في التعامل مع الوسائل التقنية وإحداث اكبر قدر من الأضرار،لا يتطلب العنف والقوة[2].

ثانيا: أوجه الاختلاف

بالرغم من التداخل الكبير بين الجريمة المعلوماتية وجريمة الإرهاب الالكتروني إلا انه هناك اختلاف بينهما من حيث ما يلي:

- إذا كانت الجريمة المعلوماتية تهدف إلى تحقيق الربح المادي فان جريمة الإرهاب الالكتروني بالإضافة إلى ذلك فهي تهدف إلى تحقيق إغراض سياسية دينية ثقافية.
- المجرم المعلوماتي اقل خطورة من المجرم الإرهابي المعلوماتي فالأول قد يتواجد داخل المنظومة المعلوماتية سواء عن طريق الصدفة أو لمجرد التسلية للبحث عن مصادر التمويل أو لنشر الفكر الإرهابي أو استقطاب أعضاء جدد أو التواصل في ما بين أعضائها للتخطيط والتنسيق للعمليات الإرهابية[3].

الفرع الثالث: تمييزها عن الجريمة المنظمة

الجريمة المنظمة العابرة للحدود أو الجريمة المنظمة عبر الدول ظهرت نتيجة التوسع التجاري بين الدول وعولمة اقتصادياتها وما نتج عنها من عولمة الثقافة والجريمة، ومع التطور التكنولوجي تطورت أساليبها الإجرامية وأنماطها خاصة باستعمال الحاسب الآلي والانترنت مما

[1] -كوثر حازم سلطان، **موقف القانون والقضاء من الجريمة الإلكترونية السيبريانية المقارنة**،(مجلة كلية التربية الأساسية، المجلد 22 العدد 96)، د.ب.ن، 2016 ص: 973

[2] – دياب موسى البداينة، **الجرائم الالكترونية المفهوم والإثبات**، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ،تاريخ 2 الى 4 سبتمبر 2014 ،عمان، ص: 20

[3] - نجاري علي فايزة كريم، **الآليات القانونية لمكافحة الإرهاب الالكتروني**، (شهادة الماجستير ،تخصص قانون دولي للأعمال)، قسم الحقوق،كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016، ص: 35

زاد في خطورتها على النظام الاقتصادي والسياسي من خلال إنشائهم شركات وسيطرتهم على التجارة العالمية[1].

نشأت منظمات خطيرة تعمل على مستوى دولي ومنظم متجاوزة للحدود الدولية ومعتمدة لاستراتيجيات معينة للمنظمات الإجرامية الوطنية والخارجية لفرض السيطرة على الدول. مما جعلها من اكبر التحديات التي تواجه الدول بكافة أشكالها وبدون تمييز بين الدول المتقدمة والمتخلفة، ومن أشهر المنظمات المافيا الايطالية وعصابة الثالوث في جنوب شرق آسيا وغيرها، فمنهم من يعرّفها استنادا إلى المنظمة الإجرامية ومنهم استنادا إلى الجريمة المرتكبة وحصر العناصر التي تقوم عليها المنظمة وهي:

- وجود منظمة إجرامية تتألف من ثلاثة أشخاص أو أكثر لارتكاب جريمة،
- الاستمرار والتعقيد في ممارسة الأنشطة الإجرامية
- استعمال وسائل وطرق في تحقيق هدفها الدافع أو الباعث وهو تحقيق الربح باستخدام العنف

تعتمد في ذلك على ركائز أساسية التخطيط والتنظيم، الاحتراف، التعقيد والقدرة على التوظيف والابتزاز[2].

ويمكن القول أن الجريمة المنظمة هي منشاة محكمة التنظيم والتركيب تتمثل أعمالها في إنتاج سلع أو خدمات أو خدمات غير قانونية لمجموعة خاصة من المستهلكين بهدف السيطرة على الهيكل العام للاقتصاد التحتي وتقوم على أساس احتكاري في منطقة النفوذ مما يمكنها من فرض أدوات وعمولات أو نظم معينة على مشروعات الأعمال القانونية وغير القانونية باستخدام والتهديد العنف[3].

---

[1] – كوركيس يوسف داوود ،**الجريمة المنظمة**، الدار العلمية والدولية دار ثقافة للنشر والتوزيع،ط1، عمان، 2001، ص: 13

[2] - وسيم حسام الدين، **مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة السعودية**، مكتبة القانون والاقتصاد،ط1، الرياض، السعودية 2016 ص ص: 16-17

[3] - صلاح هاشم، **التنمية والجريمة المعولمة- سياسات الإفقار والهدم الخلاق**، أطلس للنشر والإنتاج الإعلامي ش.م.م، ط1،الجيزة، ،2018،ص:23

الجريمة المنظمة هي الآلية المتبعة للعمل خارج إطار القانون والضوابط الاجتماعية ويعمل المجرمون وفقا لنظام بالغ التعقيد والدقة في النظم التي تتبعها أكثر المؤسسات تطورا وتقدما ويخضع أفرادها لأحكام قانونية وضعت من قبلهم تفرض عليهم أحكام بالغة القسوة [1].

أشار المشرع الجزائري بدوره إلى الجريمة المنظمة في نص المادة 176 قانون العقوبات هي كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه أو تؤلف بغرض الإعداد لجناية أو أكثر أو الجنحة أو أكثر [2] غير أن التعريف في هذه المادة لا ينطبق على الجريمة.

أولا: أوجه التشابه

- كل من الجريمتان من الجرائم ذات الطابع العابر للحدود
- الاعتماد على وسائل الاتصال الحديثة والأجهزة المعقدة التي أفرزتها التكنولوجيا العصرية في تطوير أساليب إجرامهما[3].
- كل من الجريمتين تحظيان بتكاتف الجهود الدولية والإقليمية لمكافحاتهما والتصدي لهما
- كلاهما يسعيان إلى بث الرعب والخوف في نفوس الناس لتحقيق أهدافهم المنظمة لعدم احتوائها على عناصر الجوهرية لقيام الجريمة المنظمة استمرار العضوية والبعد العابر للحدود الوطنية الطابع الجماعي التنظيمي.
- باعتبار الجريمة المنظمة من الجرائم الخطيرة مثلها مثل جريمة الإرهاب عامه تعتبر كل جريمة إرهابية جريمة منظمة وليس كل جريمة منظمة حدثا إرهابيا[4].
- لكل منهما نفس القواعد التي تحكم النظام الداخلي للجماعة من احترام وتعاون وتخطيط محكم في تنفيذ الأعمال الإجرامية
- وجود علاقة هرمية داخل تنظيماتهما وتجمعاتهما وكذا الذكاء والحنكة والدقة التي يمتاز بها أعضائها واحترافية تسير الأنشطة الإجرامية

---

[1] – عبد الكريم خالد الردايدة ،**الجرائم المستحدثة وإستراتيجية مواجهتها** ،دار ومكتبة الحامد للنشر والتوزيع،ط1 ،عمان، 2013،ص: 39.

[2] – المادة 176 من الأمر 66– 156 المتضمن قانون العقوبات المعدل والمتمم

[3] – محمد فوزي صالح،**الجريمة المنظمة وأثارها على حقوق الإنسان** ،(شهادة الماجستير، القانون الدولي لحقوق الإنسان)، قسم الحقوق،كلية الحقوق جامعة يحيى فارس، المدية، 2008– 2009 ،ص: 15

[4] – محمد أمين بشرى، **التحقيق في الجرائم المستحدثة**، مركز الدراسات والبحوث جامعة نيل العربية للعلوم الامنية د.ط. الرياض، 2004، ص:146.

- كلاهما يهدد التنمية ألاقتصادية للدول ويسعيان للبحث عن إيجاد جهات تمولها في سبيل القيام بالأعمال الإجرامية واستقطاب أعضاء جدد لاستمراريتهما.

ثانيا: أوجه الاختلاف

- يختلفان في الهدف غاية الجريمة المنظمة استخدام العنف لكسب المصالح الشخصية سياسية أو مادية اقتصادية [1].
- توفر عنصر الاستمرارية والجماعة على عكس الإرهاب الذي يمكن أن يرتكب في إطار فردي
- ترتكب الجريمة المنظمة بالسرية أما الإرهاب الالكتروني فهو عن طريق الإعلام[2].
- اعتراف الدولة بارتكاب من خلال التفاوض مع المجرمين على عكس الجريمة المنظمة لا تتفاوض مع مجرميها.

ثالثا: آثار العلاقة بين الإرهاب الالكتروني والجريمة المنظمة

لقد أدى تنامي العلاقة بين جماعات الإرهاب وعصابات الجريمة المنظمة إلى زيادة قدراتهما المادية والفنية حتى أصبحت بعض الدول عاجزة عن مواجهتها والحد منها وأدت العلاقة بينهما إلى وجود التعاون والتنسيق بين الشبكات الإرهابية وعصابات الجريمة المنظمة كقيام عصابات الجريمة المنظمة بتزويد الشبكات الإرهابية بالجوازات وبطاقات الهوية المزورة وتمويلها بما تحتاج إليه من معلومات[3].

المبحث الثاني: قيام جريمة الإرهاب الالكتروني وآثارها

إن تحقق الجريمة على الواقع الميداني لا يقوم إلا بتحقيق كافة الأركان الخاصة بها وهي التي تحدد نطاق الجريمة وتفصلها عن غيرها من الجرائم وتنطوي على تبيان أهم الأركان الركن

[1] – عمراني كمال الدين ،**الجريمة المنظمة وجريمة الإرهاب– دراسة مقارنة– (مجلة الفقه والقانون عدد 17، 2014)**، المركز الجامعي، النعامة، ،ص:103

[2] – هروال هيبة نبيلة ،مرجع سابق، ص:،329

[3] – إسراء طارق جواد كاظم الجابري ،**جريمة الإرهاب الالكتروني– دراسة مقارنة– (شهادة الماجستير، القانون العام)** ،كلية الحقوق، جامعة النهرين، العراق،2012 ص:51.

الشرعي الذي يقتضي التجريم القانوني للفعل الإجرامي والأفعال المادية التي ترتبط بإرادة مرتكب الفعل وقصده التام في إتيان هذه الأفعال على أنّها فعل إجرامي يعاقب عليها القانون.

وبما أن جريمة الإرهاب الالكتروني فعل مجرم يهدف إلى نشر الخوف والرعب ويكون لها تأثيرها ونتائجها، وأصبح يمثل بجميع أشكاله تهديدا وخطرا للسلام والأمن الدوليين نظرا لما له من أثار وخيمة على أمن المواطنين واستقرارهم وعلى الإمكانيات الاقتصادية والهيبة السياسية للدولة في محيطها الإقليمي والدولي.

وسنتناول في هذا المبحث أركان جريمة الإرهاب الالكتروني(المطلب الأول)، وآثارها (المطلب الثاني).

المطلب الأول: أركان جريمة الإرهاب الالكتروني

لكل جريمة أركانها الخاصة بها أي عناصر معينة حددها التشريع للعقاب وإن انتفى أحدهما لا تكون قائمة وهذه الأركان مستمدة كلها في النهاية من النظرية العامة للتجريم، وأركان الجريمة هي التي تقوم بتحديدها وترسم حدودها الفاصلة وتفصلها عن غيرها من الجرائم.

ولجريمة الإرهاب الالكتروني ثلاث أركان:

أولها ركن شرعي الذي يتمثل في النص القانوني الذي يجرم هذا الفعل – جريمة الإرهاب الالكتروني – ونجد المشرع الجزائري جرم بعض الأفعال إذا ارتكبت لغرض إرهابي في نص المادة 87 مكرر وأعطى لها وصف إرهاب الكتروني[1].

وثانيها ركن مادي عبارة عن المظهر الخارجي للنشاط الجاني ووسائل تنفيذ الجريمة باستخدام الوسائل الالكترونية.

وثالثا ركن معنوي يتمثل في القصد الجنائي أي العلم بموضوع جريمة الإرهاب وارادة الدخول فيه[2].

[1] – عمد المشرع الجزائري على تحديد الركن الشرعي لظاهرة الارهاب و المتمثلة في النصوص القانونية التي تجرم كافة السلوكيات لهذه الظاهرة سواء في قانون العقوبات او في قوانين خاصة.

[2] – مصطفى سعد حمد مخلف، **جريمة الإرهاب عبر الوسائل الإلكترونية دراسة مقارنة بين التشريعين الأردني والعراقي،(شهادة ماجستير، القانون العام)**، كلية الحقوق، جامعة الشرق الأوسط، 2017 ،ص: 42 ،

وهذا ما سنتطرق إليه في هذا المطلب الركن المادي للجريمة في الفرع الأول وفي الفرع الثاني الركن المعنوي لجريمة الإرهاب الالكتروني.

الفرع الأول: الركن المادي لجريمة الإرهاب الإلكتروني

يعرف قانون العقوبات ركن الجريمة المادي ويحدد عناصره في نص عام اعتمادا منه على تحديد العناصر الخاصة لكل جريمة[1]، فالركن المادي للجريمة هو الفعل خارجي له طبيعة ملموسة ولا توجد جريمة بدون ركن مادي. وهو النشاط الإجرامي كاستعمال القوة والعنف ضد الأشخاص أو الأموال أو الممتلكات العامة والخاصة وترتكب عادة بوسائل معينة مثل الأسلحة النارية والوسائل الإلكترونية والحاسب الآلي والانترنت والتي من شأنها أن تحدث دمارا واسعا[2].
الركن المادي يقوم على ثلاث عناصر السلوك النتيجة والرابطة السببية[3]

يتكون الركن المادي للجريمة من ثلاثة عناصر أساسية تتمثل مترابطة فيما بينها ولابد من اجتماعها[4]، وتتمثل في السلوك الإجرامي النتيجة الإجرامية وهي الآثار القانونية الذي يترتب على السلوك ثم علاقة سببية تربط بين الفعل والنتيجة فإذا اكتملت هذه العناصر كما نص عليها القانون تسمى جريمة تامة. ولكن أحيانا لا تكتمل عناصر الركن المادي فقد يبدل الجاني نشاطه ويأتي سلوكا إجراميا دون أن تترتب عليه النتيجة وهو ما يسمى بالجريمة الناقصة أو ما يعبر عنه بالشروع. [5]

أولا: السلوك الإجرامي

هو النشاط المادي صادر من الجاني بصفة اختيارية ويحدث آثارا في العالم الخارجي ويعاقب عليه القانون وهو نوعان سلبي يتحقق في حالة الامتناع عن فعل أو قول يأمر عليه

---

[1] – محمد أمين الرومي ،**جرائم الكمبيوتر والانترنت**، دار المطبوعات المطبوعات الجامعية، د.ط،الإسكندرية مصر، 2003 ،ص: 182.

[2] – محمد فهاد الشلالده ،احمد حسن ابو جعفر ،**إشكالية التوسع في تهم الإرهاب في المنطقة بدوافع سياسية**،(مجلة دراسات شرق أوسطية العدد 72 2015) الأردن، ص: 37.

[3] – محمد حسن مرعي، **الجوانب الموضوعية لجريمة اثارة الفتنة الطائفية دراسة تحليلية مقارنة** المركز العربي للنشر والتوزيع ،ط1، القاهرة ،2018 ،ص: 24.

[4] – خلفي عبد الرحمن، **محاضرات في القانون الجنائي العام**، دار الهدى ،د.ط ،عين مليلة– الجزائر، 2012، ص: 102.

[5] – مصطفى سعد حمد مخلف، مرجع سابق، ص:43.

القانون وايجابي قيام بفعل يجرمه القانون ويؤدي إلى إحداث نتيجة في الجرائم، يعتبر سلوكا إجراميا في ذاته ولا يعتد القانون بالوسائل المستعملة سواء معنوية في ارتكاب السلوك الإجرامي[1] بما أن المشرع الجزائري جرم فعل الإرهاب الإلكتروني في نص المادتين 87 مكرر 11 و87 مكرر 12 يمكن استخلاص السلوكيات الإجرامية المكونة للركن المادي.

تنص المادة 87 مكرر 11 ق ع ج".. **كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر من دولة لأخرى بغرض ارتكاب أفعال إرهابية أو تدريبها او الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريبا عليها**

و يعاقب بنفس العقوبة كل من:

- **يوفر او جمع عمدا أموالا بأي وسيلة وبصوره مباشرة وغير مباشرة بقصد استخدامها بأن أو علمه بأنها تستخدم في تمويل أشخاص إلى دولة أخرى بغرض ارتكاب الجرائم المذكورة في الفقرة الأولى من هذه المادة**
- **قام عمدا بتمويل او تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو الإعداد لها او المشاركة فيها او التدريب على ارتكابها او لتلقي التدريب عليها أو تسهيل ذلك السفر**
- **يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في المادة "**[2]

ونجد من خلال هذه المادة قام المشرع بتجريم جملة من الأفعال وتتمثل في:

فعل السفر باستخدام تكنولوجيا الإعلام والاتصال لارتكاب أفعال إرهابية أو التدريب عليها، ونجد المشرع الجزائري اشترط في الفقرة الأخيرة استخدام التكنولوجيا الإعلام والاتصال في ارتكاب هذا الفعل حتى يتغير شكل الجريمة من الإرهاب التقليدي إلى جريمة الإرهاب الالكتروني.

وعليه فإن السلوك الإجرامي في جريمة الإرهاب الإلكتروني يتم من خلال جهاز الكمبيوتر وباستخدام المعالجة الآلية للمعلومات ويظهر هذا السلوك بشكل واضح في صور الجريمة

[1] – منصور رحماني، **الوجيز في القانون الجنائي العام**،دار العلوم للنشر والتوزيع،د.ط، ،عنابة،2006، ص ص: 98-99

[2] – الامر 66-156 المتضمن قانون العقوبات المعدل و المتمم

المتعددة باستخدام الاعتداء على أنظمة المعالجة للمعطيات، ويتم هذا الاعتداء بالدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات والاعتداء العمدي على نظام المعالجة[1].

أ- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية:

يكون الدخول غير المشروع في النظام دون العبث به أو تغييره أما البقاء غير المشروع فهو يتم بحذف او تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروع او تخريب نظام يشتغل المنظومة وهو الأمر الأكثر شيوعا في الجريمة الإرهاب الإلكتروني وينتج عن هذا الفعلين أن يتم محو أو تحويل وتغيير المعطيات التي يحتويها النظام أو تخريبه.

وبالرجوع إلى المشرع الجزائري فقط حدد العقوبة القانونية لكل من الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات وحدد غرامة مالية لكل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات او يحاول ذلك وهذه هي العقوبة إذا تم حذف او تغيير هذه المعطيات فهذه العقوبة تتضاعف.[2]

وتجدر الإشارة أن جريمة الدخول غير مصرح به للمعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة ويكفي الوصول إلى المعلومات المخزنة داخل النظام بسبب مجرد الوصول إليها تقوم الجريمة يرتكب فعل الدخول بأي طريقة او وسيلة كانت لأن المشرع الجزائري لم يحدده[3].

ب- الاعتداء العمدي على المعطيات:

يتمثل السلوك الإجرامي في هذا الاعتداء في فعل العرقلة وتعطيل وإفساد نظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظم منه القيام به وقد نص المشرع الجزائري في قانون

---

[1] – شعنبي صابرة ،مرجع سابق ،ص:90

[2] – المادة 394 مكرر ق ع التي نصت على:" **يعاقب بالحبس من ثلاثة أشهر الى سنة وبغرامة من 50.000 دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك.**

تتضاعف العقوبة اذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة(6) اشهر الى سنتين والغرامة من 50.000دج الى 150.000دج". الامر 66-156 المتضمن قانون العقوبات المعدل و المتمم.

[3] – شعنبي صابرة، مرجع سابق ،ص:92

العقوبات على الاعتداءات التي تتم عمدا على نظام المعالجة الآلية وحدد العقوبة وهذا ما جاء في نص المادة 394 مكرر 2 التي نصت على مايلي:

" **يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1.000.000دج** إلى **5.000.000دج/ كل من يقوم عمدا وعن طريق الغش بما يأتي:**

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة او معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم المنصوص عليها في هذا القسم.

–حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم".[1]

وبما أن السلوك الإجرامي لجريمة الإرهاب الإلكتروني يتطلب وجود بيئة رقمية واتصال بشبكة الإنترنت فهو يتخذ صورا متنوعة مسايرة للتقدم التكنولوجي ومن بين هذه الصور نذكر منها[2]:

- **تدمير المواقع والبيانات والأنظمة الالكترونية:** تتمثل هذه الصورة في قيام الإرهابيين والمنظمات الإرهابية بالقيام بهجمات من خلال شبكة الإنترنت تستهدف تدمير المواقع والبيانات والنظم الالكترونية المتعلقة بالمؤسسات العامة والخاصة وإلحاق الضرر بالبنى التحتية وتدميرها. وهذا من خلال الدخول غير المشروع التي تكون متصلة بشبكة الانترنت أو ما يعرف بنظام PC serveur بهدف تخريب أو تعطيل نقطه الاتصال أو النظام.
- **التجسس الالكتروني:** وهو عبارة عن سرقة المعلومات من الأفراد والمؤسسات العامة والخاصة والدول والمنظمات من اجل معرفه الحالة الاقتصادية والمالية والسياسية التي تعيشها الدولة ثم استغلالها من طرف المنظمات الإرهابية للقيام بعمليات إرهابية أو بيعها لدول معادية للدول المستهدفة ويستخدم في ذلك طرق تجسس مستعملة في ذلك أسلوب الاستيلاء على المعلومات الحساسة الهامة عن طريق إنفاق الرسائل الإلكترونية مجهولة المصدر ببرامج وتطبيقات إلكترونية من أجل فتح ثغرات إلكترونية في حاسوب الضحية أو الشبكة الالكترونية المستعملة من طرفه.
- **إنشاء مواقع الكترونية إرهابية** تتمثل في إنشاء وتصميم المنظمات الإرهابية لمواقع الكترونية لهم على شبكة الانترنت من اجل الوصول إلى اكبر شريحة من الناس للتأثير عليهم

[1] – الامر 66–156 المتضمن قانون العقوبات المعدل والمتمم.

[2] – محمد خميخم، مرجع سابق، ص: 35

فكريا ونفسيا ثم تجنيدهم أو الاستفادة منهم ماليا عن طريق التحويلات المالية التي يقدمونها تضامنا مع هذه التنظيمات أو الاستفادة من هذه المواقع لأجل التدريب أو صناعة متفجرات أو شرح طرق اختراق البريد الالكتروني أو الدخول إلى مواقع محجوبة وصناعه الفيروسات ونشرها.

- **التهديد والترويع الإلكتروني:** يتم استعمال المواقع الالكترونية من خلال اللجوء إلى التهديد والوعيد بقتل شخصية السياسية والدينية ومؤثره في المجتمعات أو التهديد بتفجير منشآت الحيوية والإستراتيجية في الدولة أو التهديد بتعطيل او إتلاف الأنظمة الالكترونية للمنشآت القاعدية وإلحاق الضرر والدمار بالشبكات الالكترونية والأنظمة المعلوماتية عن الابتزاز وطلب الأموال[1].
- **شن الهجمات الإلكترونية:** وذلك باختراق مواقع هامة أو تنفيذ عمليات تجسس أو تدمير بنى تحتية عبر استخدام الفيروسات والبرامج الخبيثة المختلفة[2].

ثانيا: النتيجة الإجرامية

هي الأثر الخارجي الذي يتجسد فيه الاعتداء على حق يحميه القانون فالجرائم الإرهابية من الجرائم ذات النتيجة قتل تعذيب اختطاف وتشكيل المنظمات في السلوك يكون بنتيجة يجرمها القانون وتكون مقترنة بالنشاط الزمان المكان[3].

فالنتيجة الجرمية هي العنصر الثاني من عناصر الركن المادي بعد السلوك الإجرامي ويمكن تعريفها بأنها التغيير الذي يحدثه السلوك الإجرامي في العالم الخارجي وينال مصلحة او حقا قدر الشارع جدارته بالحماية الجنائية[4]، والأثر الذي يترتب على السلوك الإجرامي المتجسد الذي يقع على المصلحة التي يحميها القانون[5]. وتثير مسألة النتيجة الإرهابية الإجرامية عدة مشاكل فالأثر المادي للمجرم الإرهابي كإنشاء موقع أو تصميم موقع يحث على الانضمام إلى

---

[1] محمد خميخم، مرجع سابق، ص: 36

[2] –عبد القادر دندن وآخرون، العلاقات **الدولية في عصر التكنولوجيات الرقمية تحولات عميقة مسارات جديدة**، مركز الكتاب الأكاديمي ،ط1،عمان ،2021، ص: 147

[3] – هيثم فالح شهاب،مرجع سابق ص:89

[4] – حسين عبد الصاحب، عبد الكريم الربيعي، **جرائم الاعتداء على حق الإنسان في التكامل الجسدي– دراسة مقارنة ،(أطروحة الدكتوراه، القانون)**، كلية القانون جامعة بغداد، 2005، ص: 97

[5] – محمد علي سويلم ،**جرائم الإرهاب والإرهاب الالكتروني –دراسة مقارنة**،المصرية للنشر والتوزيع،ط1 ،القاهرة،2018 ،ص:85.

المجموعات الإرهابية[1]. كما يترتب على سلوك المجرم بأن يؤدي العمل الإرهابي إلى تحقيق أحد مظاهر الرعب وتنقسم فيه إلى جرائم الضرر وجرائم الخطر[2].

تتحقق النتيجة الإجرامية في جريمة الإرهاب الإلكتروني متى كانت هناك حالة خطر والخوف في نفوس الأفراد أي من شأنه المساس بالاستقرار الذي يعيشه الناس داخل مجتمعهم وهذا مثل ما نص عليه المشرع في نص المادة 87 مكرر من قانون العقوبات الجزائري أو من شأن الفعل الإجرامي أن يؤدي إلى حدوث ضرر جسيم مثل الإضرار بالبنية التحتية الإستراتيجية للدولة أو المساس بالمؤسسات العامة أو الخاصة أو تدميرها أو تعطيلها عن العمل وهذا بالاعتماد على شبكة الانترنت أي وجود بيئة رقمية مرتبطة بالشبكة المعلوماتية[3].

جريمة الإرهاب الالكتروني من جرائم الضرر الجرائم التي تتطلب حصول نتيجة معينة في بعض الأحيان نرى في بعض التشريعات المختصة بمكافحة الإرهاب ذكرت ذلك مثلها مثل جرائم إنشاء موقع على شبكة الإنترنت والشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعات إرهابية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصال بين القيادة والتنظيم وما شابه ذلك من أفعال تتطلب نتائج إجرامية في السلوك الإرهابي إذن قد أصبح سلوكا متطورا ومفضيا إلى نتائج خطيرة بعد اعتماد الكثير من الأنشطة الحكومية وغير الحكومية على الحاسوب والانترنت في تسيير أعمالها ومصالحها ومن هنا أصبحت الأضرار كثيرة وتتجلى في صور خطيرة ومختلفة منها التلاعب في أنظمة تشغيل إطلاق صواريخ الإستراتيجية الكهرباء والماء وشبكة الاتصال والأنظمة المصرفية والبورصة هذا السلوك الإجرامي بلا شك يعد سلوكا إرهابيا لا تختلف نتائجها عن نتائج الإرهاب التقليدي وهو بلا شك من جرائم الضرر أيضا[4].

---

[1] – محمد محمود مدين، **فن التحقيق و الإثبات في الجرائم الالكترونية**، المصرية للنشر و التوزيع،ط1،القاهرة ،2020 ،ص: 35

[2] – موفق عيد فهد المساعيد، **جرائم الإرهاب في التشريع الأردني والاتفاقيات الدولية** ،مركز الكتاب الاكاديمي،ط1 ،الاردن، 2019 ،ص ص: 49 –50

[3] – محمد خميخم، مرجع سابق، ص: 36

[4] – صدام حسين ياسين العبيدي، **جرائم الانترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية**، المركز العربي للدراسات والبحوث العلمية،ط1، القاهرة 2019، ص: 234

ثالثا: العلاقة السببية

تمثل العلاقة السببية العنصر الثالث والأخير من عناصر الركن المادي في جريمة الإرهاب الالكتروني حيث لا يكتمل هذا الركن إلا إذا قامت علاقة ما بين فعل الإرهاب الإلكتروني هو تحقق النتيجة والمتمثلة في إيجاد حالة من الخوف والذعر بين الأفراد والإخلال بالأمن العام أو البنى التحتية الإستراتيجية للدولة [1].

ويقصد بالعلاقة السببية بين الفعل المجرد والنتيجة الإجرامية للصلة الموجودة بينهما وتقوم هذه الرابطة السببية في جريمة ماء عندما تكون النتيجة الواقعة محتملة الوقوع وفقا للسير العاجل للأمور، وللعلاقة السببية أهمية بالغة تكمن في الركن المادي في كل جريمة فيها تتقرر مسؤولية الجنائية[2].

فإذا انقطعت العلاقة السببية انتفت المسؤولية الجنائية باعتبار أنها احد عناصر الركن المادي وتقتصر على فئة واحدة من الجرائم وهي الجرائم ذات النتيجة او الجرائم المادية ويستثنى من ذلك الجرائم الشكلية كون أنه لا يدخل في ركنها المادي ضرورة توافر نتيجة إجرامية معينة وعدم وجود نتيجة للفعل بطبيعته لا يطرق محل للبحث عن العلاقة السببية[3].

بما أن جريمة الإرهاب الالكتروني من الجرائم الشكلية فانه لا يثور في شانها العلاقة السببية حيث لم يستلزم المشرع في نموذجها الإجرامي تحقيق النتيجة الجرمية لقيام ركنها المادي بمجرد استخدام البيئة الافتراضية وإنشاء مواقع حسابية باستخدام بريد الكتروني لتسهيل عملية السفر أو تمويل منظماتها الإرهابية أو استقطاب واستدراج أشخاص إلى جماعتها من اجل ارتكاب إعمال إرهابية فهي تشكل جريمة تامة حتى وان لم تتحقق النتيجة أي عدم وصول المجرم الإرهابي إلى تحقيق السلوكيات الواردة في نص المادة 87 مكرر 11 و87 مكرر 12 من الأمر 66 –156 المتضمن قانون العقوبات المعدل والمتمم.

الفرع الثاني: الركن المعنوي

[1] – محمد خميخم، مرجع سابق، ص:37

[2] – شعنبي صابرة مرجع سابق ص 104

[3] – خلفي عبد الرحمن ،**القانون الجنائي العام دراسة مقارنة**، دار بلقيس للنشر، الدار البيضاء،د.ط، الجزائر، 2016 ص: 203.

الركن المعنوي هو العلاقة التي تربط بين مادية الجريمة وشخصية الجاني وجوهر هذه العلاقة هو الإرادة ومن ثم فهي ذات طبيعة نفسية أي أن المسلك الذهني والنفسي هو الأساس في تكوين الركن المعنوي لجريمة الإرهاب الإلكتروني[1].

فالركن المعنوي للجريمة بشكل عام يمثل الجانب الشخصي أو النفسي للجريمة فلا تقوم الجريمة بمجرد قيام الواقعة المادية ولا تخضع لسبب من أسباب الإباحة بل يجب أن تصدر هذه الواقعة عن إرادة فاعلها وترتبط بها ارتباطا معنويا حيث يمكن ان يقال بان الفعل هو نتيجة لإرادة الفاعل وبالتالي قيام هذه الرابطة التي تعطي للواقعة وصفها القانوني وتوصف بالجريمة ويصعب تحديد الركن المعنوي لجريمة الإرهاب الإلكتروني في أن الدوافع الذهنية أو النمطية المرتبطة بنفسية المجرم المعلوماتي هي التي ترسم معالم الركن المعنوي.

وبالتالي فان الركن المعنوي لهذه الجريمة يقوم بقصد عام وقصد خاص وسوف نتطرق اليه في ما يلي:

أولا: القصد الجنائي العام

يعبر القصد الجنائي عن إرادة الجاني في مخالفه المسار القانوني على النحو الصحيح الذي رسمه المشرع لم يتم تعريف القصد الجنائي في قانون العقوبات الجزائري صراحة بل تم الإشارة إليه بشكل ضمني في كثير من مواده، وذلك من خلال اشتراط توافر العمد لدى الجاني عند ارتكابه الجريمة وقد ترك المجال للفقه للقيام بتعريف القصد الجنائي فأعطوه تعريفات عديدة يتمحور مضمونها حول نقطتين تتمثلان في اتجاه إ رادة الجاني إلى ارتكاب الجريمة مع ضرورة العلم بكافة أركانها القانونية، و إذا تحقق العلم والإرادة لدى الجاني قام القصد الجنائي وإذا انتفى أحدهما أو كليهما انتفى قصد الجاني[2].

1- تعريف القصد الجنائي العام

[1] – إبراهيم بن محمد محمود الزنداني، **الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة**، جامعة فطاني،ط1 ،تايلند 2018، ص:35.

[2] – عبد الله سليمان، **شرح قانون العقوبات الجزائري-الجريمة-القسم العام** ، ديوان المطبوعات الجامعية ط1،الجزائر،2005، ص:249

اكتفى المشرع الجزائري بالإشارة إليه ضمنيا فقط وذلك من خلال إدراج كلمة العمد في كثير من النصوص القانونية الدالة على قصد ونية الجاني التي تنعكس مباشرة على الجريمة التي يرتكبها الجاني وإرادة تحقيق النتيجة[1].

للقصد الجنائي مرادفات عديدة، حيث يطلق عليه تسمية الخطأ المقصود أو العمدي كذلك تسمية القصد العمدي وكل هذه المصطلحات لها نفس معنى القصد الجنائي، وهو يُعرف على أنه علم الجاني علمًا يقينًا بالعناصر المكونة للجريمة مع إرادة تامة بتحقيق الواقعة الإجرامية وقبولها[2].

والاجتهاد الفقهي لم يقصر في إعطاء تعريف للقصد الجنائي حيث يدور حول نقطتين أساسيتين، رغم التعريفات المتعددة التي قدمت وتتمثل هذه النقطتين في علم المجرم بعناصر الجريمة وإرادة متجهة بتحقيق هذه العناصر[3].

2-عناصر القصد الجنائي العام

للقصد الجنائي العام عنصرين جوهريين يتمثلان في العلم والإرادة ولابد من توافرهما لقيام القصد الجنائي لدى المجرم لا يمكن الاستغناء عنهما لا على العلم ولا عن الإرادة[4].

- **العلم**

العلم في قانون العقوبات معناه توافر اليقين لدى الجاني بان سلوكه يؤدي إلى نتيجة إجرامية يعاقب عليها قانونا مع علمه بجميع العناصر القانونية للجريمة[5]، فإذا انتفى العلم بأحد هذه

[1] – خلفي عبد الرحمن ،**القانون الجنائي العام دراسة مقارنة**، مرجع سابق،ص:216

[2] – عبد القادر عدو، **قانون العقوبات الجزائري القسم العام –الجريمة–نظرية الجزاء الجنائي**، دار هومة للطباعة و النشر ،،د.ط ،الجزائر،2010، ص:181

[3] – بلعليات ابراهيم، **أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري–أركان الجريمة، اهمية الإثبات الجنائي،طرق الإثبات الجنائي**، دار الخلدونية للنشر و التوزيع،د.ط ،الجزائر،2007، ص:119

[4] – غازي حنون خلف الدراجي، **استظهار القصد الجنائي في جريمة القصد العمد** منشورات الحلبي الحقوقية، ط1، ،لبنان،2012، ص:23.

[5] – بلعليات ابراهيم،مرجع سابق ،ص:120

العناصر انتفى القصد الجنائي لأنها هي التي تمد النشاط الإجرامي الوصف القانوني بالتالي تميزها عن باقي الوقائع الإجرامية الأخرى[1]

- **الإرادة**

الإرادة هي العنصر الثاني للقصد الجنائي بعد العلم وهي قوة نفسية توجه كل أو بعض أعضاء الجسم لتحقيق غرض غير مشروع، وبانتقاء الإرادة ينتفي القصد الجنائي[2].

فالإرادة تنصب على السلوك الإجرامي والنتيجة المعاقب عليها فيجب أن تتجه إرادة الجاني إلى تبني السلوك الإجرامي فهي حلقة الوصل بين الجريمة بوصفها واقعة مادية لها كيانها والفاعل الذي صدر عنه السلوك وأراد تحقيق نتيجته[3]، باستخدام الوسائل الإلكترونية والذي يهدف إلى إثارة الرعب والخوف بين الناس وتعريض سلامة المجتمع للخطر، وإلقاء الرعب ما بين الناس وترويعهم، وتعريض حياتهم للخطر.

ونخلص مما سبق بأن القصد الجنائي العام لجريمة الإرهاب الإلكتروني، هو أن يعلم الجاني بعناصر فعله، وبطبيعة الوسيلة التي يستخدمها بتلك الأفعال، ودورها في إحداث الذعر العام والتخويف، وانصراف إرادته إلى إتيان ذلك الفعل مع علمه بما يحدث إلى ذلك.

ثانيا: القصد الجنائي الخاص

تشترط جريمة الإرهاب الالكتروني لقيامها قصدا خاصا إضافة للقصد العام السابق الذكر، ويتمثل القصد الخاص في غاية معينة يتطلبها القانون وان يكون الفعل المادي المكون للجريمة قد ارتكب في سبيلها، فإذا كان لكل فعل غاية فإن اعتداد القانون بغاية محددة أن تتجه إليها إرادة الفاعل يجعل منها قصدا ويتميز القصد في جريمة الإرهاب أن له طابع مميز وهام ويعتبر من خاصية هذا النوع من الجرائم ألا وهو الغرض من ارتكابها. [4]

[1] – عبد القادر عدو، مرجع سابق، ص:182

[2] – بلعليات ابراهيم،مرجع سابق ،ص:121

[3] – أمير فرج يوسف –**مكافحة جريمة الارهاب الالكتروني** ،مرجع سابق ،ص:165

[4] – يوسف مرين، **جريمة الارهاب في القانون الجزائري**،(مجلة جامعة القدس المفتوحة للابحاث و الدراسات،عدد 42-02، 2017).ص:314

يتمثل هذا القصد بنيه إجرامية خاصة تتعلق أساسا بالنتيجة الإجرامية ويتضح مدلوله من خلال الحالات التطبيقية اعتمادا على كل جريمة بسبب مستقل وهي تتطلب عناصر ذاتيه مجدده تتجاوز القصد العام[1].

وعليه فالقصد الخاص في جريمة الإرهاب الالكتروني هو الغاية او الغرض من ارتكاب السلوكيات السالفة الذكر ونص المشرع على الأفعال الإرهابية في نص المادة 87 مكرر من قانون العقوبات الجزائري.

[1] – بخاري جميل علي، **جريمة الإرهاب الدولي ومشروعية نضال حركات التحرر الوطني إقليم كردستان**، المركز العربي للنشر والتوزيع ،ط1، مصر،2020 ،ص:355

المطلب الثاني: آثار جريمة الإرهاب الالكتروني

تعد الآثار دائما نتائج لأسباب معينة وأيضا تدل عليها، بمعنى أن النتيجة هي مجموعة من الأسباب التي تفاعلت وأفرزت هذه النتيجة ومن خلال النتائج يمكن الوصول إلى الآثار. وتحديد مفهوم الآثار له أهمية لبيان خطورة الموضوع محل الدراسة وأبعادها على الحياة الإنسانية في جميع جوانبها وتأثيرها على القواعد التي تنظم حياة المجتمعات على المستويين الوطني والدولي وخطورة الجرائم الإرهاب الالكتروني بلغت مستوى كبير من القسوة والفظاعة وما يزيد من هذه الخطورة التطور التكنولوجي للفضاء الالكتروني[1].

و سنتطرق إلى دراسة آثار الإرهاب الالكتروني على مستوى امن وسلم الدول(الفرع الأول) وعلى آثاره في العلاقات الدولية (الفرع الثاني).

الفرع الأول: آثار الإرهاب الإلكتروني لأمن وسلم الدول

تفاقمت ظاهرة الإرهاب الإلكتروني في الآونة الأخيرة وأثرت سلبا على امن الدول في مختلف الميادين حيث تستطيع الجماعات والمنظمات الإرهابية من خلال تدمير البنية المعلوماتية وتحقيق آثار تفوق الآثار التي استخدمت فيها المتفجرات بالمؤسسات المالية وأجهزة الاتصال التي تعتمد بشكل كبير على الإنترنت والذي يؤدي بدوره إلى تعطيل المحركات الرئيسية للدولة والإضرار بالمواطنين وأمنها القومي[2]، ويواجه تأثير الإرهاب الالكتروني على الأمن والسلم تحديات كثيرة نذكر منها:

1-إمكانية استخدامها للأنظمة والشبكة المعلوماتية-تحديات زيادة الاستخدام والانتشار

إن العامل الأساسي وراء تدمير الشبكة هو عدم تحديث البنية التحتية الحالية بعدما صارت قاصرة أمام استيعاب متطلبات التحميل المتزايد والمشتركين وما بفرضه من تحديات أمام التحرك لمد سعة الانترنت لتدمير البنية التحتية الإلكترونية التي تعتمد عليها الحكومات

[1] – عمراني كمال الدين، **السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة،(أطروحة دكتوراه،قانون جنائي)**،قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2012 ، ص98

[2] – عادل عبد الصادق ،**الارهاب الالكتروني القوة في العلاقات الدولية:نمط جديد و تحديات مختلفة**،المركز العربي لأبحاث الفضاء الالكتروني،ط2، القاهرة،2016،ص ص:160

والمؤسسات العامة والشركات الاقتصادية الكبرى وهناك ما يشير إلى إمكانية انهيار البنية التحتية للأنظمة والشبكات المعلوماتية في العالم الالكتروني تستهدف من خلال:

- الهجمات من جانب المستخدمين والزبائن
- هجمات تستهدف الرسائل والأجهزة الجوالة
- شبكات بوتنينس الموجه لاستبعاد الكومبيوترات والتحكم فيها كآلات طيعة
- تهديدات تستهدف نظم التعريف بالهوية بالموجات الراديويةRFID[1]

2- تهديد للكابلات البحرية

الإرهاب الالكتروني أصبح خطرا يهدد العالم بأسره نتيجة سهولة استخدامه للسلاح الرقمي فمثلا تسبب قطع الكيبل البحري الذي يربط بين يربط أوروبا بالشرق الأوسط في نهاية شهر جانفي عام 2008 وما أعقبه الانقطاع لكيبل الآخر القريب من ساحل دبي وخليج عمان حيث قدرت الخسائر المتولدة من ذلك التي لحقت بقطاع الاتصالات والتعاملات الالكترونية بمئات ملايين الدولارات[2].

3- القرصنة والاختراق تهديد لأمن الشبكة الدولية

تتم عملية الاختراق الإلكتروني لبيانات الدول عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت. وشهدت العديد من الدول التعرض لمثل هذه الهجمات إذ تم الكشف عن شبكة تجسس الكترونية في الصين تمكنت من اختراق 1295 جهاز كومبيوتر في 103 دول. وتم اكتشاف أجهزة تنصت على الكومبيوتر في سفارات الهند وكوريا الجنوبية واندونيسيا. [3]

[1] – عادل عبد الصادق ،**الارهاب الالكتروني القوة في العلاقات الدولية:نمط جديد و تحديات مختلفة**،المركز العربي لأبحاث الفضاء الالكتروني،ط2، مرجع سابق، ص:161

[2] – رقيق ايناس، **تأثير الإرهاب المعلوماتي على على بقاء ومستقبل بناء الدول (مجلة الحوكمة والقانون الاقتصادي– جامعة باتنة،عدد 1–2022)**، ص:48

[3] – عادل عبد الصادق ،**الارهاب الالكتروني القوة في العلاقات الدولية:نمط جديد و تحديات مختلفة**،المركز العربي لأبحاث الفضاء الالكتروني،ط2، مرجع سابق، ص ص:162–163

أولا: آثار الإرهاب الالكتروني على الأمن السياسي

إن تأثير تهديدات الإرهاب الالكترونية على الوضع السياسي للدول بدأ يتخذ منحا كبير على الصعيد الداخلي والخارجي إذ بدا هذا التأثير على المواقع الافتراضية والذي كان قبل فتره ينظر اليه انه ضعيف مخرجات وضيق التأثير على الوضع السياسي ولكن بعد التطورات التكنولوجيا بدا العمل الالكتروني يتخذ منحه مؤثر في الفضاء الواقعي خاصة عن الوضع السياسي للدوري غالبا ما يقوم من إنشاء أنظمة سياسية معارضة من خلال مواقع تنشر أخبار فاسدة وتبث بين الأفراد وتهدد شخصيات بارزة بالمجتمع.

وتعمل هذه المنظمات على إلحاق الشلل بالمنظمات القيادة والسيطرة والاتصالات او قطع الاتصال بين الوحدات والقيادات المركزية واختراق البريد الالكتروني لرؤساء الدول وكبار الشخصيات السياسية والاطلاع على أسرارهم ومعلوماتهم وبياناتهم ومثال على ذلك ما تداول قبل انتخابات 2018 في العراق ان هناك مجموعة من التسجيلات الصوتية تم اكتشافها من خلال المنصات التواصل الاجتماعي الفيسبوك لعملية شراء مقعد في مجلس النواب العراقي الذي يمكن قوله هنا تم الكشف تداخل خطير وتهديد العراقي الذي يتحكم في النظام الانتخابي المستحث من قبل المفوضية المستقلة للانتخابات في العراق[1].

سنة 2010 عرف باسم إعصار ويكيليكس اذ تم استغلال شبكة الانترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولة بين الإدارة الأمريكية وقنصليتها الخارجية بدول العالم.

في 2014 مارس هجمة مجموعة سايبر بيركوت الأوكرانية المواقع الالكترونية لحلف الناتو ما أدى إلى تعطيل مواقع الحلف لعدة ساعات كما أعلن الكرملين أن قراصنة حاسوب شنوا هجوما عنيفا على موقع الرئاسة الروسية وعطلوا العمل بموقع البنك المركزي الروسي وأقر مفتش وحدة الجرائم الالكترونية الأمريكي في أوت 2014 بأن قراصنة أجانب تمكنوا من اختراق حسابات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية

[1] – اسعد طارش عبد الرضا علي ابراهيم مشجل المعموري ،**الأمن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد العام 2003 (العراق، دراسات دولية، العدد 80 مجلد 2020 الصادرة في 31 يناير 2020)**جامعة بغداد ،ص ص:167-168

وفي ابريل 2015 عمل قراصنة روسيين على الاطلاع على رسائل الكترونية من الرئيس الأمريكي باراك اوباما اختراق الشبكة الالكترونية غير السرية للبيت الأبيض [1].

وفي عام 2017 تعرضت العديد من الدول لسلسلة من الهجمات الإلكترونية، حيث وقع أكثر من 45 ألف هجمة إلكترونية لأكثر من 99 دولة، وذلك وفاقا لخبراء في الأمن المعلوماتي، وأعلنت شركة" كاسبرسكاي لابسKaspersky Labs "، أن من ضمن الدول التي تعرضت لذلك الهجوم من خلل" الفيروس العالمي الذي يطلق عليه انتزاع الفدية Grab the " Ransom، في كل من بريطانيا، ألمانيا، تركيا، اليابان، الهند، مصر، الصين، فرنسا، إسبانيا، والفلبين، المكسيك، روسيا.

وفي عام2018 ، اتهم وزير الخارجية البريطاني جيريمي هانت الاستخبارات العسكرية الروسية بالوقوف خلف هجمات إلكترونية في جميع أنحاء العالم واستهداف وسائل إعلامية وسياسية كالدخول في الانتخابات الأميركية في عام 2016 بناء على نتائج المركز الوطني البريطاني للأمن السيبراني.
كما تعرضت بريطانيا في عام 2018 كذلك لهجمات الفدية، استهدفت قطاع الصحة، بهدف جمع الأموال، وقد اتهمت روسيا وكوريا الشمالية .سبق ذلك في عام 2012 تعرض شركة أرامكو السعودية لأكبر هجوم إلكتروني عندما تم تدمير أكثر من 30 ألف جهاز باستخدام فيروس شامون.

وفي نهاية عام 2020 تعرضت الولايات المتحدة لأكبر هجوم إلكتروني وأكثرها تعقيدا، وذلك عن طريق استخدام برنامج شركة سولار ويندز كقاعدة لاختراق جهات أميركية ذات طابع حساس، وقد شمل أكثر من 18 ألف عميل من عملاء الشركة حسب تصريح شركة مايكروسوفت، ووجهت الولايات المتحدة أصابع الاتهام إلى روسيا فيما رفضت موسكو هذا الاتهام[2].

[1] – رقيق ايناس،مرجع سابق ،ص ص:50-51

[2] – وفاء لطفي حسن عبد الواحد ،**الإرهاب الإلكتروني والأمن القومي في ظل جائحة كورونا (كوفيد-19) (المجلة العلمية لكلية الدراسات الاقتصادية و العلوم السياسية، المجلد 7 –العدد 13 جانفي2022)** ،ص: 454

أما أمنيا تعمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالحها، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة،وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[1].

ثانيا: آثار الإرهاب الإلكتروني الاقتصادية

مع تزايد نسبة الجرائم الإلكترونية والتنوع في طرقها لا شك أنها تلحق خسائر مادية كبيرة وفادحة أكثر مما تسببه الجرائم التقليدية مما يؤثر بشكل سلبي على الاقتصاد فمن نواجهه اليوم هو هجوم من أشخاص أو مجموعات أو منظمات مختلفة هدفها الرئيسي تحقيق بالإضافة إلى تحقيق الربح المادي الربح المالي.

ان اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، وتعطيل عمليات التحويل المالي، مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، وإلحاق الأذى بالاقتصاد الوطني، وتعديل ضغط الغاز عن بعد في أنابيب الغاز لتفجيرها، ونُظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، ومن أمثلتها قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد إختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات بطاقات الإئتمان من بعض أكبر مراكز التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات، وكذلك قيام بعض المنظمات الإرهابية بالعمل على تدمير اقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية وبيعها بالخارج بأسعار أقل من قيمتها مما أدى لإنهيار عملتها، ولتوفير تمويل لأعمالها الإرهابية في الدول التي تم بيع السندات فيها[2].

[1]عبدالله بن عبدالعزيز بن فهد العجلان، **الإرهاب الإلكتروني في عصر المعلومات"(المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت2-4 جوان 2008)**،القاهرة، ص22.

[2]-بوحادة سارة، مرجع سابق ص:13.

كما منيت عدد من الشركات والمصارف العملاقة بخسائر اقتصادية فادحة نتيجة القرصنة الإلكترونية التي واجهتها. فحسبما أشارت أحدث دراسة أجرتها مؤسسة B2B International وشركة كاسبرسكي لاب، والتي أعلنت عنها في الخامس عشر من أبريل 2015فإن 25 %من الشركات في منطقة الخليج تعتبر هجمات (DDoS) أحد أكبر ثلاثة تهديدات تواجه الشركات في المنطقة. وباعتبارها أحد أهم التقنيات الشائعة التي يستخدمها مجرمو الإنترنت لكسب الأموال، فإن عدد وتأثير هذه الهجمات يتزايد من عام لآخر وهو ما جعل قضية حماية المستخدمين أمراً أولوياً لدى الشركات.وقبل السادس من فبراير 2015، أكدت شركة "كاسبرسكي" الرائدة في مجال الأمن المعلوماتي أن مجموعة من "الهاكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار، إذ استخدموا تقنيات معقدة من أجل الوصول للحسابات، واستغل "الهاكرز" ثغرة بأنظمة أجهزة الحاسوب في المصارف تمكنوا خلالها من نسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية واستغلوها من أجل تحويل الأموال بسرعة فائقة[1].

ثالثا: آثار الإرهاب الإلكتروني الاجتماعية

يهدد الإرهاب الإلكتروني الحياة الاجتماعية والثقافية للمواطنين مثل توجيه المنظمات الإرهابية رسائلها للإعلام في المجتمعات التي تقوم بترويعها وإرهابها وذلك بهدف شن حملات نفسية ضد الدول المستهدفة[2]. ويؤثر الإرهاب الالكتروني على حياة المدنيين ورفاهيتهم وحتى ثقافتهم كالتالي:

– توجه المنظمات الإرهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول العدوة، فهي تعرض أفلاما مرعبة للرهائن والأسرى أثناء إعدامهم، مما يؤثر على المدنيين.

– اختراق صفحة إلكترونية لمستشفى وتهديد حياة المرضى فيه عن طريق التلاعب بأنظمة العلاج عن بُعد بهدفِ قتل المرضي، وأيضا في مصانع غذاء الأطفال لتغيير مستويات نسب المواد الغذائية بهدف قتل الأطفال.

[1]– رقيق ايناس مرجع سابق، ص:50.

[2]– وفاء لطفي حسن عبد الواحد ،مرجع سابق، ص:454.

– شن عمليات إرهابية على المواقع الحيوية، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، فمثلا في يناير 2008 تم قطع الكابل البحري الذي يربط أوروبا بالشرق الأوسط والكيبل القريب من ساحل دبي وخليج عمان، مما أدى إلى خسائر بقطاع الاتصالات والتعاملات الإلكترونية أو شل محطات إمداد الطاقة والماء، حيث تشير مصادر كلية الحرب الأميركية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين 70 إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية[1].

الفرع الثاني: آثار الإرهاب الالكتروني على العلاقات الدولية

ان الإرهاب الالكتروني ذو طابع دولي، وهو بذلك يشكل تهديدا على امن الدول ومنشأتها المختلفة وعليه فهو امتداد للجريمة العابرة للقارات حيث تبنت الجرائم الإرهابية عبر الوسائل الالكترونية في الآونة الأخيرة أشكالا ذات أثار ضارة على العلاقات الدولية وأصبحت تهدد الأمن والسلم الدوليين، ويتصور حدوث هذا إذا قامت شبهات اتجاه دولة ما بأنها قامت بإيواء وتجنيد الإرهابيين عبر الوسائل الالكترونية وتحريضهم ضد الدول عبر هذه الوسائل، فان العلاقة بينها وبين الدولة المتضررة من الإرهاب تتأثر سلبا، وتتوقف أو ربما تمتد إلى المقاطعة[2].

إن من آثار الإرهاب الإلكتروني التأثير على العلاقات الدولية على:

أولا: العلاقات الدبلوماسية الدولية

وذلك من خلال جمع المعلومات والتجسس وتسهيل النشاطات السرية في العلاقات الدولية، مثل عملية الاغتيالات، فتزايدت العلاقة بين التكنولوجيا والأمن وأصبح لا يعترف بالحدود الإقليمية أو العالمية ولقد أدت ظاهرة الإرهاب الإلكتروني إلى تحول جزء من العالم من الطابع المادي إلى عالم رقمي إلكتروني، حيث أصبح الفضاء الإلكتروني مجالا جديدا للتفاعلات الدولية سواء أكانت تفاعلات صراعية أم تعاونية.

[1]– بوحادة سارة، مرجع سابق ص:14

[2]–عمراني كمال الدين،مرجع سابق،ص:11.

ثانيا :التأثير على توازن القوى

أثر الإرهاب الالكتروني وبروز تهديدات الفضاء الإلكتروني على توازن القوى، وأثر بدوره على استراتيجيات الأمن القومي للدول، وكذا على طبيعة القوة بين الدول من جهة والشبكات والمنظمات الدولية من جهة أخرى، والسعي إلى الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني لمنع تعرض بنيتها التحتية والحيوية للخطر، ومن ثم دخول المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيت طبيعتها وأنماط استخدامها وطبيعة الفاعلين إضافة انه غير معنى وأهمية المفاهيم التنظيمية الرئيسية للعلاقات الدولية بما في ذلك الأمن والسيادة والقوة.

ثالثا: العلاقات الثنائية بين الدول والجهات الفاعلة

وقد أحدث الفضاء الإلكتروني آثارا وتغيرات على صعيد العلاقات الثنائية بين الدول وبين الجهات الفاعلة من خلال إعادة [1]:

- إعادة ترتيب التسلسلات الهرمية للقوة العسكرية والاقتصادية
- إعادة تحديد العلاقات الاقتصادية الدولية
- خلق أو حل المشكلات الدولية
- إنشاء موارد جديدة وتحالفات جديدة
- إنشاء ادوات وساحات جديدة للتعاون الدولي والمنافسة

رابعا: التأثير على المعلومات والأفكار والتصورات التي يقوم عليها النظام الدولي

وذلك انّ تكنولوجيا المعلومات عملت على تغيير المفاهيم والاستعارات الجديدة للعلاقات الدولية وتغيير المواقف العامة تجاه العديد من قضايا من القضايا كالصحة والبيئة وتقديم معلومات أساسية لدعم وظائف الرصد والتقييم والإبلاغ المرتبطة بأنظمة المعاهدات.

وتتميز القوة الإلكترونية بالتحرك في مسارات متداخلة، وتعمل على نقل عملية التأثير من وإلى الفضاء الإلكتروني، إذ يتمثل المسار الأول في انتقال الأحداث من أرض الواقع إلى الفضاء الإلكتروني أما لتصفية الصراعات وأما لاستخدامه لبت العنف والتحريض كذلك التأثير

[1]– عبد القادر دندن، مرجع سابق،ص ص: 105-106.

على العلاقات الدولية من حيث وقوع هذه الجرائم من دولة إلى الدولة أخرى وتعريضها للخطر نتيجة حدوث العمل الإرهابي في إقليمها، وتأثيره على مصالح دول أخرى كوقوعه على أعضاء السلك الدبلوماسي أو على وسائل نقل أجنبية أو على رعايا أو عدة دول[1].

[1]– عادل عبد الصادق، **الإرهاب قوة في العلاقات الدولية نمط جديد وتحديات مختلفة**، مركز الدراسات السياسية والاستيراجية ط1 ، المرجع السابق، ص44 .

ملخص:

يعتبر الإرهاب الالكتروني من أخطر الجرائم المستحدثة التي تهدد أمن الدول والشعوب، وهذا نظرا لتعدد أشكالها وتنوع أساليبها واتساع مجال أهدافها، مستفيدة بذلك مما وفرته تكنولوجيا الإعلام والاتصال والتقنية الحديثة، حيث يمكن ارتكابها عن بعد ودون اللجوء إلى العنف مع توفر قدر كبير من السلامة والأمان لمرتكبيها. وقد عرف مفهوم الإرهاب الالكتروني تعاريف ومفاهيم مختلفة فلا يوجد هناك اتفاق على تعريف قانوني جامع مانع للإرهاب الالكتروني في القانون الدولي، ويرجع ذلك إلى نظرة كل دولة لهذه الظاهرة، فالبعض يعتبره سلوكا إجراميا ويعاقب عليه، بينما البعض الآخر يعتبره مقاومة مشروعة.

كما أن هناك تداخل لمفهوم الإرهاب الالكتروني مع غيره من المفاهيم الأخرى وهذا مثل الإرهاب التقليدي، الجريمة المنظمة والجريمة الالكترونية. وتمتاز جريمة الإرهاب الالكتروني بعدة خصائص، وهذا مثل أنها من الجرائم العابرة للحدود، كما أنها ترتكب عن بعد ولا يتم اكتشافها إلا بعد فوات الأوان.

وتتخذ جريمة الإرهاب الالكتروني من الفضاء الإلكتروني مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها كما ذكرت سابقا، إلا أن ذلك لا ينفي عدم وجود تشابه بينها وبين الجريمة المرتكبة في العالم المادي، فهي مثلها مثل باقي الجرائم التي ترتكب، وبالتالي فلا بد لها من وجود الركنين المادي والمعنوي الذي تقوم عليهما كل جريمة.

الفصل الثاني: الجهود المبذولة مكافحة جريمة الإرهاب الالكتروني

المبحث الأول: الجهود الدولية والإقليمية المبذولة لمكافحة جريمة الإرهاب الإلكتروني

المبحث الثاني: الجهود المبذولة وطنيا لمكافحة جريمة الإرهاب الإلكتروني

في عالم مزدحم بشبكات اتصال دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية متباعدة باستخدام تقنيات لا تكفل للمعلومات أمنا كاملًا، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضرارا فادحة، يغدو التعاون الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمرا ضروريا، وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات. وتعزيز التعاون بينها واتخاذ تدابير فعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها، وسنتناول في هذه الدراسة الجهود المبذولة والآليات الامنية التي قام بها التعاون الدولي في مكافحة جريمة الإرهاب ومحاولة ردعها على الصعيد الإقليمي والدولي وكذلك الوطني.

ومن خلال هذه الدراسة سنقوم بتقسيم الفصل إلى مبحثين الجهود الدولية والإقليمية المبذولة لمكافحة جريمة الإرهاب الإلكتروني (المبحث الأول) الجهود الوطنية لمكافحة جريمة الإرهاب الالكتروني(المبحث الثاني).

المبحث الأول: الجهود الدولية والإقليمية المبذولة لمكافحة جريمة الإرهاب الإلكتروني

تميزت طائفة جريمة الإرهاب الالكتروني بتنوعها وظهورها بأشكال مختلفة ومعقدة، منها ما يمس حقوق ومصالح عامة للمجتمع، وما يمثل انتهاك لحقوق وحريات الأفراد، وأصبحت هذه الجرائم تشكل خطراً على الصعيدين الاقتصادي والقانوني، ناهيك عما تخلفه من تراجع وانهيار في مجال الاستثمار.

لذا كان من المتعين على المجتمع الدولي أن يتصدى ويكافح جريمة الإرهاب الإلكتروني بسن المزيد من التشريعات والقوانين العقابية والإجرائية التي تتناسب وخطورة هذه الجرائم ووضع المزيد من الضوابط اللازمة لمواجهتها، وخلق آليات قانونية للحماية من أخطارها، مع ضرورة أن تنصب هذه الجهود في عدة محاور منها تنظيم وحماية استخدام تقنية المعلومات من الجرائم والانتهاكات، وحماية البيانات المتصلة بالحياة الخاصة، حماية حق المؤلف على البرامج وقواعد البيانات، حماية البيئة التقنية ذاتها. وفي سبيل تحقيق ذلك مرت العملية التشريعية في مجال مكافحة الجريمة الالكترونية بالعديد من الجهود المتطورة على المستويين الغربي والعربي، ووضع نصوص عقابية وإجرائية رادعة، وهو ما سنبينه من خلال التقسيم التالي.

المطلب الأول: الجهود الدولية لمكافحة الجريمة الالكترونية

تنوعت الجهود الدولية في مكافحة الجريمة الالكترونية حيث تم اتخاذ العديد من الآليات والإجراءات للحد والتقليل منها إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى المعلوماتية والاستعمال اللامتناهي للكمبيوتر والانترنت وسنتطرق إلى إبراز هذه الجهود مع تبيان صعوبة التعاون الدولي للقضاء على هذه الجريمة الدولي العابرة للحدود لتعاون العديد من العوامل سيتم توضيحها لاحقا

الفرع الأول: المنظمات الدولية لمكافحة جريمة الإرهاب الالكتروني

تسعى المنظمات الدولية والإقليمية إلى إرساء قواعد قوية لبناء إستراتيجية فعالة لمكافحة الإرهاب الالكتروني ومواكبه التطورات في هذا النمط الإجرامي الجديد، حيث تم إنشاء العديد من المنظمات الدولية لتي تؤدي دورا ملحوظا في إطار مكافحة الأعمال الإرهابية التي تتم عبر شبكة الإنترنت، من أجل التصدي للتحديات الأمنية التي تؤثر على المجتمعات الأمر الذي دفع العديد من الدول لإيجاد آليات تكون كفيلة بمحاربة الجريمة الالكترونية.

أولا: دور الأمم المتحدة في مكافحة الإرهاب الإلكتروني

تأسست هيئة الأمم المتحدة بموجب البند الرابع من بيان موسكو الصادر بتاريخ 30/10/1943 والذي وقع من طرف وزير خارجية الاتحاد السوفيتي ووزير خارجية المملكة المتحدة والولايات المتحدة الأمريكية وسفير الصين، فتم الاتفاق على إنشاء منظمة دولية يكون لها دور في الحفاظ على السلم والأمن الدوليين، وقد تأكد هذا المبدأ (الحفاظ على السلم والأمن الدوليين) في إعلان طهران في 01/12/1943، وفي الفترة ما بين 21/08 إلى غاية 07/10 من سنة 1944 اجتمع ممثلي هذه الدول في الولايات المتحدة الأمريكية ووضعوا الخطوة الأولى لنظام قانوني تأسيسي واتفقوا على تسميتها الأمم المتحدة، كما اتفقوا على عقد مؤتمر دولي في مدينة سان فرانسيسكو في 25/04/1945 وخلال هذا المؤتمر تم الاتفاق على ميثاق يتكون من 111 مادة تتمحور حول مبدأ المساواة بين جميع الشعوب، والحفاظ على السلم والأمن الدوليين [1]
ومنظمة الأمم المتحدة تبذل جهودا فاعلة ليست بقليلة في مجال مكافحة الإرهاب الإلكتروني وذلك من اجل منع أي محاولة اعتداء من قبل الإرهابي الإلكتروني على أمن الدولة وأفرادها، وتظهر جهودها من خلال المؤتمرات التي تعقد برعايتها والخاصة بمنع الجريمة ومعاملة السجناء[2] وكذلك مؤتمرات الجمعية الدولية لقانون العقوبات التي تعقد كل خمس سنوات، إذ تسعى منظمة الأمم المتحدة من خلال هيئاتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة.

أصدرت الأمم المتحدة عدة قرارات عبر جمعيتها العامة، في توضيح منها لتصاعد الاهتمام العالمي لاستخدام تكنولوجيا الاتصال والمعلومات استخدام غير سلمي، ففي 22 نوفمبر 2002 بينت قرارا بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس السنة اتخذت قرارا آخرا بهدف إلى إرساء ثقافة عالمية لأمن الفضاء الالكتروني، واعتبر هذا القرار من بين أهم القرارات التي استهدفت العمل على حماية البنية التحتية للمعلومات، وحث الدول والمنظمات الدولية على تكثيف جهود التعاون لمواجهة الإرهاب الالكتروني.
وفي 2004 تم إنشاء مجموعة الخبراء الحكومية GCE بهدف مناقشة الأخطار القائمة والمحتملة في شمال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية

[1] شعنبي صابرة مرجع سابق ص 338

[2] علي يوسف الشكري، **المنظمات الدولية**، دار الصفاء للنشر والتوزيع،ط1، عمان، 2012 ،ص–ص ،97– 98

أمن نظم الاتصالات والمعلومات العالمية، كما شكل الأمين العام للأمم المتحدة كوفي عنان 2004 فريقا دوليا لدراسة قضية إدارة الانترنت.[1]

وفي مؤتمر منظمة الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية (2010)، عقد هذا المؤتمر في سلفادور –البرازيل من (19-12 أفريل 2010) تحت عنوان استراتيجيات شاملة في تحديات عالمية والذي نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، وتضمن جدول الأعمال ثمانية بنود وكان من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة هذه الجريمة[2]

1- إجراءات وتدابير الأمم المتحدة لمكافحة الأعمال الإرهابية

- الامتناع عن تقديم أي شكل من أشكال الدعم الصريح والضمني للكيانات الإرهابية تم وضع حد لعملية تجنيد أعضاء الجماعات الإرهابية ومنع تزويد الإرهابيين بالسلاح.
- عدم توفير الملاذ لمن يمولون الأعمال الإرهابية أو يديرونها أو يرتكبونها، منع استخدام أراضي الدول في تنفيذ تلك المآرب، نص ضوابط مشددة على الحدود وعلى إصدار الأوراق الثبوتية ووثائق السفر.
- تعزيز التدابير الرامية إلى كشف ووقف تدفق التمويل والأموال للأغراض الإرهابية.
- وضع الإرهابيين من استغلال الأنشطة الإجرامية الأخرى كـ (الاختطاف، والاتجار بالبشر والمخدرات والأسلحة) لتمويل أنشطتهم الإرهابية، وتجريم ومحاسبة كل من يمول الأعمال الإرهابية أو يدربها أو يدعمها أو يرتكبها أو يورد السلاح إليهم.
- تشجيع الدول على تبادل المعلومات على وجه السرعة مع الدول الأعضاء وتقديم تقارير إلى لجنة مكافحة الإرهاب حسب جدول زمني تحدده اللجنة
- دعوة المنظمات الدولية لتعزيز التعاون مع الأمم المتحدة في نطاق ولايتها بهدف تطوير قدراتها على معاونة الدول الأعضاء في جهودها على التصدي لتهديدات الإرهابية[3].

ونستنتج إن الأمم المتحدة في إطار مكافحة الإرهاب الالكتروني والجرائم المتصلة بالكمبيوتر والفضاء الرقمي من خلال:

---

[1] – رائد العدواني ،**المعالجة الدولية لقضايا الإرهاب الالكتروني** (محاضرة ألقيت في دورة تدريبية بعنوان توظيف شبكة التواصل الاجتماعي في مكافحة الإرهاب في الرياض فيفري 2016)،ص:09-10

[2] -عمر عباس خضير العبيدي ،**الإرهاب الالكتروني في نطاق القانون الدولي** (**رسالة ماجستير،حقوق**) كلية الحقوق جامعة تكريت، العراق 2019 ،ص ص: 47-48

[3] عادل عبد الصادق، **الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني، دوريات – قضايا إستراتيجية**، الخميس,6 أغسطس 2015 - 12:14 م https://accronline.com/article_detail.aspx?id=22762

- ✓ التنبيه من مخاطر الإرهاب الجديد ونشر وتطوير الوعي الدولي عبر سلسلة من الجهود.
- ✓ ضمان حرية التعبير وتنقل الحر للمعلومات والأفكار والمعرفة في شبكة المعلومات مع وجوب مراقبة الانترنت من اجل الحفاظ على الأمن والسلم الدوليين.
- ✓ وضع استراتيجيات علمية شاملة لمواجهة ومكافحة مخاطر الإرهاب الالكتروني على أرض الواقع[1].

وعملت منظمة الأمم المتحدة في إطار استمرار تلك الجهود المبذولة لمكافحة الإرهاب الإلكتروني من خلال جرائم الكمبيوتر والإنترنت عن طريق ثلاث اتجاهات رئيسية:

- ➢ حماية البيانات الشخصية وهي حماية الخصوصية المعلوماتية وكل البيانات الشخصية من مخاطر التلف التزوير القرصنة الحذف والتشويه.
- ➢ حماية الملكية الفكرية للمصنفات الرقمية وحماية البرمجيات وقواعد البيانات والدوائر المتكاملة وعناصر مواقع الانترنت في الواقع الحاضر.
- ➢ حماية استخدام الكمبيوتر والانترنت من الأنشطة التي تستهدف المعلومات ونظامها وأداء الكمبيوتر ووظائفه ولهذا عملت الأمم المتحدة في ميدان تطوير التشريعات الجنائية الجديدة في مجال الانترنت[2].

أ- دور مجلس الأمن

أصدر مجلس الأمن العديد من القرارات المتعلقة بمكافحة الإرهاب الدولي بمختلف صوره وأشكاله بدءا من سبتمبر 1970، القرار الذي أعرب فيه عن قلقه البالغ إزاء التهديدات التي تتعرض لها حياة الأبرياء بسبب خطف الطائرات وطالب باتخاذ كافة الإجراءات القانونية الممكنة لمنع خطفها في المستقبل ومنع القيام بأي تدخلات في السفر البحري المدني على المستوى الدولي.

منذ عام 1972 كثفت الأمم المتحدة جهودها وانتقلت من مرحلة إدانة الإرهاب إلى مرحلة أكثر عمقا وهي الاتفاق على وسائل التعاون الدولي لمكافحة اذ قرر المجلس على اتخاذ التدابير اللازمة ضمن اختصاصاتها لردع الأعمال الإرهابية ومنعها [3].

---

[1] – توفيق شريخي، **الإرهاب الالكتروني وتأثيره على امن الدولة، (مذكرة ماستر، إستراتيجية وعلاقات دولية)**،كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة، الجزائر، 2018،ص: 60

[2] – نجاري بن حاج علي فايزة، مرجع سابق، ص:71

[3] – بن صويلح أمال ،**إستراتيجية منظمة الأمم المتحدة في مكافحة الإرهاب الدولي**،(المجلة الجزائرية للعلوم الانسانية والاجتماعية عدد02-2017)،ص:31

ب- الجمعية العامة

عملت الأمم المتحدة على المضي قدما في عملها لمكافحة الإرهاب عن طريق الجمعية العامة على كل من المسارين القانوني والتنفيذي، وقد توصلت نتيجة جهودها إلى اعتماد العديد من الاتفاقيات والبروتوكولات الدولية التي تتناول الإرهاب في 8 ايلول 2006[1].

وتعد الجمعية العامة الجهاز الرئيسي لمناقشة جميع المسائل الداخلة في نطاق هيئة ميثاق الأمم المتحدة ودراستها والوصول إلى توصيات وقرارات بشأن أنماط التعاون الدولي في الميادين الاجتماعية والاقتصادية والثقافية والتعليمية والصحية سعيا لتحقيق الأمن والسلم الدوليين وحل المشاكل والنزاعات بالطرق الودية دون اللجوء للقوة[2].

ومن بين هذه الجهود مايلي:

- عقد لقاءات ومؤتمرات لدراسة ظاهرة الإرهاب
- اتخاذ التدابير اللازمة لمعالجة الظروف المؤدية إلى انتشار الإرهاب الالكتروني
- اتخاذ التدابير لمنع الإرهاب ومكافحته لاسيما عن طريق حرمان الإرهابيين من الوصول إلى الوسائل التي تمكنهم من شم اعتداءاتهم وبلوغ أهدافهم[3].
- التدابير التي ترمي إلى بناء قدرات الدول على منع الإرهاب ومكافحته.
- اتخاذ التدابير اللازمة إلى ضمان احترام حقوق الإنسان وسيادة القانون في سياق مكافحة الإرهاب[4].

ثانيا: المنظمة الدولية للشرطة الجنائية (الانتربول)

تعد المنظمة الدولية للشرطة الجنائية(الانتربول) من أقدم صور التعاون الشرطي في مكافحة الجريمة، ففي نهاية سنة 1923 نجح الدكتور "جوهانو سويرا" مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية، وذلك في الفترة من 03الى 07 من شهر سبتمبر عام 1923، ضم مندوبي 19 دولة، وأعلن فيه عنه ولادة اللجنة الدولية للشرطة الجنائية (International Criminal Police Commission ICPO) حدد مقرها بفينا، تعمل على التنسيق

[1] – شعنبي صابرة ،مرجع سابق ، ص:339

[2] – بن صويلح أمال ،مرجع سابق ، ص:35

[3] – شعنبي صابرة ،مرجع سابق ، ص:346

[4] – شعنبي صابرة ،مرجع سابق ، ص:351

بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة[1]، والتي أطلق عليها اسم المنظمة الدولية للشرطة الجنائية (الانتربول) سنة 1956 مقرها في مدينة ليون الفرنسية[2]، حيث تنقسم شبكة اتصالات الانتربول إلى ثلاثة مستويات هرمية :المكاتب المركزية الوطنية، والمحطات الإقليمية، والمحطة المركزية الموجودة في الأمانة العامة للانتربول.

وتضم المنظمة الدولية للشرطة الجنائية الانتربول حالياً حوالي 195 بلداً عضواً، تستضيف كل دولة مكتبا مركزيا وطني للانتربول (NCB)، يربط الشرطة الوطنية بشبكة الانتربول العالمية[3].

أ- مهام المنظمة الدولية للشرطة الجنائية (الانتربول).

للمنظمة الدولية للشرطة الجنائية (الانتربول) عدة مهام كونها من أبرز المنظمات في مكافحة الجرائم الدولية العابرة للحدود في العالم، فقد وجدت الانتربول لتحقيق عدة أمور، منها:

- التعاون الدولي لمواجهة الإجرام الدولي المتزايد باستمرار،
- تأمين الاتصال الرسمي بين رجال الشرطة في مختلف أرجاء العالم، بغية تبادل الخبرات والأفكار والمناهج وأساليب العمل في مجالات الأمن المختلفة منذ وجدت الدول القومية (الوطنية) التي تفصل بينها الحدود الجغرافية والصناعية، وارتباط الظاهرة الإجرامية برغبة المجرم للانتقال من مكان إلى آخر، ابتعادا عن مسرح جريمته، واختفائه عن نظر السلطات الأمنية، ولأجل تحقيق أهدافها تقوم الانتربول بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، من مختلف المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، حيث تقوم المنظمة بعد تجميعها للبيانات والمعلومات بتنظيمها لتكون بها أرشيفا متكاملا يمكن الرجوع إليه عند الحاجة[4].

ب- أهداف الانتربول:

تهدف هذه المنظمة إلى رفع مستوى التعاون بين أجهزة تنفيذ القوانين في الدول في مختلف المجالات من تبادل المعلومات، والتحري، والمتابعة القانونية، وتوحيد الإرادة السياسية للدول بشأن

---

[1] – يوسف حسن يوسف، **الجرائم الدولية للانترنت**، المركز القومي للإصدارات القانونية،ط1، القاهرة، مصر، 2011 ، ص: 146

[2] – أمير فرج يوسف، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر**، مكتبة الوفاء القانونية،ط1، الإسكندرية، مصر، 2011 ، ص 427

[3] – المنظمة الدولية للشرطة الجنائية، عرض عام الانتربول https://www.interpol.int/ar/3/10

[4]– شنتير خضرة، **الاليات القانونية لمكافحة الإرهاب الالكتروني–دراسة مقارنة–(اطروحة دكتوراه،القانون الجنائي)**،كلية الحقوق ،جامعة أحمد دراية أدرار،2020–2021 ص:210

التصدي لهذه الجريمة وتشجيعها على تطوير التشريعات بما يكفل مكافحة الجريمة المنظمة بصورة فعالة.وتسعى إلى تحقيق:

- تأمين وتنمية التعاضد على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار الأنظمة القائمة في مختلف الدول والبيان العالمي لحقوق الإنسان
- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفاعلة في الوقاية من جرائم القانون العام.

وتطرقت المادتان 2 و3 من القانون الأساسي للمنظمة إلى أهدافها، حيث تكمن في:

- تأكيد وتشجيع المعونة المتبادلة في أوسع نطاق ممكن بين سلطات الشرطة الجنائية في حدود القوانين القائمة في البلاد المختلفة، وبروح الإعلان العالمي لحقوق الإنسان
- مرونة التعاون الدولي من خلال التعاون بين المكاتب المركزية الوطنية للمنظمة الدولية للشرطة الجنائية، والتي تلتزم الدول الأعضاء بإنشائها فوق إقليمها طبقا للمادة 32 من قانون المنظمة[1].
- تطوير وتنمية التعاون الدولي عن طريق مساهمة ناجحة، وفعالة داخل المنظومة الأمنية.
- إقامة وتنمية النظم التي من شانها وضع، ومكافحة جرائم القانون.

جـ الاختصاصات العامة للمنظمة

بمقتضى ميثاق المنظمة ونظامها الداخلي تتمتع هذه الأخيرة بجملة من الاختصاصات التي تخولها القيام بنشاطات متعددة :

– تجميع وتبادل المعلومات والبيانات المتعلقة بالجريمة والمجرم: حيث تتسلم المنظمة هذه البيانات والمعلومات وتتبادلها مع المكاتب المركزية للشرطة الجنائية في الدول الأعضاء، وتقوم المنظمة بتجميع هذه البيانات وتنظيمها لديها وهذه الوثائق تعتبر وثائق مهمة في مكافحة الجريمة على المستوى الدولي.

– تنسيق الجهود بين الدول الأعضاء خاصة في مسألة هروب المجرمين: حيث تتولى التنسيق مع الدولة العضو من خلال المكاتب المركزية الوطنية التابعة للمنظمة وذلك بتعيين مكان تواجد المجرم والإسراع في اتخاذ إجراءات القبض عليه، وتسليم المجرمين.

[1] – المادة 1-3 القانون الأساسي لمنظمة الأمم المتحدة

– مكافحة جرائم القانون العام: مثل جرائم المخدرات وجرائم تبيض الأموال وحتى جرائم الإرهاب، بحيث يمنع على الانتربول التدخل في القضايا ذات الطابع العسكري أو الديني أو العرقي أو السياسي.

– حماية الأمن الدولي: وذلك من خلال تحذير الدول من احتمال وقوع جرائم جديدة، إما نظرا لورود معلومات إليها وإما لوجود مجرم خطير في ذلك البلد وبالتالي على سلطات الشرطة في ذلك البلد التحرك واتخاذ الإجراءات الضرورية للقبض عليه[1].

ثالثا: دور مجموعة الثمانية (G8)

تتضمن أنشطة مجموعة الثمانية، أو مجموعة الدول الصناعية الثمانية، مؤتمرات على مدار السنة ومراكز بحث سياسية، مخرجتها تتجمع في القمة السنوية التي يحفزها زعماء الدول الأعضاء، أما بالنسبة للاتحاد الأوروبي، فيتم تمثيله في هذه القمم[2]. تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات والأبحاث الميدانية في مختلف المجالات التي تهم المنظمة، وهي ليست تشريعا للدول الأعضاء، ولكنها تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك ببلورة خططا عملية[3].

دعت دول الـ G8 إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن تثمير الدراسات العديدة التي وضعتها دول الـ G8 ومن بينها: مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (1997) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (1999) وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (2002) ومبادئ توافر البيانات

---

[1] – بلعيور محمد نذير. بوعيشة بوغوفالة ،**دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة (مجلة البحوث القانونية والاقتصادية المجلد02 العدد02)** المركز الجامعي افلو–ماي 2020،ص:35–36

[2] – مجموعة الثمانيةG8 ، تظم الدول ، الصناعية الكبرى في العالم ، أعضاؤها هم الولايات المتحدة الأمريكية ، اليابان ، ألمانيا ، روسيا ، إيطاليا ، المملكة المتحدة ، فرنسا وكندا ، يمثل مجموع اقتصاد هذه الدول الثمانية 65 % من اقتصاد القوة العسكرية تمثل من 7 إلى 8 مراكز الأكثر أنفاقا على التسلح وتقريبا كل الأسلحة النووية عالميا ، كل سنة الدول الأعضاء في مجموعة الثمانية تتناوب على رئاسة المجموعة ، تضع الدولة الحائزة على الرئاسة الأجندة السنوية للعمل وتستضيف القمة لتلك السنة.

[3] –غازي عبد الرحمن هيان الرشيد ، **الحماية القانونية من الجرائم المعلوماتية الحاسب والانترنت، (رسالة دكتوراه ،القانون)** ، الجامعة الإسلامية ، كلية الحقوق ، لبنان. 2004.

الأساسية لحماية السلامة العامة (2002) وإعلان بيان دول G8 على نظم حماية المعلومات (2002).

وترى دول الـ G8 أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلّب الاتصال والتنسيق والتعاون داخليًا ودوليًا بين جميع أصحاب المصلحة في القطاع الخاص والأوساط الأكاديمية، والمؤسسات الحكومية. بناءا على ذلك، فإن دول الـ G8 التزمت تدريب جميع العاملين في مجال تطبيق القانون وتجهيزهم بالمعدات الضرورية لمكافحة جرائم الإنترنت. كما تعهّدت بمساعدة جميع البلدان الأعضاء على إقامة مراكز اتصال تعمل على مدار 24 ساعة سبعة أيام في الأسبوع.

إن وجود جرائم تعتمد التكنولوجيا المتقدّمة تطرح تحديات كبيرة على الأجهزة القضائية. فغالبًا ما يكون من الصعب على المحققين ذات المهارة العالية العمل بسرعة فائقة لحماية البيانات الالكترونية وتحديد المتهمين بخرق القانون. من هنا أهمية الشبكة التي طرحت دول الـ G8 إنشاءها لأنها ستمكّن من الاستجابة بسرعة كبيرة لطلبات السلطات الرسمية أو مستخدمي شبكات الانترنت.

إن توصيات الـ G8 بالنسبة لجرائم التكنولوجيا المتقدمة والجرائم ذات الصلة بالكمبيوتر تتلخص بما يلي:

– يتعيّن على الدول أن تُجرِّم الانتهاكات على حقوق الغير الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي في ما يتعلّق بمكافحة هذه الانتهاكات.

– ينبغي للدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:

• التعاون مع القطاع الصناعي لضمان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الالكترونية للهجمات.

• سن قوانين وتدابير أخرى وتنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير والقرصنة.

• تحديد المشاكل المحتملة ومعالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.

• نشر الوعي العام في ما يتعلق بموضوع الجريمة ذات التقنية العالية.

– يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق والادعاء العام، من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيا

الكمبيوتر لارتكاب جرائمهم. ويتوجّب على الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.

– ينبغي تحسين التواصل بين الموظفين المكلّفين تطبيق القوانين في مختلف الدول، بما في ذلك تبادل الخبرات في معالجة هذه المشاكل.

– يتوجب على الدول الحفاظ على التوازن المناسب بين حماية الحق في الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.

– على الدول تشجيع وضع القوانين وتنفيذ تدابير لتوفير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسي على الإنترنت.[1]

رابعا: المنظمة العالمية للملكية الفكرية WIPO

ترجع جذور المنظمة العالمية للملكية الفكرية (الويبو) إلى عام 1883، وشهد هذا العام ميلاد "اتفاقية باريس لحماية الملكية الصناعية"، وهي تعد المعاهدة الدولية الكبرى التي تستهدف مساعدة مواطني بلد ما في الحصول على حماية إبداعاتهم الفكرية في بلدان أخرى على شكل حقوق ملكية صناعية، التي تعرف كالآتي: – اختراعات (براءات)، علامات تجارية، نماذج صناعية.

وهي إحدى الهيئات المتخصصة التابعة للأمم المتحدة، والتي تهدف إلى تطوير استخدام المصنفات الناتجة عن الفكر البشري، فضلاً عن حمايتها. تم إنشاء المنظمة العالمية للملكية الفكرية (الويبو) في عام 1967 بموافقة اتفاقية ستوكهولم في 14 يوليو 1967. ويقع المقر الرئيسي للويبو في جنيف، سويسرا. تنص الاتفاقية التأسيسية أو المعاهدة[2]

وتستحدث الويبو وفرة من مواد مخاطبة الجمهور، وتعمل على نشرها. وفي ذلك سعي وراء تشجيع الإبداع والابتكار، وزيادة الإدراك لكيفية حماية الملكية الفكرية الناتجة عنهما والانتفاع بها. وتستهدف الندوات والمنتجات الإعلامية أوساطا مختلفة كالمبدعين والشركات الصغيرة والمتوسطة،

[1]– https://www.lebarmy.gov.lb/ar/content تاريخ الزيارة في 2022/05/28/

[2] –https://www.insdip.com/ar/organizacion-mundial-de-la-propiedad-intelectual-ompi تاريخ الزيارة / 2022/05/28

ومؤسسات البحث وواضعي السياسات. ويساهم سائر أنشطة نشر الدراية مع الجهود التي تبذلها الدول الأعضاء في حقل حقوق الملكية الفكرية.

تضم المنظمة العالمية للملكية الفكرية في عضويتها 183 دولة، ونبذة عن معايير القبول. ويحيل اسم كل دولة من الدول الأعضاء إلى معلومات عن عضويتها في مختلف معاهدات الويبو، وتشريعها الوطني للملكية الفكرية، وبيانات للاتصال بمكاتبها المعنية بالملكية الفكرية، ووصف للبلد، وغيرها[1].

الفرع الثاني: الاتفاقيات الدولية لمكافحة جريمة الإرهاب الالكتروني

واجهت الدول صعوبات في مكافحة الجريمة المعلوماتية عبر قوانينها الداخلية إلا أنها واجهة العديد من التحديات، لذلك كرست الدول جهودها بالتعاون على مواجهة هذا الإجرام الجديد، وعقد اتفاقيات دولية لمواجهة هذه الظاهرة والوصول إلى حلول مشتركة لمكافحة هذا النوع من الجرائم التي تعتبر هي الأخطر من نوعها ومن بين هذه الاتفاقيات:

أولا: اتفاقية بودابست لمكافحة جريمة الإرهاب الالكتروني

وتعرف بالاتفاقية الأوربية لمكافحة جريمة الإرهاب الالكتروني ووضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في 23 / 11 / 2001 ودخلت حيز التنفيذ في 2004.

تعد معاهدة بودابست لمكافحة جرائم الانترنت أولى المعاهدات المتعلقة بتلك الجرائم والتي تمت في العاصمة المجرية بودابست، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الانترنت والاستخدام السيء لها[2].

وقد وقعت على تلك المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا، والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام وتتضمن 48 مادة موزعة على أربعة فصول. تم توقيع هذه الاتفاقية، بسبب المخاوف والقلق إزاء سوء استخدام شبكات الانترنت

---

[1]–http://www.aspip.org/page.aspx?page_key=wipo&lang=ar تاريخ الزيارة 2022/05/28

[2]–منير محمد الجهيني، ممدوح محمد الجهيني، **جرائم الانترنت والحاسب الالي ووسائل مكافحتها**، دار الفكر العربي، ط1 ، الاسكندرية، 2004 ،ص 9

والمعلومات الالكترونية، ومن اجل توفر ما يلزم لردع أي عمل موجه ضد سرية نظم الحاسوب والشبكات والبيانات[1]. وتهدف الاتفاقية إلى:

-السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية.

-التأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والانترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والانترنت.

-ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات، بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي[2]

ثانيا: توصيات المجلس الأوروبي

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية أهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم 95/13 في 11/9/1995 في شأن مشاكل الإجراءات الجزائية المتعلقة تكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجزائية الوطنية لكي تتلاءم من التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الأوروبي ما يلي:

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.
- أن تسمح الإجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان محا للتفتيش مع بيان المعلومات التي تم ضبطها، ويسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش

[1] -عمر عباس خضير العبيدي، المرجع السابق، ص50

[2] - هلالي عبد اللاه أحمد ،**جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست**، دار النهضة ، ط1، القاهرة، 2007، ص30

- أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الأخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الإجراء ضروريا.
- أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.
- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.
- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد أم بيانات، تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
- يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها. وأن تخول سلطات التحقيق
- يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.
- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.
- قد تتطلب إجراءات التحقيق مد الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات
- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع أدلة معينة ويتعين عندئذ أن تسمح السلطة الأخيرة

بإجراءات التفتيش والضبط. ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة[1].

الفرع الثالث: مكافحة الإرهاب الالكتروني في الدول الغربية

سنتعرض فيما يلي بإيجاز لتجارب بعض الدول الغربية في مواجهة الإرهاب الكتروني من خلال قوانينها واستراتيجياتها الوطنية.

أولا: الولايات المتحدة الأمريكية

تعد الولايات المتحدة من الدول السباقة في محاربة ظاهرة الإرهاب بالوسائل الإلكترونية، من خلال قوانينها الوطنية أو من خلال سعيها لعقد اتفاقيات دولية بهذا الخصوص، أو من خلال إنشاء الأجهزة المختصة بمكافحة الإرهاب بالوسائل الإلكترونية. حيث تميزت الإستراتيجية الأمريكية لمكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة، وانصبت هذه الإستراتيجية في بادئ الأمر على المجال العسكري، حيث عمد البنتاغون سنة 2005 إلى إنشاء وحدة عسكرية متخصصة، عهد إليها بمهمة تحصين الفضاء المعلوماتي الأمريكي، وتأمين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة. وتعد الولايات المتحدة الأمريكية من أولى الدول التي أصدرت قوانين لمكافحة الإرهاب الإلكتروني.وتعمل الحكومة الفيدرالية الأمريكية جاهدة على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث تحاول تقنين استخدام محرك البحثMSN- Google Yahoo في مجموعة من الشركات.

وهناك خطوات عديدة اتخذتها الولايات المتحدة لمكافحة الجريمة والإرهاب الإلكتروني منها:

- إصدار قانون تعزيز أمن المعلومات 2002
- وضع الإستراتيجية الوطنية لتأمين الفضاء الإلكتروني 2003
- أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الإلكتروني
- كما تم إنشاء لجنة حماية البنية التحتية الحساسة في الولايات المتحدة، والتي أسست مجموعة خاصة تتناول جوانب الإرهاب الإلكتروني وأطلقت عليها اسم: مركز حرب المعلومات

[1] شيخة حسين الزهراني، **التعاون الدولي في مواجهة الهجوم السيبراني**، (مجلة جامعة الشارقة للعلوم القانونية العدد01 المجلد17) كلية القانون الامارات يونيو2020، ص ص: 752-753

- كما تم إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات، وبرنامج وغيرها من المبادرات.

ثانيا: بريطانيا

تعد المملكة المتحدة البريطانية هي أخرى من أولى الدول التي سارعت إلى محاربة الإرهاب الالكتروني، حيث قامت بتحقيقات أولية على يد لجنة القانون الأسكتلندي ضمنتها مذكرة استشارية نشرت عام 1982، وفي عام 1987 تم إعداد نشاط مماثل أعدته لجنة القانون عام 1988، وقد أسفر عن هذه الأنشطة توصيات وضع بناء عليها قانون إساءة استخدام الحاسب الآلي الذي تمت الموافقة عليه في عام 1990.[1]

ولقد عرف القانون البريطاني رقم 2000 لمكافحة الإرهاب والمعروف ب(terrorism act)الذي دخل حيز التنفيذ في فبراير 2001 م، الإرهاب تعريفا موسعا ليشمل أفعال القرصنة المعلوماتية التي من شأنها إزعاج أو خلق اضطراب داخل النظام ثماني أقسام، وضعت فيه (terrorism act) الإلكتروني وتضمن القانون 2000 قوانين مكافحة الإرهاب في مدونة واحدة، وقد طرأ عليه مجموعة من التعديلات منها:

في سنة 2009 صدر تعديل لقانون مكافحة الإرهاب تضمن أفعال جديدة عدت تشجيعا للإرهاب كنشر التصريحات التي يمكن أن تفهم من الجمهور بأنها تشجيع مباشر أو غير مباشر، أو تحريض على ارتكاب الإرهاب، أو التجنيد الأعمال إرهابية، كما تضمن هذا القانون جرائم التدريب على الإرهاب والتحضير له وقرر مجلس النواب البريطاني في أوائل افريل 2012 طرح ومناقشة قانون يسمح بموجبه لأحد وكالات المخابرات البريطانية بمراقبة كل الاتصالات الهاتفية والرسائل الإلكترونية والنصية والأنشطة التي تمارس على شبكة الإنترنت لمعالجة ظاهرة الإرهاب الإلكتروني، مما أثار جدلا واسعا حول انتهاك الحرية الشخصية سواء في بريطانيا أو في العالم [2]

ثالثا: فرنسا

تعتبر التجربة الفرنسية في مكافحة الإرهاب من بين أهم التجارب التي يحتذى بها على الصعيد الإقليمي (الاتحاد الأوربي) فلقد سعت للاستعداد المبكر ولمواجهة الفعالة للإرهاب الالكتروني،

[1] –صباح كزيز، أمال كزيز، **الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي**، مجلة التراث، رقم 1، العدد 8 – 2008 ،ص 3

[2] –نور الله تلة، مرجع سابق، ص:140

حيث سن المشرع الفرنسي القانون رقم 88/19 المؤرخ في05فيفري 1988 والخاص بالجرائم المعلوماتية والحريات وضمه القانون الفرنسي في المادة 462 منه، وجرم مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريقة غير مشروعة المادة 02/462، كما شدد العقوبة في الأحوال التي ينجم عنها هذا الولوج المحو أو تعديل في معطيات آليا، واستعمال المستندات، وعاقب على هذه الجرائم بعقوبة السجن أو الغرامة. وفي 23 أفريل 2015 تما إبرام اتفاق بين الحكومة الفرنسية وكبار مشغلي الإنترنت لمكافحة الإرهاب الإلكتروني والتصدي للمواقع الجهادية، ويهدف الاتفاق إلى التصدي لمحاولات نشر التطرف والتعصب على الإنترنت، ووضع آلية سريعة لسحب المضامين ذات الطابع الإرهابي، فضلا عن تشكيل مجموعة عمل مشتركة بين وزارة الداخلية الفرنسية ومشغلي الإنترنت، وانضم إلى الاتفاق كل من شركات غوغل وفيسبوك وميكروسوفت وآبل وتويتر، إضافة إلى الجمعية الفرنسية للشركات المزودة لخدمة الإنترنت لهذا الاتفاق، وقد حجبت وزارة الداخلية الفرنسية خمسة مواقع تمجد الإرهاب عبر الإنترنت، في مسابقة منذ تبني قانون" تعزيز مكافحة الإرهاب"، وصدر أمر الحجب عن مكتب الجريمة المرتبطة بتكنولوجيا المعلومات والاتصال[1].

[1] – نور الله تلة، مرجع سابق ، ص:140 –143

المطلب الثاني: الجهود الإقليمية لمكافحة الإرهاب الالكتروني

لقد شهدت السنوات القليلة الماضية تطورات سريعة وبعيدة المدى والنطاق على صعيد القطاع الدولي بما في ذلك تنسيق الجهود للعمل على مكافحة الإرهاب الالكتروني، وباعتباره من أخطر الجرائم العابرة للحدود التي أصبحت تهدد الأمن المعلوماتي، تقتضي تبني الدول في قوانينها الداخلية لمجموعة من الأحكام الإجرائية، وتكثيفها للجهود حتى تحد من هذه الظاهرة التي باتت تؤرق العالم من شرقه الى غربه ومن شماله إلى جنوبه وكان لشان العربي هو الاخر مجموعة من الأضرار والآثار السلبية نتيجة الإرهاب الالكتروني، ولقد تطلبت الحاجة إلى اقتراح خطط واستراتجيات إقليمية، للوقاية منه على الساحة الإقليمية أيضا ولدراسة هذه الجهود سنقسم هذا المطلب فرعين

الفرع الأول: الاتفاقيات الإقليمية لمكافحة الإرهاب الالكتروني

بعد تفطن العالم بأسره لمخاطر الإرهاب الالكتروني،باتت مكافحته ضرورة حتمية على المجتمع الدولي، والعربي كذلك للتّصدي والوقاية من هذا الوباء الخطير، ولقد تطلبت الحاجة إلى اقتراح خطط واستراتيجيات إقليمية، للوقاية منه على الساحة العربيّة أيضا من خلال مجموعة من الّتشريعات والمؤتمرات الإقليمية:

أولا: اتفاقية الاتحاد الأفريقي لعام 2014[1]

أبرمت هذه الاتفاقية بموافقة رؤساء الاتحاد الأفريقي(AU) عليها وتدخل حيز التنفيذ بمصادقة 15 دولة عليها، ولقد جاءت لتعالج المشاكل الواقعة عبر الإنترنت على هذه القارة كالتجارة الإلكترونية، وحماية البيانات، والجرائم الإرهابية الإلكترونية، والأمن السيراني إذ تتيح هذه الاتفاقية للدول الأعضاء سن قوانين وطنية بموجب هذه الاتفاقية. لمكافحة الجرائم الإرهابية الإلكترونية

ولقد جاء في المادة (18) من هذه الاتفاقية، حماية أصحاب البيانات، ولهم الحق في إخبارهم، قبل أن يتم مشاركة البيانات الخاصة بهم مع أطراف ثالثة، كما نصت المادة(03/25) على الأمن السيبراني وحقوق الإنسان ويجب على الحكومات أن تكفل الميثاق الأفريقي لحقوق الإنسان، والشعوب وغيرها من الحقوق الأساسية الأخرى مثل حرية التعبير والحق في الخصوصية، والحق

[1] – درار نسيمة ،**الامن المعلوماتي وسبل المواجهة مخاطرة في التعامل الالكتروني، دراسة مقارنة،(أطروحة الدكتورة،القانون الخاص)**،كلية الحقوق قسم القانون، جامعة أبي بكر بلقايد تلمسان الجزائر، 2016،ص ص:285-286

في محاكمة عادلة في القوانين الجديدة، وكذلك إصرار الاتفاقية على أن توقع الحكومات اتفاقية المساعدة القانونية المتبادلة، وذلك لوضع المعايير الدولية لتبادل البيانات بطريقة فعالة، وكذلك حظرت الاتفاقية استخدام الحاسوب الآلي للإساءة لشخص ما الأسباب العرق أو الدين أو الأصل القومي العرقي أو الديني أو الرأي السياسي، وكذلك يجب على يتم نشر القوانين المنفذة للاتفاقية في كل دولة من دول الاعضاء على الانترنت[1].

ثانيا: الاتفاقيات العربية لمكافحة الإرهاب الإلكتروني

سنتناول الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 والقانون العربي الإسترشادي لمكافحة تقنية المعلومات وما في حكمها لعام 2004 على النحو الآتي:

1. الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام2010 :

توصلت الجهود العربية في مكافحة الجرائم الإرهابية الإلكترونية إلى توقيع اتفاقية عربية لمكافحة جرائم تقنية المعلومات في نهاية عام (2010)، والتي تهدف إلى تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الإرهابية الإلكترونية، وتتكون هذه الاتفاقية من (43) مادة، منها (21) مادة في باب التجريم، وثمانية مواد إجرائيّة تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية ويتكون الفصل الرّابع من (14) مادة تنظم التّعاون بين الدول الأعضاء في تبادل معلومات المستخدمين، حيث يكون نطاق سريان هذه الاتّفاقيّة إقليميّا[2] وتضمّنت الاتفاقية المذكورة الأحكام الموضوعية والمتمثلة في تجريم الأفعال المكونة لجرائم تقنيّة المعلومات وهي الاختراق، والاعتراض، والاعتداء على سلامة البيانات والملكية الفكرية، وإساءة استخدام وسائل تقنية المعلومات، والتزوير، والاحتيال، والإباحية، وجرائم تقنيّة المعلومات المتعلّقة بالإرهاب الإلكتروني، وغسل الأموال والمخدرات، والإتّجار بالجنس البشري والأسلحة، والاستخدام غير المشروع لأدوات

[1] – درار نسيمة ، مرجع سابق،ص ص:288-289

[2]– صفاء كاظم غازي الجيّاشي، **جريمة قرصنة البريد، دراسة مقارنة**، (رسالة ماجستير، كلية القانون)، جامعة بابل، العراق ، 2016 ، ص46

الائتمان والوثائق الإلكترونية، فضلا عن تشديد العقوبات على الجرائم التّقنيّة التي ترتكب بواسطة تقنية المعلومات[1].

فقد تضمنت المادّة (11) من هذه الاتفاقية التّسبّب بإلحاق الضّرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع، فضلا عن ذلك تجريم أفعال إنتاج أو عرض أو توزيع أو تشفير أو نشر أو شراء أو بيع أو استيراد مواقع إباحيّة أو مخلّة بالحياء بواسطة تقنيّة المعلومات، وكذلك تم تجريم المقامرة والتّحريض على الدّعارة والفجور وجرائم الآداب العامّة، بالإضافة إلى الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد أو التّشهير والسّب والقذف والإساءة إلى السّمعة بواسطة تقنيّة المعلومات بواسطة تقنية المعلومات[2].

وكذلك تضمنت المادة (10) من الاتفاقية العربية لتقنية المعلومات على أنه الجرائم المتعلقة بالإرهاب والمرتبة بواسطة تقنية المعلومات ومنها ما يأتي:

- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
- نشر النّعرات والفتن والاعتداء على الأديان والمعتقدات.

2- القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات

توجت جهود الدول العربية لمواكبة التّطورات التكنولوجيّة والمعلوماتيّة التي يشهدها العالم بإصدار قانون عربي نموذجي موحد لمكافحة جرائم تقنيّة المعلومات، ولقد اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما يسمى بقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وتم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم(495 / د 19- 2003/10/08) كما تم اعتماده من مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (418/د2004/31)

ويتكون هذا القانون من 27 مادّة[3] ووفقا للقانون المذكور يمكن تجريم الأفعال الآتية، واعتبارها من جرائم الإرهاب الإلكتروني إذا مست مصالح محمية قانونا:

---

[1] – رامي متولي القاضي، **مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية**، ط 1، دار النهضة العربية، القاهرة، 2011 ، ص75

[2] – المرجع نفسه، ص:76-77

[3] –محمد طارق عبد الرؤوف الخن، **جريمة الاحتيال عبر الانترنت والأحكام الموضوعية والأحكام الجزائية**، منشورات حلبي الحقوقية ،ط 1، بيروت، 2011 ، ص125

- الدخول غير المشروع بقصد إلغاء أو حذف أو تدمير أو إنشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصيّة.
- إعاقة أو تشويش أو التعطيل العمد وبأي وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها، والوصول إلى الخدمة أو الدخول الى أجهزة أو برامج أو مصادر البيانات أو المعلومات.
- استعمال الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها من تهديد أو ابتزاز الشخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعا.

3- جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني

تصدت جامعة الدول العربية كمنظمة إقليمية عربية للأنشطة غير المشروعة المرتكبة بواسطة تقنية المعلومات، وان ميثاقها لا ينص صراحة على مكافحة الإرهاب وما يرتبط به من تفرعات، ولكن المادة (02) منه أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها، وهذا ما يتقاطع بالضرورة مع ما تنطوي عليه وسائل الإرهاب الإلكتروني من تجاوزات وإخلال السلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية، فضلا عن إمكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدول العربية المستهدفة، الأمر الذي يستدعي الدول العربية لمواجهة مثل هذه الأنشطة الإرهابية عبر الفضاء الإلكتروني، وهو اتجاه أكدته المادة (3) من الميثاق حينما خولت مجلس الجامعة بتقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن والسلام، ويمكن اعتبار الاعتداء على نظم المعلومات التي تعتمده المؤسسات الرسمية للدول العربية ومحاولة تدميرها أو الإضرار بها وإشاعة الرعب والتحريض ضد النظام القائم التي تتم عبر آليات الإرهاب الإلكتروني من صور العدوان وفقا لقواعد القانون الدولي وميثاق منظمة الأمم المتحدة والتي تضمنت ضرورة الحفاظ على أمن المواطن العربي من المحاولات العدوانية للإرهاب والتخريب الموجهة من الداخل والخارج، وفي إطار الخطة الأمنية تشكلت لجنة الجرائم المنظمة وتناولت في اجتماعها الأول موضوع جرائم الإرهاب الإلكتروني.

أسفرت جهود الجامعة العربية للتصدي للأنشطة غير المشروعة بواسطة التقنية الإلكترونية،عن إصدار مجلس وزراء العرب القرار رقم (229 سنة 1999) متعلق بإصدار القانون الجزائي العربي الموحد كقانون عربي نموذجي، إذ أن أبرز ما يمكن رصده من جهود على صعيد منظمة

جامعة الدول العربية في مضمار التصدي لجرائم الإرهاب الإلكتروني وجرائم الحاسوب، هو اعتماد مجلس وزراء العدل العرب لهذا القانون والذي تضمن فصلا خاصة بالاعتداء على حقوق الأشخاص الناتج عن المعلوماتية [1].

إن المحاولات والجهود العربية متواصلة لسد الفراغ التشريعي الحاصل في القوانين الجنائية الموجودة، ومن أجل مواجهة هذا النوع من الجرائم المستحدثة، فلقد خصصت الجامعة العربية الاجتماع الثاني عشر للجنة المختصة بالجرائم المستحدثة في عام(2009) لموضوع التزوير في مجال بطاقات الائتمان، وقد أعدت الأمانة العامة لجامعة الدول العربية مشروع اتفاقية عربية حول جرائم الحاسوب تنفيذا للتوصية الصادرة عن الاجتماع الحادي عشر للجنة المختصة بالجرائم المستحدثة، وقد تمت المناقشة من قبل لجنة مشتركة من مجلسي وزراء الداخلية والعدل العرب، إذ عقدت حتى الآن عدة اجتماعات الوضع المشروع في صيغته النهائية في ضوء ملاحظات الدول الأعضاء، حيث يذكر إلى أنه الحد الآن لم تتكلل هذه الجهود باعتماد هذه الاتفاقية[2].

الفرع الثاني: المنظمات الإقليمية لمكافحة الارهاب الالكتروني

وضعت عدة مؤسسات إقليمية لمكافحة جريمة الإرهاب الالكتروني، والتي كانت نتاج توحيد مجهودات دول جمع بينها في كثير من الأحيان الموقع الجغرافي والحدود السياسية، والتهديد المشترك الذي تفرضه الجرائم العابرة للحدود كما هو الحال في جريمة الإرهاب الالكتروني، ومنها على سبيل المثال الأفريبول الإتحاد الإفريقي للشّرطة الجنائيّة واليوروبول في اوروبا.

أولا: الإتحاد الإفريقي للشّرطة الجنائيّة "الأفريبول"

ترجع فكرة إنشاء آلية الاتحاد الافريقي للتعاون الشرطي "أفريبول " لسنة 2013 بمناسبة انعقاد المؤتمر الإقليمي الافريقي الـ 22 للإنتربول المنعقد في الفترة الممتدة من 10 إلى 12 سبتمبر 2013 بوهران – الجزائر والتي شهدت حضور كافة قادة الشرطة الأفارقة الواحد والأربعين وبدعوة من الجزائر في شخص السيد اللواء/ المدير العام للأمن الوطني عقد المؤتمر الإفريقي للمدراء والمفتشين العامّين للشّرطة حول الافريبول أيام 10، 11 و12 فيفري 2014 والذي تم من خلاله اعتماد إعلان الجزائر بخصوص إنشاء آلية الاتحاد الافريقي للتعاون الشرطي بينما وصفت المادة

[1] عمر عباس خضير العبيدي،مرجع سابق،ص:80

[2] رامي متولي،مرجع سابق،ص:74-75

الثانية من هذا النظام هذه الآلية على أنها مؤسسة تقنية باعتبارها آلية للتعاون الشرطي بين الدول الأعضاء في الاتحاد الإفريقي.

حيث تتخذ هذه الآلية من الجزائر العاصمة مقرا لها بالرجوع لنص المادة 5 من النظام الأساسي الآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" نجدها قد حددت لنا جملة من المبادئ التي يفترض على هذه الآلية أن تراعيها لدى ممارسة مهامها والمتمثلة في:

– يجب أن تعمل هذه الآلية في إطار احترام سيادة الدول وبهذا فلا يجوز لها بأي شكل من الإشكال أن تتدخل في الشؤون الداخلية لدولة أخرى وقوانينها الوطنية.

– تراعى هذه الآلية لدى ممارسة المهام المنوطة بها احترام أخلاقيات الشرطة

–يجب على هذه الآلية وهي تباشر مهامها أن تأخذ بعين الاعتبار مبدأ قرينة البراءة

بالرجوع إلى نص المادة الثالثة من النظام الأساسي لآلية الاتحاد الإفريقي للتعاون الشرطي "أفريبول" نجدها قد سطرت جملة من الأهداف التي ينتظر من هذه الآلية تحقيقها الاعتراف صراحة آلية الاتحاد الافريقي للتعاون الشرطي " أفريبول" بإبرام اتفاقيات مع منظمة الشرطة الجنائية الدولية "أنتربول" وأي منظمات أخرى ذات صلة تعاون، وكذلك إقامة علاقات وتعاون مع المنظمات الحكومية والدولية الممثلة طبعا في إطار سياستها الرامية لمكافحة الجريمة المنظمة العابرة للحدود الوطنية

وفي هذا الإطار قامت أفريبول بعدة مساعي تصب جلها في إرساء أطر للتعاون مع المنظمات الأخرى لا سيما من خلال الشروع في إبرام اتفاقات للتعاون مع أجهزة الشرطة الاقليمية والدولية مثل أنتربول وأمريبول. هذه الاتفاقيات هي حاليا قيد الدراسة على مستوى المكتب القانوني الاتحاد الافريقي تلتزم كل دولة عضو في آلية الافريبول بأن تنشئ وفقا لتشريعاتها الوطنيّة مكتبا للاتصال الوطني لضمان سلاسة وسير وتنفيذ أنشطة هذه الآلية[1] وقد بلغ عدد هذه المكاتب المنشأة تقريبا أكثر من 30 مكتبا.

وتجدر الاشارة في هذا الصدد أن المادّة 6 من النّظام الأساسي المنشئ لآليّة الأفريبول قد أناطت باللّجنة الفنيّة المتخّصصة للدّفاع والسّلامة والأمن" مسؤولية توفير القيادة السياسية والتّوجيه فيما يتعلّق بشؤون الشّرطة في إفريقيا، فضلا عن ذلك أنيط بهذه اللّجنة عدّة اختصاصات كما

[1] https://www.asjp.cerist.dz/en/downArticle/65/11/1/59399 التصفح بتاريخ 2022/05/28 الساعة 22:00

سبق الإشارة إليه، ومن أبرزها الوساطة بين الجمعيّة العامة وأجهزة صنع السّياسة للإّتحاد الإفريقي كما يسميها النظام المنشئ لآليّة الأفريبول والمساهمة في اعتماد البرنامج السنوي لهذه الأخيرة.

ثانيا: اليوروبول لمكافحة الارهاب الإلكتروني

اليوروبول وكالتين مهمة على المستوى الأوربي في مكافحة الجريمة الخطيرة بصفة عامة، والجريمة الإلكترونية بصفة خاصة، هذه الجريمة التي فرضت نفسها على جميع المستويات الدولية والاقليمية والوطنية.

إن مكتب الشرطة الأوروبية" يوروبول (Europol) "هو وكالة لإنفاذ القانون تابع للاتحاد الأوروبي، يحتل موقعًا مركزيًا في بنية الأمن الأوروبي، يوظف أفضل محللي الجريمة المدربين في أوروبا والذين يستخدمون أدوات فنية متطورة من أجل مساعدة الوكالات الوطنية في تحقيقاتها اليومية[1].

ولأجل المكافحة الفعالة للجريمة الإلكترونية قام اليوروبول بإنشاء مراكز ووحدات تابعة له، على غرار الفريق العامل المعني بالجريمة الإلكترونية التابع للإتحاد الأوروبي(EUCTF)، والذي تم إنشاؤه سنة 2010 بهدف توفير منصة لمديري التحقيقات والملاحقات القضائية في مجال الجريمة الإلكترونية، وتطوير وتعزيز نهج منسق داخل الاتحاد الأوروبي لمكافحة الجريمة الإلكترونية، لجعل الفضاء الإلكتروني مكاناً آمنا لمواطني الإتحاد الأوروبي ومؤسساته وحكوماته.

ويتألف (EUCTF) من رؤساء الوحدات الوطنية لمكافحة الجرائم الإلكترونية لمختلف الدول الأعضاء بالإضافة إلى ممثلين عن المفوضية الأوروبية، وممثلين عن اليوروبول والاوروجيست، كما تم إنشاء المركز الأوربي للجريمة الإلكترونية (EC3) سنة 2013، والذي قدم مساهمة كبيرة في الجهود التي تبذلها الدول الأعضاء في الإتحاد الأوربي من أجل حماية المواطنين والشركات والحكومات الأوروبية من هذه الجريمة، هذا المركز الذي ساهم كثيرا في مكافحة الجريمة الإلكترونية من خلال عمليات الدعم العملياتي الفوري، مما سهل في اعتقال المجرمين، إضافة إلى قيامه بتحليل مئات الآلاف من الملفات، والتي في غالبيتها تكون خبيثة أو تحتوي فيروسات إلكترونية، كما يهتم المركز(EC3) بدراسة التهديدات التي قد يشكلها الإجرام الإلكتروني المنظم وبالأخص الإرهاب الإلكتروني، وكل الجرائم الإلكترونية التي تؤثر على البنية التحتية الحيوية

[1]– شنتير خضرة، ،مرجع سابق، ص:246

والمعلوماتية للاتحاد الأوروبي، والجرائم الإلكترونية التي تتسبب في أضرار جسيمة لضحاياهم، مثل الاستغلال الجنسي للأطفال عبر الإنترنت[1].

الفرع الثالث :الجهود العربيّة لمكافحة الإرهاب الالكتروني:

سعت الدول العربية جاهدة وبكل الوسائل المتاحة لها من اجل حد ظاهرة الإرهاب الالكتروني والأخطار التي يخلفها ومن خلال هذا الفرع سنقوم بدراسة بعض الجهود التي قامت بها الدول العربية.

لقد سعت العديد من الدول العربية الأخرى تشريعات وقوانين في إطار تجريم الإرهاب بالوسائل الالكترونية (الإرهاب الالكتروني)[2]:

أولا: المملكة العربية السعودية

تبنت المملكة العربية السعودية مجموعة من المبادرات المختلفة والتي شملت تدابير قضائية ومعايير أخرى استجابة للتطورات الدولية في هذا المجال عن طريق إصدار مؤسسة النقد العربي السعودي قواعد مكافحة غسل الأموال وتمويل الإرهاب فبراير 2012 م، حيث نصت هذه القواعد في أحدى المواد منها على مكافحة الإرهاب الإلكتروني ومن هذه المواد

– عند تطبيق أي نظم إلكترونية جديدة لتحويل الأموال والمدفوعات فإنه يجب التأكّد من أنها صممت على أن تكون لديها قدرات تسمح بمنع واكتشاف عمليات غسل الأموال وتمويل الإرهاب، فإنه يجب التأكّد من أن لا يتم تقديم هذه الخدمات إلاّ إلى العملاء الذين يملكون حساباً أو علاقة مصرفية أخرى مع البنك أو محل الصرافة [3]

– تشمل العمليات البنكية الإلكترونية تقديم المعلومات والمنتجات والخدمات من خلال وسائل إلكترونية، وتوفر هذه العمليات فرصاً عديدة للبنوك لتقدّم مجموعة متنوعة من منتجاتها وخدماتها بطريقة أسرع وأرخص وأكثر راحة.

–الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح

[1]– شنتير خضرة، مرجع سابق ص:247–248

[2] – رائد العدوان، **المعالجة الدولية لقضايا الإرهاب الالكتروني**، دورة تدريبية حول: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، ص ص:16–17

[3]–مؤسسة النقد العربي السعودي، **قواعد مكافحة غسل الأموال وتمويل الإرهاب**، فبراير 2012، المملكة العربية السعودية، ص: 47

-الامتناع عن إشراك الآخرين في حسابات الاستخدام، أو إطلاعهم على الرقم السري للمستخدم.
- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها
- الامتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.
- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دومًا، ويمنع الآخرين من الاستفادة من خدماتها.
- الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للإنترنت والتي تتنافى مع الدين الحنيف والأنظمة.
- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.
وهذا القرار يبين مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطها[1]

ثانيا: الجمهورية العربية المصرية

ظهر في الآونة الأخيرة نوع من الحروب الجديدة التي لا تقتصر على الهجوم المباشر باستخدام القوة العسكرية، وسبب ذلك ظهور الشبكات الإلكترونية التي ساعدت في ظهور ما يُسمَّى بالهجمات الإلكترونية التي تستهدف كل المواقع الحيوية بالدولة. وتعد جمهورية مصر العربية واحدة من أكثر الدول الأفريقية التي تكون عرضة لخطر الإرهاب الإلكتروني تعرضت العديد من الدول لسلسلة من الهجمات الإلكترونية بتاريخ 12 مايو 2017، وقد وقع أكثر 45 ألف هجمة إلكترونية لأكثر من 99 دولة، وذلك وفقًا لخبراء في الأمن المعلوماتي وجاءت الدولة المصرية بمجموعة من الجهود.

-**الجهود القانونية:** وتنص المادة 31 من الدستور المصري 2014 على "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون

-**الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:** تمت الموافقة على انضمام مصر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات من قبل رئيس جمهورية مصر العربية بتاريخ 19 أغسطس 2014.[2]

[1] -بوحادة سارة،مرجع سابق،ص:17-20

[2] -قرار رئيس جمهورية مصر العربية رقم 276 لسنة 2014، الجريدة الرسمية، العدد 46، 13 نوفمبر 2014، ص 3

وقد انضمت مصر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات في سبيل تعزيز التعاون بين الدول العربية لمكافحة جريمة الإرهاب الإلكتروني، علاوة على اقتناعها بضرورة "تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات"

-قانون مكافحة جرائم تقنية المعلومات وفقًا للقانون المصرى :يعد صدور قانون مكافحة تقنية المعلومات بمثابة خطوة مهمة في ضوء القانون المصري، حيث تضمن القانون المصري لأول مرة "تجريم الممارسات الإلكترونية غير المشروعة"

تتمثل أهم الجهود التنفيذية لجمهورية مصر العربية في وضع الإستراتيجية الوطنية للأمن السيبرياني (2017-2021)، والتي تهدف "لإعداد إستراتيجية وسياسات وبرامج وخطط تأمين البني التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة.

وزارة الاتصالات والمعلومات: تم إنشاء المركز الوطني "للاستعداد لطوارئ الحاسبات والشبكات CERT-EG "عام 2009، من أجل مواجهة خطر الإرهاب الإلكتروني، ويختص المركز بتقديم الدعم للقطاع الحكومي والمالي، من خلال الدعم التقني والميداني وتقديم التقارير الفنية للجهات المختصة [1].

مؤشِّر الجاهزية للأمن السيبراني :تُعدُّ مصر واحدة من أكثر الدول الأفريقية عُرضةً لخطر الإرهاب الإلكتروني، وجاءت مصر في الترتيب 23 ما بين 155 دولة في مؤشر الجاهزية للأمن السيبراني، Global Cybersecurity Index GCI الصادر عن "الاتحاد الدولي للاتصالات" لعام 2018، ويقيس المؤشر الجهود والاستعدادات التي قامت بها الدولة من خلال خمسة معايير هي: "المعيار القانوني، والمعيار التقني، والمعيار التنظيمي، ومعيار بناء القدرات، ومعيار التعاون

ثالثا: في القانون الأردني

تصدى المشرع الأردني لتجريم الأفعال الإرهابية الالكترونية المستخدم فيه الحاسوب والانترنت، وذلك من خلال

أ - وجود برمجيات وبرامج مجانية تخفي هويات المستخدمين وتجعل من الصعب تعقبهم وكشفهم.

ب - توافر المعلومات وسهولة الحصول عليها وإمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية والخبرة في استخدامها من مواقع مجانية عديدة على مواقع الشبكة العالمية

[1] المركز العربي للبحوث والدراسات: سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً(acrseg.org) 2022/05/29

ج- الشبكة الخفية، التي تشكل مرتعا خصبا للأعمال غير المشروعة بما في ذلك استئجار أشخاص للقيام بعمليات القتل، وتجارة المخدِّرات، والإتجار بالأشخاص، واستغلال الأطفال، الأمر الذي يجعل عملية رصد هذه المواقع ومراقبتها مهمة صعبة، بسبب استخدام التشفير لمنع كشف هوية المستخدمين؛

د- بطء الإجراءات وتبادل المعلومات في قضايا الجرائم السيبرانية التي تقع في عدة دول، لاسيما بالنظر إلى أن الجريمة السيبرانية تتطلب سرعة الإجراءات والمعالجة؛

ه-عدم تجاوب بعض منصات التواصل الاجتماعي وعدم تعاونها بخصوص تبادل المعلومات مع أجهزة إنفاذ القانون؛

و- الحاجة إلى بناء القدرات من خلال برامج تدريبية دولية وتبادل الخبرات مع الدول المتقدمة النمو في مسائل الجريمة السيبراني[1].

[1] المركز العربي للبحوث والدراسات: سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً(acrseg.org) 2022/05/29

المبحث الثاني: الجهود المبذولة وطنيا لمكافحة الإرهاب الالكتروني

لقد عمدت الجزائر على غرار باقي الدول إلى السعي في بذل كل الجهود لمكافحة الإرهاب بصفة عامة والإرهاب الالكتروني بصفة خاصة حيث كثفت جهودها لتحقيق مساعيها والسعي لمواكبة الدول المتقدمة في هذا المجال حيث بدأت بالجانب التشريعي لما له من دور فعال في إثبات الجريمة الإلكترونية وسن القوانين الردعية التي تجرم الأفعال الماسة بالأنظمة المعلوماتية وكذا الإجراءات الجزائية إضافة إلى تجنيد كل الهياكل والمصالحة المتخصصة لمواجهة الإرهاب الإلكتروني الذي أصبح خطرا يهدد الأمن السيبرياني العالمي والوطني.

المطلب الأول: الآليات التشريعية لمكافحة الإرهاب الإلكتروني والتعديلات الطارئة عليها

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة للتصدي للإرهاب الإلكتروني، ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام.

الفرع الأول: آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات العامة

لقد أخص المشرع الجزائري تنظيم الجرائم الإلكترونية بقوانين عامة وخاصة العامة في:

أولا: الدستور الجزائري

كفل دستور 1996 الأساسية والحريات الفردية وذلك عن طريق أهم المبادئ الدستورية في مواده:

- المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.
- المادة 44 حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلفين يحميها القانون.
- لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي.
- الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.[1]

[1]- القانون رقم 16-01 المؤرخ في 06 مارس2016 ،**المتضمن التعديل الدستوري**، المؤرخة في 7 مارس 2016، الجريدة الرسمية عدد: 14

ثانيا: قانون العقوبات:

استدرك المشرع الجزائري في السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الجريمة الإلكترونية، وذلك لما أصدر القانون 04-15 المتضمن تعديل قانون العقوبات[1]، حيث خصص قسمه السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وتضمن ثمانية مواد، إذ تعلقت المادة 394 مكرر بمعاقبة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، أما المادة 394 مكرر1 فنصت على معاقبة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، ونصت المادة 394 مكرر2 على معاقبة كل من يقون عمدا عن طريق الغش بما يأتي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن تتركب بها الجرائم المنصوص عليها في القسم الأول

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. أما المادة 394 مكرر3 فنصت على مضاعفة العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني، أوالهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد. وفي المادة 394 مكرر4 شدد المشرع على معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. وجاء في المادة 394 مكرر5 أن كل من شارك في مجموعة أو إتفاق تألف بغرض الإعداد جريمة أو أكثر من الجرائم المنصوص عليها، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها. وأوردت المادة 394 مكرر6 على أنه مع الاحتفاظ بحقوق الغير حسن النية، بحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم

[1] – القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات جريدة رسمية عدد:71

مالكها. أما المادة 394 مكرر7 فنصت على أنه يعاقب الشروع في ارتكاب الجنح المنصوص عليها بالعقوبات المقررة للجنحة[1]

ليصدر في 2009 القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصالات ومكافحتها.[2]

ثالثا: قانون الإجراءات الجزائية:

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة وإستجواب المتهم والضبط والتسرب والشهادة والخبرة.[3]

نجد أن المشرع نص على تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية، ونص على التفتيش في المادة 45 الفقرة 7 من نفس القانون[4] المعدلة حيث إعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على «إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور من المادة 65 مكرر5.[5]

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06-

[1]-بارة سمير، **الدفاع الوطني و السياسات الوطنية للأمن السيبراني في الجزائر: الدور و التحديات** كلية الحقوق و العلوم السياسية جامعة قاصدي مرباح ورقلة، 2017 ، ص: 432.

[2]- نفس المرجع السابق ص: 433.

[3]- فضيلة عاقلي، **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية،» طرابلس، بتاريخ 24- 25 مارس 2017، ص: 130.

[4]- مولود ديدان، **قانون الإجراءات الجزائية**، الأمر 11- 02، دار بلقيس،الجزائر، ص: 33.

[5]- فضيلة عاقلي، مرجع سابق، ص: 130.

22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها والتسرب.

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها. ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في المادة 65 مكرر5 من قانون الإجراءات الجزائية على النحو: « إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في. ..الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذن:

– باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكي.

– وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص. »

فموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء اعتراض المراسلات السلكية اللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة.

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.[1]

رابعا:القانون المدني الجزائري

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا

[1]– براهيمي جمال، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، (**المجلة النقدية للقانون والعلوم السياسية، العدد 2، كلية الحقوق والعلوم السياسية**)، جامعة مولود معمري، تيزي وزو، 15 / 11 / 2016، ص ص" 138– 140

الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري «كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض » وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهما هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض «فالفعل الضار هو أساس المسؤولية » وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الانترنت، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدى، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة.[1]

الفرع الثاني: آليات مكافحة الإرهاب الإلكتروني في ظل القوانين والتشريعات الخاصة

أولا: القانون الخاص بحماية حق المؤلف والحقوق المجاورة:

يرى معظم الفقه أن «الموقع الإلكتروني مصنف متعدد الأغراض »، يتم إستخدامه من الشركات. التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسويق أو الدعاية عن غيرها على شبكة الانترنت، أو كإسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم السينمائية أو لوحاتهم الزيتية أو ألعاب الفيديو... وغيره، وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عند إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة، وبمجرد تسجيل إسم الموقع يحضى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه، أي بتحديد القانون الواجب التطبيق حسب الطبيعة القانونية للمواقع فعند تسجيل الموقع كمصنف أدبي أو فني «لا يجوز أن يعتدي على أي

[1]– حسين نوارة، **آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا**، الملتقى الوطني "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017، ص 121– 122.

جانب من جوانب الحياة الخاصة للأفراد » كإستعمال إسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها أو إستغلال صورة أي شخص في الموقع دون الموافقة منه، والمصنف من حيث المفهوم لا ينصرف فقط إلى المادة الملموسة في الخطوط والتماثيل أو اللوحات الزيتية وإنما هي الفكرة المدرجة في المحل الملموس وهي جوهر الإبداع الأدبي أو الفني لأنها الأساس الذي يقوم عليه المصنف، أما المادة التي نفذت عليها المادة ما هي إلا وسيلة لنقله إلى الجمهور وقياسا لذلك على موضوعنا تصبح مواقع الأنترنت الوسيلة المستخدمة لعرض المصنفات على الجمهور، وبهذه الصورة فإن حماية مواقع الأنترنت التي تستغل مصنفا أدبيا أو فنيا على شبكة الأنترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الأدبي والمالي للموقع المسجل كمصنف، وحماية قانونية لأي حق آخر يتم الإعتداء عليه مثل الحياة الخاصة للأفراد كالحق في الإسم والصورة والمعلومات الخاصة... وفي كل الأحوال لا يمكن الفصل بين حماية المصنف المستعمل في الموقع وحماية الموقع في حد ذاته لأنهم يخضعون لقانون حق المؤلف والحقوق المجاورة في الوقت نفسه، لأن حماية الموقع تؤدي بالضرورة إلى عدم محتوياته بما في ذلك المصنف.[1]

ثانيا: قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

خصّ المشرع جرائم انتهاك الحياة الخاصة في البيئة الرقمية باهتمام ملحوظ فميّزها عن الجرائم التقليدية وسنّ قانونا خاصا بها هو القانون رقم 09/04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] الذي عرّف هذه الجرائم في المادة الثانية منه كما يلي: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

ولقد حصر المشرع – في المادة الرابعة من هذا القانون– أربع حالات سمح فيها للسلطات المختصة باللجوء إلى مراقبة الاتصالات الإلكترونية تتمثل فيما يلي:

[1] – حسين نوارة، مرجع سابق، ص 120 – 121.

[2] – القانون رقم 09–04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 **المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**. الصادر في 25 أوت 2009 ،الجريدة الرسمية، العدد 47

– الوقاية من جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة عند توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدّد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحري والتحقيقات القضائية عندما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة كما ألزم المشرع مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات والمراسلات ووضعها تحت تصرفها، والالتزام بحفظ المعطيات التي تساعد في الكشف عن الجرائم ومرتكبيها، وكذلك التدخل الفوري لسحب المحتويات التي يطلعون عليها بمجرد العلم بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.[1]

ثالثا: قانون البريد والإتصالات السلكية واللاسلكية

حيث نصت عدة مواد منه فيما يخص – المادة 87، والتي نصت على سهولة إجراء التحويلات المالية الكترونيا، والمادة 2/84 على استعمال حوالات النفع العادية والإلكترونية، كما نصت 105 على إحترام المراسلات، أما المادة 127 بجزاء كل من يفتح أو يخرب بريد.

ولقد أصدر المشرع الجزائري القانون رقم 18/04 المؤرخ في 10 ماي 2018 المحدّد للقواعد العامة المتعلق بالبريد والاتصالات الإلكترونية[2]، والذي أكّد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد[3]، وفي حالة مخالفة ذلك يتعرّض المخالف للأحكام الجزائية التي تضمنها هذا القانون، والمتمثلة فيما يلي:

1-انتهاك سرية المراسلات الإلكترونية

وفقا لنصّ المادة 164 من هذا القانون يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500000 دج إلى مليون دينار كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد

[1] – انظر المواد 10 ، 11 ، 12 من القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[2] – القانون رقم 18– 04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، **يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية** الصادر في:2018/05/13 ،الجريدة الرسمية، العدد 27

[3] – المادة 117 من القانون رقم 04/18.

أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله بدون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها.

تتحقق هذه الجريمة باطلاع الشخص على الرسائل الإلكترونية أو سماع المحادثات الإلكترونية بصورة غير مشروعة، بصرف النظر عن مضمونها أو محتواها فيما إذا كان يتضمن أسرار أم لا، إضافة إلى إفشاء مضمونها أو نشره أو استعماله بدون ترخيص.

2- تحويل المراسلات الصادرة عن طريق البريد الإلكتروني

تعاقب المادة 165 من القانون رقم 18/04 بالحبس من سنة إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمس ملايين دينار أو بإحدى هاتين العقوبتين كل متعامل للاتصالات الإلكترونية يحوّل بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية.

رابعا: قانون التأمينات

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر2[1].

[1] – فضيلة عاقلي، مرجع سابق، ص 132 .

المطلب الثاني: الهيئات الخاصة كآلية لمكافحة الإرهاب الإلكتروني

نظرا لتفاقم ظاهرة جريمة الإرهاب الالكتروني من يوم لآخر وبالنظر إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة المعلوماتية، لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الانتربول واليوروبول والافريبول.

أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى وحدات قضائية وأخرى تابعة لسلك الأمن والدرك الوطني

الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الالكترونية.

الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تسند مهام الوقاية ومكافحة الجرائم الالكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الالكتروني.

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

التي أنشئت سنة 2009، ووضعت تحت السلطة المباشرة لوزير العدل حافظ الاختام، ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 15-261 المؤرّخ في 2015/10/08، غير أنّه في 2019 صدر مرسوم رئاسي 19-172[1] المعدّل بالإلغاء للأ حكام المرسوم الرّئاسي 15-261 وذلك نتيجة االظّروف السّياسيّة والأمنيّة التي عرفتها البلاد في تلك الفترة ممّا أفضى إلى ظهور مخاطر فعليّة لتعرّض الأمن العمومي وكذا المؤسّسات الدّستوريّة للخطر فجاء هذا المرسوم ليغيّر من الطّبيعة القانونيّة للهيئة حيث نقل الإشراف عليها.

[1] - المرسوم الرئاسي 19-172 المؤرخ في 03 شوّال عام1440 الموافق لـ06 يونيو 2019 **يحدّد تشكيلة الهيئة الوطنيّة للوقاية من الجرائم المتّصلة بتكنولوجيّات الإعلام والاتصال و تنظيمها و كيفيات سيرها**، الجريدة الرّسمية عدد 37 الصّادرة في 09 يونيو 2019.

وبموجب المرسوم الرئاسي رقم:20-183 تم أعاد تكييفيا من جديد على أنها سلطة إدارية مستقمة، لكن تحت سلطة رئيس الجميورية، غير انه وبموجب المرسوم الرئاسي رقم 21-439[1] الذي يهدف إلى اعادة تنظيمها.

- استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغرات، مع العلم ان هذا المجال أصبح مفتوحا على كل الاحتمالات في ظل التطور السريع لتكنولوجيا الاعلام والاتصال.

- تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني وحماية الحقوق والحريات الساسية.[2]

- اقتراح الارضية اللازمة لتجسيد الاستراتيجية الوطنية للوقاية ومحاربة الجرائم الالكترونية.

- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الاجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

ثانيا:المصلحة المركزية لمكافحة الجريمة المعلوماتية: (SCLC)

التابعة لمديرية المن الوطني، وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة) أنتبول، أفريكوم (أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الاجرام (الشرطة القضائية).

ثالثا: مركز الوقاية من جرائم العلام الآلي والجرائم المعلوماتية (CPLCIC)

التابعة للقيادة العامة للدرك الوطني، لا تختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت لمسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.

---

[1] المرسوم الرئاسي 21-439 المؤرخ في 02 ربيع الثاني عام1443 الموافق لـ07 نوفمبر 2021 يتضمن إعادة تنظيم الهيئة الوطنيّة للوقاية من الجرائم المتّصلة بتكنولوجيّات الإعلام والاتصال و مكافحتها، الجريدة الرّسمية عدد 86 الصّادرة في 11 نوفمبر 2021.

[2] جمال بوازدية، **الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية " التحديات والافاق المستقبلية"**، (مجلة العلوم القانونية والسياسية، المجلد 10 العدد 01، أفريل 2019)، جامعة الجزائر 3، الجزائر، تاريخ الاستلام 2018/11/26، تاريخ القبول 2019/02/13.ص 1281.

رابعا: المعهد الوطني للأدلة الجنائية وعلم الجرام للدرك الوطني (INCC)

التابع للقيادة العامة للدرك الوطني، يعتمد المعهد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة، من أجل تنوير العدالة وتوجيه الجهات المنية كلما تعلق الأمر باستكمال التحقيق.

ومن بين النتائج المتوصل إليها من طرف هذه المصالح، اتضح أن الجرائم الالكترونية بالجزائر تتضاعف بطريقة سريعة جدا، وهذا ما كشفت عنه ا لرقام المسجلة التي تم البت فيها، حيث سجلت سنة 2017 أكثر من 2500 جريمة ويتعلق أبرزها 70 % انتهاك الحريات الشخصية، والتهديد عبر الإنترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الإلكترونية وغيرها.

وحسب تقدير نفس الأجهزة، فإن هذه الارقام لا يمكن تسجيلها لولا الممارسات الغير عقلانية التي جسدها الاستعمال المفرط وغي ر المنتظم لوسائل الاتصال وتكنولوجيات الإعلام، فقد تم إحصاء أكثر من حيث 28 مليون مستعمل للانترنت، 18 مليون لهم حسابات ومواقع فايسبوك و13 مليون متفحص يومي لشبكة التواصل الاجتماعي.[1]

الفرع الثاني:الهيئات القضائية الخاصة للبث في الجرائم الالكترونية

لقد أثمر مسار إصلاح العدالة الذي شرعت في الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية: دعم حقوق الإنسان وتسهيل حق اللجوء إلى القضاء وإعادة الاعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة. ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائي بشقيه الموضوعي والإجرائي لمواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية والمعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايدا في العمليات الإرهابية وتزايدا في أعمال المنظمات الإجرامية واستعمالها الفضاء الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

من أجل كل هذا عكف المشرع الجزائري وبقية التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون

[1] – جمال بوازدية، مرجع سابق، ص 1280.

04-14 المؤرخ في 10 نوفمبر 2004. المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر وتوصف أنها خطيرة وعلى درجة عالية من التعقيد والتنظيم وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف.[1]

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 2006/10/05 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم التعديل بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3-4-5 المعدلة للمواد 3-4-5 من المرسوم السابق وجاء التقسيم كالتالي: [2]

- محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية:الجزائر، الشلف، الاغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة وبومرداس.

- محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية التالية: قسنطينة، ام البواقي، وباتنة وبجاية وتبسة وجيجل وسطيف وعنابة وبرج بوعريج والطارف وخنشلة وسوق اهراس وميلة.

- محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة وادرار وتامنراست وايليزي وبسكرة والوادي وغرداية.

- محكمة وهران ويمتد اختصاصها للمجالس القضائية التالية: وهران وبشار وتلمسان وتيارت وتندوف وسيدي بالعباس ومستغانم ومعسكر والبيض وتيسيمسيلت والنعامة وعين تموشنت وغليزان.[3]

[1] - كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني،.المجلد 11 عدد 01 2015 ، ص 117.

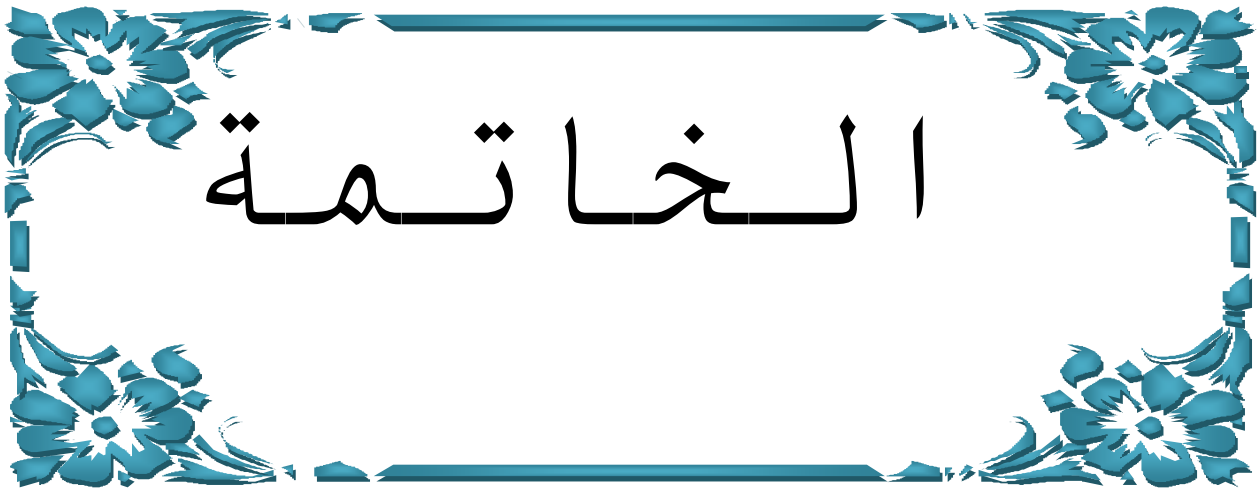
[2]- كور طارق، **آليات مكافحة جريمة الصرف**، دار هومة، الجزائر، ط2، 2014. ص: 154

[3] المواد 65 مكرر 5 الى 65 مكرر 18 من قانون الاجراءات الجزائية

ملخص:

يعاني المجتمع الدولي في كل شبر من أرجائه في هذا العصر من جرائم مستحدثة التي غطت على الجرائم التقليدية، حيث بات الإرهاب الالكتروني وما يفرزه من مشاكل وتهديدات الشغل الشاغل للمجتمع الدولي، وفي ظل زيادة خطورة هذا الإرهاب الجديد وانتشاره الرهيب أصبحت محاربته ضرورة حتمية تستوجب على دول تكثيف جهودها بسن تشريعات وإبرام الاتفاقيات وإنشاء منظمات الدولية والإقليمية لمكافحة هذا الوحش الذي أضحى من أكبر التحديات التي تواجهها الدول.

وان خطورة هذا الإرهاب فرضت على الحكومات تطوير وسائلها وقدراتها لتصدي لتهديداته المختلفة بتوفير التقنيات اللازمة للحماية وتقنين قواعد وتشريعات على مستوى الإقليمي والدولي. وان الطابع العالمي لهذه الظاهرة ا زدها تعقيد في شان مكافحتها دوليا، خاصة مع عدم وجود إطار قانوني دولي واضح يتناول هذه الظاهرة المستحدثة.ولقد حضي الإرهاب الالكتروني باهتمام كبير على كافة الأصعدة سواء الدولي أو الإقليمي إذ عقدت في شانه العديد من الاتفاقيات وندوات مختلفة وتسابقت جل الدول الكبرى إلى سن تشريعات بهدف الحد منه.


الـــخـــاتـــمـــة

تعتبر جريمة الإرهاب الإلكتروني من أهم جرائم العصر الحالي التي تؤثر على الفقهاء والمفكرين والقانونيين بعد أن كشفت عن مدى خطورتها وتنامي إنتشارها وبروز العديد من التنظيمات الإرهابية في مختلف أرجاء العالم لا تربطهم بينهم منطقة معينة أو ثقافة محددة ولا إعتقادات دينية أو عرفية موحدة، بل تربطهم عوامل جديدة أفرزتها الثورة التكنولوجية سواء من حيث التخطيط والتنظيم وكثافة التسليح وضخامة الإمكانيات المتاحة للجماعات الإرهابية، إضافة إلى تصعيد مستوى الأهداف بتدمير الموارد الحيوية والبنى الأساسية المهمة لإستقرار الدول وضمان أمنها، حيث يعد من الجرائم المستحدثة الذي يعتمد على الموارد المعلوماتية على عكس الإرهاب التقليدي، وهو إرهاب المستقبل، والهاجس الأكبر للدول التي أصبحت عرضة لهجمات الإرهابيين والجماعات المتطرفة الذين يمارسون نشاطهم التخريبي في أي مكان وزمان، الأمر الذي أوجب على مكافحة الإرهاب الإلكتروني والتصدي لو بكل الإمكانيات العملية والعلمية والأجهزة القانونية سواء التشريعية والتنفيذية والقضائية لكل دولة على حدى بما في ذلك الجزائر التي لازالت تسعى بشكل صارم إلى التصدي للإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص بمختلف مظاهره وأشكاله لحماية الناس من العمليات الإرهابية الالكترونية والتي سببت أضرارا جسيمة على الأفراد والدول، مما يستدعي تضافر الجهود الدولية والإقليمية والوطنية لوضع استراتيجيات هادفة لمكافحة هذا الخطر الداهم أو التقليل من حدة أثره وضرره.

وعليه فإننا سجلنا مجموعة من النتائج والاقتراحات تضمنتها الدراسة نذكر منها:

أولا: النتائج

- لا يوجد هناك اتفاق على تعريف قانوني جامع مانع للإرهاب الالكتروني في القانون الدولي، ويرجع ذلك إلى نظرة كل دولة لهذه الظاهرة، فالبعض يعتبره سلوكا إجراميا ويعاقب عليه، بينما البعض الآخر يعتبره مقاومة مشروعة، كما أن هناك تداخل لمفهوم الإرهاب الالكتروني مع غيره من المفاهيم الأخرى، وهذا مثل الجريمة المنظمة الالكترونية والجريمة المنظمة.
- يعتبر الإرهاب الالكتروني امتداد للجريمة الإرهابية التقليدية، ويكمن الفرق في الوسيلة المستعملة، والتي تتمثل في استغلال الوسائل الالكترونية والتقنية وشبكة الانترنت لارتكاب هذه الجريمة الخطيرة على الدول والشعوب.
- تتميز جريمة الإرهاب الالكتروني بعدة خصائص، وهذا مثل أنها من الجرائم العابرة للحدود، كما أنها ترتكب عن بعد ولا يتم اكتشافها إلا بعد فوات الأوان.

- تتنوع وتتميز صور الإرهاب الالكتروني، فمن إنشاء المواقع الالكترونية الإرهابية إلى استهداف البنية التحتية للدول عن طريق شبكة الانترنت، وهذا مثل البنى الاقتصادية ووسائل الاتصال والمواقع العسكرية والمؤسسات العامة والخاصة.
- اختلفت التشريعات المقارنة في تجريم ظاهرة الإرهاب الالكتروني والعقاب عليها، فالبعض نص على تجريمها بطريقة غير مباشرة من خلال تجريم الدخول على المواقع الالكترونية أو تعطيلها أو إتلافها، والبعض الآخر نص على تجريمها بطريقة مباشرة من خلال تجريم استعمال وسائل تكنولوجيا المعلومات في الإرهاب أو تسهيله أو تمويله أو تجنيد الأفراد للقيام بالأعمال الإرهابية.
- وجود تعاون بين أجهزة الشرطة في مختلف الدول وأبرز هذا التعاون إنشاء المنظمة الدولية للشرطة الجنائية(الإنتربول) وذلك لمكافحة الجرائم العابرة للحدود ومن بينها جرائم الإرهاب الالكتروني. كذلك تنفيذ عمليات شرطية مشتركة بين الدول لتعقب الجناة الذي يبدأ في دولة وينتهي على إقليم دولة أخرى.
- سعى المجتمع الدولي إلى إبرام اتفاقيات دولية لمكافحة الإرهاب الالكتروني وذلك من خال إبرام معاهدة بودابست لمكافحة جرائم الإنترنت التي تعد أولى المعاهدات التي تعلقت بمكافحة تلك الجرائم.
- وجود نظام مثل نظام تسليم المتهمين كان له الأثر البالغ على إظهار دور المجتمع الدولي في مواجهة جرائم الإرهاب الالكتروني وما لها من خصوصية عابرة للحدود.
- التعاون الدولي في مجال مكافحة جرائم الإرهاب الالكتروني عن طريق عقد دورات التدريب الدولية للأجهزة الوطنية للدول المنوط بها التصدي لتلك الجرائم على المستوى الوطني، والوصول إلى نتيجة مهمة وهي أن الدول المتقدمة لن تستطيع بمفردها مواجهة تلك الجرائم دون تعاون مشترك مع الدول النامية والعمل على تدريب الجهات الأمنية داخل الدول النامية لمواجهة تلك الجرائم.

ثانيا: التوصيات والاقتراحات

وفي هذا الإطار يمكننا رصد مجموعة من التوصيات والاقتراحات لمواجهة الإرهاب الالكتروني وتحقيق أمن واستقرار الدول نذكر منها:

- العمل على مواجهة أسباب الإرهاب وتحقيق رفاهية الشعوب عامة والشباب خاصة.
- تطوير تقنيات مراقبة شبكة الانترنت وتعزيز إجراءات الأمن والحراسة للمواقع الرسمية.

- تجريم الإرهاب الالكتروني في التشريعات الوطنية والقوانين الدولية والإقليمية.
- تعزيز التعاون الثنائي والإقليمي والدولي في مكافحة ظاهرة الإرهاب الالكتروني لتسليم المجرمين وتحقيق أمن واستقرار الدول.
- إقامة شراكات دولية جديدة لمكافحة الإرهاب لترجمة الرؤية المشتركة للدول الأعضاء المجسدة في إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب إلى واقع وإحداث تأثير حقيقي على أرض الواقع.
- انشاء غرفة عمليات دولية متخصصة في مراقبة الهجمات الارهابية الالكترونية، الي تتعرض لها أنظمة معلومات المؤسسات الحساسة، كتلك الخاصة بالدفاع، والجيش والمؤسسات الأمنية، والحد من آثارها.
- تعزيز الجهود الدولية في مكافحة الإرهاب الإلكتروني والاستفادة من الخبرة الدولية في مجال مكافحته وإنشاء مراكز دولية متخصصة لوضع سياسات وإستراتيجيات لرصد ومجابهة مخاطر الإرهاب الإلكتروني.
- ابرام اتفاقية دولية تتضمن تحديد مفهوم الإرهاب الإلكتروني وخطوات عملية لمنعه ومكافحته وضرورة وضع إطار تشريعي شامل لتجريم الإرهاب الإلكتروني وتحديد أركانه وإعتباره جريمة دولية والأعمال الإرهابية على شبكة الإنترنت والتعاون الدولي في تبادل البيانات والمعلومات بشأن فرض التزام دولي على مرتكبي الإرهاب الإلكتروني.
- ضرورة تقرير قوانين جنائية مستقلة عن التقليدية، تحتوي هذا النوع من الجرائم المستحدثة بشكل مفصل ودقيق.
- وضع إستراتيجية واضحة وطنيا ودوليا من أجل مكافحة ومواجهة جريمة الإرهاب الإلكتروني والتنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحة من خلال الإتفاقيات والمعاهدات الدولية وحث الدول فيها على ضرورة التعاون الدولي.

قـــائـــمـة

الـــمـــراجـــع

أولا: قائمة المصادر

1- القرآن الكريم.

- الآية 116 سورة الأعراف
- الآية 40 من سورة البقرة

2- التشريع العادي

- القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الصادر في 25 أوت 2009، الجريدة الرسمية، العدد 47
- القانون رقم 16-01 المؤرخ في 06 مارس2016، المتضمن التعديل الدستوري، المؤرخة في 7 مارس 2016، الجريدة الرسمية عدد: 14
- القانون رقم 18- 04 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية الصادر في:2018/05/13، الجريدة الرسمية، العدد 27

3- التشريع التنظيمي

- الامر رقم 66- 156، المؤرخ بثمانية جوان 1966 والمتضمن قانون العقوبات الجريدة الرسمية عدد 49 الصادرة في 19 جوان 1966
- المرسوم الرئاسي 19-172 المؤرخ في 03 شوّال عام1440 الموافق لـ06 يونيو 2019 يحدّد تشكيلة الهيئة الوطنيّة للوقاية من الجرائم المتّصلة بتكنولوجيّات الإعلام والاتصال وتنظيمها وكيفيات سيرها، الجريدة الرّسمية عدد 37 الصّادرة في 09 يونيو 2019
- مرسوم تشريعي رقم92-03، يتضمن مكافحة الارهاب والتخريب، المؤرخ في 30سبتمبر 1992،ج.ر، عدد 70 الصادرة بتاريخ01أكتوبر 1992.

ثانيا: قائمة المراجع

1- المراجع باللغة العربية

أ- الكتب

1. إبراهيم بن محمد محمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة، جامعة فطاني،ط1 ، تايلند 2018

2. أحمد فتحي سرور، مواجهة الارهاب الإلكتروني دار النهضة العربية،ط 03، القاهرة،مصر ، 2011
3. أسامة حسين محي الدين، جرائم الإرهاب على المستوى الدولي، المكتب العربي الحديث،د.ط، الإسكندرية، 2009
4. أمير فرج يوسف، مكافحة الإرهاب، مكتبة الوفاء القانونية،ط1، الاسكندرية، 2011
5. أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني–في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب ، دار الكتب والدراسات العربية، الاسكندرية، د.ط، 2015
6. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر ، مكتبة الوفاء القانونية،ط1، الإسكندرية، مصر ، 2011
7. بخاري جميل علي، جريمة الإرهاب الدولي ومشروعية نضال حركات التحرر الوطني إقليم كردستان،، المركز العربي للنشر والتوزيع، ط1، مصر ،2020
8. بلعليات ابراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري–أركان الجريمة، اهمية الإثبات الجنائي،طرق الإثبات الجنائي، دار الخلدونية للنشر والتوزيع،د.ط، الجزائر ،2007
9. جبران مسعود، معجم الرائد الفبائي في اللغة العربية والاعلام، دار العلم للملايين،ط3، بيروت، 2005،
10. جعفر حسن جاسم الطائي، جرائم التكنولوجيا المعلومات جديدة للجريمة الحديثة، دار البداية،ط1، عمان، 2007
11. حسنين شفيق، الإعلام الجديد والجرائم الالكترونية –التسريبات. .التجسس الالكتروني..الإرهاب،، دار فكر وفن للطباعة والنشر والتوزيع، ط1، مدينة 6اكتوبر، 2015
12. خلفي عبد الرحمن، القانون الجنائي العام دراسة مقارنة، دار بلقيس للنشر، الدار البيضاء،د.ط، الجزائر، 2016
13. خلفي عبد الرحمن، محاضرات في القانون الجنائي العام، دار الهدى، د.ط، عين مليلة– الجزائر، 2012
14. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط 1، دار النهضة العربية، القاهرة، 2011
15. سامي علي حامد عياد، تمويل الارهاب، دار الفكر الجامعي،ط1، الإسكندرية،2008
16. صدام حسين ياسين العبيدي، جرائم الانترنت وعقوباتها في الشريعة الإسلامية والقوانين الوضعية، المركز العربي للدراسات والبحوث العلمية،ط1، القاهرة 2019

17. صلاح هاشم، التنمية والجريمة المعولمة- سياسات الإفقار والهدم الخلاق، أطلس للنشر والإنتاج الإعلامي ش.م.م، ط1،الجيزة،، 2018
18. عادل عبد الصادق ، الارهاب الالكتروني وتأثيره على الدول، دار الأهرام للنشر والتوزيع، ط1، القاهرة، مصر ،2014،
19. عادل عبد الصادق، الارهاب الالكتروني القوة في العلاقات الدولية:نمط جديد وتحديات مختلفة،المركز العربي لأبحاث الفضاء الالكتروني،ط2، القاهرة،2016
20. عادل عبد الصادق، الارهاب الالكتروني-القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مطبوعات مركز الدراسات السياسية والاستيراجية،ط1، القاهرة، 2009
21. عبد السلام محمد، مفهوم الارهاب في الشريعة الاسلامية،دار الكتب العلمية،ط1،بيروت،2005
22. عبد العال الديربي محمد صادق اسماعيل، الجرائم الالكترونية دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية،ط1،القاهرة، 2012
23. عبد القادر الشيخلي، طبيعة الارهاب الالكتروني، رابطة العرب الإسلامي،ط1، السعودية، 2015
24. عبد القادر دندن وآخرون، العلاقات الدولية في عصر التكنولوجيات الرقمية تحولات عميقة مسارات جديدة، مركز الكتاب الأكاديمي، ط1،عمان، 2021
25. عبد القادر عدو، قانون العقوبات الجزائري القسم العام -الجريمة-نظرية الجزاء الجنائي، دار هومة للطباعة والنشر ،،د.ط، الجزائر ،2010
26. عبد الكريم خالد الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار ومكتبة الحامد للنشر والتوزيع،ط1، عمان، 2013
27. عبد الله سليمان، شرح قانون العقوبات الجزائري-الجريمة-القسم العام،الطبعة الاولى، ديوان المطبوعات الجامعية، الجزائر ،2005
28. عبد الله نورشعت، التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي،مكتبة الوفاء القانونية، ط1،الإسكندرية،2017
29. عثمان علي الحسن ويسي، الارهاب الدولي ومظاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام، دار الكتب القانونية،د.ط، مصر ،2011
30. علي يوسف الشكري، المنظمات الدولية، دار الصفاء للنشر والتوزيع،ط1، عمان، 2012،
31. غادة نصار، الإرهاب والجريمة الالكترونية، العربي للنشر والتوزيع ط1،القاهرة، 2017

32. غازي حنون خلف الدراجي، استظهار القصد الجنائي في جريمة القصد العمد منشورات الحلبي الحقوقية، ط1،، لبنان،2012،
33. كوركيس يوسف داوود، الجريمة المنظمة، الدار العلمية والدولية دار ثقافة للنشر والتوزيع،ط1، عمان، 2001
34. الكيالي عبد الوهاب، الموسوعة السياسية،الجزء السابع، المؤسسة العربية للدراسات والنشر، بيروت، د.ط،1994،.
35. محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات المطبوعات الجامعية، د.ط،الإسكندرية مصر، 2003.
36. محمد امين بشرى، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث جامعة نيل العربية للعلوم الامنية د.ط. الرياض، 2004،
37. محمد حسن عمر برواري، غسيل الاموال وعلاقته بالمصارف والبنوك–دراسة مقارنة ، دار قنديل للنشر والتوزيع،ط1، عمان، 2013
38. محمد حسن مرعي، الجوانب الموضوعية لجريمة اثارة الفتنة الطائفية دراسة تحليلية مقارنة المركز العربي للنشر والتوزيع، ط1، القاهرة، 2018،
39. محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت والأحكام الموضوعية والأحكام الجزائية، منشورات حلبي الحقوقية ط 1، بيروت، 2011
40. محمد علي سويلم، جرائم الارهاب والارهاب الالكتروني –دراسة مقارنة،المصرية للنشر والتوزيع،ط1، القاهرة،2018
41. محمد فتحي عيد، واقع الإرهاب في الوطن العربي ، أكاديمية نايف للعلوم الأمنية،الرياض،د.ط، 1999
42. محمد محمود مدين، فن التحقيق والإثبات في الجرائم الالكترونية، المصرية للنشر والتوزيع،ط1،القاهرة، 2020
43. محمود عبد العزيز محمد، الإرهاب النفق المظلم في تاريخ البشرية وعلاقته بالأديان السماوية، دار الكتب القانونية، د.ط، القاهرة، 2013
44. مصطفى يوسف كافي، جرائم الفساد، غسيل الاموال،السياحة،الارهاب الالكتروني المعلوماتي، مكتب المجتمع العربي للنشر والتوزيع، ط1، عمان، 2014
45. مصطفى يوسف كافي،، الإدارة الإلكترونية، دار ومؤسسة راسلان للنشر والطباعة والتوزيع،ط1،دمشق،2011

46. مصطفى يوسف كافي، ماهر عودة الشمايلة،محمود عزت اللحام،الإعلام والارهاب الالكتروني،دار الاعصار العلمي للنشر والتوزيع، ط1، الاردن،2015
47. منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الاسلامي، دار الفكر الجامعي،ط1، الإسكندرية،2008
48. منصور رحماني، الوجيز في القانون الجنائي العامدار العلوم للنشر والتوزيع،د.ط، عنابة،
49. منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي، ط1، الاسكندرية، 2004
50. موفق عيد فهد المساعيد، جرائم الإرهاب في التشريع الأردني والاتفاقيات الدولية، مركز الكتاب الاكاديمي،ط1، الاردن، 2019،
51. مولود ديدان، قانون الإجراءات الجزائية، الأمر 11- 02، دار بلقيس،الجزائر.
52. نسيب نجيب، التعاون القانوني والقضائي الدولي في ملاحقة مرتكبي جرائم الإرهاب، مركز الكتاب الأكاديمي، ط1، عمان، 2017
53. هلالي عبد اللاه أحمد، جرائم المعلوماتية وأساليب المواجهة وفقاً لاتفاقية بودابست، دار النهضة، ط1، القاهرة، 2007،
54. هيثم عبد الرحمن البقلي، الجرائم الإلكترونية الواقعة على العرض بين الشريعة والقانون المقارن، دار العلوم للنشر والتوزيع،ط1، القاهرة، 2010
55. هيثم فالح شهاب، جريمة الإرهاب وسبل مكافحتها في التشريعات الجزائية المقارنة، دار الثقافة للنشر والتوزيع، ط1، عمان، 2010
56. وسيم حسام الدين، مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة مكتبة القانون والاقتصاد،ط1، الرياض، السعودية 2016
57. وضاح زيتون، المعجم السياسي.، دار أسامة المشرق الثقافي، ط1، الأردن، 2006
58. ولد الصديق ميلود، مكافحة الإرهاب بين مشكلة المفهوم واختلاف المعايير، مركز الكتاب الأكاديمي، ج1، ط1،عمان، 2018
59. يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية،ط1، القاهرة، مصر، 2011
60. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كرديستان للدراسات الاستراتيجية، د.ط، السليمانية، 2007

ب –الاطروحات والمذكرات

ب1– أطروحات الدكتوراه

1. جمال بوازدية، الإستراتيجيات المغاربية لمكافحة الإرهاب، (اطروحة دكتوراه، الدراسات الدولية)، قسم الحقوق،جامعة الجزائر 2012،03-2013

2. حسين عبد الصاحب، عبد الكريم الربيعي، جرائم الاعتداء على حق الإنسان في التكامل الجسدي– دراسة مقارنة، (أطروحة الدكتوراه، القانون)، كلية القانون جامعة بغداد، 2005،

3. خذيري عفاف، الحماية الجنائية للمعطيات الرقمية، (أطروحة دكتوراه، علوم في القانون الجنائي)، قسم الحقوق،كلية الحقوق والعلوم السياسية جامعة تبسة، 2017-2018

4. درار نسيمة، الامن المعلوماتي وسبل المواجهة مخاطرة في التعامل الالكتروني، دراسة مقارنة،(أطروحة الدكتورة،القانون الخاص)،كلية الحقوق قسم القانون، جامعة أبي بكر بلقايد تلمسان الجزائر، 2016

5. شعنبي صابرة، الجهود الدولية في مكافحة الارهاب الالكتروني(، أطروحة دكتوراه، العلوم في الحقوق)، قانون جنائي،جامعة العربي التبسي، تبسة،2019

6. شنتير خضرة، الاليات القانونية لمكافحة الإرهاب الالكتروني–دراسة مقارنة–(اطروحة دكتوراه،القانون الجنائي)،كلية الحقوق، جامعة أحمد درايةأدرار ،2020-

7. عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة،(أطروحة دكتوراه،قانون جنائي)،قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2012

8. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية الحاسب والانترنت، (رسالة دكتوراه، القانون)، الجامعة الإسلامية، كلية الحقوق، لبنان. 2004.

9. هروال هبة نبيلة،جرائم الانترنت دراسة مقارنة، (أطروحة دكتوراه،قانون) قسم الحقوق، كلية الحقوق والعلوم السياسية ابي بكر بلقايد،تلمسان،2013-2014،

ب2– رسائل ومذكرات الماجستير

1. اسراء طارق جواد كاظم الجابري، جريمة الإرهاب الالكتروني– دراسة مقارنة– (شهادة الماجستير، القانون العام)، كلية الحقوق، جامعة النهرين، العراق،2012

2. توفيق شريخي، الإرهاب الالكتروني وتأثيره على امن الدولة، (مذكرة ماستر، إستراتيجية وعلاقات دولية)،كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة، الجزائر، 2018

3. صفاء كاظم غازي الجيّاشي، جريمة قرصنة البريد، دراسة مقارنة، (رسالة ماجستير، كلية القانون)، جامعة بابل،العراق، 2016

4. عمر عباس خضير العبيدي، الإرهاب الالكتروني في نطاق القانون الدولي (رسالة ماجستير،حقوق) كلية الحقوق جامعة تكريت، العراق 2019،

5. محمد فوزي صالح، الجريمة المنظمة وأثارها على حقوق الإنسان، (شهادة الماجستير، القانون الدولي لحقوق الإنسان)، قسم الحقوق،كلية الحقوق جامعة يحيى فارس، المدية، 2008-2009

6. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية دراسة مقارنة بين التشريعين الأردني والعراقي،(شهادة ماجستير، القانون العام)، كلية الحقوق، جامعة الشرق الأوسط، 2017، ص: 42 ،

7. نجاري علي فايزة كريم، الآليات القانونية لمكافحة الإرهاب الالكتروني، (شهادة الماجستير، تخصص قانون دولي للأعمال)، قسم الحقوق،كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016

8. نور الله تلة، الإرهاب بالوسائل الالكترونية، (مذكرة ماجستير، القانون الجزائي) كلية الحقوق، جامعة دمشق،2015-2016،

ج- المداخلات

1. بن صويلح أمال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام،الملتقى الدولي حول الاجرام السيبراني المفاهيم والتحديات خطوة عامة نحو مكافحة الارهاب الالكتروني في الجزائر،جامعة 8ماي قالمة، يومي 11-12 أفريل 2017

2. بوحادة سارة، أثر الإرهاب الالكتروني على أمن واستقرار الدول، مداخلة، د.ط،2017،

3. حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الإعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017،

4. دياب موسى البداينة، الجرائم الالكترونية المفهوم والإثبات، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، تاريخ 2 الى 4 سبتمبر 2014، عمان،

5. رائد العدواني، المعالجة الدولية لقضايا الإرهاب الالكتروني (محاضرة ألقيت في دورة تدريبية بعنوان توظيف شبكة التواصل الاجتماعي في مكافحة الإرهاب في الرياض فيفري 2016

6. عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات" (المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت2-4 جوان 2008)،القاهرة،

7. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر «الجرائم الإلكترونية،» طرابلس، بتاريخ 24- 25 مارس 2017.

8. وداعي عز الدين، تطور الجريمة الارهابية من الجريمة التقليدية الى الجريمة المعلوماتية، ملتقى وطني حول الجريمة المعاصرة – كلية الاداب والعلوم الانسانية والعلوم الاجتماعية،جامعة باجي مختار عنابة، يومي 13-17 ديسمبر 2017

هـ- المجلات

1. اسعد طارش عبد الرضا علي ابراهيم مشجل المعموري، الأمن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد العام 2003 (العراق، دراسات دولية، العدد 80 مجلد 2020 الصادرة في 31 يناير 2020)جامعة بغداد

2. براهيمي جمال، مكافحة الجريمة الالكترونية في التشريع الجزائري، (المجلة النقدية للقانون والعلوم السياسية، العدد 2، كلية الحقوق والعلوم السياسية)، جامعة مولود معمري، تيزي وزو، 15 / 11 / 2016

3. بلعيور محمد نذير. بوعيشة بوغوفالة، دور المنظمة الدولية للشرطة الجنائية في مكافحة الجريمة المنظمة (مجلة البحوث القانونية والاقتصادية المجلد02 العدد02) المركز الجامعي افلو-ماي 2020

4. بن صويلح أمال ، إستراتيجية منظمة الأمم المتحدة في مكافحة الإرهاب الدولي،(المجلة الجزائرية للعلوم الانسانية والاجتماعية عدد02-2017

5. بواب بن عامر،المواجهة التشريعية للإرهاب الإلكتروني،(مجلة البحوث العلمية العدد 09،ديسمبر 2017)،

6. توفيق مجاهد،طاهر عباسة، جريمة الإرهاب الإلكتروني في ضوء أحكام الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، (مجلة العلوم القانونية والسياسية، المجلد 09–العدد 03 ديسمبر 2018)،
7. رقيق ايناس، تأثير الإرهاب المعلوماتي على على بقاء ومستقبل بناء الدول (مجلة الحوكمة والقانون الاقتصادي– جامعة باتنة،عدد 1–2022)
8. سعد صالح كشطي، موقف الشريعة الاسلامية من الارهاب (مجلة الرافدين للحقوق، العراق مجلد 12 العدد 44)، ، كلية الحقوق جامعة الموصل، ، 2010
9. سلوى أحمد ميدان، الارهاب والجهود الدولية لمكافحته، (العراق، مجلة كلية القانون للعلوم القانونية والسياسية،جامعة كركوك،، العدد2006،05)،
10. شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، (مجلة جامعة الشارقة للعلوم القانونية العدد01 المجلد17) كلية القانون الامارات يونيو2020
11. صباح كزيز، أمال كزيز، الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم 1، العدد 8 –2008
12. علي جاسم التميمي، الارهاب الالكتروني واثره على المجتمع –المجلة السياسية والدولية،جامعة المستنصرية العراق،د.س،
13. عمراني كمال الدين، الجريمة المنظمة وجريمة الإرهاب– دراسة مقارنة– (مجلة الفقه والقانون عدد 17، 2014)، المركز الجامعي، النعامة
14. كوثر حازم سلطان، موقف القانون والقضاء من الجريمة الإلكترونية السيبريانية المقارنة، (مجلة كلية التربية الأساسية، المجلد 22 العدد 96)، د.ب.ن، 2016
15. محمد خميخم، موقف التشريع الجزائري من جريمة الإرهاب الالكتروني، مجلة حوليات جامعة الجزائر 1، المجلد 34،العدد02–2020، جوان 2020،
16. محمد فهاد الشلالده، احمد حسن ابو جعفر،إشكالية التوسع في تهم الإرهاب في المنطقة بدوافع سياسية،(مجلة دراسات شرق أوسطية العدد 72 2015) الأردن،
17. وفاء لطفي حسن عبد الواحد، الإرهاب الإلكتروني والأمن القومي في ظل جائحة كورونا (كوفيد–19) (المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية، المجلد 7 –العدد 13 جانفي2022)
18. يوسف مرين، جريمة الارهاب في القانون الجزائري،(مجلة جامعة القدس المفتوحة للابحاث والدراسات،عدد 42–02، 2017)

و- المواقع الالكترونية

1. عادل عبد الصادق، الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني، دوريات – قضايا إستراتيجية، الخميس,6 أغسطس 2015 - 12:14 م https://accronline.com/article_detail.aspx?id=22762
2. المنظمة الدولية للشرطة الجنائية الانتربول، عرض عام https://www.interpol.int/ar/3/10
3. http://www.aspip.org/page.aspx?page_key=wipo&lang=ar
4. https://www.insdip.com/ar/organizacion-mundial-de-la-propiedad-intelectual-ompi
5. https://www.lebarmy.gov.lb/ar/content

الـفـهـرس

المحتويات

الملخص:

يشهد العالم اليوم مجموعة من التحولات والتغيرات في شتى المجالات، ومن أبرز هذه التحولات ظهور الثورة التكنولوجية الهائلة والعولمة التي تهدف إلى جعل العالم قرية صغيرة. فكان لهذه التحولات أثر على مختلف المفاهيم وتطويرها إلى مفاهيم جديدة مواكبة للعصر. ومن أهم هذه المفاهيم مفهوم الإرهاب الالكتروني كشكل جديد من أشكال الإرهاب الذي يعتمد على استخدام التقنيات الرقمية الحديثة لنشر الخوف والرعب لأغراض سياسية، أي هي جريمة الكترونية عابرة للحدود عالمية خطيرة تمس بأمن الدول خاصة المتقدمة منها التي تستعمل بشكل كبير تكنولوجيا المعلومات والاتصال في معظم المجالات. ومن مظاهر تهديد الإرهاب الالكتروني لأمن الدولة، عمل الجماعات الإرهابية على نشر أفكارهم وقيمهم على شبكات التواصل الاجتماعي، وضم أكبر قدر ممكن من الأفراد وتجنيدهم وتعليمهم كيفية استخدام المتفجرات واختراق المواقع الالكترونية وغيرها من العمليات الإجرامية غير المشروعة، إضافة إلى اختراق الشبكات الحساسة للدول والتجسس عليها وإرسال رسائل تهديد للدول لقبول مطالبهم. فنتيجة لجملة هذه التهديدات المتنوعة، يتوجب على المجتمع الدولي بمختلف أشكاله تبني مجموعة من الاستراتيجيات لمواجهة الإرهاب الالكتروني، وتحقيق أمن واستقرار الدول. فالغاية الاساسية من هذه الورقة البحثية التعرف على الإرهاب الالكتروني (تعريفه – اثاره– والجهود المبذولة لمكافحته)

الكلمات الاستدلالية: الإرهاب الإلكتروني – الأمن – الدولة- الإنترنت- المواقع الالكترونية- الجريمة

Résumé

today is witnessing a set of advances and changes in various fields, the most important of which is the emergence of the technological revolution and globalization, which made the world a small city. But at the same time, they influenced various concepts, which led to their development into new ones in line with the era. Accordingly, the connotation of cyber-terrorism appeared as a new form of terrorism, which relies on the use of modern digital technologies to spread fear and terror for political purposes, which led to the emergence of the problem of cross-border cybercrime, which has become affecting the security of countries, especially the developed ones because it uses more the information and communication technology in various fields. The research identified cyber-terrorism as one of the most substantial threats that affect the security of countries because terrorist groups can quickly and widely spread their ideas and values on social networks, enabling them to recruit more individuals by teaching them how to use explosives and penetrate websites and other criminal operations. In addition to penetrative security network countries, spying on them, and sending threatening messages to accept their demands. As a result of the combination of these various threats, the international community in its various forms must adopt a set of strategies to confront cyber-terrorism, to enhance the security and stability of countries. Therefore, the main objectives of this research paper are to identify cyber-terrorism (its definition - its effects - and the efforts made to combat it).