وزارة التعليم العالي والبحث العلمي

جامعة العربي التبسي- تبسة-

كلية الحقوق والعلوم السياسية

قسم الحقوق

# الجهود الدولية في مكافحة الإرهاب الالكتروني

أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق

تخصص قانون جنائي

إعداد الطالبة : شعنبي صابرة

مدير الأطروحة: الأستاذ: دلول الطاهر

أعضاء لجنة المناقشة:

| الاسم واللقب | الرتبة | الجامعة | الصفة |
|---|---|---|---|
| بشير هادفي | أستاذ | جامعة-تبسة- | رئيسا |
| الطاهر دلول | أستاذ | جامعة -تبسة- | مشرفا ومقررا |
| الأخضر بوكحيل | أستاذ | جامعة -عنابة- | عضوا مناقشا |
| دليلة مباركي | أستاذ | جامعة -باتنة- | عضوا مناقشا |
| محمد بوكماش | أستاذ | جامعة -خنشلة- | عضوا مناقشا |
| سعاد نويري | أستاذ محاضر-أ- | جامعة -تبسة- | عضوا مناقشا |

السنة الجامعية:

**2019**

## شكـــــر وعرفـــــان

**الحمد لله الذي هدانا إلى هذا ولولاه ما كنا لنهتدي، الأحق بالثناء لا نجيد ثناء كما أثناه على نفسه والصلاة والسلام على من لا نبي بعده سيدنا محمد ﷺ .**

**أتوجه بالشكر الجزيل إلى الأستاذ الفاضل البروفيسور دلول الطاهر لإشرافه طيلة السنوات الماضية على هذا العمل المتواضع ولما قدمه لي من نصائح وتوجيهات أنارت دربي وذللت المصاعب أمامي، فكان نعم المشرف وخير مرشد وموجه فلك مني جزيل الشكر والامتنان أستاذي الفاضل**

**كما أتوجه بالشكر الكبير إلى أساتذتي الأفاضل رئيس وأعضاء لجنة المناقشة كل باسمه .**

**ولا يفوتني أن أن أتقدم بأسمى عبارات الشكر إلى كل من دعمني وساعدني لإتمام هذا العمل.**

# مقدمة

من المعلوم أن الانفتاح على شبكة المعلومات في جميع المجالات السياسية والثقافية والقانونية والتجارية وعدم ارتباطها بدولة معينة أو حدود جغرافية أو سياسية معينة وكذلك صعوبة الرقابة أو المحاسبة على كل ما ينشر فيها أفكار، كل هذا جعل من شبكة الإنترنت الموطن المختار للإرهابيين والمتطرفين لما يمارسونه من أعمال إرهابية وتخريبية ، كما أنها أصبحت البيئة الخصبة لنشر الأفكار المتطرفة التي تسيطر على وجدان الأفراد وإفساد عقائدهم وزيادة تمردهم واستغلال معاناة الآخرين في تحقيق مآرب خاصة تتعارض ومصلحة المجتمع أو القيام بأعمال تخريبية بشكل يخفي هويتهم المباشرة وبشكل أبسط مما يقوم به الإرهابيون في الصورة التقليدية، ففي حين يحتاج الإرهاب الفعلي إلى أسلحة وعتاد ومدرعات وقنابل وتحركات سرية جداً قد تصيب أو تخفق، فضلا على التكاليف المادية الباهضة لإنجاح هذه العمليات، يحتاج الإرهاب الإلكتروني إلى بعض المعلومات ليستطيع اقتحام الحواجز الإلكترونية، كما أن تكاليف القيام بهذه الهجمات لا تتجاوز جهاز حاسوب والدخول إلى الشبكة الانترنت، الأمر الذي أدى إلى زيادة خطورة الجرائم الإرهابية وتعقيدها، سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة .

## أهمية الموضوع.

لما أصبح الإرهاب الالكتروني خطرا يهدد العالم بأسره إذ لم يفرق بين مجتمع وآخر ولا بين دين وآخر، فكل الشعوب أصبحت عرضة للهجمات الإرهابية عبر الانترنت في أي وقت وفي كل مكان من العالم فباتت الآليات القديمة والتقليدية لوحدها غير كافية ولا قادرة على حماية المجتمع من هذا الخطر ومن أجل ذلك حاولت جميع الدول التصدي لهذه الجريمة التي فتكت بالدول والمجتمعات.

ولأن قضايا الإرهاب باتت من القضايا الخطيرة والتي تهدد مختلف المجالات ومن أهمها زعزعة الأمن الوطني، وهذا على المستوى الداخلي لكل دولة، أما على المستوى الدولي فإنها تهدد الأمن والسلم الدوليين، من أجل ذلك تمثلت الأهمية العملية لهذه الدراسة في تسليط الضوء على كيفية استغلال التطور التكنولوجي من طرف الجماعات الإرهابية لتنفيذ مخططاتهم التخريبية، وكيف سهل هذا التطور التكنولوجي التواصل بي الجماعات الإرهابية من مختلف دول العالم حيث أصبح العالم

قرية صغيرة، فينفذون عملياتهم الإرهابية دون الحاجة إلى دخول المطارات أو إخفاء المتفجرات أو تفخيخ السيارات وعبور البوابات.

أما الأهمية العلمية لدراسة الإرهاب الالكتروني فتتمثل في محاولة إثراء المكتبة القانونية، إذ لاحظنا من خلال دراستنا واهتمامنا بالموضوع كثرة الدراسات المتعلقة بالإرهاب التقليدي والجهود الدولية في مكافحته وتوعها، أما دراسته في صورته العصرية والمتطورة فكانت محتشمة تحتاج إلى توسع أكثر يوازي التوسع في دراسة جريمة الإرهاب التقليدي وهذا بهدف الوصول إلى أحسن السبل وأنجعها لمواجهة هذه الظاهرة الخطيرة وخاصة أمام ضعف الأمن في البيئة المعلوماتية وخاصة في دولنا العربية والتي عانت كثيرا من هذه الجريمة الخطيرة.

## دوافع اختيار الموضوع.

أدى الاستخدام السيء لتقنية المعلومات إلى ظهور الكثير من الجرائم المستحدثة ومنها الإرهاب الالكتروني والذي يعد من أخطر هذه الجرائم وأبشعها، بالإضافة إلى الآثار السلبية التي يتركها على نفس الفرد والمجتمع على السواء، ومن أجل ذلك كان دافعنا الشخصي هو اهتمامنا بهذا الموضوع المستحدث وكيف تصدت له مختلف الدول، وهذا لما يشكله من خطورة على السلم والأمن الدوليين.

وأما عن الدوافع الموضوعية فيمكن أن نذكر أن أهمها يتمثل في أهمية دراسة هذا الموضوع في حد ذاتها والتي سبق أن تحدثنا عنها في العنصر السابق، كما يتمثل السبب الموضوعي الآخر لهذه الدراسة في بغية الوصول إلى معرفة مدى نجاح مختلف الجهود الإقليمية والدولية في مكافحة هذه الجريمة الخطيرة والمتطورة.

## أهداف الدراسة.

تهدف هذه الدراسة إلى الوقوف على أهم الأحكام الموضوعية والإجرائية المتعلقة بالإرهاب الالكتروني، على اعتبار أنه جريمة مستحدثة وجد خطيرة، وأيضا التعرف على أهم الجهود الدولية والإقليمية لمكافحة هذه الجريمة.

هذا وتهدف هذه الدراسة إلى التعرف على مدى جدوى الجهود الدولية والإقليمية والوقوف على مختلف جوانب القصور فيها ومحاولة إيجاد بعض الحلول المناسبة لها من خلال اقتراح بعض التوصيات في هذا الخصوص.

## الدراسات السابقة.

في الحقيقة وعند الحديث عن الدراسات السابقة في هذا الموضوع فإننا لم نصادف دراسة سابقة تحمل نفس العنوان أي الجهود الدولية في مكافحة الإرهاب الالكتروني إلا أن هذا لا ينفي أننا اعتمدنا على العديد من الدراسات التي فتحت الباب أمامنا وساعدتنا ليرى هذا العمل النور، ومن أهم هذه الدراسات والتي اعتمدنا عليها بنسبة كبيرة ما يلي:

_ ساعد الهام حورية، وسائل مكافحة الإرهاب، أطروحة دكتوراه في القانون العام، كلية الحقوق سعيد حمدين– يوسف بن خدة، جامعة الجزائر 01، 2016/2015، وقد ركزت الباحثة في هذه الأطروحة على الوسائل التقليدية في المكافحة كما انصبت دراستها على جريمة الإرهاب التقليدي في حين سعت دراستنا إلى الجمع بين الوسائل التقليدية والحديثة في مكافحة الإرهاب الالكتروني.

_ عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ القوة في العلاقات الدولية، مذكرة ماجستير في العلوم السياسية، كلية الاقتصاد والعلوم السياسية– قسم العلوم السياسية، القاهرة، 2009 وقد استفدنا من هذه الدراسة في توضيح العديد من المفاهيم المتعلقة بالإرهاب الالكتروني إلا أن هذه الدراسة تميل إلى الجانب السياسي في حين أن دراستنا قانونية بحتة.

## المنهج المتبع.

بهدف الوصول إلى النتائج المرجوة من هذه الدراسة، ونظرا لخصوصية هذه الجريمة اتبعنا المنهج التحليلي، وذلك من خلال تحليلنا للنصوص القانونية لمحاولة الوصول إلى مقصد كل مشرع من وراء النصوص التي سنها في هذا الشأن، بالإضافة إلى استنادنا على المنهج الوصفي في العديد من الجزئيات الخاصة بهذه الأطروحة.

## إشكالية الدراسة.

تخلف جريمة الإرهاب الالكتروني آثارا مدمرة سواء على المستوى النفسي أو الاجتماعي وحتى على المستويين الاقتصادي والأمني، وهذا الخطر لم يقتصر على نطاق إقليم الدولة الواحدة بل تعداها إلى مختلف الدول بل شمل العالم بأسره، الأمر الذي خلق حالة من الاستنفار التي عمت معظم دول العالم وسارعت إلى اتخاذ العديد من الإجراءات على الصعيدين الدولي والوطني، وعليه يثور تساؤل مهم مفاده: ما مدى فعالية كل من الجهود الإقليمية والدولية في التصدي لجريمة الإرهاب الالكتروني، وهل حققت الجهود الإقليمية نوع من التكامل مع الجهود الدولية لتحقيق الحماية اللازمة؟؟؟

## التصريح بالخطة,

قصد الإحاطة بمختلف جوانب الموضوع، وللإجابة على إشكالية البحث وأهم الإشكاليات القانونية التي يثيرها هذا الموضوع، ارتأينا تقسيم هذا الموضوع إلى بابين كما يلي:

_ الباب الأول: الأحكام العامة لمكافحة جريمة الإرهاب الالكتروني، وقد قسمنا هذا الباب بدوره إلى فصلين خصص الفصل الأول للأحكام الموضوعية لجريمة الإرهاب الالكتروني، وعالجنا فيها ماهية جريمة الإرهاب الالكتروني والبنيان القانوني لهذه الجريمة وذلك من خلال مبحثين اثنين، وأما الفصل الثاني فقد خصص للأحكام الإجرائية لجريمة الإرهاب الالكتروني، وقد تطرقنا من خلاله إلى كل من القواعد الخاصة باستخلاص الدليل في جريمة الإرهاب الالكتروني واثبات جريمة الإرهاب الالكتروني من خلال مبحثين .

_ الباب الثاني: الآليات الإقليمية والدولية في مكافحة الإرهاب الالكتروني، وقد قسمنا هذا الباب أيضا إلى فصلين خصص الفصل الأول للآليات الإقليمية لمكافحة الإرهاب الالكتروني، وقسمناه بدوره إلى مبحثين خصصنا الأول إلى دور المنظمات الغربية في مكافحة الإرهاب الالكتروني، وأما الثاني إلى الدور العربي في مكافحة الإرهاب الالكتروني، وأما الفصل الثاني خصص إلى الآليات الدولية العالمية في مكافحة الإرهاب الالكتروني، ومن خلاله تعرضنا إلى دور المنظمات الدولية العالمية في مكافحة جريمة الإرهاب الالكتروني في مبحث أول، التعاون القضائي الدولي لمكافحة الإرهاب الالكتروني من خلال مبحث ثاني.

وفي الأخير ختمنا الموضوع بخاتمة اشتملت على مجموعة من النتائج التي تمخضت عن هذه الدراسة، وكذلك اقترحنا مجموعة من التوصيات، دون أن ننسى أننا افتتحنا هذه الدراسة بمقدمة مشتملة على مختلف عناصرها المنهجية.

# الباب الأول:

## الأحكام العامة في مكافحة جريمة الإرهاب الالكتروني

## الباب الأول: الأحكام العامة لمكافحة جريمة الإرهاب الالكتروني.

يقصد بالأحكام العامة لمكافحة جريمة الإرهاب الالكتروني مختلف الأحكام الموضوعية والإجرائية لمكافحة هذه الجريمة، فحتى يتمكن أي تشريع من مكافحة جريمة ما وجب أن يحدد معالمها وأطرها وخاصة في مجال الإرهاب وجريمة الإرهاب الالكتروني بالخصوص.

فكما هو معلوم أن هناك اختلاف فقهي كبير جدا حول تحديد مفهوم شامل وكامل ودقيق لجريمة الإرهاب سواء كانت الجريمة التقليدية أو المستحدثة (إرهاب الكتروني)، ومن أجل ذلك وجب محاولة الوصول إلى تعريف يناسب جسامة هذه الجريمة ويماشي تطورها، بالإضافة إلى ذلك فإن الجريمة لا تقوم إلا بأركانها ومن أجل ذلك فحتى تتحدد الجريمة بدقة وتتميز عن غيرها من الجرائم وجب تحديد أركان هذه الجريمة .

والأحكام الموضوعية لا تكفي لوحدها لمكافحة أي جريمة فتكتمل المكافحة بالأحكام الإجرائية أي مختلف الإجراءات القانونية التي يتخذها المشرع لمتابعة هذه الجريمة وملاحقة الجناة (الإرهابيون).

ومن أجل كل هذا ومما سبق قسمنا هذا الباب إلى فصلين اثنين

- الفصل الأول: الأحكام الموضوعية لمكافحة جريمة الإرهاب الالكتروني.
- الفصل الثاني: الأحكام الإجرائية لمكافحة جريمة الإرهاب الالكتروني.

## الفصل الأول:الأحكام الموضوعية لجريمة الإرهاب الالكتروني.

نظرا لأن جريمة الإرهاب الالكتروني تعتبر من الجرائم المستحدثة، والتي انتشرت في العالم بعد التطور التكنولوجي الخطير، حيث أصبح من السهل بما كان الحصول على حاسب آلي وتزويده بشبكة انترنت، فأمام ضعف تأمين البيئة الرقمية في الدول النامية وخاصة العربية، وقلة التكاليف وجدت الجماعات الإرهابية فرصتها في تنفيذ مخططاتها الإجرامية التخريبية دون تحمل تكاليف باهظة، ودون تعريض أنفسهم للخطر.

وعلى ذلك فإن الهدف من وراء العمليات الإرهابية لم يختلف بل بقي كما هو الاختلاف فقط كان في الوسيلة المستخدمة، حيث تغيرت هذه الوسيلة، وتطورت مع التطور العلمي والتكنولوجي، إلا أن السؤال الذي يطرح نفسه هنا هو هل تغيرت الطبيعة القانونية لجريمة الإرهاب الالكتروني عن طبيعة الإرهاب التقليدي أم حافظت على نفس الطبيعة؟؟؟ .

ومن أجل ذلك سوف نحاول من خلال هذا الفصل التعرف على جريمة الإرهاب الالكتروني والإحاطة بمختلف جوانبها القانونية من خلال التعرض إلى مفهومها وكذلك الأركان المميزة لها وذلك من خلال مبحثين اثنين، المبحث الأول وخصص لماهية الإرهاب الالكتروني، والمبحث الثاني خصص البنيان القانوني لجريمة الإرهاب الالكتروني.

## المبحث الأول: ماهية الإرهاب الالكتروني.

لما كان الإرهاب الالكتروني صورة أو مرحلة متقدمة وحديثة لتطور الإرهاب التقليدي كان لزاما علينا أن نتعرض أولا لمفهوم الإرهاب التقليدي حتى نتمكن من توضيح مفهوم الإرهاب الالكتروني بطريقة أفضل وأسهل .

وبما أن مفهوم الإرهاب كمصطلح تقليدي أصبح واضحا إلى حد ما فان الإرهاب الالكتروني كمفهوم مستحدث لا يزال يعتريه الغموض وذلك لأنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه. وكذا من حيث دور الفاعل فيه وطبيعة سلوكه.

ومن أجل ذلك ومن كل ما سبق سوف نتطرق أولا إلى مفهوم جريمة الإرهاب الالكتروني في مطلب أول، وبعدها سوف نتعرض إلى أركان جريمة الإرهاب الالكتروني مطلب ثاني.

### المطلب الأول: مفهوم جريمة الإرهاب الالكتروني.

قبل التطرق إلى مفهوم جريمة الإرهاب الالكتروني وجب أولا استعراض مفهوم الإرهاب التقليدي وهذا لأن جريمة الإرهاب الالكتروني نوع مستحدث لجريمة الإرهاب التقليدية .

ومن أجل ذلك قسمنا هذا العنصر إلى فرعين تطرقنا في الفرع الأول إلى تعريف الإرهاب الدولي أي التقليدي، وفي فرع ثاني إلى تعريف جريمة الإرهاب الالكتروني.

#### الفرع الأول: تعريف الإرهاب الدولي( الإرهاب التقليدي).

لقد ملأت قضية الإرهاب الدنيا، وشغلت كل المجتمعات، فأصبحت هذه القضية حديثا مشتركا في كل اللغات وعلى اختلاف الحضارات إلا انه ورغم هذا الاشتراك هذه المجتمعات اختلفت في تحديد معناها، أجل ذلك يصعب حصر تعريفات محددة للإرهاب[1].

ومن أجل محاولة الوصول إلى تعريف أكثر وضوحا يتعين علينا التطرق أولا إلى التعريف اللغوي للإرهاب وذلك في فرع أول، ومن ثمة نتعرض إلى التعريف الاصطلاحي من خلال فرع ثاني.

[1] أغادير عرفات حويجان، محمد عوض الترتوري علم الإرهاب– الأسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب، الطبعة الأولى، دار الحامد، عمان– الأردن، 2006،ص 19 .

## أولا: التعريف اللغوي.

يحمل الإرهاب في طياته معاني الخوف أو التخويف، فلفظ إرهاب مصدره " رهب" والذي جاءت مشتقاته في أكثر من موضع في القرآن الكريم، وجميع الآيات التي ورد فيها هذا المصدر تشير إلى تلك المعاني[1]

فقد جاء في القرآن الكريم قوله تعالى:" **وَأَوْفُوا بِعَهْدِي أُوفِ بِعَهْدِكُمْ وَإِيَّايَ فَارْهَبُونِ** "[2] وقوله أيضا:" **إِنَّمَا هُوَ إِلَٰهٌ وَاحِدٌ فَإِيَّايَ فَارْهَبُونِ** "[3]، وقال تعالى: " **وَفِي نُسْخَتِهَا هُدًى وَرَحْمَةٌ لِّلَّذِينَ هُمْ لِرَبِّهِمْ يَرْهَبُونَ** "[4].

كما نجد أيضا مصدر "رهب" في قوله تعالى:" **تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ وَآخَرِينَ مِن دُونِهِمْ** "[5]وقوله " **وَاسْتَرْهَبُوهُمْ وَجَاءُوا بِسِحْرٍ عَظِيمٍ** "[6]، وقال تعالى: " **وَاضْمُمْ إِلَيْكَ جَنَاحَكَ مِنَ الرَّهْبِ** "[7] وأيضا " **لَأَنتُمْ أَشَدُّ رَهْبَةً فِي صُدُورِهِم مِّنَ اللَّهِ** "[8]، كما قال في سورة الأنبياء " **إِنَّهُمْ كَانُوا يُسَارِعُونَ فِي الْخَيْرَاتِ وَيَدْعُونَنَا رَغَبًا وَرَهَبًا** "[9].

أما عن معنى الإرهاب في اللغة العربية فقد ورد في لسان العرب لابن منظور في معنى كلمة الإرهاب ومشتقاتها رهب بالكسر، يرهب، رهبة، ورهبا بالضم، ورهبا بالتحريك أي خاف.

ورهب الشيء رهبا ورهبة أي خافه، وفي حديث الدعاء " رغبة ورهبة إليك"، الرهبة الخوف والفزع وترهب غيره أي توعده وأرهبه ورهبة واسترهبه أي أخافه وأفزعه[10].

---

[1] أغادير عرفات حويجان، محمد عوض الترتوري، مرجع سابق، ص 20.

[2] سورة البقرة، الآية 40 .

[3] سورة النحل، الآية51 .

[4]سورة الأعراف، الآية 154.

[5]سورة الأنفال، الآية 60.

[6]سورة الأعراف، الآية 116.

[7]سورة القصص، الآية 32.

[8]سورة الحشر، الآية 13.

[9]سورة الأنبياء، الآية 90.

[10] ابن منظور، لسان العرب، الجزء الثاني، دار المعارف، مصر، ص 1748.

أما المجمع اللغوي للغة العربية فقد أقر كلمة " إرهاب" ككلمة حديثة في اللغة العربية، وأصلها "رهب" بمعنى خاف، وأرهب بمعنى خوف.

وكلمة إرهاب هي مصدر الفعل"أرهب" وتستعمل الرهبة في اللغة العربية للتعبير عن الخوف المشوب بالاحترام وهي بذلك تختلف عن الإرهاب الذي يعني الخوف والفزع الذي يأتي من قوة سواء كانت حيوانية أو طبيعية أو مالية والإرهابي هو وصف يطلق على الذي يسلك سبيل العنف لتحقيق هدف سياسي كما جاء في معجم الوسيط الصادر عن مجمع اللغة العربية[1].

ويعني الإرهاب في معجم مصطلحات العلوم الاجتماعية" بث الرعب الذي يثير الخوف، والفعل أو الطريقة التي تحاول بها جماعة منظمة أو حزب أن يحقق أهدافه عن طريق استخدام العنف وتوجه الأعمال الإرهابية ضد الأشخاص سواء كانوا أفراد أو ممثلين للسلطة ممن يعارضون أهداف هذه الجماعة[2].

وأما عن مفردة الإرهاب –بكسر الهمزة – فإنها لم تستعمل إلا عند بعض علماء اللغة، مثل الصاحب بن عباد والفيروز آبادي، والزبيدي، وقد وردت عندهم بمعنى الرد، ومنه قولهم: " أرهب عنك الإبل، أي ردها"[3].

أما عن معاني الإخافة والذعر ونشر الرعب التي تحملها هذه المفردة فقد وردت في معجم الزبيدي، الذي مزج دلالتها مع معناها اللغوي لجذرها الثلاثي الذي ترجع إليه[4].

أما حديثا فقد اقر المجمع اللغوي كلمة إرهاب ككلمة حديثة في اللغة العربية وأساسها "رهب" أي خاف، وكلمة إرهاب هي مصدر الفعل أرهب،وأرهب بمعنى "خوف"[5].

---

[1] أغادير حويجان، محمد عوض الترتوري، مرجع سابق، ص 22.

[2] حسن عزيز نور الحلو، الإرهاب في القانون الدولي–دراسة مقارنة، مذكرة ماجستير في القانون العام، الأكاديمية العربية المفتوحة، هلسنكي–فنلندا، 1427هـ/2007، ص 18 .

[3]عمار تيسير بجبوج، التعاون الدولي في مكافحة جرائم الإرهاب، أطروحة دكتوراه في الحقوق،جامعة القاهرة– قسم القانون الجنائي، 2010، ص 75.

[4] محمد الزبيدي، تاج العروس من جواهر القاموس، الجزء الثاني، ص 541.

[5]مختار الصحاح، طبعة الحادية عشرة، 1962، ص 256.

وأوضح المجمع اللغوي أن الإرهابيين وصف يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم السياسية، ويتضح بذلك أن كلمة إرهاب في اللغة العربية يدور معناها حول الخوف والفزع والرعب والخشية[1].

ويشير بعض الفقهاء إلى أن الرهبة في اللغة العربية عادة تستخدم للتعبير عن الخوف المشوب بالاحترام، وهي تختلف عن الإرهاب الذي يقصد به الخوف والفزع الناتج تهديد قوة مادية أو حيوانية أو طبيعية، ومن هنا فان ترجمة كلمة "TERRORISM" الشائع في اللغة العربية هو إرهاب، وهي ترجمة في حقيقة الأمر غير دقيقة لغويا لان الخوف من القتل أو الجرح أو الخطف أو التدمير أو التفجيرات التي يقوم بها الجماعات الإرهابية لا تقترن بالاحترام بل تقترن بالرعب وليس الرهبة، ولهذا يرى البعض أن التعبير الأكثر دقة لهذه الكلمة هو إرعاب وليس إرهاب، ومع ذلك فقد شاع أن تطلق على تلك الأفعال المرعبة كلمة إرهاب[2].

### * تعريف الإرهاب في اللغتين الانجليزية والفرنسية.

تشير كلمة "Terrorisme" الانجليزية المكونة من شقين إلى معنى الفزع والرعب والهول، كما يشتق منها الفعل "Terrorise" بمعنى يرهب ويفزع.

أما معجم "oxford" الانجليزي فيعرف الإرهاب بأنه:"استخدام العنف لأسباب سياسية"[3].

وفي قاموس "Webster " فيعرف الإرهاب بأنه أسلوب لاستعمال العنف للتخويف أو التهديد من أجل الوصول إلى أغراض سياسية [4].

ومما سبق يتضح أن التعريف اللغوي في اللغة الانجليزية قد يكون متأثر بالتعريف في اللغة العربية، لان العرب لديهم فعل الفزع والخوف رديف لكلمة "رهب"، وبالتالي فان التصريف من مميزات اللغة العربية، لان العرب لديهم فعل الفزع والخوف رديف لكلمة " رهب، ودليل ذلك أن كلمة

[1] عمار تيسير بجبوج ، مرجع سابق، ص 77.

[2] أسامة حسين محي الدين، جرائم الإرهاب على المستوى الدولي والمحلي، المكتب العربي الحديث، الإسكندرية 2009، ص 40.

[3] oxford, word power, dictionnary of English language, Oxford University press, Oxford,1981,p 773.

[4] Webster desk, dictionnary English language portland house, new York, 1990, p 924.

"TIERRS" هو أصل لاتيني ليس له مقابل في اللغة الانجليزية، وان العرب تأكد لديهم هذا المعنى لهذا الغرض من القرآن الكريم حيث وظفوا الآية الكريمة في قوله تعالى" **تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ**"[1] خير توظيف على أنها شرعية للقتل والتفجير وغفلوا عن الكثير من الآيات التي تحرم قتل النفس وتدعو إلى صيانتها و القرآن بريء من هذه التأويلات[2].

أما في اللغة الفرنسية فان كلمة الإرهاب هي كلمة حديثة العهد ولم تدخل إلى اللغة كمصطلح بدلا عن المفهوم العام للإرهاب إلا بعد عام 1794 إبان الثورة الفرنسية وما مارسته السلطة آنذاك من عنف ورعب وتعسف تجاه الثورة والمجتمع الفرنسي.

وقد ورد في القواميس الفرنسية لفظ " Terrorisme" ليعني الاستخدام المنهجي لتدابير استثنائية أو العنف لتحقيق هدف سياسي الاستيلاء أو المحافظة أو ممارسة السلطة"[3].

وبناء على ذلك فان العمل الإرهابي يعني مجموعة من أعمال العنف من اعتداءات فردية أو جماعية تنفذها منظمة سياسية للتأثير على السكان، وخلق مناخ عام بانعدام الأمن[4] .

وجميع القواميس الفرنسية لم تخرج عن هذا المعنى وترى أن الإرهاب هو الاستعمال المنظم للرهبة كوسيلة للإكراه فمثلا نجد أن قاموس " oxford" قد عرف لفظة " terrorisme" هو استعمال العنف والتخويف خاصة لتحقيق أغراض سياسية وأن الإرهابي هو الشخص الذي يستخدم العنف لإحداث حالة من الفزع لتحقيق أغراض سياسية[5].

---

[1] سورة الأنفال الآية 60.

[2] أمير فرج يوسف، مكافحة جريمة الإرهاب الالكتروني– في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، دار الكتب والدراسات العربية، الإسكندرية 2015 ، ص 45.

[3] طارق عبد العزيز حمدي، المسؤولية الدولية الجنائية والمدنية عن جرائم الإرهاب الدولي، دار الكتب القانونية، القاهرة 2008، ص 11.

[4] تجدر الإشارة إلى أن هذه الكلمة استخدمت تاريخيا في الفترة التي تلت سقوط روسبيرو للدلالة علا سياسة الرعب التي هيمنت خلال السنوات مابين 1793 ـ 1794 .للتفصيل أكثر: راجع محمود عبد العزيز محمد، الإرهاب النفق المظلم في تاريخ البشرية وعلاقته بالأديان السماوية، دار الكتب القانونية القاهرة، 2013، ص 15.

[5] نفس المرجع، ص 10.

ومما سبق نجد أن كلا من اللغة العربية والفرنسية والانجليزية ترى أن الإرهاب هو السلوك الذي يقوم على ارتكاب العنف لتحقيق أهداف سياسية[1] .

إلا أن هذا المفهوم لا يستقيم وأصبح قاصرا إذ أن هناك صورا جديدة من الإرهاب لا تستعين فقط بالعنف فهناك الإرهاب الحديث الذي يمكن أن يصل إلى تحقيق أهدافه وأغراضه بالترغيب أو الإغراء بعيدا عن العنف، كما أن الغرض السياسي لا يعتبر الغرض الوحيد من الإرهاب فهناك أغراض تتجاوز هذا الغرض السياسي كالصراع الديني أو الطائفي أو صراع عصابات على مصالح مادية ومناطق نفوذ.

## ثانيا: التعريف الاصطلاحي.

ليس من السهل إيجاد تعريف محدد للإرهاب وذلك نظرا لتباين الرؤى السياسية والقانونية للعديد من القضايا الدولية والعالمية، فما تراه بعض الدول من قبيل الإرهاب وأنه من أعمال العنف تراه دول أخرى أنه عمل بطولي ووطني وفدائي أيضا.

ومن المعروف أن الدول لم تتفق على وضع تعريف محدد للإرهاب إلا انه في الوقت نفسه نجد أن كل دولة أو منظمة إقليمية أعطت تعريف للإرهاب انطلاقا من وضعها ومصالحها والزاوية التي تنظر منها [2] .

وعلى الرغم من أن الفقه حاول وضع العديد من التعريفات المتعلقة بالإرهاب والتي ركزت في معظمها على إبراز فكرة الاستخدام غير المشروع للقمة أو العنف وبث الرعب لتحقيق هدف معين، إلا انه توجد نقاط خلاف بارزة بين هذه التعريفات، فكل تعريف اعتمد في قيامه على الجهات المرتكبة لأفعال العنف أو اعتمد على ضرورة النظر إلى الدافع أو الباعث من وراء هذا العمل العنيف[3].

ومنهم من يرتكز في تعريفه على صفة التنظيم في العمل الإرهابي، أو بالنظر إلى صفة المستهدف من العنف.

---

[1] أمير فرج يوسف، مرجع السابق، ص 46.

[2] أمير فرج يوسف، مكافحة الإرهاب، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، 2011، ص 10.

[3] عمار تيسير بجبوج، مرجع السابق، ص 78 .

وقبل أن نتعرض إلى مجموع المحاولات الفقهية والقانونية لتعريف الإرهاب تجدر الإشارة إلى أن هذه الاختلافات الكثيرة والواضحة بين الدول والمنظمات الدولية والفقهاء الدوليين، حول إعطاء تعريف موحد للإرهاب، يمكن أن ترجع إلى مجموعة من الاعتبارات، لعل أهمها[1]:

1. اختلاف وجهات النظر فيما يعد عملا إرهابيا من عدمه، وهذا حسب اختلاف الأهواء والمصالح والسياسات ومدى قوة وعمق العلاقات الدولية أو فتورها.
2. أيضا يختلف تعريف الإرهاب باختلاف النظرة إلى العمل محل النظر أو المنفذون له أو الغاية أو الهدف منه، والنتائج المترتبة عليه والأدوات المستخدمة في تنفيذه[2].

ولقد أدت صعوبة إيجاد هذا التعريف الموحد والشامل للإرهاب إلى تشكيل عقبة كبرى في طريق الجهود المبذولة للحد من هذه الظاهرة وإيجاد علاج نهائي لها[3].

وبالرجوع إلى تعريف الإرهاب سوف نتعرض إلى بعض التعريفات الفقهية وبعد ذلك سوف نعرج على ما جاء في بعض الاتفاقيات والمؤتمرات الدولية لنصل في الأخير إلى موقف التشريع الوطني وبعض التشريعات المقارنة من هذه الظاهرة الإجرامية.

### * المحاولات الفقهية لتعريف الإرهاب.

لقد أشرنا سابقا إلى انه لم يتم التوصل إلى تعريف جامع مانع للإرهاب ولأسباب ذكرنا أهمها إلا أن ذلك لا يمنع أن الفقه قدم تعريفات مختلفة تشترك معظمها في إبراز فكرة الاستخدام غير المشروع للقوة أو العنف وبث الرعب لتحقيق هدف معين، إلا أنها تختلف في المعيار الذي اعتمد عليه كل تعريف، وهذا ما أدى إلى ظهور الاتجاهات الآتية :

[1] محمود عبد العزيز محمد، مرجع السابق، ص 19.

[2] نفس المرجع، ص 19.

[3] أغادير حويجان، محمد عوض الترتوري، المرجع السابق، ص 27.

**الاتجاه التقليدي.**

وفقا لهذا الاتجاه فهناك أعمال معينة إذا تم ارتكابها فإنها تشكل عملا إرهابيا بغض النظر عن ظروف ارتكابها أو بواعث مرتكبيها أو درجة الخطر الناجم عنها ومثال ذلك خطف الطائرات ومهاجمة الدبلوماسيين وأخذ الرهائن[1].

وعلى الرغم من أن هذا التعريف لا يتضمن وصف للجريمة الإرهابية ، لأن الأعمال الحصرية التي ذكرها أنصار هذا الاتجاه لا تعتبر أعمال إرهابية بالمفهوم القانوني إلا إذا تخللها معرفة الباعث، فقد يكون الباعث مثلا من اختطاف مبعوث دبلوماسي مجرد الحصول على فدية وليست له أي دافع سياسي إلا انه هو السبيل الأفضل للتعرف على ماهية الإرهاب حسبما يراه أنصار هذا الاتجاه[2].

**الاتجاه الوصفي.**

يرى أنصار هذا الاتجاه أنه من الصعوبة وضع تعريف محدد شامل وجامع للإرهاب وإن كانوا لا يرفضون مبدأ تعريفه إلا أنهم يرتكزون في هذا التعريف على إبراز خصائص العمليات الإرهابية، والتركيز على عناصر الإرهاب ليسهل التعرف عليه ويستندون في ذلك إلى أن وصف الإرهاب أسهل من تعريفه[3]، ويلخصون تلك الخصائص فيما يلي:

- العنف غير المتوقع أو المفاجئ أو التهديد به.
- الصفة الرمزية للضحايا بهدف الدعاية وإرسال رسالة للمستهدفين لأجل تغيير سلوكهم.
- الطبيعة الخاصة والسرية الشديدة التي تحاط بها العمليات الإرهابية.
- عنصر التقليد في الأسلوب المستخدم واستخدام التقنيات الحديثة في التنفيذ.
- الأهداف والدوافع السياسية أو الإيديولوجية وراء العمليات الإرهابية[4].

[1] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 47

[2] نفس المرجع ص 47.

[3] أمير أغادير حويجان، محمد عوض الترتوري، مرجع السابق، ص 29.

[4] فرج يوسف، (مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 49.

**الاتجاه التحليلي.**

يركز أنصار هذا الاتجاه على إعطاء تعريف يغطي كل الأفعال التي يمكن أن تعتبر إرهابية وضمن الاتجاه نفسه يركز البعض على طبيعة الأفعال المكونة للإرهاب وما تتسم به من عنف فجائي يخلق حالة من الرعب وبالتالي فإن أنصار هذا الاتجاه يرتكزون في تعريفهم على وسيلة العنف، ودرجة جسامة الفعل [1].

وحسب هذا الاتجاه فان كل عنف مستخدم لا يعتبر إرهابا إلا إذا وصل إلى درجة معينة من الجسامة، إلا أن هذا التعريف يعاب عليه انه أهمل مرتكبي هذه الأفعال ودفاعهم.

هذا ونشير إلى انه وفقا لهذا الاتجاه فان العمل كي يكون عملا إرهابيا وجب أن يتصف بالخصائص التالية:

- عنف غير عادي على درجة عالية من الجسامة، ويستوي في ذلك الاستعمال المادي للعنف أو مجرد التهديد به.
- أن يتصف هذا العنف بالتنظيم والاتصال، أي أن يكون العمل ممنهجا لا أن يكون عشوائيا أو عارضا
- القصد الجنائي لدى الجاني وذلك بان يكون استخدام العنف بغرض تحقيق الرعب والفزع، واعتمادا على ذلك لا يتصور وجود جرائم إرهابية غير عمدية.
- أن تحدث وسيلة الرعب المستخدمة قدر من الرهبة في نفوس أفراد المجتمع أو في فئة منه بقصد السيطرة عليهم أو توجيههم بما يحقق أهداف الإرهاب النهائية.
- السرية والمفاجأة والمباغتة في العمل الإرهابي
- عدم مشروعية الفعل[2].

[1] أغادير حويجان، محمد عوض الترتوري، مرجع سابق، ص 30.

[2] وعدم مشروعية الفعل هذه محل خلاف بين الفقهاء، فالبعض يستبعد عنصر عدم المشروعية الموضوعية من عنصر الإرهاب لان القواعد الموضوعية لا تعتبر المقياس النهائي والوحيد الذي يصلح للحكم على الإرهاب، أما البعض الآخر فيرى في الإرهاب عمل عنف غير مشروع، وذلك لتمييزه عن أعمال العنف المشروعة وبالتالي فإن هذا الاتجاه=

وتجدر الإشارة في هذا الخصوص أن المتخصصين في القانون الدولي العام بذلوا جهودا محمودة لتعريف الإرهاب وتحديد طبيعته، وتوضيح جوانبه على الرغم من أن هذه التعريفات غير كافية لتفهم هذه الظاهرة المعقدة وتلمس طبيعتها وأبعادها، ومن ابرز المساهمات الفقهية في هذا الصدد والتي نأخذها على سبيل المثال :

– نجد على الصعيد الفقه الغربي تعريف الفقيه "Saldana" الذي يميز بين مفهومين للإرهاب مفهوم واسع والآخر ضيق، فعن المفهوم الواسع فهو يرى أن الإرهاب هو :" كل جناية أو جنحة سياسية أو اجتماعية ينتج عن تنفيذها أو التعبير عنها ما يثير الفزع العام لما لها من طبيعة ينشأ عنها خطر عام"، وأما عن المفهوم الضيق الذي قدمه " Saldana " فكان بقوله:" أن الإرهاب هو الأعمال الإجرامية التي يكون هدفها الأساسي بث الخوف والرعب كعنصر شخصي–وذلك باستخدام وسائل من شانها خلق حالة من الخطر العام"[1] .

الفقيه "Galor Noemi" يرى في الإرهاب أنه:" طريقة عنيفة أو أسلوب عنيف للمعارضة السياسية وهو يتكون من العنف والتهديد به، وهذا العنف قد يكون عنف بدني حقيقي أو أن يمارس هذا العنف نفسيا، وقد يمارس الإرهاب على أبرياء أو ضد أهداف لها ارتباط مباشر بالقضية التي يعمل الإرهابيون من أجلها[2].

– أما على الصعيد العربي فقد تم تعريف الإرهاب بأنه:" كل اعتداء على الأرواح والممتلكات العامة أو الخاصة المخالفة لأحكام القانون بمصادره المختلفة بما في ذلك المبادئ العامة للقانون بالمعنى الذي تحدده المادة 38 من النظام الأساسي لمحكمة العدل الدولية"[3]

ويتضح من التعريف المذكور أعلاه أنه يفرق بين حالة استعمال القوة غير المشروعة والحالة المشروعة في استخدام القوة كحالة الدفاع الشرعي مثلا.

---

= الأخير يعتبر أن الإرهاب جريمة عالمية تتضمن كل السلوكيات الخارجة عن القانون والتي تهدف إلى تخويف الآخرين لتفصيل أكثر راجع أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 48.

[1] عثمان علي حسن، الإرهاب الدولي ومظاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام،الطبعة الأولى مطبعة مناره، هه وليـر–كردستان،2006، ص 73.

[2] أغادير حويجان، محمد عوض الترتوري، مرجع سابق، ص 33.

[3] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 50.

فإذا كان الدافع من استخدام القوة هو حق تقرير المصير أو مقاومة الاحتلال ففي هذه الحالات يعتبر استخدام القوة مشروع ويشتمل على حقوق أقرها القانون الدولي.

كما يعرف فقيه آخر الإرهاب بأنه:" تعبير عن العمليات العنيفة –المادية والمعنوية– أو التهديد بها بصورة غير مشروعة لخلق حالة من الرعب والفزع، تقوم به أفراد أو جماعات أو كيانات أو منظمات أو دول لتحقيق أهداف معينة"[1].

ومن خلال التعاريف السابقة على الصعيدين العربي والغربي يمكن أن نستخلص بعض العناصر المتفق عليها في معظم التعاريف –والتي ذكرنا بعضها على سبيل المثال– كما يلي:

- الإرهاب يقوم على استعمال العنف أو التهديد به.
- أن يستخدم هذا العنف على وجه غير مشروع.
- بث حالة من الخوف والفزع والذعر في أفراد المجتمع أو فئة منه .
- أن يصدر هذا العمل العنيف من قبل فرد أو مجموعة أفراد أو منظمات أو كيانات أو من الدولة ذاتها.
- يوجه العمل الإرهابي ضد الفرد أو المجتمع بأسره أو الممتلكات سواء كانت عامة أو خاصة

### * تعريف الإرهاب في المعاهدات والتشريعات الوطنية .

جاء في مؤتمر"سوفيا" لتوحيد القانون الجزائي المنعقد عام 1930 عرفه بأنه: "الاستعمال العمدي لكل وسيلة قادرة على إحداث خطر جماعي، ويعتبر الرعب عنصرا أساسيا في تكوين هذه الجريمة"[2].

أما الاتفاقية العربية لمكافحة الإرهاب التي أبرمت في أفريل سنة 1998 فقد عرفته في مادتها الأولى:"بأنه كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم

[1] عثمان علي حسن، مرجع سابق، ص 75.

[2] محمود عبد العزيز محمد، مرجع السابق، ص 19.

أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو تعريض احد الموارد الوطنية للخطر"[1].

بدورها معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب لسنة 1999 عرفت الإرهاب في الفقرة الثانية من مادتها الأولى بأنه:" كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو إغراضه يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو أعراضهم أو حريتهم أو أمنهم أو حقوقهم للخطر، أو إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية أو المرافق الدولية للخطر، أو تهديد الاستقرار أو السلامة الإقليمية أو الوحدة السياسية أو سيادة الدول المستقلة"[2] .

مجمع الفقه الإسلامي أعطى تعريفا للإرهاب وذلك في الدورة السادسة عشر لرابطة العالم الإسلامي التي عقدت في مكة المكرمة في 21 شوال عام 1423 هـ الموافق لـ 2002 م وذلك بقوله:" العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دمه، عقله، مله وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصورة الحرابة، وقطع الطريق وكل فعل من أفعال العنف أو التهديد، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أقوالهم للخطر ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو تعريض احد الموارد الوطنية أو الطبيعية للخطر"[3]

ونلاحظ هذا التعريف لا يختلف كثيرا عن التعريفين السابقين بل ويصب في نفس المعنى ويرمي إلى نفس الهدف.

[1] الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 والتي اعتمدها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك بالقاهرة يوم 1998/04/22 ودخلت حيز النفاذ بتاريخ 1999/05/07.

[2] مصطفى محمد موسى، الإرهاب الالكتروني– دراسة قانونية–أمنية– نفسية– اجتماعية، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، مطابع الشرطة،(دون مكان نشر) ، 2009، ص 92.

[3]محمود عبد العزيز محمد، مرجع سابق، ص 22،23.

هذا وقد أصدر مجمع البحوث الإسلامية بالأزهر بيانا عقب أحداث الحادي عشر من سبتمبر لسنة 2001 م والتي أبرزت الوجه الحقيق والبشع للإرهاب إذ أسفر على تدمير برجي التجارة العالميين بالولايات المتحدة الأمريكية وسقوط أكثر من ثلاثة آلاف قتيل ووقوع الآلاف من الجرحى كم مختلف الجنسيات ينكر فيه هذا العمل الإرهابي وقد كان تعريفه للإرهاب كالتالي:" ترويع الآمنين وتدمير مصالحهم ومقومات حياتهم والاعتداء على أموالهم وكرامتهم الإنسانية بغيا وإفسادا في الأرض"[1].

وجدير بالذكر أن أول اتفاقية تعرضت لتعريف أعمال الإرهاب كانت اتفاقية عصبة الأمم في نوفمبر 1937 وذلك في نص الفقرة الثانية من المادة الأولى منها بقولها:" أفعال إجرامية موجهة ضد دولة ويقصد بها أو يراد منها خلق حالة من الرعب في أذهان أشخاص معينين أو مجموعة من الأشخاص أو الجمهور العام"[2] .

ويعاب على هذا التعريف انه جاء قاصرا على الإحاطة بكافة أنواع الإرهاب كما أنه حصر الإرهاب في الأعمال الإجرامية الموجهة ضد الدولة[3].

إلا أن هذا القصور لا ينفي أبدا أن هذا التعريف يعتبر انطلاقة جيدة ومحاولة هامة في وضع تعريف للإرهاب كظاهرة إجرامية خطيرة.

هذا وقد جاء في تقرير الأمين العام للأمم المتحدة "كوفي عنان" المقدم إلى الأمم المتحدة في سبتمبر 2004 تحت عنوان " في جو من الحرية أفسح صوب تحقيق التنمية والأمن وحقوق الإنسان للجميع" ما يلي:" إنني أؤيد تأييدا تاما دعوة الفريق الرفيع المستوى إلى وضع تعريف للإرهاب يوضح أن الإرهاب هو أي عمل، إلى جانب الأعمال المحظورة فعلا في الاتفاقيات القائمة يراد به التسبب في وفاة مدنيين أو أشخاص غير محاربين، أو إلحاق إصابات جسمانية خطيرة لهم بهدف ترويع مجموعة سكانية أو إرغام حكومة أو منظمة دولية على القيام بعمل أو الامتناع عنه، وأحث بقوة قادة العالم

[1] محمود عبد العزيز محمد، مرجع سابق، ص 23.

[2] مصطفى مصباح دبارة، الإرهاب– مفهومه وأهم جرائمه في القانون الدولي الجنائي، منشورات جامعة قار يونس، بن غازي– ليبيا، 1995، ص 87.

[3] مصطفى محمد موسى، مرجع سابق، ص 90.

على تأييد ذلك التعريف وإبرام اتفاقية شاملة لمكافحة الإرهاب قبل نهاية الدورة الستين للجمعية العامة"[1].

وقد تناول مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية عام 2005 [2] لمقصود بالإرهاب:"الهجوم على مبادئ القانون والنظام وحقوق الإنسان والتسوية السلمية للمنازعات"[3].

وتجدر الإشارة أنه منذ 1963 إلى غاية 2005 صدرت ثلاثة عشرة اتفاقية وبروتوكولا كلها متعلقة بالإرهاب دخلت جميعها حيز التنفيذ فيما عدا الاتفاقية التي تم اعتمادها في 13 أفريل 2005 بشان الإرهاب النووي بمقتضى قرار الجمعية العامة للأمم المتحدة رقم 290/59 وتم التوقيع عليها اعتبارا من 2005/09/14.[4]

أما عن موقف التشريعات الوطنية من تعريف الإرهاب فقد أشارت دراسة حديثة عن المركز الحقوقي انه يوجد ما يقارب ثلاث وستون (63) تشريع لدول مختلفة، سنت كل هذه التشريعات ضد الإرهاب[5] ، وهذا يدل على الرغبة الشديدة لمختلف دول العالم من أجل السيطرة على هذه الظاهرة العالمية الخطيرة.

ولأنه يتعذر علينا الإحاطة بكل التشريعات السالفة الذكر سوف نكتفي بالتعرض إلى التشريع الفرنسي والمصري وبالتأكيد سنتعرض إلى موقف المشرع الجزائري من تعريفه للإرهاب.

فبالنسبة للتشريع الفرنسي نجد أن المشرع الجنائي قد اتبع في هذه المسألة الأسلوب الغائي[6] حيث أنه لو يورد لا تعريف للإرهاب ولا للجريمة الإرهابية ولكنه اكتفى بالنص على مجموعة من

---

[1] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 63.

[2] انعقد هذا المؤتمر في بانكوك في الفترة من 18-20 أفريل 2005 م.

[3] مصطفى محمد موسى، مرجع سابق، ص 91.

[4] علاء الدين راشد، الأمم المتحدة والإرهاب قبل وبعد 11 سبتمبر، دار النهضة العربية، القاهرة، 2005، ص (100،229)

[5] محمد عزيز شكري، الإرهاب الدولي –دراسة قانونية ناقدة، الطبعة الأولى، دار العلم للملايين،( دون مكان نشر) 1999 ص 51 .

[6] ويقصد بالأسلوب الغائي الاعتماد على النشاط الإجرامي إما بالنسبة لارتكاب جريمة معينة أو بصرف النظر عن نوع الجريمة المرتكبة، أو سواء بالنص على هذه الغاية مباشرة أو بالنص عليها بطريقة غير مباشرة.

الجرائم ضمن قانون العقوبات الفرنسي، وأخضعها لنظام خاص وقواعد أكثر صرامة إذا ما ارتكبت بدافع معين.

وقد صنف المشرع الفرنسي هذه الجرائم إلى ثلاث مجموعات تضم الأولى جرائم العنف الواقعة على الأشخاص باستثناء العنف الواقع على الأبناء والأصول، وأما المجموعة الثانية فتشتمل على جرائم الاعتداء على الأموال والتي من شأنها خلق خطر عام، وأما المجموعة الثالثة فهي تضم الإعداد للجرائم وتنفيذها أو ما يعرف بجمعية الأشقياء[1]

وقد عد المشرع الجنائي الفرنسي هذه المجموعة الأخيرة على أنها جرائم إرهابية إذا ما اتصلت بمشروع فردي أو جماعي بهدف الإخلال بالنظام العام بصورة جسيمة عن طريق التخويف والترويع[2] .

وعليه فوفقا لهذا القانون فانه يلزم ليعد الفعل جريمة إرهابية عنصرين، الأول شخصي مفاده اتصال إحدى الجرائم المذكورة على سبيل الحصر بمشروع فردي أو جماعي، والثاني شخصي يتمثل في الدافع أو الباعث من هذا الفعل الإجرامي والمتمثل في إثارة الخوف والترويع لدى المجتمع أو فئة منه بقصد الإخلال بالنظام العام بصورة جسيمة، وهذا ما تبين في معظم القوانين ذات الصلة بالإرهاب والتي صدرت في السنوات السابقة(1986-1991-1996-2001-2003)[3] .

أما المشرع المصري فقد قام بتعريف جريمة الإرهاب في القانون رقم 97 لسنة 1992، والذي عدل المادة 86 من قانون العقوبات المصري،حيث جاء فيها:" يقصد بالإرهاب في تطبيق أحكام هذا القانون كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجا إليه الجاني تنفيذا لمشروع إجرامي فردي أو جماعي، بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع و أمنه للخطر، إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق ضرر بالبيئة، أو بالاتصالات أو المواصلات أو بالأموال، أو بالمباني العامة أو الخاصة، أو احتلالها

[1] محمد عبد الكريم عيسى العفيف، جرائم الإرهاب في قانون العقوبات الأردني- دراسة مقارنة، أطروحة دكتوراه في فلسفة القانون العام،جامعة عمان العربية للدراسات العليا الأردن، 2006/2005، ص 83 .

[2]Jean Pradel, Les infractions de terrorisme, un nouvel exemple de L'eclatement du droit pénal, Recual Dalloze Sirey, 7e chaier-chronque, p 42

[3] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص80.

أو الاستيلاء عليها، أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور، أو القوانين واللوائح"[1].

ويتضح من خلال هذا التعريف أن المشرع المصري حاول حسم الخلاف حول مدلول الإرهاب بحيث حصر كل الصور الممكنة للإرهاب حتى لا يخرج أيا منها من دائرة التجريم والعقاب[2].

ويؤخذ على هذا التعريف أنه حاول حصر جميع الصور الممكنة للإرهاب دون أن يحدد مقدار هذا العنف أو التهديد به أو مقدار الترويع حتى يمكن أن نعتبر هذا العمل عملا إرهابيا[3] .

***موقف المشرع الجزائري من تعريفه للإرهاب.**

بعد سقوط المعسكر الاشتراكي وتفككه سارعت معظم الدول الاشتراكية إلى تبني النظام الليبرالي الغربي واعتناق المبادئ الديمقراطية التي نادى بها هذا النظام، والجزائر وكغيرها من الدول الاشتراكية في تلك الفترة قامت بإصدار ترسانة من النظم القانونية الممهدة لعملية الانتقال من نظام اشتراكي موجه إلى نظام ليبرالي حر, كان من أبرز القوانين وفي مقدمتها دستور 23 فبراير 1989, والقانون رقم 89-11, المتعلق بالجمعيات ذات الطابع السياسي والذي أقر التعددية الحزبية كمظهر من مظاهر الديمقراطية التي يقوم عليها الفكر الليبرالي الرأسمالي.

ومما زاد الأمر تعقيداً هو ظهور الحركات الإسلامية بداية التسعينات على غرار الحركة من أجل الدولة الإسلامية والجبهة الإسلامية للإنقاذ, وغيرهما, ودخول هذه الحركات للمعترك السياسي مستغلة بذلك حالة الاحتقان التي سادت المجتمع الجزائري في تلك الفترة, وبالأخص مع عودة الكثير من الجزائريين ممن شاركوا في الحرب الأفغانية متشبعين بالأفكار المتطرفة حاملين معهم منطقاً جهادياً بتجربة ميدانية وخبرة كبيرة في مجال حرب العصابات ومختلف أنماط الجرائم الإرهابية.

تأسيساً على ما ذكر, ونتيجة لفوز الأحزاب الإسلامية تم توقيف المسار الانتخابي الذي أدى إلى الدخول في صراع ما بين النظام ومختلف الجماعات الإسلامية مستعينة بجناحها العسكري المنظم

[1] أسامة أحمد شتات، قانون العقوبات المصري، دار الكتب القانونية، القاهرة، 2004، ص 53.

[2] عمار تيسير بجبوج ، مرجع سابق، ص 87.

[3] المشرع الفرنسي من بين المشرعين الذي حدد مقدار العنف وعبر عنه بالجسامة .

مسبقاً، وهو ما أدى إلى الدخول في دوامة عنف شاملة خلفت مالا يقل عن 150 ألف قتيل, وأكثر من مليون متضرر[1].

وأول نص للإرهاب في التشريع الجزائري كان بموجب المرسوم التشريعي 92- 03 المؤرخ في 30 سبتمبر 1992 المتعلق بمكافحة الإرهاب والتخريب، والذي ألغي بموجب الأمر 95-11 المؤرخ في 25 فبراير 1995 الملحق بقانون العقوبات حيث أضاف إليه قسم رابع مكرر يحمل عنوان "الجرائم الموصوفة بأفعال إرهابية وتخريبية".

فبالرجوع إلى نص المادة 87 مكرر من هذا الأمر[2] والتي جاء فيها:" يعتبر فعلا إرهابيا أو تخريبيا في مفهوم هذا الأمر، كل فعل يستهدف امن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه مايلي:

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم

للخطر أو المس بممتلكاتهم.

- عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية.
- الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني.

[1] باخوية إدريس، جرائم الإرهاب في دول المغرب العربي- تونس، الجزائر، المغرب نموذجا، مقالة منشورة في مجلة الحقوق والعلوم السياسية، العدد 11 لسنة 2014 ، جامعة ورقلة متوافرة في موقع: www.revues /ouargla.dz تاريخ الاطلاع : 2017/07/17 على الساعة 00:20.

[2] الأمر 66-156 المؤرخ في 18 صفر 1386هـ الموافق لـ 8يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم .

- الاعتداء على المحيط أو إدخال مادة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه بما فيها المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر.
- عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام.
- عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات.

ويلاحظ أن المشرع الجزائري قد نص على فعل الاعتداء في الجرائم الإرهابية دون تحديد الأسلوب الذي من خلاله يتحقق هذا الاعتداء، فقد نصت الفقرة الثانية من المادة سالفة الذكر على الاعتداءات ضد السلامة الجسدية للأفراد وتعريض حياتهم للخطر، وقد تعمد المشرع عدم تحديد طبيعة هذا الاعتداء لأنه أراد الإحالة إلى القواعد العامة في مجال القتل والضرب والجرح لكن بشرط أن ترتكب في سياق المادة 87 مكرر أي بواسطة العنف أو التهديد به بغرض بث الرعب بين الناس وتعريض حياتهم وأمنهم للخطر حتى تعتبر من قبيل الجرائم الإرهابية أو التخريبية هذا وقد نص المشرع الجزائري على لفظ التخريب إلى جانب لفظ الإرهاب كونه يحمل نفس المعنى تقريبا فيؤكد على معنى فعل الإرهاب، بحيث يقصد بالتخريب الدمار الكلي أو الجزئي باستخدام أي وسيلة كانت[1].

أما المادة 87 مكرر3 من ذات القانون فقد أضافت صورة أخرى حيث جاء نصها كالتالي"...كل من ينشئ أو يؤسس أو ينظم أو يسير أية جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام المادة 87 مكرر.

كما جاء في فقرتها الثانية" ... كل انخراط أو مشاركة مهما يكن شكلها، في الجمعيات أو التنظيمات أو الجماعات أو المنظمات المذكورة في الفقرة السابقة مع معرفة غرضها أو أنشطتها"[2].

[1] ساعد إلهام حورية، وسائل مكافحة الإرهاب، أطروحة دكتوراه في القانون العام، كلية الحقوق –سعيد حمدين– يوسف بن خدة، جمعة الجزائر 01، 2016/2015، ص 200، 201.

[2] الأمر 66–156 السالف الذكر.

أيضا المواد 87 مكرر4، 78 مكرر 5، 87 مكرر6، 87 مكرر 7، 87 مكرر 10 من القانون السالف الذكر[1] تتضمن أعمال أخرى تعتبر من قبيل الأعمال الإرهابية وهي كالتالي:

- كل من يشيد بالأعمال المذكورة في المادة 87 مكرر والمذكورة سابقا أو يشجعها أو يمولها بأي وسيلة كانت

- كل من يعيد عمدا طبع أو نشر الوثائق أو المطبوعات أو التسجيلات التي تشيد بالأفعال المذكورة في هذا القسم

- كل جزائري ينشط أو ينخرط في الخارج في جمعية أو جماعة منظمة إرهابية أو تخريبية مهما كان شكلها أو تسميتها حتى وان كانت أفعالها غير موجهة ضد الجزائر .

- كل من يحوز أسلحة ممنوعة أو ذخائر يستولي عليها أو يحملها أو يتاجر فيها أو يستوردها أو يصدرها أو يصنعها أو يصلحها أو يستعملها دون رخصة من السلطة المختصة.

- كل من أدى خطبة أو حاول تأديتها داخل مسجد أو في أي مكان عمومي تقام فيه الصلاة دون أن يكون معينا أو معتمدا من السلطة العمومية المؤهلة أو مرخصا له من طرفها للقيام بذلك.

كما أضافت الفقرة الثانية من المادة 87 مكرر 10 فعل آخر بقولها" ...كل من بواسطة الخطب أو بأي فعل على أعمال مخالفة للمهمة النبيلة للمسجد أو يكون من شانها المساس بتماسك المجتمع أو الإشادة بالأفعال المشار إليها في هذا القسم"[2].

أما المادة 87 مكرر 11 الجديدة فقد أضافت صورة من صور الإرهاب وذلك بقولها: " ...كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى

[1] الأمر 66-156 السالف الذكر.

[2] الأمر 66-156 السالف الذكر.

بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها"[1] .

الفقرتين الثانية والثالثة من ذات المادة السابقة أضافتا الفعلين التاليين من الأفعال التي تعتبر من قبيل الأعمال الإرهابية:

– كل من يوفر أو يجمع عمدا أموالا بكل وسيلة وبصورة مباشرة أو غير مباشرة بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من المادة 87 مكرر 11.

– كل من قام عمدا بتمويل أو تنظيم سفر أشخاص إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها أو تسهيل ذلك السفر .

أما الفقرة الثالثة من نفس المادة فقد أضافت استخدام تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة سابقا وهو ما سوف نتعرض له في العناصر القادمة .

وبالرجوع إلى نص المادة 87 مكرر وما يليها نجد أن المشرع الجزائري تعرض إلى تعريف الإرهاب بشكل عام وعلى الرغم من انه جمع بين الأعمال المادية وما يعتبر من العناصر المفترضة الوجود حال ارتكاب الأعمال المادية[2]، إلا أنه أطال في هذا التعريف إلى حد يصعب معه الإلمام بالمعنى الدقيق المراد الوصول إليه .

[1] القانون رقم 16–02 المؤرخ في 14 رمضان 1437هـ الموافق لـ 19 يونيو 2016 المتمم للأمر 66–156 المؤرخ في 18 صفر 1386 هـ الموافق لـ 08 يونيو 1966 المتضمن قانون العقوبات الجزائري، العدد 37 من الجريدة الرسمية ص 04.

[2] ديش موسى، النظام القانوني لتعويض ضحايا الجرائم الإرهابية– دراسة مقارنة، رسالة دكتوراه في القانون العام، كلية الحقوق، جامعة تلمسان 2016/2015، ص 49.

## الفرع الثاني: مفهوم الإرهاب الالكتروني.

مع التطور التكنولوجي الهائل شهد العالم تغييرا كبيرا على جميع الأصعدة حيث دخلت الانترنت إلى قطاعات واسعة من الخدمات سواء كانت خدمات مالية أو صناعية أو على مستوى الاتصالات وكذلك الخدمات الحكومية، فالاعتماد الكبير والمتزايد لشبكة الانترنت في جميع مجالات الحياة جعل منها حتمية لا يمكن الاستغناء عنها، لكن بالمقابل زادت مع هذه الحتمية درجة التهديدات المحتملة التي يمكن أن تتعرض إليها هذه الشبكة من اختراقات وتدمير وغيرها من التهديدات أو أن تستغل هذه الأخيرة للقيام بالعمليات الإرهابية والتخريبية[1].

وإذا كان الإرهاب التقليدي أو كما أطلق عليه بعض الفقه الإرهاب المادي عموما هو الاستخدام المشروع للقوة أو العنف ضد الأشخاص أو الممتلكات لترويع أو إجبار الحكومات أو الأفراد كلهم أو فئة منهم من أجل تحقيق أغراض سياسية أو اجتماعية أو غيرها –مثلما وضحنا سابقا، فان انتشار موجة الانتشار التكنولوجي عالميا وتصاعد مستوى الاهتمام بقطاع تكنولوجيا الاتصال والمعلومات أدى إلى ظهور تسميات جديدة للإرهاب ارتبطت بهذا التطور التكنولوجي وهذا بسبب الاستخدام السلبي لهذه المعطيات التكنولوجية فإمكانية استخدام هذه التكنولوجية الحديثة في التحضير أو القيام أو التنسيق أو التعبئة أو الحشد للعمل الإرهابي تعتبر أنشطة غير سلمية للفضاء الالكتروني، وهو ما يؤثر في طبيعته ويغير في دوره وهو ما يؤثر بدوره على النظام الدولي، ومن أبرز المسميات التي أطلقت على هذا النوع من الإرهاب المتعلق بالاستخدام السلبي لشبكة الانترنت الإرهاب الالكتروني .

ومن أجل توضيح هذا الخطر الجديد وما المقصود به سوف نتعرض إلى عنصرين أولهما تعريف الإرهاب الالكتروني والآخر خصائصه.

### أولا : تعريف الإرهاب الالكتروني.

وجدت الجماعات الإرهابية في الشبكة العالمية للانترنت مجالا حيويا لأنشطتها التخريبية وقد برز ذلك جليا من العلاقة الوطيدة بين العمليات الإرهابية والإنترنت بهدف ضرب الدولة والمجتمع وزعزعة استقراره فبعدما كانت العمليات الإرهابية محلية أو تنفذ على المستوى المحلي تحولت لتصبح

[1] عادل صادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015، ص 104.

من أبرز الجرائم العابرة للحدود فاستخدام الموارد المعلوماتية والوسائل الالكترونية التي جلبها عصر المعلومات هو ما ميز الإرهاب الالكتروني عن غيره من صور الإرهاب الأخرى.

وقد كان أول استخدام للإرهاب الالكتروني في فترة الثمانينات في دراسة "Barry Collin" حيث توصل من خلالها إلى صعوبة إعطاء تعريف دقيق للإرهاب الالكتروني، واكتفى باعتبار الإرهاب الالكتروني هو التقارب بين عالمين مادي وافتراضي،كما أفضت هذه الدراسات إلى وجود صعوبة في تحديد دور الحاسوب والانترنت في العمل الإرهابي[1].

ففي سنة 1980 كان مصطلح الإرهاب الالكتروني يدل على الهجمات الموجهة ضد اقتصاد وحكومة الولايات المتحدة الأمريكية والتي تتم بواسطة الحاسوب ومع بداية التسعينات تغير هذا المفهوم واتسع بسبب انتشار أدوات تكنولوجيا الاتصال والمعلومات دوليا في إطار ظهور مجتمع المعلومات العالمي، وقد ظهرت العديد من الدراسات التي تناولت المخاطر المحتملة التي تواجه الدول الغربية وعلى رأسها الولايات المتحدة الأمريكية جراء اعتمادها الكبير على تكنولوجيا المعلومات ومن أجل ذلك وخلال تلك الفترة صدر تقرير عن الأكاديمية الوطنية الأمريكية للعلوم عن امن الكمبيوتر جاء فيه:" نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر، حيث غدا بإمكان الإرهابيين إحداث تدمير اكبر بالاعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربر الكتروني جديد"[2].

وبعد هذا التقرير جاءت اجتهادات عديدة لوضع تعريف دقيق للإرهاب الالكتروني مركزة في مجملها على هدف الهجمات التي يمكن أن تتعرض لها الشبكة العالمية للانترنت والذي وجب أن يكون ذو طابع سياسي حتى نطلق على هذه الهجمات بالإرهابية وحيث أن الإرهاب الالكتروني هو استخدام الفضاء الالكتروني كأداة لإلحاق الضرر أو تعطيل البنية التحتية القومية كالطاقة والمواصلات وأنشطة الحكومة، فيدخل الإرهاب الالكتروني ضمن الأعمال التي تصب في اتجاه

[1] B. Collin, " The Future of CyberTerrorism : Where the Pysical and Virtual Worlds Converge ", 11 the Annual International Symposium on Criminal Justice Issues, 1996 http// www.irsem.defense.gouve.fr).(06/08/2017 à 22:32).

[2] عادل صادق، مرجع سابق، ص 104.

سياسي واحد والتي قد تتحالف مع الجريمة أو تكون إحدى أدواتها[1]، أي انه نتاج التفاعل بين العالم المادي والعالم الافتراضي – كما جاء في تعريف "barryCollin"– فالعالم المادي هو المادة والطاقة الموجودة حيث العيش والعمل..، أما العالم الافتراضي فهو الرمز القائم حيث تعمل برامج الكمبيوتر وتتحرك المعلومات بصورة رقمية ومجازية، فعلى الرغم من تباين العالمين فإنهما يتفاعلان عند التقارب بينهما مشكلين السمات الرئيسية للإرهاب الالكتروني والتي تأتي في صورة أعمال تخريبية توجه للشبكات وقواعد المعلومات لدى الطرف الضحية .[2]

ومن أجل ذلك عرف بعض الفقهاء الإرهاب الالكتروني بأنه:" هو خرق للقانون يقدم عليه فرد من الأفراد، أو تنظيم جماعي بهدف إثارة اضطراب خطير في النظام العام، عن طريق شبكة المعلومات العالمية الانترنت" في حين عرفه جانب آخر من الفقه بأنه:" الاستخدام العدائي أو العدواني غير المشروع للانترنت بهدف ترويع الحكومة، والمدنيين أو قسم منهم، في إطار السعي إلى تحقيق أهداف سياسية أو اجتماعية".[3]

أما "دورثيدابينج"[4] فقد عرفت الإرهاب الالكتروني بقوله:" التقاء للإرهاب مع الفضاء التخيلي" وهو بذلك يعني التهديدات غير القانونية ضد الحاسبات والشبكات والمعلومات المخزنة، وذلك لإخافة أو إجبار الحكومات أو الناس لتعزيز أهداف سياسية أو اجتماعية فهو العنف ضد الأفراد أو الممتلكات أو انه مؤذ لدرجة كافية لخلق الخوف، والتعديات المفضية للموت أو الإصابة بالانفجارات أو الخسارة الاقتصادية" وعلى ذلك يمكن تصنيف المستهدفين من الإرهاب الالكتروني إلى ثلاثة فئات: الأفراد، الممتلكات والحكومات.[5]

---

[1] Dan Verton, Black ice-The Invisible Threat of Cyber-Terrorism, New York,McGraw-Hill,Osborne,2003,p 180

[2] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 105.

[3] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 126.

[4] دورثي هي أستاذة علوم الحاسب في جامعة جورج تاون،كانت تعمل على قضايا المن السيبيراني والتكنولوجيات لمدة 30 سنة تقريبا،مؤلفة كتاب حرب المعلومات والأمن، ولهت مؤلفات كثيرة أخرى، نالت العديد من الجوائز من أهمها جائزة امن الكمبيوتر الوطنية،واعتبرت محاضرة متميزة، تحصلت على درجة الدكتوراه في علوم الكمبيوتر من جامعة بورد، للمزيد من المعلومات حولها :www.denning@georgetown.edu

[5] ذياب موسى البداينة، الإرهاب المعلوماتي،أبحاث الحلقة العلمية حول "الانترنت والإرهاب"، كلية التدريب جامعة نايف للعلوم الأمنية بالتعاون مع جامعة عين شمس، 2008، ص 13.

عما عرفه "كولنز" بقوله:" الإرهاب الالكتروني هو سوء الاستخدام المتعمد لنظام المعلومات الرقمي والشبكات أو المكونات تجاه هدف يدعم أو يسهل حملة إرهابية أو فعل إرهابي"[1]

وكالة المخابرات المركزية الأمريكية بدورها قدمت تعريف للإرهاب الالكتروني بقولها:الإرهاب الالكتروني هو أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر، وبرامجه والبيانات والمعلومات والتي تنتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين"[2].

"دينينجدوروثي" تعرف الإرهاب الالكتروني على أنه:" هجمات غير قانونية وتهديدات بالهجوم ضد أجهزة الحاسبات والشبكات والمعلومات المخزنة وذلك لكي توظف لتخويف أو إجبار حكومة أو شعبها بهدف تعزيز أهداف سياسية أو اجتماعية، ولكي يكون إرهابا وجب أن ينتج عنه عنف اتجاه الأفراد أو الممتلكات أو على الأقل التسبب في ضرر ينتج عنه توليد الخوف"[3].

الباحث الأمريكي "POLITT Mark"الباحث في مكتب معهد أمن المعلومات بالتعاون مع مكتب التحقيقات الفيدرالية للولايات المتحدة الأمريكية يعرف الإرهاب الالكتروني بقوله:" هجوم ذو دوافع سياسية، اقتصادية أو شخصية ضد المعلومات ونظم الحاسوب وبرامجه، من قبل مجموعة إرهابية أو عملاء سريين"[4]

[1] محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الالكترونية، دار الناشري للنشر الالكتروني 2012، ص29 (متوافرة في الموقع www.nashiri.net) (تمت الزيارة في 2017/04/19 على الساعة 20:00 )

[2] عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية، مذكرة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم السياسية، كلية الاقتصاد والعلوم والسياسية –قسم العلوم السياسية، القاهرة، 2009، ص 79.

[3] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 106.

[4] ذياب موسى البداينة، الإرهاب المعلوماتي، مذكرة ماجستير في القانون، كلية التدريب، جامعة نايف للعلوم الأمنية،2008، ص 13.

أما مركز الدراسات الإستراتيجية والدولية فانه يعرف الإرهاب الالكتروني على أنه:" استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القومية، مثل الطاقة المواصلات وعمليات الحكومة، أو إكراه أو ترهيب الحكومة أو السكان المدنيين"[1].

وزارة الدفاع الأمريكية أيضا عرفت الإرهاب الالكتروني بقولها:" الإرهاب الالكتروني عمل إجرامي يتم الإعداد له باستخدام أجهزة الحاسبات ووسائل الاتصالات، ينتج عنه عنف وتدمير، أو بث الخوف تجاه متلقي الخدمات، مم يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل إلى أجندة سياسية أو اجتماعية أو فكرية معينة"[2].

والملاحظ على التعريفات السابقة أن جانب منها ركز على أن الانترنت وجهاز الحاسوب أداة يستخدمها الإرهاب لتحقيق أهدافه، وأما الجانب الآخر فإنه ركز على أن الانترنت هي هدف العمليات الإرهابية، في حين نرى أنه من الضروري أن نجمع بيه العنصرين في تعريف واحد (الأداة والهدف).

فالإرهابي يمكن أن يستخدم الوسائل الالكترونية في شن هجومه، كما يمكنه أن يستخدم أدوات عسكرية تقليدية في تدمير هذه الوسائل وبالتالي تكون هذه الأخيرة هي المستهدفة من العمليات الإرهابية.

فقهاء العالم العربي حاولوا بدورهم إعطاء تعريف للإرهاب الالكتروني ومن ابرز هذه التعرف تعريف الدكتور "عبد الرحمان السند" –والذي يعتبر مرجعية كل المحاولات العربية التي تلته– حيث عرف الإرهاب الالكتروني بقوله:" الإرهاب الالكتروني هو العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه، وصور الإفساد في الأرض"[3] .

كما ذهب البعض منهم إلى تعريف الإرهاب الالكتروني بأنه:" الاستخدام غير الأمثل للشبكة العالمية، بما يؤدي إلى ترويع المواطنين بشكل خطر، أو يسعى إلى زعزعة الأمن والاستقرار، أو

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص ، ص 106.

[2] عادل الصادق ، (أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية)، مرجع سابق، ص 80.

[3] عبد الرحمان السند، وسائل الإرهاب الالكتروني–حكمها في الإسلام وطرق مكافحتها، بحث مقدم للجنة العلمية للمؤتمر العالمي عن موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، 2004، ص 5.

تعريض المؤسسات السياسية أو الدستورية، أو الاقتصادية أو الاجتماعية، لإحدى الدول أو المنظمات الدولية، عن طريق استخدام لغة التهديد والعدوان"[1].

أيضا عرف الإرهاب الالكتروني في العالم العربي:" بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الالكترونية، بشتى صنوف العدوان وصور الإفساد"[2].

ونلاحظ أن التعريفات العربية أيضا ذهبت في معظمها إلى التركيز على استخدام الوسائل الالكترونية في الهجمات حتى يطلق عليه إرهاب الكتروني وأهملت الحالة التي تكون فيها هذه الوسائل الالكترونية هدف الهجمات الإرهابية.

ومن أجل ذلك يعتبر التعريف التالي هو التعريف الأمثل والأشمل لأنه جمع بين الوسيلة والهدف حيث جاء فيه:" الإرهاب الالكتروني يعني العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادر من الدول أو الجماعات أو الأفراد عبر الفضاء الالكتروني، أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له"[3].

ومن التعريفات السابقة للإرهاب الالكتروني سواء المقدمة من طرف الفقه العربي أو الغربي يستخلص أن الإرهاب الالكتروني لا يختلف في مضمونه عن الإرهاب التقليدي حيث يعتبر صورة معاصرة ومتقدمة له، فجاء الاختلاف بينهما في الوسيلة المستخدمة في حين أن الهدف أو يكون واحد في كلا الصورتين.

ومن الاختلافات بين الإرهاب بصفة عامة والإرهاب الالكتروني والتي يمكن أن نستخلصها من التعريفات السابقة:

[1] أمير فرج يوسف،(مكافحة الإرهاب الالكتروني)، مرجع سابق، ص 126.

[2] عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الانترنت، المنعقد في القاهرة في من 2 إلى 4 يونيو 2008.

[3] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 109.

– الإرهاب التقليدي عمل مادي يقع في الحيز الواقعي، ويتضح ذلك سواء من خلال الوسائل المستخدمة أو من النتيجة المتوصل إليها، في حين أن الإرهاب الالكتروني يتم في العالم الافتراضي.

– الإرهاب التقليدي ركزت معظم تعريفاته على أن الدولة هي المقصودة من الاعتداء بغية تحقيق هدف سياسي، ويكون هذا الاعتداء سواء من طرف دولة أو من جماعات إرهابية، وان هذا العدوان نفسه يعتبر عمل عسكري محدد يهدف لإلحاق الضرر بالدولة، أما الإرهاب الالكتروني فيرتبط بفكرة الإرهاب الثقافي الناتج من العولمة والثورة التكنولوجية.[1]

– الإرهاب التقليدي يعتمد على وسائل عنيفة من أجل إحداث حالة الرعب في حين الإرهاب الالكتروني يعتمد على وسائل متطورة وتكنولوجيو ولكنها تصل إلى إحداث حالة رعب قد تفوق الوسائل التقليدية ومثال ذلك أحداث الحادي عشر من سبتمبر 2001 والتي بسببها تأثر اقتصاد العالم بأسره ومما نتج عنه أيضا تغيير الاتجاهات الدولية نحو الحرب الوقائية وما تسببت في من انتهاكات وحروب وجرائم .

ويستخدم الإرهابيون الانترنت بطريقة سلبية وتتحقق هجماتهم الإرهابية مستهدفة شبكات الحاسوب بما يلي:

– **تبادل المعلومات:** تمكن غرف الدردشة والمنتديات من جمع الكثير من الأشخاص حيث يتبادلون المعلومات وأطراف الحديث وهم متواجدون في أماكن جغرافية متفرقة وبذلك يتمكن الإرهابيون من تبادل المعطيات والاستراتيجيات، فضلا على البريد الالكتروني ودوره المهم في نقل الملفات المعلومات بسرعة وبطريقة آمنة – وهو ما سوف يتم تفصيله في عناصر لاحقة– كما توفر هذه الغرف والمنتديات مجالا خصبا لإخفاء الهوية، إذ يصعب كثيرا التعرف على من يختفي وراء هذه الشخصيات وبالتالي يستفيد الإرهابيون من عدم وجود آثار ثابتة للجريمة.[2]

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 108.

[2] إيناس محمد البهجي، يوسف المصري، الجريمة في القانون الدولي والشريعة الإسلامية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2013، ص76.

- **المواقع الدعائية للجماعات الإرهابية:** حيث تسعى الجماعات الإرهابية إلى كسب الدعم والتأييد ولا يتسنى لها ذلك إلا عن طريق شبكة الانترنت عن طريق الدعاية والإشهار ،إذ تقوم بإصدار بياناتها ومخططاتها من اجل جلب الأشخاص وتجنيدهم للانخراط في نشاطاتهم[1].

هذا وتستطيع الجماعات الإرهابية من خلال هذه المواقع الدعائية من أن تقدم خدمات تدريبية في التعامل مع النشاطات الإرهابية، وذلك عن طريق الإرشادات الكتابية والفيديوهات التي ترشد إلى طرق تصنيع القنابل والأسلحة المدمرة....[2].

ويمكن ان نتعرض لبعض المواقع لجماعات متطرفة بشيء من التفصيل كما يلي[3]:

-**موقع كوكالوكس كلان:** وهي منظمة تتبنى فكرة تفوق الجنس الأبيض في تقديم الطريقة المثلى للعيش أو ما يعرف "المسيحيين الغربيين المدنيين"، حيث تعني كلمة "كوكالوكس" التنظيم والتوحيد وهي كلمة يونانية الأصل، ويتضمن هذا الموقع البيانات والمعلومات الخاصة بزعيم هذا التنظيم، والمدعو "توماس روب" كما تضمن الموقع عنوانه ورقم هاتفه، ويعرض هذا الخير من خلال موقعه اللائحة الداخلية للتنظيم وبرنامجها، كما يشير إلى مختلف الأعمال والمظاهرات التي شارك فيها التنظيم لإعلان وجهة نظرها العنصرية، وقد تم حجب هذا الموقع بطلب من الحكومة الأمريكية بسبب التطرف الديني لهذه المنظمة، وعنصريتهم وتمييزهم السياسي للجنس الأبيض[4].

- **موقع منظمة مافيا ترنشكوت:** وهي منظمة عنصرية تضم مجموعة أشخاص يكنون الكراهية للأشخاص الملونين وخاصة السود، ويرتدي أعضاء هذا التنظيم ملابس غريبة ويطلقون شعارات دموية وعنيفة عبر موقعهم كعبارة "ينبغي قتلهم جميعا"، ويمتاز أعضاء هذا التنظيم بالذكاء الخارق خاصة في مجال الكمبيوتر وهو ما اكتشفته الشرطة الأمريكية بعد تحقيقها في جريمة

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص128.

[2] إيناس محمد البهجي، يوسف المصري، مرجع سابق، ص 77.

[3] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 129.

[4] مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب والوثائق القانونية، القاهرة، 2003، ص 213.

ارتكبها طالبين من هذا التنظيم المتطرف[1]، وبضغط من الرأي العام وطلب من الحكومة الأمريكية تم حجب هذا الموقع من طرف شركة أمريكا أون لاين "American on line"[2].

- **موقع النداء:** وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر 2001 ومن خلاله تصدر البيانات الإعلامية لهذه المنظمة الإرهابية.

- **ذروة السنام:**وهي صحيفة الكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

- **صوت الجهاد:** وهي مجلة نصف شهرية يصدرها تنظيم القاعدة أيضا في جزيرة العرب وتتضمن مجموعة من البيانات والحوارات مع قادة تنظيم القاعدة ومناظريه.

- **البتار:** وهي مجلة عسكرية الكترونية متخصصة تصدر عن تنظيم القاعدة وتختص بالمعلومات العسكرية، والمدنية، والتجنيد.

### * موقف التشريعات الوضعية من الإرهاب الالكتروني.

حيث أن جريمة الإرهاب الالكتروني تصنف من الجرائم المعلوماتية، فقد أقر مجلس الشورى السعودي القرار رقم 43/68 في السادس من سبتمبر 1427 هـ نظام مكافحة الجرائم المعلوماتية كما أقره مجلس الوزراء السعودي بتاريخ 26 مارس 2007، حيث يهدف هذا النظام إلى تحقيق الأمن المعلوماتي ويكافح الجرائم المستحدثة التي تستخدم التقنية الالكترونية الرقمية وشبكات المعلومات في نشاطها[3]

[1] حيث قاما طالبان أمريكيان عضوين في هذه المنظمة بإطلاق النار من مسدسيهما على طلبة الثانوية التي يزاولان فيها دراستهما في مدينة "لتيلتون" التابعة لولاية "كلورادو" في الولايات المتحدة الأمريكية حيث أسفر عن هذه الجريمة الإرهابية 15 قتيلا، ثم اختبآ في مكتبة المدرسة إلى أن وجدتهما الشرطة منتحرين بعد الحادثة بساعات،عقب تفكيك العديد من العبوات الناسفة في السيارات المجاورة للمدرسة والتي كاد أن ينجم عنها سقوط العديد من الضحايا، وبعد التحريات ثبت فعلا أن الطالبين كانا يعلنان صراحة أنهما سوف يجعلان من شهر أبريل يوما يتذكره الأمريكيين عامة.

[2] حسنين محمدي البوادي، إرهاب الانترنت الخطر القادم، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006 ص89.

[3] مصطفى محمد موسى،(الإرهاب الالكتروني) مرجع سابق، ص 112.

فعن الإرهاب الالكتروني نصت المادة سبعة من نظام مكافحة الجرائم المعلوماتية السعودي على عقوبة السجن مدة لا تزيد عن العشر سنوات وغرامة مالية لا تزيد عن خمسة ملايين ريـــال، أو بإحدى هاتين العقوبتين لكل شخص ينشئ موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أخد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات أو أية أداة تستخدم في الأعمال الإرهابية، أو لمن يقوم بالدخول غير المشروع إلى مواقع الكترونية، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني[1] .

من خلال التعريفات السابقة للإرهاب بوجه عام (الإرهاب التقليدي) –والتي سبق وأن فصلنا فيها – وباستقرائنا للمادة السابقة من النظام السعودي لمكافحة الجرائم المعلوماتية يتبين أن الإرهاب الالكتروني يقوم على العناصر التالية:

– **العنصر الأول:** أن تكون الجريمة الإرهابية ذات طبيعة عنيفة، أي تكتسي شكل من أشكال العنف، وهذه النقطة محل اتفاق بين جميع الدول دون استثناء، وهو ما انعكس على الاتفاقيات الدولية التي وقعتها الأمم المتحدة، وأن يكون الإرهاب وسيلة لتحقيق غايات سياسية أو مادية.

– **العنصر الثاني:** وأن يهدف الإرهاب إلى انتهاك حقوق الإنسان الفكرية أو السياسية أو العقلية أو البدنية...

– **العنصر الثالث:** أن يكون للإرهاب طابع رمزي، فقتل الإرهابي للشخص يكون بهدف بث الرعب في نفوس الآخرين .

– **العنصر الرابع:** فضلا عن العناصر السابقة، فحتى يعتد بالإرهاب الالكتروني وجب توافر عنصر مهم وهو الوسيلة الالكترونية الرقمية المستخدمة في الاتصال وتنفيذ الجرائم الإرهابية بواسطتها وعبر شبكات المعلومات[2].

[1] مصطفى محمد موسى،(الإرهاب الالكتروني) مرجع سابق، ص 112.

[2] نفس المرجع، ص 112، 113.

سلطنة **عمان** بدورها اهتمت بالتشريع المتعلق بمكافحة جرائم المعلوماتية، حيث اعتبرت من أولى دول الخليج العربي التي تبنت قواعد قانونية تجرم الأفعال الإجرامية الناجمة عن إساءة استعمال تقنية المعلومات، ومن أجل ذلك قام المشرع العماني بتعديل قانون الجزاء العماني، وذلك بموجب المرسوم السلطاني رقم 2001/72 حيث أضاف فصل ثاني مكرر للباب السابع[1] .

وفي سنة 2011 صدر المرسوم السلطاني لسلطنة عمان رقم 12، الذي يتضمن قانون مكافحة جرائم تقنية المعلومات[2]، والذي بموجبه الغي المرسوم السابق، حيث يتألف هذا المرسوم من 35 مادة تصدت المادة العشرون (20) منه للإرهاب الالكتروني باستعمال الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات ففرضت على مرتكب هذا الجرم عقوبة السجن المطلق والغرامة التي لا تقل عن مائة ألف ريـــال عماني، ولا تزيد عن مائتي ألف[3].

هذا بالإضافة إلى نصوصه الأخرى التي تجرم كافة الجرائم الماسة بتقنية المعلومات والتي لها علاقة بالإرهاب الالكتروني، بل وتعتبر أسلوب من أساليبه –والتي سوف نتعرض إليها لاحقا بشيء من التفصيل–حيث جرمت المادة الثالثة منه الدخول العمدي ودون وجه حق إلى أي موقع الكتروني أو نظام معلوماتي أو وسائل تقنية المعلومات، أو جزء منها، كما شددت هذه المادة العقوبة في حالة ترتب عن هذا الدخول إلغاء أو تعيير أو تعديل أو تشويه أو إتلاف أو نسخ أو تدمير أو نشر أو إعادة نشر البيانات أو معلومات الكترونية مخزنة في النظام المعلوماتي، أو وسائل تقنية المعلومات أو تدمير ذلك النظام، أو وسائل تقنية المعلومات، أما المادة السادسة منه(6) فقد جرمت الدخول العمدي إلى مواقع الحكومية للحصول على بيانات أو معلومات حكومية سرية بطبيعتها أو بموجب تعليمات صادرة بذلك [4] .

---

[1] محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر والقانون القاهرة، 2015، ص 212.

[2] هذا القانون منشور على موقع هيئة تقنية المعلومات العمانية: www.ita.gov.com تمت الزيارة في 2017/08/22 على الساعة 20:01.

[3] حسين بن سعيد الغافري، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت، مقالة منشورة على الموقع:www.hussain-alghafri.blogspot.com، تاريخ الاطلاع : 2017/08/22 على الساعة: 21:07.

[4] محمد كمال محمود الدسوقي، مرجع سابق ص 215.

أما القانون الاتحادي رقم 2 لسنة 2006 لدولة الإمارات العربية المتحدة والذي يتضمن مكافحة جرائم تقنية المعلومات فقد نص على الإرهاب الالكتروني في المادة 21 منه بقولها:" كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد عن خمس سنوات"[1].

أما المادة الثانية من هذا القانون فقد منعت الدخول أو البقاء غير القانوني داخل النظام المعلوماتي وشددت العقوبة إذا ما ترتب على هذا الدخول إتلاف أو نشر أو إعادة نشر لبيانات أو معلومات شخصية، في حين تناولت المادة 22 من ذات القانون حالة الدخول غير القانوني إلى موقع أو نظام الكتروني مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أما المادة الثامنة(8) فقد تناولت أفعال التنصت أو الالتقاط أو التعرض العمدي دون وجه حق لما هو مرسل عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات[2].

المشرع الأردني كغيره من المشرعين اهتم بالإرهاب الالكتروني، حيث نص في المادة الثانية من قانون منع الإرهاب رقم 55 لسنة 2006 بقوله:" العمل الإرهابي كل عمل مقصود يرتكب بأي وسيلة كانت.."، وعليه وفقا لهذه المادة يشترط في العمل الإرهابي الالكتروني مايلي[3]:

– أن يكون العمل مقصودا .

– أن يرتكب هذا العمل المقصود بأي وسيلة كانت، وعليه فان الوسائل التكنولوجية الحديثة كالحاسب الآلي والانترنت تدخل ضمن هذا التعريف، طالما حققت نفس الهدف المرجو من الإرهاب.

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت–الجرائم الالكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت–لبنان، 2007، ص 75.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 215.

[3] فهد يوسف الكساسبة، الإرهاب الالكتروني في التشريع الأردني، مجلة العلوم القانونية والسياسية، جامعة عمان العربية، العدد التاسع، 2015، ص 150.

– وأن يؤدي هذا الفعل إلى قتل شخص أو مجموعة أشخاص، أو التسبب بإيذائهم جسديا أو إيقاع أضرار في الممتلكات العامة أو الخاصة أو في وسائل النقل أو البيئة، أو في البنية التحتية أو في مرافق الهيئات الدولية أو البعثات الدبلوماسية إذا كانت الغاية منه الإخلال بالنظام العام، وتعريض سلامة المجتمع وأمنه للخطر، أو تعطيل أحكام الدستور أو القوانين، أو التأثير في سياسة الدولة أو الحكومة أو إجبارها على عمل ما، أو الامتناع عنه أو الإخلال بالأمن الوطني بواسطة التخويف أو الترهيب أو العنف.

وعلى ذلك وحسب المشرع الأردني أن الإرهاب الالكتروني لا يختلف عن الإرهاب التقليدي إلا في الطريقة والوسيلة المستخدمة، إذ أن هذا الأخير يقوم على استخدام التقنيات العصرية في تنفيذ العمليات والمخططات الإرهابية بدلا من الوسائل التقليدية، والتي تقوم على الاتصال المباشر بين الإرهابيين والضحايا والأماكن المستهدفة.[1]

أما في سنة 2010 فقد سن المشرع الأردني قانون مكافحة جرائم أنظمة المعلومات حيث نصت المادة الرابعة منه على ما يلي:" كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام المعلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات، أو الوصول إليه أو تغيير موقع الكتروني، أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح، أو بما يجاوز أو يخالف التصريح، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار، أو بكلتا هاتين العقوبتين[2].

[1] هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،(سنة النشر غير مذكورة) ص 37.

[2] رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، مقالة مقدمة في الدورة التدريبية الموسومة بالعنوان:" توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب" خلال الفترة 13-2012/04/17 إلى غاية 23-2013/02/27 ، الرياض، 2013، ص 24.

أما المادة 14 فقد نصت على:" كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب عليها بالعقوبة المنصوص عليها في ذلك التشريع.[1]

جمهورية السودان أيضا كغيرها من الدول السابقة شهدت حركة تطوير للبنية التشريعية للتصدي للجرائم المعلوماتية، ويعتبر قانون جرائم المعلوماتية لسنة 2007 ابرز التشريعات التي عرفتها هذه الحركة، وقد صدر هذا القانون في 20 جوان 2007 وتضمن هذا القانون 30 مادة موزعة علة تسعة فصول، وقد جاء الفصل الخامس بعنوان:" جرائم الإرهاب والملكية الفكرية"، حيث نصت المادة 18 منه على انه:" كل من ينشي أو ينشر أو يستخدم موقعا على شبكة المعلومات أو احد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابية تحت أي مسمى لتسهيل الاتصال بقيادتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في العمليات الإرهابية، يعاقب بالسجن مدة لا تتجاوز سبع سنوات، أو بالغرامة، أو بالعقوبتين معا"، حيث قام الإرهابيون باستغلال شبكة المعلومات في عملياتهم الإرهابية التي انتشرت في جميع أنحاء العالم[2].

المشرع المصري كغيره من المشرعين حرص على مكافحة الإرهاب الالكتروني حيث خصص المادة 29 من قانون مكافحة الإرهاب الصادر في 16 أغسطس 2015 حيث نصت على أنه:" يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن أي جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج.

[1] الجريدة الرسمية الأردنية رقم 2010/5056 الصادرة في 2010/09/16 متوافرة في الموقع:
www.lawjo.net/vb/showthread.php?، تمت الزيارة يوم 2017/08/24 على الساعة: 17:48.

[2] شرح قانون جرائم المعلوماتية السوداني لسنة 2007، مقالة منشورة في
الموقع:http://ibrahimtahaa.blogspot.com/2013/07/2007 وتمت الزيارة في 2017/08/25 على الساعة: 23:26.

ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من دخل بغير حق أو بطريقة غير مشروعة موقعا إلكترونيا تابعا لأية جهة حكومية بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها"[1].

وما يعكس حرص دولة مصر كغيرها من الدول على مكافحة ظاهرة الإرهاب الالكتروني هو العديد من المبادرات التي قامت بها حول هذا الشأن ، فقد سبق وان صرح مساعد وزير الخارجية المصري للشؤون القانونية الدولية والمعاهدات ومكافحة الإرهاب أن هدف هذه المبادرات هو معرفة كيفية التعامل مع ظاهرة استخدام شبكة الانترنت والتي اعتبرت من أخطر الوسائل التي نشرت ظاهرة الإرهاب، كما تهدف المبادرة أيضا إلى تحقيق تنسيق أفضل بين دول العالم لتجريم استخدام الأفراد أو الجماعات الإرهابية شبكة الانترنت لخدمة أهدافها[2].

كما تضمن قانون مكافحة الجريمة الالكترونية المصري تجريم الممارسات الالكترونية غير المشروعة، والتي لا يوجد ما يجرمها في قانون العقوبات المصري، ومنها التزوير الالكتروني، وتجريم إنشاء مواقع للتشجيع على الإرهاب أو نقل المعلومات، حيث تتراوح العقوبة من السجن شهرا حتى الإعدام، وهذا في حالة الجرائم الالكترونية التي يترتب عليها وفاة الشخص أو مجموعة من الأشخاص أو تهديد الأمن القومي والسلم الاجتماعي، ومن اجل ذلك سن المشرع المصري قانون مكافحة الجريمة الالكترونية سنة 2016[3].

الدول الغربية أيضا اهتمت بجريمة الإرهاب الالكتروني نظرا لتفشي هذه الجريمة الخطيرة في العالم بأسره، ومن الدول الغربية نأخذ على سبيل المثال الولايات المتحدة الأمريكية، التي ظهر فيها الإرهاب الالكتروني بصورة علنية عام 1996 عندما قام "**بيل كلينتون**" بإنشاء لجنة حماية منشآت

[1] قانون مكافحة الإرهاب المصري الصادر في 15 أغسطس 2015 منشور في الموقع
:http//www.aljazeera.net/encyclopedia/events/2015/8/17، تاريخ الاطلاع 2017/08/27، على الساعة 13:41.

[2] عبد الله عبد الكريم عبد الله، مرجع سابق، ص 28.

[3] مشروع قانون الجريمة الالكترونية المصري، منشور في جريدة الوطن متوافر في الموقع:
http://Fr.scribd.com/document/266804184 تاريخ الاطلاع في 2017/08/27 على الساعة: 15:57 .

البنية التحتية، فكان من بين الاستنتاجات التي توصلت إليها هذه اللجنة أن مصادر الطاقة والاتصالات وشبكات الكمبيوتر ضرورية جدا لبقاء الولايات المتحدة الأمريكية ونجاتها، وبما أن هذه المنشات تعتمد بشكل كبير على المعلومات الرقمية، وبالتالي فان هذه المنشات سوف تكون الهدف الأول لأي هجمة إرهابية تستهدف امن الولايات المتحدة الأمريكية، ومن أجل ذلك قامت الولايات المتحدة الأمريكية بإنشاء هيئات ومراكز خاصة للتعامل مع هجمات الإرهاب الالكتروني[1] .

وقبل ذلك وفي سنة 1986 عرف التشريع الأمريكي رقم 1213 الجريمة الالكترونية بقوله:" الاستخدام غير المصرح به لأنظمة الكمبيوتر المحمية أو ملفات البيانات أو الاستخدام المتعمد الضار لأجهزة الكمبيوتر ملفات البيانات"[2]

أما كلية الحرب التابعة لوزارة الدفاع الأمريكية فقد قامت بتعريف الحرب الالكترونية سنة 1996 دون أن تتطرق إلى تعريف الإرهاب الالكتروني وذلك بقولها:" إن الحرب الالكترونية هي الإجراءات التي تم اتخاذها بشكل سلبي على المعلومات والنظم الالكترونية، لتخريبها وتخريب النظم الالكترونية التي تحتويها"، وعلى ذلك وحسب هذا التعريف فان الحرب الالكترونية تشتمل على تخريب امن المعلومات، وأيضا الهجمات على النظم الالكترونية ، وكذا التدمير الفيزيائي لأجهزة الخصم أو النقاط الهامة ضمن شبكاته وذلك بفعل الهجمات المباشرة[3] .

وإذا كان التشريع الأمريكي لم يعط تعريفا للإرهاب الالكتروني إلا أن الولايات المتحدة الأمريكية اهتمت كثيرا بهذه الجريمة الخطيرة وينعكس ذلك من خلال الإجراءات المختلفة التي اتخذتها لمكافحة هذه الجريمة الخطيرة كإنشائها وكالة استخبارات مركزية خاصة بالحرب المعلوماتية، كما

[1] نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الالكتروني، مذكرة مكملة لنيل شهادة الماجستير في القانون الدولي العام، كلية الحقوق والعلوم السياسية– جامعة مولود معمري– تيزي وزو، ص 24.

[2] خالد حمد محمد الحمادي، الإرهاب الالكتروني– دراسة في التشريع الاتحادي لدولة الإمارات العربية المتحدة أكاديمية الاتصالات، الشارقة، 2007، ص15 .

[3] نفس المرجع، ص 24.

قامت المكاتب الفدرالية باتخاذ إجراءات أمنية في نفس المجال وهذا من أجل الرد السريع ومحاولة القضاء على آفة الإرهاب الالكتروني[1] .

الاتحاد الأوروبي بدوره اهتم لموضوع الإرهاب الالكتروني، حيث اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ سنة 1976، وفي سنة 1996 تم إنشاء اللجنة الأوربية لحل مشاكل الإجرام في أوروبا، من خلالها يمكن للمجلس الأوروبي من ممارسة نشاطه في مكافحة الجريمة المنظمة بكل أنواعها بما فيها الجرائم الالكترونية وهذه اللجنة قد عملت في الفترة مابين 1997 إلى غاية 2000 على اتفاقية مشروع بودابست التي اعتمدها البرلمان الأوروبي في الجزء الثاني من الجلسة العامة في شهر أفريل 2001، والتي تم التصديق عليها رسميا من قبل 30 دولة في 23 نوفمبر 2001 [2]

في سنة 2002 قدم الاتحاد الأوروبي تعريفا للإرهاب بشكل عام ولم يخص الإرهاب الالكتروني بتعريف خاص به وذلك بقوله:" كل عمل يرتكب بهدف ترويع الأهالي، أو إجبار حكومة أو هيئة دولية على القيام بعمل أو الامتناع عنه، أو تدمير الهياكل الدستورية،أو الاقتصادية أو الاجتماعية، لدولة ما أو هيئة دولية ما، أو زعزعة استقرارها"[3].

وبما أن الإرهاب الالكتروني يعتبر نوع من أنواع الإرهاب فهو يدخل ضمن هذا التعريف، فهذا التعريف لم يحدد لا نوع الإرهاب ولا الوسيلة التي ارتكب بها، بل اعتبر كل عمل يروع الآخرين عموما.

أما الدول الأعضاء في الاتحاد الأوربي فقد حاولت كل منها إعطاء تعريف للإرهاب الالكتروني كل حسب وجهة نظرها، فالإرهاب الالكتروني تم تعريفه من طرف ايطاليا بقولها:" كل جماعة إرهابية

[1] نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة مكملة لنيل الماجستير في القانون ،كلية الحقوق والعلوم السياسية –جامعة مولود معمري–تيزي وزو، 2009، ص 19.

[2] نجاري بن حاج علي فايزة، مرجع سابق، ص 25.

[3] نفس المرجع ، ص 26.

تستعمل الوسائل التكنولوجية كالانترنت من أجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق وتبادل المهارات والأساليب والخبرات أو جمع التبرعات من أجل تمويل عملياتهم الإرهابية"[1].

ايطاليا ركزت في تعريفها للإرهاب الالكتروني على الدعاية وتمويل الإرهاب، كما حددت الوسيلة المستخدمة في الجريمة الإرهابية وبالتالي حددت الهدف وغفلت عن الجهة المستهدفة من الهجوم، كما ركزت على الإرهاب الجماعي وأغفلت النشاط الفردي .

فرنسا بدورها أعطت تعريفا للإرهاب الالكتروني، حيث جاء انه:" كل هجوم الغرض منه الحصول على المعلومات المرتبطة بالغير، وإمكانياته واستراتيجياته التي تخذها للدفاع عن نفسه، أو تدمير نظم معلوماته، أو نشر معلومات زائفة من أجل تضليله بتوظيف تكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنت"[2].

والملاحظ على التعريف المقدم من طرف فرنسا انه لم يحدد الجهة المستهدفة من الهجمات الإرهابية شأنها في ذلك شأن سابقتها فرنسا ، مع أنه حدد أسباب الهجوم والوسيلة بدقة .

## الإرهاب الالكتروني في التشريع الجزائري.

المشرع الجزائري على غرار مشرعي معظم دول العالم قام بتجريم أفعال المساس بنظم المعالجة الآلية، وهذا من أجل حمايتها من كافة الاعتداءات التي يمكن أن تتعرض إليها المكونات غير المادية مما يؤدي إلى إعاقة دورة تقدمها في المجتمع، وسبب سن هذا التشريع يرجع إلى تأثر الجزائر بثورة تقنية المعلومات وما أفرزته من جرائم حديثة تطول مصالح مستحدثة لم يكن قانون العقوبات القديم قد حماها بعد، الأمر الذي جعل المشرع الجزائري يعمد إلى تعديل قانون العقوبات بموجب القانون رقم 04/15 .[3]

وقد أفرد هذا القانون قسم منه تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" ويتضح أن المشرع الجزائري خطا هذه الخطوة متأثرا بالمشرع الفرنسي الذي بدوره أقر بأنها ظاهرة

[1] Steven FURNEL, cyber crime vandalizing the information society,London, Addison cuesely, 2002, p253.

[2]Pitter BELLEY, Hachedattacked, Abused digital crime exposed, London, Regan page 2002, p 107.

[3] صدر هذا القانون في 2004/10/10 والذي عدل وتمم الأمر رقم 156/66 السالف الذكر.

مستجدة وخطيرة، ومن خلال هذا القانون عمد المشرع الجزائري إلى حماية سرية نظم المعالجة الآلية ومعلوماتها، ومن أجل ذلك جرم الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات، كما حمى سلامة المعلومات ونظم معالجتها وتكاملها فجرم بذلك التلاعب بالمعلومات إدخالا، إزالة وتعديلا ما لم يكن مصرحا بذلك، وكذلك تخريب نظام المعالجة الآلية للمعطيات (وجميع هذه الجرائم تعتبر أساليب للإرهاب الالكتروني التي سوف نوضحها لاحقا)[1].

وعن الإرهاب الالكتروني وباعتباره جريمة الكترونية من جهة، كما يعتبر امتداد لجريمة تقليدية وهي الإرهاب الدولي، حيث يعتبر الإرهاب الالكتروني من قبيل الجرائم المستحدثة، والتي أعطت للإرهاب شكلا وبعدا جديدين- كما سبق وان بينا- فقد نص المشرع بموجب القانون رقم02/16 المؤرخ في 14 رمضان 1437 هـ الموافق لـ 19 يونيو 2016 م المتمم لقانون العقوبات الجزائري على تجريم الإرهاب الالكتروني وذلك بموجب المادة 87 مكرر 11 في الفقرة 11 منها والتي تنص:"... يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة"[2].

ونلاحظ أن المشرع الجزائري يحاول بهذه المادة مسايرة التطور التكنولوجي الرهيب الذي شهدنه البشرية في السنوات الأخيرة، فبعد الحادي عشر من سبتمبر 2001 دخل النظام الدولي منعطفا جديدا الأمر الذي جعل من الجريمة الإرهابية ترتكب بوسيلة أسهل لكنها الأكثر تطورا، الأمر الذي دفع بالمشرع الجزائري كغيره من معظم مشرعي العالم إلى تعديل تشريعاتهم لتساير هذا التطور الرهيب والذي انجرت عنه جرائم جد خطيرة.

وبالرجوع إلى نص المادة 87 مكرر 11 عددت أفعال معينة واعتبرتها أعمال إرهابية- سبق وان تعرضنا لها بالشرح- وفي آخر فقرة في هذه المادة نصت على أن سائر الأفعال التي عددتها المادة إذا ما ارتكبت باستخدام الانترنت تعتبر جرائم إرهابية، فالمادة 87 مكرر11 في فقرتها الحادية عشر حددت الوسيلة وهي استعمال تكنولوجيات الإعلام والاتصال وعلى ذلك تبقى نفس الأهداف ونفس الجهة المستهدفة من الهجمات الإرهابية .

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت- لبنان، 2012، ص 127.

[2] الجريدة الرسمية الصادرة في 19 يونيو 2016، عدد 37، ص 4.

أما نص المادة 87 مكرر 12 فقد نصت على أنه:" يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر(10) سنوات، وبغرامة من 100.000 دج إلى 500.000 دج كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة"[1].

من خلال نص هذه المادة فانه يعاقب على تجنيد الإرهابيين باستخدام شبكة الانترنت مهما كانت هذه الجهة سواء كانت جمعية أو تنظيم أو جماعة أو تنظيم المهم أن يكون النشاط الذي تمارسه هذه الجهة نشاط إرهابي.

## ثانيا: خصائص الإرهاب الالكتروني

لأن جريمة الإرهاب الالكتروني جريمة ليست ككل الجرائم، فهي تختلف عن كل الجرائم سواء كانت جرائم عادية، أو حتى الكترونية، فهي تختلف حتى عن الإرهاب التقليدي على الرغم من أنها تعتبر نوع حديث من أنواع الإرهاب .

ومن أجل ذلك فالإرهاب الالكتروني يتميز بالعديد من الخصائص يمكن إيجازها كمايلي:

- **الإرهاب الالكتروني جريمة أداتها الحاسب الآلي:** فالإرهاب الالكتروني لا يحتاج في ارتكابه إلى عنف أو قوة أو عمليات عسكرية باهظة التكاليف، فيكفي لتتم هذه الجريمة أن يتوافر حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة لذلك[2].

- **الإرهاب الالكتروني جريمة عابرة للحدود:** فالإرهاب الالكتروني عبارة عن هجمات استباقية يحدد فيها المجرم هدفه من أي نقطة في العالم متجاوزا بذلك الزمان والمكان مما يضفي عليه إطارا عالميا، وبالتالي لا يعيق هذه الجريمة نطاق إقليمي محدود بل هي جريمة عابرة للدول والقارات[3].

[1] الأمر رقم 156/66 السالف الذكر.

[2] علي عدنان الفيل، الإجرام الالكتروني- دراسة مقارنة، الطبعة الأولى، مكتبة زين الحقوقية والأدبية، لبنان، 2011 ص 74.

[3] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 111.

– **الإرهاب الالكتروني جريمة صعبة الإثبات:** وهذا نظرا إلى سرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره

– **الإرهاب الالكتروني جريمة صعبة الاكتشاف:** نظرا لتطور الوسائل المستخدمة في هذه الجريمة فمن الصعوبة بما كان اكتشافها هذا من ناحية، وأيضا نقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم[1].

– **المجرم مرتكب جريمة الإرهاب الالكتروني مجرم ذو طبيعة خاصة:** حيث يكون هذا المجرم عادة من ذوي الاختصاص في مجال تقنية المعلومات، وكأقل تقدير هو شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية[2]، ومن الفقهاء من عبر عنه بأنه مجرم خارق الذكاء.

– **الإرهاب الالكتروني جريمة جماعية في الغالب:** حيث انه في اغلب الأحيان إذا لم نقل كلها تتم جريمة الإرهاب الالكتروني بتعاون أكثر من شخص[3] .

## المطلب الثاني: أساليب الإرهاب الالكتروني والجرائم المرتبطة به .

جريمة الإرهاب الالكتروني كغيرها من الجرائم لابد لقيامها واكتمالها ولتحقيق الأهداف الدنيئة المرجوة من ورائها إتباع أساليب معينة، هذه الأساليب قد تختلف بينها وبين جرائم أخرى ، كما قد تتفق مع غيرها من الجرائم في ذلك، ومن أجل ذلك وللتعرف على الأساليب المتبعة لجريمة الإرهاب الالكتروني خصصنا لها فرع أول من هذه الدراسة.

ونظرا لوجود جرائم مرتبطة بالإرهاب الالكتروني لدرجة التداخل وهذا لتشابه الأسلوب المتبع أو لتشابه الأهداف التي ترمي إليها هذه الجرائم مع جريمة الإرهاب الالكتروني توجب علينا أن نتعرض لأهم هذه الجرائم محاولين من خلال ذلك أن نوضح سبب هذا الترابط الذي جعل بعض الكتاب يعتبر

[1] ماهر عودة الشمايلة، وآخرون، الإعلام والإرهاب الالكتروني، الطبعة الأولى، دار الإعصار العلمي، عمان– الأردن 2015، ص 152 .

[2] علي عدنان الفيل، مرجع سابق، ص 75.

[3] ماهر عودة الشمايلة، وآخرون، مرجع سابق، ص 152.

هذه الجرائم من قبيل صور للإرهاب الالكتروني ولتحقيق هذا الغرض –من الدراسة– خصصنا لها فرع ثاني.

## الفرع الأول: أساليب الإرهاب الالكتروني.

يقصد بأساليب الإرهاب الالكتروني الطرق المتبعة أو الوسائل المستخدمة لارتكاب هذه الجريمة فجريمة الإرهاب الالكتروني كغيرها من الجرائم تستلزم وسائل معينة لإتمامها، ووسائل الإرهاب الالكتروني هي ما يميزها عن غيرها من الجرائم وخاصة عن الإرهاب التقليدي.

فللإرهاب الالكتروني والإرهاب التقليدي نفس الغاية إلا أنهما يختلفان في الوسيلة المستعملة ووسائل الإرهاب الالكتروني تتمثل في:

### أولا: البريد الالكتروني[1].

نظرا للتطور العلمي والتكنولوجي الذي عرفه العالم في الوقت الحاضر أصبح البريد لالكتروني أهم خدمة تقدمها لنا شبكة الانترنت، فهو خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين بطريقة سريعة، كما يسهل الاطلاع عليها في أي مكان وزمان.

والبريد الالكتروني هو عبارة عن رسالة عادية بكتبها شخص على جهازه الحاسوب بطريقة الكترونية، وهي رسالة لها رقم سري واسم مستخدم خاص ولا يمكن لأي شخص آخر الدخول إليها أو الاطلاع عليها[2].

وميزة البريد الالكتروني أو ما يعرف ب "E-MAIL" انه يمكن أن يرسل لأي شخص في لحظات معدودة ومنتهى الأمان والسرية حتى ولو كان هذا الشخص موجود في دولة أخرى، إذ لا

[1] اخترع البريد الالكتروني من طرف "راي توم لينسون" حيث كان يبحث عن طريقة للتفرقة بين اسم الشخص الذي يريد أن يرسل الرسالة الالكترونية وبين اسم جهازه الحاسوب واخذ يبحث عن رمز مناسب من الرموز المتوافرة على لوح المفاتيح فلفت نظره الرمز @ والذي عرف باللفظ(AT)، وقد أعلن بذلك عن مولد معيار هام من معايير عصر الانترنت، وبذلك تحول هذا الرمز إلى رمز عالمي يشير إلى الانترنت.لمزيد من التفاصيل راجع: مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، القاهرة، 2005 ، ص 169.

[2] عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة– دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي الإسكندرية، 2008، ص 20.

يمكن اختراق هذه الرسالة إلا بمعرفة الكلمة السرية الخاصة بالمستخدم أو بطرق فنية معقدة لا يتقنها إلا الأشخاص المحترفين في الاختراق لشبكات الحاسب الآلي كما يتميز البريد الالكتروني أيضا أنه أقل تكلفة فتكلفته رخيصة مقارنة بالمراسلات الأخرى[1].

ومن أجل ذلك ونظرا للمميزات البريد الالكتروني يعتبر من أهم أساليب الإرهاب الالكتروني فيستخدمه الإرهابيون في تبادل المعلومات بينهم وتناقلها لتسهيل القيام بالعمليات الإرهابية، كما يستغل الإرهابيون أيضا البريد الالكتروني في نشر أفكارهم والترويج لها والسعي لجمع أكبر عدد ممكن من الأتباع والمتعاطفين معهم عبر هذه المراسلات الالكترونية[2].

هذا يقوم الإرهابيون أيضا باختراق البريد الالكتروني للآخرين كالحكومات مثلا للاطلاع على معلوماتهم وهتك أسرارهم والبيانات الخاصة بهم والتجسس عليها لمعرفة مضامين مراسلاتهم للاستفادة منها في العمليات الإرهابية التي يقومون بها[3].

### ثانيا: إنشاء مواقع إرهابية على شبكة الانترنت.

حتى تستطيع الجماعات الإرهابية نشر أفكارها المتطرفة، ونشر مبادئها المنحرفة ولتحقيق أهدافها المغرضة تقوم هذه الجماعات بإنشاء وتصميم مواقع لهم على شبكة الانترنت، فمن خلال هذه المواقع الالكترونية تتمكن هذه الجماعات المتطرفة من التلقين الالكتروني وإعطاء التعليمات الخاصة بها من أجل التعبئة الفكرية وتجنيد اكبر عدد ممكن من الإرهابيين الجدد[4] .

والموقع الالكتروني هو عبارة عن معلومات مخزنة في الحاسب الآلي في شكل صفحات، حيث تشتمل كل صفحة على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 20.

[2] عبد الرحمان بن عبد الله السند، مرجع سابق، ص 7.

[3] ماهر عودة الشمايلة، وآخرون، مرجع سابق، ص 153 .

[4] علي عدنان الفيل، جريمة الإرهاب الالكتروني، مجلة الملحق القضائي، العدد 44، المعهد العالي للقضاء، المملكة المغربية، 2011، ص 212.

Hyper text markup langage (HTML) ، وبذلك تقوم شبكة المعلومات باستعراض هذه البيانات لأجل رؤية هذه الصفحات عن طريق حل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة[1].

وعلى ذلك يمكن القول أن المواقع الالكترونية التي تنشئها المنظمات الإرهابية تعتبر بمثابة مقرات افتراضية لها لتأكيد حضورها خاصة بعدما تم التضييق عليها واقعيا بعد إحداث الحادي عشر من سبتمبر، ونشير إلى أن الدراسات الحديثة تذهب إلى أن معظم التنظيمات الإرهابية لها العديد من المواقع الالكترونية فقط دون وجود مقرات لها في العالم الواقعي، فتنفذ أعمالها عن طريق شبكة الانترنت دون الاتصال المادي بين أفرادها[2].

وتجدر الإشارة إلى أن هذه المواقع تحافظ على بقائها وتواجدها في العالم الافتراضي مستغلة ضعف الرقابة على شبكة الانترنت وخصوصا في مواقع الاستضافة المجانية التي تقوم بتوفير مساحات محدودة للمواقع الشخصية، حيث تعتمد هذه الشركات على استخدام المواقع الشخصية المجانية لجلب الزوار للموقع والحصول على الدخل من خلال الإعلانات، وبما أن هذه الشركات هي من تقدم هذه الخدمات مجانية فليس لها مراقبة هذه المواقع [3].

ولما وجدت الجماعات الإرهابية هذه السهولة في إنشاء الموقع الالكترونية الخاصة بها فسرعان ما تغير هذه المواقع بطريقة مراوغة فإذا ظهرت جماعة إرهابية في موقع ما سرعان ما يختفي هذا الموقع لتظهر في موقع جديد وبنمط آخر وتصميم مغاير تماما ومن أجل ذلك نجد للمنظمة الإرهابية الواحدة ألاف المواقع وهذا من أجل ضمان انتشار أوسع، فإذا ما تم تدمير بعض هذه المواقع أو حجبها ومنع الدخول إليها بقيت بقية المواقع الأخرى ويمكن الوصول إليها[4].

---

[1] أيسر محمد عطية القيسي، الآليات الحديثة للحد من الجرائم المستحدثة- الإرهاب الالكتروني وطرق مواجهته، ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان- الأردن، في الفترة من 2-2014/09/4 ، ص 16.

[2] علي بن عبد الله عسيري، الإرهاب والقرصنة البحرية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006، ص 224.

[3] نفس المرجع، ص 225.

[4] علي عدنان الفيل (الإجرام الالكتروني)، مرجع سابق، ص 85.

### ثالثا: تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية.

تهدف الجماعات الإرهابية من وراء شنها هجمات الكترونية إلى تدمير المواقع والبيانات والنظم المعلوماتية ويقصد بهذا التدمير الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بالانترنت من خلال نظام آلي (Server- PC) أو مجموعة نظم مترابطة شبكيا بهدف تخريب نقطة الاتصال أو النظام[1] .

فالجماعات الإرهابية تهدف من وراء هذا الدخول غير المشروع أو ما يسمى باختراق المواقع إلى إلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، فالهجمات الإرهابية في عصر المعلومات تهدف إلى تحقيق ثلاثة أهداف أساسية يمكن حصرها في أهداف عسكرية، سياسية واقتصادية، فمن خلال هذه الأهداف الإستراتيجية تحاول هذه الجماعات إخضاع إرادة الشعوب والمجتمعات الدولية[2] .

وعملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت، ولا يشترط أن يكون المخترق متواجد في نفس مكان الاختراق ففي كثير من الأحيان يكون الشخص المخترق في دولة أخرى غير الدولة التي تم فيها الاختراق، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الالكترونية[3] .

ويستخدم المخترق في عملية اختراقه أو في هجومه على المواقع طرق أهمها الفيروسات ومن أمثلتها ما يعرف بالقنبلة المنطقية وهي برنامج يدمر البيانات، كما قد يستخدم حصان طروادة وهو برنامج لاقتحام امن النظام بشكل برئ حتى يدخل إلى النظام فيفسده ويدمره تماما، وهو ما سوف نتعرض إليه بشيء من التفصيل.

ويمكن حصر أفعال الاختراق فيما يلي:

- **الاقتحام أو التسلل:** فحتى تتم عملية الاختراق لابد من برامج مصممة خصيصا لإتمام هذه العملية، وفي الحقيقة لقد تم تصميم الكثير من هذه البرامج إلا أن معظمها اشتملت على نقطة ضعف

[1] ماهر عودة الشمايلة، وآخرون، مرجع سابق، ص 155.
[2] علي عدنان الفيل (الإجرام الالكتروني)، مرجع سابق، ص 86.
[3] ماهر عودة الشمايلة، وآخرون، مرجع سابق، ص 156.

أساسية قللت كثيرا من إمكانياتها وجعلت من صاحب الموقع المحترق يشعر بهذا البرنامج فيتابعه ويستطيع القضاء عليه تماما، ماعدا برنامج حصان طروادة حيث استطاع مصممو معالجة هذا العيب ومن أجل ذلك اعتبر هذا البرنامج من اخطر برامج الاختراق والتسلل على الإطلاق، حيث يقوم مستخدم هذا البرنامج بالتسلل والاختراق دون أن يشعر به صاحب الموقع المخترق، فحصان طروادة يتيح لمستخدمه أن يحصل على كلمة السر الخاصة بالجهاز المعني وذلك بطريقة لا تثير الريبة أو الشك، كما لا يمكن للبرامج المتخصصة في كشق الفيروسات أن تكتشفه، ومثال ذلك ما قام به قراصنة أجانب باقتحام صفحة انترنت إعلامية خاصة ببنك فلسطين المحدود، ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى إلغاء الصفحة نهائيا ومحوها كليا (أي تم تدميرها)[1] .

– **الإغراق بالرسائل:** يلجا بعض المخترقين أو الإرهابيين الذين يهدفون إلى تدمير المواقع باختراقها إلى إغراق البريد الالكتروني بمئات الرسائل، وذلك من أجل الإضرار بصاحب البريد وذلك بشغل كل مساحته بهذه الرسائل لعدم إمكانيته من استقبال رسائل أخرى[2] فضلا على إمكانية انقطاع الخدمات عنه تماما وبالتالي يكون هدفهم الأول والأخير إلحاق الضرر بهذا الجهاز مثبتين بذلك تفوقهم في هذا المجال، فتلك الرسائل قد تكون محملة بملفات كبيرة الحجم لمجرد الإضرار بمستخدم جهاز الحاسب الآلي نظرا لصغر المساحة المخصصة للبريد الالكتروني، وهذه الرسائل تصل إلى الجهاز مرة واحدة وفي وقت واحد، فتؤدي إلى توقف الجهاز عن العمل على الفور نظرا لما تسببه من ملء منافذ الاتصال أو ملء المساحة المتاحة لهذا الجهاز أو المستخدم وكذلك ملء قوائم الانتظار وبمجرد توقف ذلك الجهاز عن العمل وبالتالي تنقطع الخدمة التي يؤديها هذا الجهاز وهو ما يعتبر صورة أخرى من صور التدمير عن طريق الاختراق[3] .

– **الفيروسات والديدان:** والفيروسات والديدان الالكترونية هي برامج مصممة لأحداث تدمير أو تعطيل برمجيات أجهزة الحاسوب وذلك طبعا دون علم أصحابها، وهناك أنواع كثيرة، منها ما هو صعب التحديد ومنها ما هو عكس ذلك، ومنها ما هو سريع الانتشار ومؤذي للغاية ومنها ما هو بطيء وأقل

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 82.

[2] سامي علي حامد عياد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية، (دون سنة نشر)، ص 71.

[3] أمير فرج يوسف، (الجرائم المعلوماتية على شبكة الانترنت)، مرجع سابق، ص 84.

ضررا وإيذاء، بل ويحتاج إلى أسابيع أو حتى شهور للانتشار، ومنها ما هو غير مؤذي إنما هدفها الإرباك وإحداث الفزع فقط[1].

وتختلف الديدان عن الفيروسات في أنها تعتبر برامج قائمة بذاتها لا تعتمد على برامج أخرى في أداء عملها، وهي سريعة الانتشار ويصعب التخلص منها نظرا لقدراتها الفائقة للتلون والتناسخ والمراوغة، وتصيب الدودة الجهاز المتصل بشبكة الانترنت تلقائيا ودن تدخل من المستخدم، الأمر الذي يجعلها أسرع انتشارا ، ولا تقوم الدودة بحذف أو تغيير الملفات بل تقوم باستهلاك موارد الجهاز واستخدام الذاكرة بشكل كبير، وعلى ذلك فان خطورة الديدان تكمن في استقلاليتها وعدم اعتمادها على برامج أخرى[2].

ولطالما شكلت الفيروسات والديدان خطرا كبيرا على مختلف الحواسيب المتواجدة في مختلف دول العالم، بل وإنها ألحقت بالكثير منها خسائر مادية ضخمة، هذا وقد أوضحت الدراسات أن بعض أنواع الفيروسات يستخدم هجمات Brute Force Attack، لاستخراج كلمات المرور من أجهزة الكمبيوتر والشبكات الداخلية للمنشآت المتعرضة لهجوم الفيروس، ومن أجل ذلك أكد الباحثون على مستخدمي أجهزة الكمبيوتر ومدراء الشبكات من استخدام كلمات مرور معقدة وصعبة الاختراق وتفادي كلمات المرور الضعيفة كتواريخ الميلاد مثلا، ومن أشهر الفيروسات والديدان الالكترونية بل وأخطرها:

* **فيروس Brain:** يعتبر أول فيروس حقيقي وقد أنشئ سنة 1986 من طرف أخوين من باكستان، وكان سبب إنشاء هذا الفيروس أن الأخوين تضايقا من سرقة البرامج التي صمموها، فكانت فكرة الأخوين تصميم برنامج يشبه "مضاد النسخ المسروقة"، وهذا كحماية للملكية الفكرية للبرامج التي قاما بكتابتها، وما حول هذا البرنامج إلى فيروس هو وجود عيب في البرمجة بسببه استطاع البرنامج من استنساخ نفسه، وقد عمل هذا الفيروس على تغيير قطاع الإقلاع(Boot Sector) للقرص المرن فإذا تم وضع القرص المرن في جهاز الكمبيوتر يقوم الفيروس بنسخ نفسه في ذاكرة الجهاز، ومن هنا يصيب كل قرص يوضع في الجهاز المصاب، كما قام الأخوان بوضع اسميهما وأرقام هواتفهما

[1] محمد بن عبد الله آل فايع العسيري، حسين بن أحمد الشهري، استعمال الانترنت في تمويل الإرهاب وتجنيد الإرهابيين– الإرهاب الالكتروني وبعض وسائله والطرق الحديثة لمكافحته، مركز البحوث والدراسات– جامعة نايف للعلوم الأمنية، الرياض، 2012، ص225.

[2] أمير فرج يوسف، (الجرائم المعلوماتية على شبكة الانترنت)، مرجع سابق، ص 91.

وعنونيهما في الفيروس، وهذا ليتمكن الأشخاص المالكين للأجهزة المصابة بهذا الفيروس من التواصل معهم لتصليح أجهزتهم، والأمر الذي لم يتوقعه الأخوان هو كثرة المتصلين بهم من مختلف دول العالم مما أدى إلى إصابتهم بالذهول مما اضطرهم إلى قطع خط الهاتف وهذا دليل على أن الفيروس أصاب الكثير من الأجهزة وفي وقت قصير جدا[1].

* **دودة شجرة الكريسماس:** ويعتبر هذا الفيروس أول دودة حاسوبية تخريبية واسعة النطاق، وكان ذلك في سنة 1987 حيث شلت العديد من شبكات الكمبيوتر الدولية في ديسمبر من نفس السنة وصمم هذا الفيروس من قبل طالب جامعي بلغة REXX والشيء الطريف في هذا الفيروس أن مصممه رسم شجرة الكريسماس بواسطة النصوص ثم كتب رسالة تهنئة بالعيد، وتعمل شجرة الكريسماس على إرسال نفسها عبر العناوين البريدية، وكانت اكبر الشركات المتضررة من هذا الفيروس هي شركة IBM التي اضطرت إلى إغلاق احد شبكاتها بسبب الأضرار التي سببها لها هذا الفيروس[2].

* **دودة موريس:** وتعتبر أول فيروس صمم ضد الحاسوب، وقد صمم من طرف "روبرت موريس" سنة 1988 وكان بدافع الفضول، وكان مهمة هذا الفيروس هو معرفة حجم الانترنت وذلك بمعرفة عدد الأجهزة المتصلة بها، وحقيقة أصابت دودة موريس 6000 جهز من أصل 60.000 جهاز كان وقتها متصلا بشبكة الانترنت وعندها قام موريس بتعديل الرمز وجعل الدودة تنسخ نفسها بالقوة على الحاسب الآلي، وفي ساعات معدودة وبسبب التعديل الذي أجراه موريس على الرمز تمكنت دودته من نسخ نفسها على الآلاف من الأجهزة ، وعندما خرج هذا الفيروس عن سيطرة موريس ابلغ بذلك السلطات فتحرك المختصون بالبرمجة لإصلاح هذه الخسائر الفظيعة التي قاربت 100 مليون دولار واستمرت الإصلاحات عددا من الأيام، وبذلك يعتبر موريس أول شخص يحاكم بموجب قانون الاحتيال الالكتروني الأمريكي[3].

---

[1] محمد فارس، أخطر عشرة فيروسات في التاريخ، مقالة منشورة يوم 2011/08/18 في الموقع: http//itwadi.com/node/1928، تاريخ الاطلاع 2017/09/23 على الساعة 22:35.

[2] ما هي أشهر فيروسات الحواسيب التي هددت العوالم الرقمية؟، مقالة منشورة في الموقع:www.alwasatnews.com/news/1126869 تاريخ الاطلاع في 2017/09/24، وعلى الساعة 16:42.

[3] محمد فارس، مرجع سابق، ص 1.

* **فيروس مايكل أنجلو** : اكتشف هذا الفيروس أول مرة في أفريل 1991 في نيوزلندا وهو فيروس يصيب نظام Ms Dos لكنه يبقى ساكنا في الجهاز غير محدث لأية أضرار حتى مجيء يوم 6 مارس – ذكرى الفنان مايكل أنجلو– حيث يحدث اكبر عدد من التدمير، ويعتبر فيروس "مايكل أنجلو" من فيروسات قطاع التشغيل Boot Sector، حيث يقوم هذا النوع بزراعة نفسه في منطقة التشغيل بالقرص الصلب، وهو المكان الذي يتجه إليه الكمبيوتر عند بداية تشغيل الجهاز، مما يمنع مستخدم الجهاز من الوصول إلى النظام ويمنعه من الإقلاع، وكان الحل لتفادي هذا الفيروس هو ضبط وقت الجاز في وقت مخالف ل 6 مارس، وبحلول سنة 1997 انتهى الحديث تماما عن هذا الفيروس[1].

* **فيروس تشرنوبيل** : يعبر من أكثر الفيروسات تدميرا، حيث يصيب هذا الفيروس الحواسيب التي تعمل بنظام الويندوز، وقد جاء اسمه نسبة إلى حادثة "تشرنوبيل" التي حدثت في أوكرانيا سنة 1986 بسبب انفجار في احد المفاعلات النووية، ويقوم هذا الفيروس بمسح الماستر بوت ريكورد للقرص الصلب فيصبح جهاز الكمبيوتر غير قادر على الإقلاع، محاولا في ذات الوقت مسح البيوس حيث يكون هذا الخير محمي من الكتابة في الغالب، فان حدث وتمكن من المسح فعلا فان ذلك يفرض إعادة تنصيب البيوس، وهو الأمر الصعب على المبتدئين، ومن أجل ذلك قام كل من أصيب جهازه بهذا الفيروس من تغييره واقتناء جهاز أخر[2] .

* **فيروس Melissa**:هذا الفيروس هو أول فيروس ينتقل عبر البريد الالكتروني، حيث يقوم هذا الفيروس بتحديد عناوين البريد الالكتروني ثم يقوم بإرسال نفسه إلى الأصدقاء المتواجدين في هذه العناوين، وهذه الطريقة الذكية تسمح لهذا الفيروس بالانتقال والانتشار بشكل كبير، وسر انتشاره أن هذا الفيروس يصل إلى البريد الالكتروني المراد مهاجمته من مصدر موثوق، فلا يمكن للضحية أن يشك في أن الفيروس مرسل من طرف صديقه، وانطلاقا من هذه النقطة فان فتح الرسالة سوف يكون مؤكد، وبعد الإصابة بالفيروس وتكرر العملية فسينتشر الفيروس بطريقة كبيرة وسريعة

[1] محمد فارس، مرجع سابق، ص 1.

[2] ما هي أشهر فيروسات الحواسيب التي هددت العوالم الرقمية؟، مقالة منشورة في الموقع:www.alwasatnews.com/news/1126869 تاريخ الاطلاع 2017/09/24، وعلى الساعة 16:42

فهذا الفيروس يخترق نظام الورد في الجهاز المصاب ويعدل فيه ويستخدم ملفات ورد المصابة لإرسال نفسه عبر قوائم البريد الموجودة في الاوتولوك ولأكثر من 50 شخص[1].

* **فيروس I love you:** هذا الفيروس عبارة عن دودة حاسوبية مدمرة سريعة الانتشار ضربت أجهزة الحاسوب سنة 2000 مستغلة ثغرة في نظام الويندوز، وضعف نظام البريد الالكتروني، وقد عرف هذا الفيروس بخداعه للمستخدمين عند فتح ملف ما، ويأتي هذا الفيروس على شكل رسالة غرامية وترسل إعداد هائلة منها بعنوان "I love you" وقد وصل عدد الأجهزة التي تأثرت بهذا الفيروس 10 % من مجموع الأجهزة، مما سبب خسائر ضخمة وهو ما جعله الفيروس الأسوء على الإطلاق، مما دفع بالرئيس الأمريكي في تلك الفترة أن يخرج بنفسه للشعب الأمريكي من أجل أن يطمئنه على سلامة أجهزة البنتاغون ( الجهاز الرئيسي لدى الحكومة الأمريكي)[2].

* **دودة كونفيكر:** ونشا هذا الفيروس في الصين سنة 2008، وبعدها انتشر إلى ما يقارب 83 دولة عبر مختلف العالم، وأبرزها الولايات المتحدة الأمريكية، البرازيل المكسيك، وتايوان، وهذا الفيروس يصيب أجهزة الكمبيوتر التي تعمل على أحد أنظمة " مايكروسوفت ويندوز" إذ يقوم بنشر نفسه من خلال الشبكات المتصلة مستغلا نقاط الضعف الموجودة في خوادم ويندوز، وذلك بدمج بعض الشفرات التنفيذية إلى بعض المكتبات الديناميكية المتصلة لهذه الخدميات ( Dynamical Linked Libraries- DLL) ولهذا الفيروس خمس إصدارات تختلف في كيفية الإصابة بها وتأثيرها على النظام، وقد ظهر الإصدار الأول في نوفمبر 2008 والمسمى "Conficker.A"، أما آخر إصدار فكان في شهر أفريل عام 2009 والمسمى " Conficker.E" وقد اشتهر هذا الفيروس بصعوبة اكتشافه من قبل خبراء الأمن ومشغلي الشبكات، وذلك لاستخدامه مركبات مختلفة من التقنيات المتقدمة في صناعة البرامج الخبيثة[3].

ومن أشهر الهجمات التي شنها هذا الفيروس كان في عام 2009 حيث صرحت البحرية الفرنسية بان جزء من شبكة الحواسيب التي تمتلكها قد تعطلت بشكل تدريجي وذلك بسبب إصابتها بفيروس"

[1] محمد فارس، مرجع سابق، ص 1.

[2] نفس المرجع.

[3] عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الالكترونية، الطبعة الأولى، الدار العالمية للنشر والتوزيع، مصر 2014، ص 205 ،207 .

كونفيكر"، الأمر الذي أدى إلى شلل في حركة النقل كليا لعدم تمكنهم من تحميل مخطط السير كذلك الأمر في مجلس العموم البريطاني الذي لم يسلم من خطر هذا الفيروس، حيث أشارت مذكرة تخص احد مدراء البرلمان بعد تسريبها بأنه في 24 من شهر مارس أصيب عدد من أجهزة الكمبيوتر في مجلس العموم البريطاني بهذا الفيروس، كما جاء في المذكرة بان المجلس حذر المستخدمين من إيصال أي أجهزة غير مصرح لها بالشبكة[1].

* **حصان طروادة:** أطلق على هذا الفيروس اسم حصان طروادة نسبة إلى الحصان الذي استخدمه الإغريق لغزو حصن "طروادة"، وسمي بهذا الاسم تحديدا لان هذا الفيروس يختبئ داخل البرامج الموجودة في الذاكرة ثم ينشط في الوقت المحدد له، وينفذ الأمر المعطى إليه سواء بالإتلاف الجزئي أو الكلي للبيانات أو تشويهها[2].

ونشير إلى انه يمكن زرع فيروس حصان طروادة بعدة طرق[3] وهي:

– يرسل عن طريق البريد الالكتروني كملف ملحق فيقوم المستخدم باستقباله وتشغيلها وفي أغلب الأحيان يرسل هذا الفيروس ضمن العديد من البرامج والملفات ولا يرسل وحيدا.

– كما قد يرسل فيروس حصان طروادة عند استخدام برنامج المحادثات الشهيرة والذي أنتجته إسرائيل وهو برنامج ICQ.

– كما يمكن أن ينتقل عند تحميل برامج من مواقع غير موثوق بها.

– والطريقة الأكثر شيوعا هي عند اتصال الجهاز بشبكة الانترنت.

– كما يمكن أن ينقل فيروس طروادة بواسطة برنامج TELNET أو FTP.

– أما الطريقة الأخرى التي يمكن أن ينتقل بواسطتها فيروس طروادة فهي نقله من خلال بعض البرامج الموجودة على الحاسب الآلي مثل الماكرو الموجودة في برامج معالجة النصوص[4].

[1] عبد الحليم موسى يعقوب، مرجع سابق، ص 207.

[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص 96.

[3] أمير فرج يوسف، (الجرائم المعلوماتية على شبكة الانترنت)، مرجع سابق، ص 83.

[4] عبد الفتاح بيومي حجازي، مرجع سابق، ص 96.

* **فيروس Stuxnet** : تم إنشاء هذا الفيروس في سنة 2010 ، ويعتبر من أكثر الفيروسات خطورة وإحداثا للضرر، فهذا الفيروس لم يصمم بمهاجمة أجهزة المستخدمين العاديين، بل تعدت إلى القيام بإعمال التجسس على الأنظمة الصناعية التي تعمل على نظام ويندوز وإعادة برمجتها، وخاصة نظام SCADA الذي يستخدم في تنظيم حركة السير، وخطوط الأنابيب وإدارة المفاعلات النووية، وعمليا ضرب هذا الفيروس عدة منشات صناعية هامة منها مفاعل نووي إيراني، وكذلك حولي 15 مؤسسة صناعية أخرى، وتجدر الإشارة أن إيران تحملت بسبب هذا الفيروس خسائر قدرت ب 60 % من إجمالي الخائر التي سببها هذا الفيروس، مما يعكس أن أهداف فيروس Stuxnet تعتبر أهداف سياسية تقف وراءها قوى دول معينة[1] .

وعلى ذلك فان جميع الفيروسات التي ذكرناها على سبيل المثال والتي تعذر علينا ذكرها تعتبر بمثابة قنابل موقوتة يفجرها مستخدمها في الوقت الذي يحدده والمناسب لتنفيذ جرائمه، وبدرجة الضراوة التي يبتغيها، فخطر هذه الفيروسات انتقل من الأجهزة الشخصية إلى المؤسسات العسكرية وهذا من أجل أن يتذكر مستخدمي الكمبيوتر بعدم الاعتماد بصورة مطلقة على تقدم التقنية.

هذا وتجدر الإشارة أنه نظرا لخطورة هذا الأسلوب الذي يستخدمه الإرهاب الالكتروني(اختراق المواقع وتدميرها) اقترح وزير العدل الأمريكي بعد أحداث الحادي عشر من شهر سبتمبر 2001 مشروع قانون يعتبر أن المتسللين إلى البرامج الكمبيوترية (الهاكرز) إرهابيين، كما أضاف هذا المشروع مخالفات التسلل إلى برامج الكمبيوتر إلى قائمة الجرائم الإرهابية، وقد تصل عقوبة هذه الجريمة إلى السجن مدى الحياة بالإضافة إلى ذلك اقترح هذا المشروع أيضا توسيع صلاحيات الاحتجاز والمصادرة قبل الإدانة بالإضافة إلى اشتراك كل من يساعد المتسللين أو يأويهم حتى وان كانت الأضرار الناتجة عن هذا التسلل ضمن الحد الأدنى، إلا أن الجمعيات التي تدافع على الحقوق المدنية ترى أن هذا المشروع قد اقترح باستعجال ودون بحث على تأثيراته على الحريات الشخصية التي قد ينتهكها[2].

[1] محمد فارس، مرجع سابق، ص 2.

[2] أمير فرج يوسف، (الجرائم المعلوماتية على شبكة الانترنت)، مرجع سابق، ص 88.

وفي الأخير وبعد أن تعرفنا إلى كيفية تدمير المواقع كان لزاما علينا ان نجيب على سؤال مهم هل الإرهاب الالكتروني يهدف إلى تدمير أي موقع أم أن هناك مواقع مستهدفة دون سواها؟

وهنا وللإجابة على هذا السؤال قام خبراء الجرائم الالكترونية والأمن المعلوماتي بمحاولة لحصر المواقع المستهدفة من الإرهاب الالكتروني، ويمكن حصر هذه المواقع المستهدفة في خمسة أهداف مهمة:

1. **استهداف النظم العسكرية:** كثيرا ما تستهدف الجماعات الالكترونية للإرهاب الالكتروني الأهداف العسكرية غير المدنية المرتبطة بشبكة الانترنت، وتعتبر هذه الهجمات من اخطر الهجمات التي يمكن أن يقوم بها الإرهاب والتي قد تسبب أضرار جسيمة في مجتمعنا المعاصر، فتتم هذه الهجمات عن طريق اختراق النظم الخاصة بالأسلحة الإستراتيجية، ونظم الدفاع الجوي، والصواريخ النووية، فنظرا للذكاء الخارق الذي يتمتع به الإرهابي الالكتروني تتسنى له فرصة فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة[1].
2. **استهداف محطات توليد الطاقة والماء:** لما ازداد اعتماد الإنسان المعاصر على الطاقة الكهربائية فان شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات هذه الطاقة تعد من الأهداف الأولى والمهمة والتي قد يستهدفها الإرهاب الالكتروني،فالانترنت أصبحت من الوسائل المهمة لإدارة نظم الطاقة الكهربائية في كل دول العالم، وخاصة في الدول المتقدمة وعلى ذلك فان الهجمات الالكترونية التي يشنها الإرهاب على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية عدد من مرافق الحياة في البلاد، وتسود الفوضى وتشل الحركة والأمر نفسه بالنسبة لشبكات مصادر المياه وطرق توزيعها[2] .
3. **استهداف البنية التحتية الاقتصادية:** عالم المال والأعمال بدوره اعتمد بشكل كلي على الشبكات المعلوماتية، نظرا لطبيعة هذه الشبكات المترابطة، وانفتاحها على العالم الأمر الذي يجعلها هدفا مغريا للمجرمين عموما والإرهابيين على وجه الخصوص، فالبنية الاقتصادية والمالية تتأثر بالانطباعات السائدة والتوقعات، الأمر الذي يجعلها هدفا مغريا للهجمات الإرهابية، وعلى ذلك فان

[1] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 146.

[2] خلدون غسان سعيد، الإرهاب والجرائم المعلوماتية– اختطاف وتسميم يومي لمواقع والملفات، منشورة في الموقع: www.aawsat.com، وتم الاطلاع بتاريخ 2012/06/24 على الساعة 23:38.

التشكيك في صحة المعلومات الاقتصادية أو تخريب هذه المعلومات حتى ولو كان بشكل بسيط يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي، وعليه فان هذا الاستهداف يكون من خلال إحداث خلل واسع في نظم الشبكات التي تتحكم بسريان أنشطة المصارف وأسواق المال العالمية ونشر الفوضى في الصفقات التجارية الدولية، فضلا عن ذلك يمكن إحداث توقف جزئي أو كلي في منظومات التجارة والأعمال، إذ تتعطل الأنشطة الاقتصادية وتتوقف عن العمل[1].

4. **استهداف نظم المواصلات:** ويتحقق هذا الاستهداف من خلال اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، كإحداث خلل في برامج هبوط الطائرات وإقلاعها مما قد ينتج عنه تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات كما يمكن للإرهابي الالكتروني أن يسيطر على نظم التحكم بتسيير القطارات، وتغيير مواعيد الانطلاق، وبالتالي تسود الفوضى أو تتصادم هذه القطارات فيما بينها، والأمر نفسه بالنسبة للسفن والناقلات البحرية والغواصات[2] .

5. **استهداف نظم الاتصالات:** ويكون ذلك عن طريق اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية، هذا وقد يقوم الإرهابيين بشن سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية، الأمر الذي ينشر حالة من الرعب والفوضى –وهو الهدف الذي تسعى الهجمات الإرهابية تحقيقه من خلال تلك الهجمات– وبالتالي لا تستطيع الدولة تقدر على متابعة تداعيات الهجمات الإرهابية المعلوماتية[3].

## رابعا: التهديد والترويع الالكتروني.

إذا كان التهديد يعني التخويف والتوعد بالعقوبة في اللغة، فان الأمر في القانون الجنائي لا يبتعد كثيرا عن هذا المعنى فالتهديد يتحقق بالضغط على إرادة المجني عليه وذلك بتخويفه وتوعده بأن خطرا

[1] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 147.

[2] نفس المرجع، ص 148.

[3] عبد الله بن عبد العزيز فهد، الإرهاب الالكتروني– بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنت القاهرة، 2008، ص 16.

أو ضررا ما سوف يلحقه أو يلحق أحد الأشخاص أو أشياء ذات صلة به ويعتقد الجاني أن المجني عليه يهمه تفادي هذا الضرر[1] .

وفي الحقيقة أن هناك العديد من التعريفات الفقهية للتهديد،فمن الفقهاء من عرفه بأنه:" فعل الشخص الذي ينذر آخر بخطر يريد إيقاعه بشخصه أو ماله"، كما غرفه البعض الآخر بأنه:" توجيه عبارة أو ما في حكمها إلى المجني عليه عمدا يكون من شأنه إحداث الخوف عنده من ارتكاب جريمة أو إفشاء سر أو نسبة أمور خادشة بالشرف إذا وجهت بالطريقة التي يعاقب عليها القانون"[2] .

وكثيرا ما يتداخل التهديد بالعنف فيكون التهديد تهديد ووعيد بعنف مستقبلي، غير أن لكل منهما كيان خاص به، فالعنف يفترض علاقة بين حركة جسدية للجاني وبين ضرر جسماني لحق المجني عليه، بينما التهديد ينتج عنه نتيجة معنوية تتمثل في الضغط على إرادة المجني عليه فلا يعدمها كلية وصحيح أنه قد ينتج عن العنف إكراه لإرادة المجني عليه لكن هذا الإكراه ليس هو النتيجة المستهدفة من العنف وبه فان عدم توافر الإكراه لا ينفي وجود العنف، فالعنف يوجه إلى جسم المجني عليه، في حين أن الإكراه يتوجه إلى إرادته[3] .

أما الترويع فيقصد به " تخويف المجني عليه وإلقاء الرعب في قلبه بتوعده بإنزال شر معين به سواء كان بشخصه أو ماله، ويتحقق الترويع في مجال القانون الجنائي بكل سلوك غير موجه للمجني عليه، ويؤدي إلى إزعاجه مما يفقده توازنه، وبذلك تفقد إرادته السيطرة على سلوكه، وقد يتحقق الترويع بصوت مفاجئ أو حركة قوية تصدر من الجاني، كمن يريد أن يأخذ شيء من المجني عليه دون رضاه، فيلجأ إلى أحد أساليب الترويع كصوت مفاجئ فيسقط ذلك الشيء من يد الضحية فيختطفه الجاني، كما قد يتحقق الترويع بمجرد رؤية شخص معين أو شيء ما في مكان معين ولكن يشترط في هذه الحالة حتى نستطيع أن نحكم على هذه الحالة أنها ترويع إذا ما قام الجاني بسلوك إيجابي أسفر

[1] محمود صالح العادلي، موسوعة القانون الجنائي للإرهاب– المواجهة الجنائية للإرهاب، الجزء الأول، دار الفكر الجامعي، الإسكندرية، 2003، ص 46.

[2] رؤوف عبيد، جرائم الاعتـــداء على الأشخـاص والأموال، الطبعة السابعـة، دار الفكر العربي، القاهـــرة، 1985 ص 422.

[3] محمود صالح العادلي، مرجع سابق، ص 47.

عنه بث حالة من الرعب في نفس المجني عليه، ويستوي في الحكم سواء كان السلوك الايجابي سابقا على ارتكاب الجريمة أو معاصر لها[1] .

ويعتبر كل من التهديد والترويع أسلوب من أساليب الإرهاب الالكتروني، إذ تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، ومن خلال شبكة الانترنت، وتتعدد أساليب التهديد وتتنوع طرقه، لنشر الخوف والرعب بين الأشخاص والدول والشعوب، ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات والجماعات والحصول على التمويل المالي، هذا فضلا على الرغبة في إبراز قوة التنظيم الإرهابي [2].

ومن الطرق التي تستخدمها الجماعات الإرهابية الالكترونية إرسال الرسائل الالكترونية المتضمنة للتهديد، وكذلك التهديد عن طريق المواقع الالكترونية وغرف الدردشة الالكترونية والمنتديات، والتهديد يكون بعدة أساليب كما يكون عبر مراحل، فتارة يكون التهديد بقتل الشخصيات السياسية البارزة في المجتمع، وتارة يكون التهديد بتفجير منشآت وطنية مهمة وحيوية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية، كما قد يكون التهديد بتدمير البنية التحتية المعلوماتية، ...الخ من أساليب وطرق التهديد والترويع الالكتروني[3].

### خامسا: التجسس الالكتروني.

بعد أن شهد العالم هذا التطور المذهل في وسائل تقنية المعلومات أصبح اعتماد جميع دول العالم على شبكة الانترنت كبيرا جدا، ونتيجة لذلك توسعت استخدامات الحاسب الآلي لدى الأفراد والوحدات الحكومية وأيضا في الوحدات الإدارية والعلمية والبحثية، وبسبب ذلك تزايدت الأخطار على البيانات الحكومية في كل الدول، ولا يكمن الخطر في مجرد ارتباط هذه الدول والمؤسسات الحكومية بشبكة الانترنت ولكن الخطر يكمن في الضعف الأمني لهذه الشبكات وخاصة في الدول العربية ونظرا لغياب التواصل العربي في مجال الاتصال الالكتروني، ولا شك أن معظم خبراء الشبكات

[1] إبراهيم نايل عيد، السياسة الجنائية لمكافحة الإرهاب الالكتروني، بحث مقدم للحلقة العلمية بعنوان" الانترنت والإرهاب" في الفترة 15-2008/11/19، عين شمس – القاهرة، ص 17.

[2] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 148.

[3] عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق .

يعرفون جميع التفاصيل عن الشبكات العالمية، فإذا لم تتوافر الحلول الأمنية لهذه الشبكات سهل اختراقها نسبيا.

وكما رأينا في العنصر السابق أن الاختراق يكون بهدف تدمير الموقع، كما قد يكون الاختراق بهدف التجسس حيث يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الالكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والأنظمة الالكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وعمليات التجسس الالكتروني التي يقوم بها الإرهابيون تستهدف ثلاث نقاط رئيسية هي:التجسس العسكري التجسس السياسي والتجسس الاقتصادي[1].

وبعد أن أصبحت حدود الدول مستباحة بأقمار التجسس والبث الفضائي وذلك بعد انتشار الوسائل التقنية الحديثة بسبب التطور التكنولوجي المذهل الذي عرفه العالم، ومن أجل ذلك تحولت الرسائل التقليدية من الطرق التقليدية إلى الطرق الالكترونية، وخاصة مع ظهور الانترنت وانتشارها عالميا، فمع توسع التجارة الالكترونية تحولت مصادر المعلومات التجارية إلى أهداف للتجسس الاقتصادي[2].

وتتم عملية التجسس الالكتروني بعدة طرق منها البريد الالكتروني،حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، أو عن طريق أحصنة طروادة –التي سبق وأن تعرضنا لشرحها– أو عن طريق إنزال بعض البرامج من المواقع غير الموثوق بها، كما يمكن للإرهابي الالكتروني أن يتجسس باستخدام فيروسات الاختراق[3].

ومن الأساليب الحديثة للتجسس الالكتروني أسلوب إدخال المعلومات داخل المعلومات، ويتم ذلك عن طريق لجوء الإرهابي إلى إخفاء المعلومات الحساسة المهمة والمستهدفة داخل المعلومات الأخرى العادية والموجودة داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة التي تبدو عادية

[1] جميل عبد الباقي الصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الانترنت عبر الانترنت بحث مقدم في الحلقة العلمية بعنوان "الانترنت والإرهاب"، في الفترة 15-2008/11/19، عين شمس– القاهرة ص17.

[2] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 150.

[3] جميل عبد الباقي الصغير، مرجع سابق، ص 17.

في مظهرها وبذلك لا يمكن لأحد أن يشك أن هناك معلومة سرية وحساسة ومتخفية يتم تهريبها حتى ولو تم ضبط الشخص متلبسا[1].

وتكمن خطورة التجسس الالكتروني في ضعف الوسيلة الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية، ولا يمن الاعتماد بشكل كبير على وسائل الحماية التي تنتجها الشركات الأجنبية لأنها غير آمنة[2].

وتجدر الإشارة إلى أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخداما في المستقبل من التنظيمات الإرهابية، نظرا لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية ولاسيما العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها للأضرار بمصلحة المجتمع والوطن[3].

## الفرع الثاني: الجرائم المرتبطة بالإرهاب الالكتروني.

يرتبط الإرهاب الالكتروني بالعديد من الجرائم التي سوف نتحدث عنها كونها تهدف إلى نفس الهدف الذي يرمي إليه الإرهاب الالكتروني أو موجهة لخدمته فتكون مرتبطة به لدرجة التداخل، لدرجة أن البعض من الباحثين في هذا المجال اعتبر كل جريمة من هذه الجرائم صورة من صور الإرهاب الالكتروني

ومن أهم هذه الجرائم التي ترتبط بالإرهاب الالكتروني:

[1] حسين بن سعيد، جرائم الإرهاب الالكتروني، بحث منشور في الموقع: www.moheet.com تاريخ الاطلاع 2012/10/05 على الساعة 19:17 .

[2] جميل عبد الباقي لصغير، مرجع سابق، ص 17.

[3] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 151 .

## أولا: جريمة تزوير المعلومات.

تعد هذه الجريمة من أكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من هذه الجريمة، فالتزوير بشكل عام"هو تغيير الحقيقة أيا كانت وسيلته وأيا كان موضوعه"، وهو يتسع للعديد من الجرائم التي نص عليها قانون العقوبات[1].

وأما التزوير في المحررات فقد اتفق كل من الفقه في فرنسا وفي مصر على تعريفه بأنه:" تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه إحداث ضرر مقترن بنية استعمال المحرر المزور فيما أعد له"[2] .

ومع الانتشار الواسع للكمبيوتر وحلوله محل الأوراق (المحررات والوثائق) وذلك في اغلب مجالات نظم المعالجة الآلية للمعطيات، وبتزايد حجم الاعتداءات الواقعة على المعطيات المخزنة داخل الحاسب الآلي والتي تمس الأفراد في حقوقهم وأموالهم وحياتهم الخاصة، تزايدت فرص الأشخاص للعبث والتلاعب في معطيات الحاسب الآلي بتبديلها وتغييرها وفقا للشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد، ومن اجل ذلك أصبح لزاما على الحكومات بسط الحماية لهذه المعلومات وضمان أمنها وذلك بسن التشريعات التي تبسط الحماية لهذه المعلومات[3].

وبالرجوع إلى قوانين العقوبات العربية نجد ان معظم التشريعات العربية جرمت تزوير المحررات فالمشرع الجزائري خص لتجريم المحررات قسمين كاملين أحدهما القسم الثالث والذي جاء بعنوان" تزوير المحررات العمومية أو الرسميـــة"، وأما القســم الرابع فجاء بعنوان "التزوير في المحررات العرفية أو التجارية أو المصرفية"، فضلا عن قسم خامس وقد خصه لتجريم تزوير في بعض الوثائق الإدارية والشهادات وكلها تحت فصل واحد وهو فصل "التزوير"[4]، وهذا إن كان يدل فانه يدل على حرص المشرع الجزائري على بسط الحماية على حقوق الأفراد وأموالهم وحياتهم الخاصة، وقد فرض

[1] عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية، 2011، ص 135.

[2] محمود نجيب حسني، شرح قانون العقوبات –القسم الخاص، دار النهضة العربية، القاهرة، 1994، ص 215.

[3] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة، عمان–الأردن، 2009، ص 107.

[4] وتجدر الإشارة إلى أن المشرع الجزائري لم يعرف التزوير في المحررات لكنه حدد حالته وصوره وبين أحكامه.

المشرع الجزائري عقوبات متفاوتة وتختلف بين القائم بالتزوير ومستعمل هذا المحرر المزور[1]، وبذلك يكون المشرع الجزائري قد نهج منهج المشرع المصري والذي بدوره فرق في العقوبة بين القائم بالتزوير ومستعمل المحرر المزور، فتتفاوت العقوبات في هذه الحالة تبعا لنوع المحرر محل التزوير وأيضا حسبما كان الشخص قائم بالتزوير أو مستعملا له[2].

وتجدر الإشارة إلى أن جرائم التزوير تتشابه مع جرائم الاحتيال من حيث أن كليهما يومان على تغيير الحقيقة، إلا أن نقاط اختلافهما متعددة وأهم نقطة في هذا الاختلاف هو أن جريمة تزوير المحررات لابد أن تقع على محرر ولا يشترط ذلك في جريمة الاحتيال، إلا أنه غالبا ما تجتمع جريمة التزوير مع جريمة الاحتيال في وقت واحد وبذلك ينتج ما يعرف بتعدد الجرائم[3].

وإذا كانت التشريعات جرمت تزوير المحررات التقليدية فهل تعد هذه التشريعات وسيلة كافية لتطبق على جريمة التزوير المعلوماتي؟.

وفي هذا الصدد يتضح أن التشريعات تباينت فيما بينها، فإذا كانت بعض التشريعات قد أوردت تعريفا للتزوير كالقانون الأردني الذي عرف التزوير في المادة 260 منه[4] فإن فهناك تشريعات أخرى لم تورد تعريفا للتزوير، ويرى أغلب الفقه أن هذا الاتجاه هو الأسلم فهذه التشريعات بعدم إيرادها تعريفا للتزوير فإنها تبقي الباب مفتوح لدخول أنماط مستحدثة من الأفعال التي تعد تزويرا مقارنة بالاتجاه الأول الذي يعتبر مقيدا[5].

وعلى الرغم من أن معظم الدول كان موقفها واضحا بعدم انطباق نصوص التزوير التقليدي على تزوير المعطيات واتخذت تدابير تشريعية لتجريم تزوير المعطيات وتوفير أداة قانونية لمكافحتها، أما الدول المتبقية فاتخذت موقف معاكس تماما بخصوص هذه التشريعات، وفي هذا الصدد انقسم الفقه

[1] المواد (213-218) من الأمر 156/66 السالف الذكر.

[2] محمود نجيب حسني، مرجع سابق، ص 215.

[3] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 246.

[4] تنص المادة 260 من قانون العقوبات الأردني:" تعريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"، ونفس المادة نص عليها القانون اللبناني في مادته 435، والقانون السوري في مادته 440.

[5] محمود أحمد عبابنة، مرجع سابق، ص 107.

إلى رأيين متعاكسين تماما، فالفقه في فرنسا مثلا انقسم إلى اتجاهين، اتجاه يرفض فكرة إمكانية تطبيق نصوص القانون التقليدي لجريمة التزوير على التزوير المعلوماتي مستندا في ذلك إلى أن جريمة التزوير تستلزم أن تكون هناك كتابة، وأن تغيير الحقيقة في الأشرطة الممغنطة لا يعد من قبيل التزوير لانتفاء شرط الكتابة، بالإضافة إلى عدم صلاحية الوثائق المعلوماتية للإثبات[1].

أما أنصار الرأي الثاني فإنهم يرون ضرورة إخضاع تزوير المعلومات المخزنة لنصوص قانون العقوبات التقليدية وذلك لأن القضاء في فرنسا لا يفرق بين محرر منسوخ أو مختزن كما لا يوجد ما يمنع من الاعتماد على الوثائق المعلوماتية في الإثبات سيما وأن تسجيل المعلومات بوسائل معلوماتية يعد شكلا من أشكال المحررات[2].

ويتضح أخيرا أن الرأي الأول هو الراجح لأنه الرأي الذي استند الى الحجج الأقوى إقناعا، الأمر الذي دفع التشريعات المقارنة المتعلقة بالحاسب الآلي إفراد نصوص خاصة بالتزوير المعلوماتي.

وعلى ذلك فجريمة التزوير المعلوماتي جريمة تزوير مستحدثة محلها المحرر الالكتروني، ويعرف المحرر على أنه:" مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين"[3] وبناء على هذا التعريف يعرف المحرر الالكتروني على أنه:" بيانات ومعلومات ذات معنى لا تدركها الحواس، وإن أمكن معرفتها وإدراك محتواها وتداولها باستخدام أجهزة العرض والإخراج والتقنية الخاصة"[4].

وعلى ذلك وبناءا على هذا التعريف فإن المعلومات والبيانات المخزنة على ذاكرة الحاسب الآلي داخل النظام أو الموجودة على دعائم الكترونية تشكل محررات تصلح محلا لجريمة التزوير، وعليه فالتزوير المعلوماتي جريمة قائمة بذاتها ولها أركانها، فركنها المادي يتمثل في السلوك الجرمي التقني وهو التغيير المفتعل للحقيقة، ومظاهر هذا التغيير تكون أكثر خصوبة لنمو التزوير المعلوماتي

[1] محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستخدمة ، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، في الفترة 25-1993/10/28، القاهرة، ص 158.

[2] محمود أحمد عبابنة، مرجع سابق، ص 110 .

[3] محمود نجيب حسني، مرجع سابق، ص 247.

[4] أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية،الطبعة الثانية، دار الثقافة عمان-الأردن، 2014، ص 163.

كظاهرة جرمية مستحدثة، وذلك أن من طبيعة المحررات الالكترونية أنها تقبل التعديل والتحوير وذلك دون حك أو تحشية أو محو بعلامات ظاهرة وبارزة، ومن أجل ذلك ركزت التشريعات المختلفة على إحداث التغيير بصورة مفتعلة، توقع الضرر أو تهدد به، دون التركيز على وسيلة التغيير أو مظهره[1].

وأما ركنها المعنوي فلا يقوم وتتحقق المسؤولية الجزائية إلا إذا ثبت بحق الفاعل القصد الخاص القائم على نية استعمال المحرر بعد تزويره في ذات الغاية التي ارتكب فعل التزوير من أجلها[2].

وتشتمل جريمة التزوير المعلوماتي على تزوير البريد الالكتروني، وكذلك تزوير الوثائق والسجلات وتزوير الهوية[3]، ومن أجل ذلك إذا ارتكبت جريمة التزوير المعلوماتي من طرف الجماعات الإرهابية ولتحقيق أغراض إرهابية فإن هذه الجريمة تعتبر صورة من صور الإرهاب الالكتروني، فكثيرا ما تلجأ الجماعات الإرهابية الالكترونية إلى تزوير البريد الالكتروني، بأن يظهر أن مرسل الرسالة هو شخص معين وذو منصب معين ويطلب طلبا ما متذرعا بحجة يصدقها المستخدم فينخدع بذلك ويلبي طلبات هذا الشخص فتحقق هذه الجماعة غرضها الدنيء من وراء هذا التزوير المعلوماتي، أو كأن تقوم الجماعات الإرهابية بتزوير وثائق أو سجلات أو الهويات لبعض الأشخاص من أجل تسهيل عملياتها الإرهابية .

## ثانيا: غسيل الأموال عبر الانترنت.

كثيرا ما تلجأ المنظمات الإرهابية إلى غسيل الأموال التي تتحصل عليها من خلال عملياتها الإرهابية أو من الجهات التي تمولها وهذا من أجل أن تتزايد هذه الأموال أكثر ومن أجل إخفاء مصادرها غير المشروعة، ويعتبر مصطلح غسيل الأموال حديث نسبيا[4] مما تعرف هذه الجريمة أيضا

[1] أسامة أحمد المناعسة، جلال محمد الزغبي، مرجع سابق، 166.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 443.

[3] يوسف حسن يوسف، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011 ص 46.

[4] لم يكن هذا المصطلح معروفا لدى رجال الشرطة، حيث بدا استخدام هذا المصطلح في أمريكا نسبة إلى مؤسسات الغسيل التي تمتلكها المافيا، وكان أول استخدام قانوني لها سنة 1931 إثر محاكمة لأحد زعماء المافيا، وقد اشتملت هذه المحاكمة على مصادرة أموال قيل أنها جاءت من الاتجار غي المشروع بالمخدرات، لتفصيل أكثر راجع: محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1419هـ، ص 124.

بتبييض الأموال[1]، وقد اختلف الكثير من الفقهاء حول تعريف غسيل الأموال، إلا أنه ورغم تعدد هذه التعريفات فهي متفقة من حيث المضمون والجوهر، ومن بين تعريفات جريمة غسيل الأموال:" أنها كل تمويه لمصدر الأموال المكتسبة بطريقة غير شرعية أو هي العملية التي يلجا إليها القائمون على الاتجار غير المشروع لإخفاء وجود دخل، أو لإخفاء مصدره غير المشروع أو لاستخدام الدخل في وجه غير مشروع فضلا عن تمويه ذلك الدخل ليبدو وكأنه دخل مشروع"[2].

كما عرف الفقه الجنائي جريمة غسيل الأموال بأنها:" عملية إضفاء الصفة الشرعية على الأموال الناتجة من الجريمة المنظمة في محاولة لإخفاء المصدر الحقيقي للدخل".

كما عرفت أيضا بأنها:" عملية إلغاء الأصل غير الشرعي لبعض الأموال المتحصلة من جريمة بكافة الطرق الممكنة كي يعاد استثمارها في أعمال اقتصادية بعيدة كل البعد عن الأعمال غير الشرعية التي تحصلت منها هذه الأموال"[3].

وعلى ذلك فإن الفقه العربي يرى أن جريمة غسيل الأموال هو مجموعة من الطرق التي تسمح بإعطاء المظهر الخارجي الشرعي للأموال، أو العائدات المتحصلة أو المرتبطة بالنشاط الإجرامي الأصلي، أو أنها إخفاء أو تمويه طبيعة المال المتحصل عليه من النشاطات التي يعتبرها القانون العام من الجرائم ذات الخطورة وجعل ذلك المال وكأنه دخل مشروع.

الفقه الفرنسي يرى تقريبا نفس الرأي فيما يتعلق بجريمة غسيل الأموال ، فعرفها بأنها مجموعة الطرق والتقنيات المختلفة المشروعة وغير المشروعة والمعقدة يرتكبها الجاني بقصد إضفاء المشروعية على الأموال المتحصلة من النشاط الإجرامي وبذلك يتسنى إعادة استثمارها في أنشطة مشروعة، ومن

[1] من التشريعات التي استخدمت هذا المصطلح:

- فرنسا: القانون رقم 96-392 المتعلق بمكافحة تبييض الأموال والاتجار في المخدرات والتعاون الدولي في مجال حجز ومصادرة متحصلات الجريمة.
- الجزائر: القانون رقم 05-01 المتعلق بمحاربة تبييض الأموال وتمويل الإرهاب.

[2] إبراهيم حامد طنطاوي، المواجهة التشريعية لغسيل الأموال في مصر- دراسة مقارنة، دار النهضة العربية، القاهرة 2003، ص 07.

[3] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 185.

الفقهاء الفرنسيين أيضا من اعتبر هذه الجريمة إخفاء الأصل غير المشروع للأموال والأرباح والعائدات المتحصلة من جرائم جنائية بقصد استغلالها مرة أخرى في أنشطة مشروعة[1].

الفقه الأمريكي يرى أن غسيل الأموال هو وسائل لتحويل الاعتمادات التي تنبثق من الأنشطة غير المشروعة مثل المخدرات والدعارة وألعاب القمار وغيرها من الجرائم الأخرى واستخدامه في أغراض مالية بواسطة آليات وطرق مصرفية وقانونية مثل الودائع والاستثمارات والأسهم والسندات وذلك لإعطاء دليل على مشروعية الأموال ، وهناك من الفقهاء من عرف جريمة غسيل الأموال بأنها:" مجموعة من العمليات والتقنيات المختلفة يخفي فيها الجاني المصدر الحقيقي للأموال غير المشروعة بقصد إضفاء المشروعية عليها وجعلها وكأنها محصلة من نشاط مشروع[2].

أما الفقه الانجليزي فقد أعطى مفهوما متميزا لغسل الأموال يعتمد على مصادرة الأموال غير المشروعة المتحصلة من الجريمة، ومن هذه التعريفات الفقهية الانجليزية: "غسل الأموال هي العملية التي يقوم فيها المجرمون بإخفاء أصل أو الملكية الحقيقية غير المشروعة، وذلك لتجنب مصادرتها وبقصد استغلال تلك الأموال في أنشطة مشروعة وفي هذا السياق عرف فقيه آخر غسيل الأموال بأنه:" أموال غير مشروعة يحصل عليها الجاني من جريمة ثم يرتكب مجموعة من المعاملات المعقدة بقصد إضفاء المشروعية عليها[3].

أما على صعيد المؤتمرات والاتفاقيات الدولية فقد عرفت اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع للمخدرات والمؤثرات العقلية لسنة 1988 هذه الجريمة في مادتها الثالثة بقولها:" عملية تحويل الأموال أو نقلها مع العلم بأنها مستمدة من أية جريمة أو فعل من أفعال الاشتراك في مثل هذه الجريمة بهدف إخفاء أو تمويه المصدر غير المشروع للأموال بقصد مساعدة أي شخص متورط في ارتكاب مثل هذه الجريمة على الإفلات من العواقب القانونية لأفعاله"[4].

[1] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 190.

[2] نفس المرجع، ص 191.

[3] نفس المرجع، ص 191 .

[4] عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية الإسكندرية، 2011، ص 100.

أما دليل اللجنة الأوربية لغسيل الأموال الصادر سنة 1990 فقد عرف غسيل الأموال بأنه:" عملية تحويل الأموال المتحصلة من أنشطة جرمية بهدف إخفاء أو إنكار المصدر غير الشرعي[1] والمحظور لهذه الأموال، أو مساعدة أي شخص ارتكب جرما ليتجنب المسؤولية القانونية الناجمة عن الاحتفاظ بمتحصلات هذا الجرم"، ويشترط في هذه الحالة توفر المعرفة بأن هذه الأموال متحصلة من جريمة.

ويستنتج من التعريفات السابقة وخاصة التعريفين الأخيرين أن جريمة غسيل الأموال هي جريمة تبعية، أي أنها لاحقة لجريمة أخرى أو لأنشطة جرمية سابقة عليها، ودليل ذلك أن جميع التعاريف اتفقت على أن غاية هذه الجريمة إخفاء المصدر غير المشروع للأموال أو المساعدة غير القانونية.

وأما على صعيد التشريعات، فهناك من التشريعات من أوردت مفهوم خاص لجريمة غسيل الأموال ضمن قانون متعلق بهذا الخصوص، كالإمارات العربية المتحدة، العراق السودان، فرنسا وهناك من التشريعات من أوردت تعريفات واسعة لهذه الجريمة كالمملكة العربية السعودية (القانون رقم 39 لسنة 2005)، وقد اقترن تجريم غسيل الأموال بتمويل الإرهاب ، فبمجرد قيام الشخص بتمويل الإرهاب يعد فاعلا أصليا في هذه الجريمة، وهذا للانتشار الكبير للإرهاب في مختلف أنحاء العالم وزيادة الدعوات من الشيوخ المتطرفين لتمويله باسم الجهاد[2].

هذا ونشير إلى أنه هناك مجموعة من التشريعات لم تعرف جريمة غسيل الأموال كالتشريع الجزائري الذي لم يعرف جريمة غسيل الأموال في النصوص التشريعية والتنظيمية التي صدرت في

[1] بخاوية إدريس، جريمة غسل الأموال ومكافحتها في القانون الجزائري، أطروحة دكتوراه في القانون الجنائي الخاص جامعة أبو بكر بلقايد، تلمسان، 2012/2011، ص 21.

[2] أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 184.

هذا المجال[1]، وبذلك اكتفى بتحديد الأفعال المكونة لها فاعتبر كل العائدات الإجرامية الناتجة عن جناية أو جنحة والتي يكون الغرض منها إخفاء أو تمويه ذلك المصدر غير المشروع[2].

وعلى ذلك ومن كل ما سبق فإن جريمة غسيل الأموال تفترض بالضرورة وقوع جريمة سابقة عليها، وهي الجريمة التي تحصل منها الأموال المراد غسلها، وبالتالي وهو بمثابة ركن مفترض في جريمة غسيل الأموال، وقد وسع المشرع في نطاق الجرائم الناتج عنها المال المراد غسله، فلم يقتصر الأمر على مجرد المال المتحصل من جرائم المخدرات وتوابعها ولكنه أدخل فيها جرائم أخرى، وفي هذه النقطة نقول أن التشريعات حذت حذو الاتفاقيات الدولية، فتركت المجال مفتوحا لإدخال طائفة أخرى من الجرائم المنظمة التي نصت عليها هذه الاتفاقيات الدولية.

وتجدر الإشارة إلى أنه بالإضافة إلى الركن المفترض في جريمة غسيل الأموال فإن هذه الجريمة عمدية، فلا يتصور أن ترتكب هذه الجريمة على سبيل الخطأ أو بسبب الإهمال، وقد اشترط المشرعين لكي يعتد بهذه الجريمة بأن يكون مرتكبها عالما أن الأموال المغسولة محل جريمة من الجرائم التي عددها المشرع ونصت عليها الاتفاقيات، هذا بالإضافة إلى أن لهذه الجريمة ركن معنوي يقوم على قصد جنائي عام الذي يتمثل في العلم والإرادة، وقصد جنائي خاص لدى الجاني يتمثل في إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال[3].

ومع التطور التكنولوجي الذي عرفه العالم في مجال تكنولوجيا المعلومات والاتصالات كان من البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه هذه التقنية الحديثة لخدمة أنشطتهم الإجرامية

[1] قانون 01/05 المؤرخ في 2005/02/06 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والذي عدل بموجب القانون 06/15 المؤرخ في 2015/02/15، الجريدة الرسمية عدد 8 الصادرة بتاريخ 2015/02/15 ص 4 .

[2] تناول المشرع الجزائري جريمة غسيل الأموال في نص المادة 389 مكرر من القانون 04/15 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات الجزائري، وأيضا في المادة 02 من القانون 01/05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.

[3] عماد مجدي عبد الملك، مرجع سابق، ص 102.

والمتمثلة في هذا العنصر غسيل الأموال، فقد لجؤوا إلى الانترنت لتوسعة وتسريع أعمالهم في غسيل الأموال[1].

وتعود فكرة غسيل الأموال عبر الانترنت إلى عصابات الجريمة المنظمة من حيث المصدر حيث تملك هذه الجماعات أموالا كثيرة ناجمة عن عمليات غير مشروعة مثل الاتجار بالمخدرات وغيرها، وقد أرادت هذه العصابات حل مشاكل السيولة وعدم قدرتها على الاحتفاظ بالأموال داخل البنوك، ومشاكل اكتشاف أنشطتها في غسل الأموال بالصور التقليدية، فعمدت إلى إضفاء صفة الشرعية على مصادر أموالها غير المشروعة خلال غسل الأموال عبر استخدام الانترنت في هذه العملية، وهذه الجريمة لا تقتصر على القائمين بها فقط، بل تتعداه إلى كل من شارك بها من مساهمين ومتدخلين ومستفيدين، وكل من أخفى معلومات أو أنكر حقائق تتعلق بطبيعة المصدر أو بعلاقة الملكية[2].

ومن المميزات التي تمنحها الانترنت لعملية غسيل الأموال السرعة، وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما تساهم البطاقات الذكية، والتي تشبه في عملها بطاقات البنوك المستخدمة في أكائن الصرف الآلية، في تحويل الأموال بواسطة المودم أو الانترنت مع ضمان تشفير وتأمين العملية[3].

إن كل المميزات التي سبق وأن ذكرناها جعل عمليات غسيل الأموال عبر الانترنت تتم بسرعة أكبر ودون أن تترك أي أثر على ارتكابها في الغالب، فإلى وقت قريب لم تكن جريمة غسيل الأموال تشكل جرما بذاتها إلى أن تضخمت الأموال المتحصلة من الجرائم خاصة من تجارة المخدرات فأصدرت بعض الدول قوانين خاصة تسمح بتعقب وتجميد ومصادرة عائدات الجرائم الخطيرة[4].

---

[1] يوسف حسن يوسف، المرجع السابق، ص 123.

[2] ممدوح محمد الجنبيهي، منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص 100.

[3] يوسف حسن يوسف، مرجع سابق، ص 124.

[4] ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة 2001، ص (68،72).

من العوامل أيضا التي ساهمت في انتشار جريمة غسيل الأموال عبر الانترنت في السنوات الأخيرة انتشار التجارة الالكترونية في العالم بأسره، حيث ساعدت هذه الأخيرة القائمين بجريمة غسيل الأموال، بل وكانت خير معين له حيث أن سرعة الاتفاق على الصفقات وإتمامها عبر الاتفاق على خطوات وترتيبات تنفذ عبر شبكة الانترنت وبطريقة تشفير معقدة لا يمكن حلها، وبالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفقات[1] .

أما عن علاقة جريمة غسيل الأموال بالإرهاب فلطالما أثبتت الدراسات وجود علاقة وثيقة بينهما سواء في شكليهما التقليدي أو المستحدث (الالكتروني)، فعمليات غسيل الأموال تستخدم في توفير الدعم المالي للإرهاب من أجل شراء الأسلحة اللازمة للعمليات الإرهابية وذلك بالتعاون مع أجهزة متخصصة، بالإضافة إلى أن وجود العلاقة بين غسيل الأموال والإرهاب الالكتروني يدفع بالإرهابيين إلى اللجوء إلى أجهزة المخابرات والتجسس واستخدام الأموال المغسولة في تأسيس منظمات إرهابية وتنفيذ بعض العمليات تخريبية الموجهة ضد أنظمة أو حكومات معينة في أي مكان من العالم باستخدام شبكات الانترنت، ونظرا لاتساع نطاق العلاقة بين جريمة غسيل الأموال وجريمة الإرهاب نصت الاتفاقيات الدولية على إدراج جرائم الفساد والإرهاب ضمن جرائم غسيل الأموال بهدف تجفيف منابع الفساد والإرهاب، بعدما كانت تقتصر على جرائم إنتاج المخدرات وتسويقها[2]

## ثالثا: الجريمة المنظمة.

يرى الكثير من الفقه أن كل من الإرهاب والجريمة المنظمة وجهان لعملة واحدة فأوجه الشبه بينهما كبير بحيث تهدف كلا الجريمتين إلى بث الرعب والخوف، كما أنهما تتفقان في أسلوب العمل والتنظيم، وكثيرا ما يكون أعضاء المنظمات الإرهابية هم أساس من محترفي الجرائم المنظمة، حيث

[1] ممدوح محمد الجنبيهي، منير محمد الجنبيهي، مرجع سابق، ص 100.

[2] في هذا السياق نصت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة في 2000/12/15 "اتفاقية باليرمو" على أن يطلق تجريم غسيل الأموال على جرائم مشتركة في جماعة إجرامية نظامية وجرائم الفساد وجرائم تزييف أو تزييف العملة وجرائم الإرهاب والقرصنة وتهريب الأسلحة النارية وأجزائها ومكوناتها والذخائر والمتفجرات وسائر المواد ذات الصلة بها أو صنعها أو الاتجار بها بصورة غير مشروعة.لتفصيل أكثر راجع: أمير فرج يوسف (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 188 .

يسعون إلى الاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ لأجل ذلك جاءت هذه الصلة الوثيقة والمتداخلة بين الجريمتين[1].

وتعرف الجريمة المنظمة بأنها:" الظاهرة الإجرامية التي يكون وراءها جماعات معينة تستخدم العنف أساسا لنشاطها الإجرامي وتهدف إلى الربح، وقد تمارس نشاطها داخل إقليم الدولة أو تقوم بأنشطة إجرامية عبر وطنية، أو تكون لها علاقات بمنظمات متشابهة في دول أخرى"[2].

ففي الولايات المتحدة الأمريكية شرعت لجنة من مجلس الشيوخ الأمريكي سنة 1950 في التحقيق عن الجريمة المنظمة، وذلك في إطار تنظيم التجارة بين الولايات وركزت هذه اللجنة على العديد من الشخصيات البارزة في عالم الإجرام في "شيكاغو" آنذاك والتي كان لها دور كبير في التحكم في دور القمار غير القانونية، وسلطات المجالس البلدية، وتوصلت هذه اللجنة إلى أن عددا كبيرا من المجموعات الإجرامية ترتبط فيما بينها في منظمة كبيرة تدعى "المافيا"، ونطاق هذه المجموعة يخرج عن نطاق المحلية، ففي هذه الفترة بدأت بوادر ظهور مفهوم للجريمة المنظمة بعدما كان مكتب التحقيقات الفيدرالي يرفض هذا الأمر رفضا تاما[3].

وقد قدم الباحث الأمريكي "John E.conklin" تعريفا للجريمة المنظمة بأنها نشاط إجرامي تقوم به منظمة شكلية تسعى للكسب بطريقة غير مشروعة، وأما الفقيه "Warenolney" من جامعة "ماسا شوست" الأمريكية فيرى أن الجريمة المنظمة بشكلها الحديث ليست نوعا خاصا من النشاط، بل هي تقنية للعنف والفساد، ولها القدرة على دخول أي عمل أو صناعة لتحقيق أرباح كبيرة باعثها الأساسي إقامة وضمان احتكار بعض الأنشطة التي تحقق أرباحا طائلة[4].

أما على صعيد الفقه الأوروبي فقد ظهرت في فرنسا بوادر مفهوم الإجرام المنظم في منتصف القرن التاسع عشر، حيث كتب الفقيه الاشتراكي "Louis Blanc" في مؤلفه "تنظيم العمل" مايلي:" ينتظم اليوم القتلة والسارقون ويخضعون لقواعد انضباط، واوجدوا قانونا يحكم نشاطهم..."، والأمر نفسه

1 أشرف توفيق شمس الدين، مبادئ القانون الدولي الجنائي، المؤسسة الجامعية للطباعة، بيروت، 1990، ص 301.
2 أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 227.
3 شبلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة ، الجزائر، 2013، ص 32.
4كوركيس يوسف داود، الجريمة المنظمة، الدار العلمية، عمان– الأردن، 2001، ص 151.

في كل من ألمانيا وايطاليا حيث كان مفهوم الجريمة المنظمة لصيقا بالمافيا، والتي كان الانتساب إليها عائليا أو جهويا.

وقد عرف الفقيه "Grassin" الجريمة المنظمة بأنها الجريمة التي ترافق الإرادة المتعمدة والبينة لارتكاب الفعل المجرم أو مجموعة الأفعال المكونة لهذه الجريمة، وهذه الجريمة تعني أن التحضير لها وتنفيذها يتميز بتنظيم دقيق وطريقة ممنهجة تمكن من تواجد هذه الجريمة[1].

هذا وقد حددت وزارة الداخلية الفرنسية سنة 1996 الأوصاف التي تعرف بها الجريمة المنظمة وهي الأنشطة الإجرامية ذات البعد الدولي والمتواترة، والتي تستعمل طرقا حديثة في التسيير بنية الحصول على أرباح معتبرة[2].

لم تكن الجريمة المنظمة معروفة في العالم العربي بنفس المفهوم الذي عرف في الغرب، على الرغم من أن قصص التاريخ تشهد على الكثير من جرائم العصابات كالسرقة والاعتداءات في أماكن وأوقات محددة، أي ما عرفه الفقه الإسلامي بـ "الحرابة" ففي الأفعال المكونة لجريمة الحرابة في الشريعة الإسلامية ما يشبه الإجرام المنظم من اشتراك في مجموعة، وديمومة نشاطها، والقيام بأفعال إجرامية كالسرقة والقتل والترهيب[3].

ومن التعريفات التي قدمها الفقع العربي للجريمة المنظمة تعريف الأستاذ الدكتور"محمد فاروق النبهان" حيث عرف الجريمة المنظمة بأنها:" الجريمة التي أوجدتها الحضارة المادية لكي تسهل للمجرم تحقيق أهدافه الإجرامية بطريقة متقدمة بحيث لا يتمكن القانون من ملاحقته بفضل ما أحاط به نفسه من وسائل يخفي بها أغراضه الإجرامية، ولا بد من تحقيق هذه الغاية من تعاون مجموعة من المجرمين[4].

---

[1] LECLERC Marcel, La criminalité organisée Ed, la documentation française , paris, France, 1996,p 155.

[2] شبلي مختار، مرجع سابق، ص 40.

[3] عبد الفتاح مصطفى الصيفي، وآخرون، الجريمة المنظمة– التعريف والأنماط والاتجاهات، أكاديمية نايف للعلوم الأمنية، الرياض، 1999، ص 34.

[4] شبلي مختار، مرجع سابق، ص 43.

كما حظيت الجريمة المنظمة أيضا باهتمام مختلف الهيئات والمنظمات الدولية منذ منتصف القرن العشرين، وهذا نظرا لخطورتها فقد أبرمت في شانها اتفاقيات ومعاهدات دولية، كما عقدت الكثير من المؤتمرات حولها، وأولها مؤتمرات الأمم المتحدة لمنع الجريمة ومعاملة المجرمين، حيث قدم المؤتمر الخامس الذي عقد في "جنيف" سنة 1975 تعريفا للجريمة المنظمة بأنها:" الجريمة التي تتضمن نشاطا إجراميا معقدا على نطاق واسع، تنفذه مجموعة من الأشخاص على درجة من التنظيم تهدف الى تحقيق ثراء للمشتركين فيها على حساب المجتمع وأفراده، وهي غالبا ما ترتكب الجرائم بتجاهل تام للقوانين، وتتضمن جرائم ضد الأشخاص، وتكون مرتبطة في معظم الأحيان بالفساد السياسي[1].

أما اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000 فقد عرفت الجريمة المنظمة من خلال نص المادة الثانية بقولها:" – يقصد بتعبير "جماعة إجرامية منظمة" جماعة ذات هيكل تنظيمي مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن، وتعمل بصورة متضافرة بهدف ارتكاب واحد أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة، وفقا لهذه الاتفاقية من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو منفعة مادية أخرى.

– يقصد بتعبير "جريمة خطيرة" كل سلوك يمثل جرما يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة اشد.

– يقصد "بجماعة ذات هيكل تنظيمي" جماعة غير مشكلة عشوائيا لغرض الارتكاب الفوري لجرم ما، ولا يشترط أن يكون لأعضائها أدوارا محددة أو صفة الدوام لأعضائها أو استمرارية في تشكيلتها أو هيكلتها ...."[2].

وبذلك تعتبر هذه الاتفاقية (اتفاقية باليرمو) إطارا مهما ومرجعية عالمية في مجال الجريمة المنظمة ووسائل مكافحتها.

[1] شبلي مختار، مرجع سابق، ص 45.

[2] المادة الثانية من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، التي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم (25) في الدورة الخامسة والخمسون بتاريخ 2000/11/15، منشورات الجمعية العامة للأمم المتحدة 2001/01/08.

المنظمة الدولية للشرطة الجنائية قدمت بدورها تعريفا للجريمة المنظمة سنة 1988 بقولها:" الجريمة المنظمة هي أي مشروع إجرامي أو مجموعة من الأشخاص ينخرطون في أنشطة إجرامية مستمرة هدفها جني أرباح متحصلة منها بغض النظر عن الحدود الوطنية[1].

ومن كل التعريفات السابقة نجد –حسب رأيينا– أن التعريف الأكثر شمولا ودقة هو الذي جاء به بعض الفقهاء العرب بقولهم:" الجريمة المنظمة هي مشروع إجرامي يقوم على أشخاص يوحدون صفوفهم للقيام بأنشطة إجرامية دائمة ومستمرة، ويتميز هذا التنظيم بكونه يشبه البناء الهرمي، وتحكمه لوائح ونظم داخلية لضبط سير العمل داخله في سبيل تحقيق أهدافه، باستخدام وسائله من عنف وتهديد وابتزاز ورشوة لإخضاع وإفساد المسؤولين سواء في أجهزة إدارة الحكم أو أجهزة إدارة العدالة وفرض السيطرة عليهم بهدف تحقيق الاستفادة القصوى من النشاط الإجرامي، سواء كان ذلك بوسائل مشروعة أو غير مشروعة"[2].

وتجدر الإشارة إلى أن الجريمة المنظمة قد تكون عابرة للأوطان أو الحدود الوطنية كما قد لا تلحق بها صفة العبور وتكون بذلك جريمة منظمة فقط أي ترتكب داخل حدود الدولة الواحدة.

وتكمن العلاقة الوطيدة والترابط القوي بين جريمة الإرهاب الالكتروني والجريمة المنظمة من خلال الخصائص المشتركة بين الجريمتين والتي تتمثل في مايلي:

- إن كل من الجريمتين تتخذان من العنف غاية لتحقيق أهدافها غير المشروعة بالإضافة إلى نشرهما الرعب والذعر بهذه الوسائل.
- تشابه الهيكل التنظيمي لكل منهما والقائم على العلاقة الهرمية بين أعضائه.
- تعد شبكات الإرهاب والجريمة المنظمة غاية في التنظيم والدقة فضلا عن السرية في تنفيذ المهام، كما تعد هذه الشبكات عقبة أمام التنمية الاقتصادية.
- تمتد كل من الجريمتين في اغلب الأحيان عبر حدود الدول.

[1] محمد فتحي عيد، مرجع سابق، 93.

[2] أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة– التجريم وسبل المواجهة، الطبعة الأولى، دار الشروق القاهرة، 2004،ص 16.

– انعقاد مؤتمرات وندوات دولية عديدة لبيان العلاقة بين الجريمة المنظمة والجماعات الإرهابية وخاصة المتعلقة بالانترنت(الإرهاب الالكتروني)، ومن أهم هذه المؤتمرات التي تدل على ارتباط الجريمتين[1]:

1. مؤتمر الأمم المتحدة الثامن لمنع الجريمة (هافانا 1990)، حيث أشار القرار الخامس عشر المتعلق بالجريمة المنظمة إلى خطورة الجرائم التي ترتكبها جماعات الجريمة المنظمة ولا سيما الإرهاب.
2. قرار رقم 1373 الصادر عن مجلس الأمن سنة 2001، حيث أشارت الفقرة الرابعة منه إلى القلق من العلاقة الوثيقة بين جرائم الإرهاب والجريمة المنظمة عبر الوطنية.
3. إعلان القاهرة لمكافحة الإرهاب الصادر في 2003/12/04 حيث عبرت القاهرة عن قلقها الكبير من العلاقة الوثيقة بين جرائم الإرهاب والجريمة المنظمة عبر الوطنية.

من هذه الخصائص المشتركة لكل من جريمة الإرهاب والجريمة المنظمة، جعلت الكثير يرى أن الإرهاب هو شكل من أشكال الجريمة المنظمة بأبعادها الجديدة بالنظر إلى آثارها السلبية التي تمتد إلى مناطق متعددة من العالم[2].

## رابعا: المواقع المعادية .

بعدما انتشرت الانترنت بشكلها الرهيب في كافة أنحاء العالم كثرت المواقع غير المرغوب فيها فقد تكون هذه المواقع موجهة ضد سياسة دولة ما أو ضد عقيدة أو ضد مذهب معين ، كما قد تكون ضد شخص معين، وهذه المواقع تهدف في المقام الأول إلى تشويه صورة الدولة أو المعتقد أو الشخص المستهدف[3].

فإذا كان هذا الموقع المعادي ذو طبيعة سياسية أي موجه ضد سياسة دولة ما يتم من خلاله تلفيق الأخبار والمعلومات، ويكون هذا التلفيق للحقائق إما كليا أو جزئيا وغالبا ما يعمد أصحاب هذه المواقع إلى إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التي تبيع قواعد

[1] محمد سامي الشوا، الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية، القاهرة، 2001، ص 55.
[2] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 230.
[3] نفس المرجع، ص 241.

البيانات تلك أو بطرق أخرى، وبعدا يقومون بإضافة تلك العناوين قسرا إلى قائمتهم البريدية، ويبدؤون بإغراق تلك العناوين بمنشوراتهم، وعادة ما يلجؤون إلى هذه الطريقة رغبة في تجاوز الحجب الذي قد يتعرضون له ولإيصال أصواتهم إلى اكبر قدر ممكن من الناس[1].

أما المواقع المعادية للعقيدة فمنها ما يكون موجه من قبل أعداء حاقدين من إتباع ديانات أخرى كالمواقع التي تنشئها الجاليات اليهودية أو النصرانية تحت مسميات إسلامية بقصد بث معلومات خاطئة عن الإسلام والقرآن الكريم، أو بهدف الدعاية للأديان الأخرى [2]، وأما القسم الثاني من المواقع المعادية للعقيدة فهي المواقع التي يكون أفرادها من ذات العقيدة الواحدة ولكن يختلفون في المذهب[3].

أما المواقع المعادية للأشخاص أو الجهات فهي المواقع المخصصة للقذف والجرائم المرتبطة به كالجرائم الجنسية.

ويرتبط الإرهاب الالكتروني بهذه المواقع لأنه من خلالها يمكن لهذه الجماعات الإرهابية الالكترونية أن تحقق غاياتها وخاصة إذا كانت لهما نفس الغاية والهدف.

### خامسا: جرائم القرصنة.

يقصد بجرائم القرصنة الالكترونية الاستخدام أو النسخ غير المشروع لنظم التشغيل أو لبرامج الآلي المختلفة.

---

[1] يوسف حسن يوسف، مرجع سابق، ص 125.

[2] ومن أمثلة المواقع المعادية للإسلام: http://www.ansering-islam.org
http://www.aboutislam.com
http://www.thequran.com

[3] يونس عرب، صور الجرائم الالكترونية واتجاهاتها وتبويبها، بحث مقدم في مؤتمر مجموعة عرب للقانون، 2-4 نيسان، مسقط-عمان، 2006، ص 33.

وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الانترنت تطورت صور القرصنة واتسعت وأصبح من الشائع جدا العثور على الموقع بالانترنت خاصة لترويج برامج القرصنة مجانا، أو بمقابل مادي رمزي[1].

وقد أدت قرصنة البرامج إلى خسائر مادية ضخمة جدا خاصة في مجال البرمجيات ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد بينها وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات، ومثالها منظمة اتحاد البرمجيات، وهذه الأخيرة قامت بدراسة استخلص منها أن القرصنة الالكترونية ستطغى على كافة أنواع القرصنة الأخرى، وهذا التقرير دق ناقوس الخطر بالنسبة للشركات المعنية، والتي قامت باتخاذ إجراءات الحماية، ومن أمثلتها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الانترنت، لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة، إلا أن تلك الشركات تراجعت عن هذا التهديد اثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الانترنت.

كما قامت تلك الشركات بالاتفاق مع مزودي الخدمة لإبلاغهم عن أي مواقع مخصصة للبرامج المقرصنة تنشا لديهم، وذلك لتقديم شكوى ضدهم، ومقاضاتهم إن أمكن، كما قد يكون الإجراء المناسب إغلاق تلك المواقع[2] .

دول العالم العربي كغيرها من دول العالم عرفت القرصنة الالكترونية، بل وسبقت حتى الدول الغربية في هذا المجال وهذا نظرا لعدم توفر الحماية الفكرية أو في عدم جدية تطبيق قوانين الحماية إن وجدت[3].

والإرهاب الالكتروني أيضا يرتبط بهذه الجريمة حيث يهدف الإرهاب الالكتروني إلى اختراق المواقع التي تخدم أهدافه وينسخ كل المعلومات التي يريدها والتي تحقق غايته الدنيئة، كما تؤدي إلى إضعاف الضحية المستهدفة من وراء هجماته.

[1] يوسف حسن يوسف، مرجع سابق، ص 129.

[2] نفس المرجع، ص 129.

[3] ماهر الجنيدي، النصر للأقوى والذكي والقذر، مجلة انترنت العالم العربي، العدد 36، نوفمبر 1999، ص (28-35).

## المبحث الثاني: البنيان القانوني لجريمة الإرهاب الالكتروني.

لكل جريمة من الجرائم بنيان قانوني يميزها عن غيرها من الجرائم، ولجريمة الإرهاب الالكتروني بيانها القانوني المتكون من الأركان القانونية المميزة لهذه الجريمة من ركن مادي ومعنوي كما أنه كثيرا ما يحث تداخل بين المساهمة الجنائية باعتبارها عنصر من عناصر الركن المادي للجريمة محل الدراسة وبين الاتفاق الجنائي كونهما يشتركان في العديد من العناصر، وهذا كله بهدف تحديد الإطار القانوني الدقيق لجريمة الإرهاب الالكتروني.

ومن أجل ذلك قسمنا هذا العنصر إلى فرعين فرع أول يحمل عنوان أركان جريمة الإرهاب الالكتروني، وأما الفرع الثاني فيحمل عنوان المساهمة الجنائية والاتفاق الجنائي لجريمة الإرهاب الالكتروني.

### المطلب الأول: أركان جريمة الإرهاب الالكتروني.

قبل أن نتعرض إلى أركان جريمة الإرهاب الالكتروني تجدر الإشارة إلى أن الفقه الجنائي تنازع بخصوص التكييف القانوني للإرهاب الالكتروني، وقد نتج عن هذا التنازع رأيين رأي يرى أن جريمة الإرهاب الالكتروني هي جريمة وطنية، حيث يرى المشرع أنها جريمة جنائية تشتمل على كل الأبعاد المختلفة من الجرائم، كالقتل والسرقة والإتلاف.

فالتكييف القانوني لجريمة الإرهاب يتطلب تعريفا قانونيا للجريمة بموجبه يحدد أركانها، وهذا التعريف يتبناه المشرع استنادا على مبدأ شرعية الجرائم والعقوبات، مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب للأفعال التي يتضمنها التعريف ومن بين المشرعين الذين قالوا بهذا الرأي وعملوا به المشرع العراقي، في قانون رقم 13 لسنة 2005 المتعلق بمكافحة الإرهاب الذي عرف الإرهاب بالأفعال المكونة له وحدد العقوبة الخاصة بكل عمل[1]، وكذلك المشرع الجزائري عمل بهذا الرأي في الأمر 156/66 المتضمن بقانون العقوبات الجزائري المعدل والمتمم وذلك من خلال نصوص المواد من المادة 87 مكرر وما بعدها[2].

[1] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 155.

[2] القانون 156/66 السالف الذكر.

فهذه الجريمة تتمتع بذاتية خاصة من الناحية القانونية نظرا إلى جسامتها، وهو ما ينعكس بشكل خاص في تجريم مجرد تأسيس الجماعات الإجرامية ومختلف الأعمال التي تساعد على وقوع الإرهاب ومن بينها التمويل[1].

واستنادا إلى ذلك يثور تساؤل مهم مفاده هل جريمة الالكتروني بهذا الوصف تعتبر جريمة جنائية في حد ذاتها أو هي مجرد ظرف تشديد نظرا إلى وسائلها وأهدافها وضحاياها، ولا شك أن العامل الإرهابي يتجاوز كونه ظرفا مشددا لجريمة إرهابية عادية ويندمج فيها اندماجا حتى يصبح مكون طبيعي فيها يعكس ويكشف خطورتها وخطورة مرتكبيها[2].

ولأن جريمة الإرهاب عموما جريمة جد خطيرة فإنها تخضع إلى نظام إجرائي متميز من خلال هذا النظام يتم مراعاة عدة عوامل منها درجة الجسامة، ومختلف أبعادها كالبعد الدولي، إذا ما تجاوزت الأفعال المكونة لهذه الجريمة حدود الدولة المعينة، فالإقليمية ليست التي تحسم الاختصاص القضائي بل ينظر حتى في حالة التجاوز، بل ينظر إلى جنسية الجناة والضحايا وإلى عبور وسائل الجريمة للأوطان وإلى تنظيماته التي تصل إلى حد تكوين الخلايا المنظمة في بعض الدول، وفي هذا الشأن اهتم مكتب الأمم المتحدة لمكافحة الجريمة والمخدرات في فيينا على إثر قرار مجلس الأمن الصادر سنة 2001 بوضع دليل للوثائق الدولية التي تكافح الإرهاب، وقد أشار هذا الدليل إلى أن الإطار القانوني لمكافحة الإرهاب يمكن أن يتم بتعديل القانون الجنائي الوطني في شقيه الإجرائي والموضوعي، أو بالاقتصار على التصديق على الوثائق الخاصة بمكافحة الإرهاب[3].

وأما الرأي الثاني والذي يقول بأن الإرهاب الالكتروني جريمة دولية وذلك في حالة ما كانت هذه الجريمة مخالفة للقواعد الدولية التي تترتب عليها المسؤولية الجنائية الشخصية سواء تلك التي نصت عليها الاتفاقيات الدولية، أو تضمنتها القواعد الدولية العرفية، ومن أجل ذلك وجب أن تتوفر العناصر الآتية:

[1] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 155.

[2] أحمد فتحي سرور، حكم القانون في مواجهة الإرهاب، الدار الجامعية، بيروت،2005، ص 109.

[3] يونس زكور، الإرهاب وإشكالية تحديد المفهوم، مقالة منشورة في مجلة الحوار المتمدن، العدد 1785 2006/12/08، ص 36.

- أن تتجاوز جريمة الإرهاب الإليكترون الحدود الوطنية للدولة ، سواء فيما يتعلق بالمتهمين أو بالوسائل المستخدمة، أو بنوع العنف المستخدم
- أن تتم الأعمال الإرهابية بدعم الدولة أو تشجيعها أو موافقتها أو بدعم من دولة أجنبية[1].
- تعلق الإرهاب الالكتروني بالمجتمع الدولي بأسره، فبعض الفقه وصف الإرهاب الالكتروني بأنه أصبح عدوا للدولة الوطنية والمجتمع الدولي بأكمله، فهو لا يقبل أي حل تفاوضي[2].
- أن تبلغ هذه الأعمال حدا من الجسامة تتمثل في أدواته التي تصل إلى حد استخدام التكنولوجيا الحديثة، واتساع نطاقها.

وبالتالي حتى تعد جريمة الإرهاب الالكتروني جريمة دولية وجب أن تشتمل على كل العناصر السابقة، وتوصف بأنها ماسة بالقيم التي يؤمن بها المجتمع الدولي[3].

وتعرف أركان الجريمة بأنها:"مجموعة الأجزاء التي تشكل منها الجريمة، أو كل الجوانب التي يتشكل منها بنيان الجريمة أو التي يترتب على وجودها في مجموعها وجود الجريمة، ويترتب على انتفائها أو انتفاء أحدها انتفاء الجريمة"[4].

وقد اختلف الفقهاء حول الأركان العامة للجريمة سواء على الصعيد الوطني أو الدولي، فعلى المستوى الوطني ظهرت ثلاث جهات فقهية مختلفة حول أركان الجريمة فيرى الاتجاه الأول أن للجريمة أربعة أركان عامة، ركن مادي وركن معنوي وركن شرعي وأما الرابع حسب رأي هذا الاتجاه ركن عدم الشرعية، وهو عدم وجود سبب قانوني لإباحة الفعل، وأما الاتجاه الثاني فإنه يرى أن هناك ثلاث أركان للجريمة، مادي ومعنوي والثالث شرعي، وأما الاتجاه الثالث فهو الذي يرى أن للجريمة ركنين فقط، ركن مادي والآخر معنوي، أما عن الركن الشرعي فينفي عنه أنصار هذا الاتجاه كونه ركن من أركان الجريمة، لأنه من ينشئها (النص القانوني هو الذي يجرم الفعل) ومن المستحيل أن

[1] المادة الثانية من اتفاقية المعاقبة على تمويل الإرهاب لسنة 1996، والتي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 54 109/، المؤرخ في 9 كانون الأول/ديسمبر 1999.

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 157.

[3] أحمد فتحي سرور، مرجع سابق، ص 109 .

[4] محمود صالح العادلي، الجريمة الدولية- دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2004، ص67.

يكون خالق الجريمة –على حد تعبيرهم– احد العناصر المكونة لها، وقد امتد هذا الخلاف حول الركن الشرعي إلى الصعيد الدولي[1].

وقد بينت معظم الدراسات السابقة ان الجرائم الإرهابية تتم بصور وأشكال مختلفة فبعضها محلي والبعض الآخر يكون دولي، فجريمة الإرهاب الدولي تتميز ببعدها الدولي عن الجرائم الأخرى، لذلك سوف نحاول من خلال هذا العنصر ان نتعرض الى الركنين المادي والمعنوي للإرهاب الالكتروني من خلال فرعين كما سوف نعرج على الركن الدولي إذا اشتملت هذه الجريمة على عناصر الجريمة الدولية.

### الفرع الأول: الركن المادي.

يعبر الركن المادي على الوجه الظاهر للجريمة، وبه يتحقق اعتداء الفاعل على مصلحة يحميها القانون، وبانعدام الركن المادي تنعدم الجريمة ومعها العقوبة، فالركن المادي ينصب على الفعل والسلوك[2]، فالقانون لا يعاقب على الأفكار والنوايا السيئة ما لم تظهر إلى العالم الخارجي، وتكون هذه النية مجسدة في فعل أو عمل.

وجريمة الإرهاب الالكتروني لا يختلف ركنها المادي عن الجرائم العادية، من حيث توافر سلوك يؤدي إلى نتيجة يعاقب عليها القانون، إلا انه في جريمة الإرهاب يكون السلوك دائما ايجابيا ولا يتصور وجود سلوك سلبي يمثل ركنها المادي[3]، ويشترط في هذا السلوك حتى يحقق النتيجة التي يرجوها الإرهابي أن تربطه بهذه النتيجة علاقة تعرف بالعلاقة السببية.

ومن أجل ذلك وفي سبيل معرفة السلوك المادي والنتيجة الضارة لجريمة الإرهاب الالكتروني بشيء من التفصيل قسمنا هذا العنصر إلى فرعين اثنين، الفرع الأول ويحمل عنوان السلوك الإجرامي والفرع الثاني والذي يحمل عنوان النتيجة الضارة.

---

[1] عبد الله علي عبو سلطان، دور القانون الدولي الجنائي في حماية حقوق الإنسان، أطروحة دكتوراه في القانون العام كلية الحقوق، جامعة الموصل–العراق، 2004/2003، ص72.

[2] يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الإستراتيجية، السليمانية– العراق، 2007، ص 82 .

[3] طارق عبد العزيز حمدي، مرجع سابق، ص 71 .

**أولا: السلوك الإجرامي.**

يعرف السلوك الإجرامي على أنه:" مجموعة الأفعال الجرمية المكونة للجريمة، فلا جريمة دون سلوك إجرامي"[1].

فالسلوك الإجرامي في الجريمة الإرهابية ستمثل في الفعل، أو مجموعة من الأفعال فليس هناك شرط محدد في صفة هذا الفعل، سواء أكان عنيفا أم فعل قوة أو تهديد أو ترويع، فلا يشترط مثلا حدا من الجسامة، بل إن هناك مجموعة من الأفعال تتحقق بمجرد نشر أفكار منحرفة (كتمجيد الإرهاب) فالسلوك الإجرامي يمكن أن يكون قولا أو كتابة أو عملا[2].

ومن اجل ذلك يمكن حصر السلوك الإجرامي فيما يلي:

**- العنف.**

عرف الفقهاء العنف بأنه:" كل سلوك مادي بحت ينشأ منه حدث مادي في شخص كالضرب أو الجرح"، كما عرف أيضا بأنه:" كل فعل يترتب عليه المساس بسلامة الإنسان، قد يكون ماديا أو جرحا بالغا، وقد يكون مساسا معنويا كالتعرض لضوضاء صاخبة أو سماع دوي انفجار ينتج عنه إصابة بصمم"[3].

كما يعرف العنف بأنه:" تجسيد للطاقة أو القوة المادية في الإضرار المادي بشخص آخر أو بشيء، فهو صفة لسلوك إنساني يتحقق عن طريق القوة أو الطاقة المادية الضارة سواء تمثل في عنف شخصي، أو عنف عيني على الأشياء مثل تدمير والتخريب والإتلاف حيث تفترض هذه المصطلحات نوعا معينا من العنف"[4].

[1] يوسف كوران، مرجع سابق، ص 83.

[2] نفس المرجع، ص 83.

[3] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني) مرجع سابق، ص 96.

[4] مأمون سلامة، إجرام العنف، مجلة القانون والاقتصاد ، العدد الثاني للسنة الرابعة والأربعون، جويلية 1974، ص 270 .

وبالتالي يمكن القول أن العنف هو فعل مادي أو معنوي يؤدي بالمساس بسلامة الإنسان ويعتبر العنف الصورة البارزة للجريمة الإرهابية، بل وإنها أخذت الحيز الأكبر من اهتمام الفقهاء في هذا الشأن.

- **التهديد.**

عرف الفقهاء التهديد بأنه إثارة الخوف لدى الغير من ضرر أو شر يصيبه سواء حدث ذلك بالقول أو الكتابة أو الرسم أو الحركة أو الإشارة، وبذلك لا يشترط أن يحدث التهديد بالفعل فقط.

كما عرف التهديد أيضا بأنه:"زرع الخوف في النفس من خلال الوعيد بشر يصيب الإنسان والضغط على إرادته وتخويفه بأمور تمسه أو تمس أشخاص أو أشياء له صلة بها، مثل العرض أو تلويث السمعة"[1].

فالتهديد في حد ذاته يكفي لإثارة الرعب والفزع في نفس الإنسان وبين الناس ، وبهذا يعتبر أوضح صورة يمكن أن تمثل الإرهاب، حتى ولو تصاحبه قوة أو عنف، وإذا كان التهديد في جوهره تعبيرا عن إيقاع الأذى، فان وسائل التعبير عنه يمكن أن تكون كتابية كما يمكن أن تكون شفوية وتستوي كذلك الصور التي تتخذها الكتابة أو العبارات الشفوية كما يستوي أن يكون التهديد صراحة أو ضمنا، طالما استطاع المجني عليه فهم هذا التهديد بغض النظر عن الظروف التي صدر فيها هذا التهديد[2]، وعلى ذلك لا يشترط إفراغ التهديد في عبارات معينة.

وفي هذا الشأن ذكرت محكمة النقض المصرية أن "القانون لم يبين ما هو التهديد، ولم يشترط القانون ذكر عبارات خاصة، وقد ترك الأمر في ذلك الى تقدير المحكمة، فكل عبارة من شأنها إزعاج المجني عليه وإلقاء الرعب في نفسه، أو إحداث الخوف عنده من خطر يراد إيقاع بشخصه، أو ماله يعتبر تهديدا معاقبا عليه"[3]

[1] أحمد محمد أبو مصطفى، الإرهاب ومواجهته جنائيا، أطروحة دكتوراه في القانون،كلية الحقوق، جامعة القاهرة 2007/2006 ، ص 154 .

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني) مرجع سابق، ص 96.

[3] نفس المرجع، ص 97.

وخلاصة ذلك نرى أن السلوك الإجرامي للإرهاب يتألف من صورتين الصورة المعنوية المتمثلة في التهديد، والصورة المادية المتمثلة في العنف وهو ما ذهبت إليه التشريعات في مختلف نصوصها كما وجب أن نشير أن كل من التهديد والعنف أفعال مذكورة على سبيل المثال لا الحصر.

وهو ما أخذ به المشرع المصري حيث لم يقصر السلوك الإجرامي على الجانب المادي فقط بل تعدى ذلك إلى اعتبار التهديد والترويع جزءا لا يتجزأ منه، فبالرجوع إلى نص المادة 86 من قانون العقوبات المصري نجدها تنص على أنه:" يقصد بالإرهاب في تطبيق أحكام هذا القانون كل استخدام للقوة أو العنف أو التهديد أو الترويع..."[1]، كما أضافت هذه المادة أن الجريمة الإرهابية يمكن أن ترتكب عبر الوسائل المعنوية من خلال التهديد والترويع، وكل وسيلة يلجأ إليها الجاني وذلك من خلال استخدام القوة أو العنف أو التهديد أو الترويع [2].

ويرى جانب من الفقه أن السلوك الإجرامي وبالضبط عندما يكون فعلا في الجريمة الإرهابية يكون ايجابيا في جميع الحالات، فالسلوك الايجابي وحده من له القدرة على إحداث خطر عام أو ضرر، ويستنتج من ذلك أن الجريمة الإرهابية ينعدم فيها الفعل السلبي، أي الامتناع عن فعل شيء ما، كما أن معظم الأفعال الإرهابية التي نصت عليها مختلف التشريعات تعتبر أفعال ايجابية كالقتل والتفجير والتخريب[3].

إلا أن المشرع الجزائري يرى خلاف هذا الرأي ويستنتج من خلال نصوصه القانونية المتعلقة بالجريمة الإرهابية أن السلوك الإجرامي في الجريمة الإرهابية يمكن أن يكون ايجابيا كالأفعال المذكورة سابقا، كما يمكن أن يكون سلبيا كالامتناع عن التبليغ على جماعة إرهابية معلومة النشاط أو مكان اختباء إرهابي أو جماعة من الإرهابيين.

أما بالنسبة للركن المادي لجريمة الإرهاب الالكتروني فان ركنها المادي يشترك مع الجريمة المعلوماتية بشكل عام، فهو عبارة عن سلوك يتضمن وجود بيئة رقمية وجهاز كمبيوتر، وتوافر

[1] أضيفت هذه المادة بموجب القانون 97 لسنة 1992 المعدل والمتمم لقانون العقوبات المصري.

[2] أحمد محمد أبو مصطفى، مرجع سابق، ص 155 .

[3] عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة، القاهرة، 2005، ص 71.

الاتصال بشبكة الانترنت، وبالتالي فإن السلوك الإجرامي في جريمة الإرهاب الالكتروني يتم من خلال جهاز الكمبيوتر وباستخدام المعالجة الآلية للمعلومات[1].

وعلى ذلك وجب أن تتم مباشرة النشاط التقني المؤدي إلى الجريمة، حيث أن ذلك يؤثر على بناء الأدلة، وإلا فلا يمكن القول بإمكانية توافر الأدلة لاحقا، فلا جريمة من هذا القبيل إذا بنيت على مجرد الاعتراف[2].

ويظهر السلوك الإجرامي في جريمة الإرهاب الالكتروني بشكل واضح من خلال صور هذه الجريمة المتعددة، فتتوافر عند استخدام تقنية الانترنت لبث الأفكار الإرهابية كاللجوء إلى الانترنت من أجل تعليم الآخرين طرق صناعة القنابل من خلالها أو بث الأفكار الإرهابية والتشجيع على تجنيد الإرهابيين من خلال شبكة الانترنت[3].

ومن الصور المتعددة للركن المادي في جريمة الإرهاب الالكتروني الاعتداء على نظام المعالجة الآلية، وهذه الصورة بدورها تتضمن نوعين من الاعتداء، اعتداء متمثل في الدخول والبقاء غير المشروع في نظام المعالجة الآلية، وتنطوي تحت هذا النوع ثلاث أفعال فعل الدخول والبقاء وعرقلة أو التعطيل ، وأما النوع الثاني متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل،وأما الصور الثانية متمثلة في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي وبالتالي سوف نقصر الركن المادي لجريمة الإرهاب الالكتروني على الصورة الأولى .

## الاعتداءات على أنظمة المعالجة للمعطيات .

يتم هذا الاعتداء بالدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو الاعتداء العمدي على نظام المعالجة الآلية للمعطيات، وكلتا الصورتين صورة من صور الإرهاب الالكتروني ومميزتان لركنه المادي.

---

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، أطروحة دكتوراه في القانون، كلية الحقوق– جامعة عين شمس، القاهرة، 2004/2003، ص 256.

[2] نفس المرجع، ص 256.

[3] فهد يوسف الكساسبة، مرجع سابق،ص 159 .

**الدخول أو البقاء غي المشروع في نظام المعالجة الآلية للمعطيات.**

ويكون هذا الدخول أو البقاء غير المشروع من خلال صورتين، حيث تكون الصورة الأولى من خلال مجرد الدخول أو البقاء غير المشروع في النظام بالنظام دون العبث به أو تغييره وتعرف هذه الصورة بالصورة البسيطة، وأما الصورة الثانية فتعرف بالصورة المشددة وتتحقق بحذف أو تغيير معطيات المنظومة بعد الدخول أو البقاء غير المشروعين، أو تخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين[1] وتعتبر الصورة الثانية هي الشائعة في جريمة الإرهاب الالكتروني.

وقد نصت المادة 323 في فقرتها الأولى من قانون العقوبات الفرنسي بقولها:" فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه يعاقب عليه بالحبس لمدة سنة وبغرامة 100.000 ف.ف، فإذا نتج عن الدخول أو البقاء سواء محو أو تغيير في النظام فإن العقوبة تصبح الحبس لمدة سنتين والغرامة التي تصل إلى 200.000 ف.ف"[2]

أما المشرع الجزائري فقد نص على الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات في المادة 394 مكرر من قانون العقوبات الجزائري وذلك بقولها:" يعاقب بالحبس من ثلاثة أشهر، وبغرامة من 50.000 دج إلى 10.000 دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك .

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج"[3]

---

[1] محمد فريد قورة، نائلة عادل، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2005، ص 223.

[2] القانون رقم 97-1159 المؤرخ في 19 ديسمبر 1997 المتضمن قانون العقوبات الفرنسي.

[3] الأمر 66-155 المؤرخ في 18 صفر 1386هـ الموافق لـ 8يونيو 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

ومن خلال هذين النصين يتضح أن النشاط الإجرامي في الصورة البسيطة يتمثل في الأفعال التالية:

- **فعل الدخول.**

يتحقق فعل الدخول بمجرد الوصول الى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبها، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات[1].

وقد تباينت التشريعات المختلفة حول تحديد محل ركنها المادي في جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات، وبذلك يمكن التمييز بين ثلاث صور للمحل في هذه الجريمة فالصورة الأولى تمثلت في المعلومات في ذاتها، وأما الثانية فتمثلت في أنظمة المعالجة الآلية للمعطيات التي ترتبط فيما بينها من خلال شبكة الاتصال، والثالثة شبكات المعلومات .

وتمخض عن هذا التباين ثلاث اتجاهات، موسع يجمع بين الصور الثلاث ويتخذها جميعا كمحل الجريمة وهي المعلومات الواسعة للمعالجة الآلية للمعطيات وشبكات المعلومات، وتبنى هذا الاتجاه المشرع الفرنسي ونحى نحوه المشرع الجزائري، وأما الاتجاه الثاني فقد استبعد شبكات المعلومات من نطاق التجريم، ويتبنى هذا الاتجاه المشرع الانجليزي، وأما الاتجاه الثالث فقد جرم فعل دخول عبر شبكات المعلومات وتبنى هذا الاتجاه التشريع السويسري[2].

وتجدر الإشارة إلى أن جريمة دخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية، لأنها لا تشترط تحقق النتيجة يكفي الوصول إلى المعلومات المخزنة داخل النظام، فبمجرد الوصول إليها تقوم الجريمة فيرتكب فعل الدخول بأية طريقة أو وسيلة كانت لأن المشرع الجزائري لم يحددها[3] .

ويستوي أن يتم الدخول بطريق مباشر يستطيع من خلاله الجاني الوصول إلى المعلومات المخزنة لدى الأنظمة باستخدام الشاشة والاطلاع بالقراءة على ما هو مكتوب عليه وباستخدام آلة طباعة مرفقة

[1] محمد فريد قورة، نائلة عادل، مرجع سابق، ص 323.

[2] نفس المرجع، ص 323.322 .

[3] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2007، ص 100

بجهاز الحاسب الآلي استخراج قائمة البرامج الموجودة داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالالتقاط المعلوماتي بعد التقاط المعلومات المتواجدة في الحاسب الآلي والتقاط الإشعاعات الالكترومغناطيسية المنبعثة من الجهاز المعلوماتي.

- **فعل البقاء.**

ويقصد بالبقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، ويتحقق هذا البقاء غير المشروع عند دخول شخص في نظام بتصريح ولكن تجاوز المدة المسموح له بالبقاء، أو يكون ذلك التحول خطأ أو سهو في نظام آخر ولم ينسحب فورا ولا يقطع وجوده، أو يقوم بطبع نسخة من المعلومات في حين سمح له بالرؤية فقط هنا تقوم جريمة البقاء غير المشروع في نظام المعالجة آليا للمعطيات[1].

ويجتمع فعل البقاء مع فعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات فالجاني عندما يدخل للنظام دون وجه حق أي أنه يدخل عن طريق الغش ويبقى داخل النظام عد ذلك بقاء إلا أن كل من المادتين 1/323 من قانون العقوبات الفرنسي والمادة 394 مكرر من قانون العقوبات الجزائري نصتا فقط على الدخول غير المشروع دون النص على البقاء غير المشروع ، وفي هذا الصدد جرمت محكمة الاستئناف في باريس في حكمها في 05 أفريل 1994 البقاء غير المشروع سواء تم بطريقة مشروعة داخل نظام المعالجة الآلية للمعطيات إلا أنه اكتسب بعد ذلك صفة عدة المشروعية[2].

بالرجوع إلى نص المادة 394 مكرر في فقرتيها 2 و 3 من قانون العقوبات الجزائري نجدها تشدد عقوبة جريمة الدخول والبقاء غي المشروع عندما ينتج عن هذين الفعلين إما محو أو تحويل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه نتيجة تخريبه، ومن المعلوم أن ظرف التشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية حينها يمكن القول أن الشرط متوافر.

[1] أمال قارة، مرجع سابق، ص 110.

[2] محمد فريد قورة، نائلة عادل، مرجع سابق، ص 347.

فحسب المادة 394 مكرر شدد المشرع عقوبة المحو وتعديل المعطيات كل واحد منها على حذا وكذا تخريب اشتغال المنظومة والتي عقوبتها أشد لأن عقوبة المحو أو التغيير هي ضعف عقوبة الدخول والبقاء غير المشروعين ، وفي هذه الحالة خالف المشرع الجزائري المشرع الفرنسي الذي جمع بين المحو أو التغيير والتخريب في فقرة واحدة وأعطاها عقوبة واحدة من خلال المادة 323 في فقرتها الأولى من قانون العقوبات الفرنسي[1].

## الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.

لم ينص المشرع الجزائري على الاعتداء العمدي على سير النظام بنص خاص واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة داخل النظام ويرجع تفسير هذا الموقف للمشرع الجزائري أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام ووظائفه[2].

وبالرجوع إلى نص المادة 323 في فقرتها الثانية من قانون العقوبات الفرنسي نجدها تنص على هذه الصورة وذلك بقولها:" بمجرد إعاقة أو إفساد اشتغال نظام المعالجة الآلية للمعطيات".

كما نصت على ذات الصورة كل من المادتين 5 و8 من اتفاقية بودابست لسنة 2001 [3]، وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 نصت على هذه الصورة من خلال المادة السادسة منها والتي نصت على أنه:" جريمة الدخول غير المشروع:

1. الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

[1] أمال قارة، مرجع سابق، ص 114.

[2] نفس المرجع، ص 190.

[3] تنص المادة 5 من اتفاقية بودابست لسنة 2001 على أنه:" يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم، تبعا لقانونه المحلي، الإعاقة الخطيرة إذا تم ذلك عمدا ودون حق لوظيفة نظام الحاسب عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية"

أما المادة 8 فتنص:" يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم تبعا لقانونه الداخلي عمدا ودون حق التسبب في إحداث ضرر مالي للغير عن طريق:

1. الإدخال، الإتلاف، المحو، أو الطمس لبيانات الحاسب.
2. كل شكل للاعتداء على وظيفة الحاسب بنية الغش نية إجرامية مشابهة من أجل الحصول دون حق على منفعة اقتصادية له أو للغير"

2. تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ- محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين

ب- الحصول على معلومات حكومية سرية".

وكذلك نص المادة الثامنة من نفس الاتفاقية والتي جاءت بعنوان "الاعتداء على سلامة المعلومات" بقولها:"

1. تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.
2. للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة ، أن تتسبب بضرر جسيم"[1].

وتجدر الإشارة إلى أن الفقه اختلف حول ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات، ومع عدم وجود نص خاص بالاعتداءات العمدية على نظام المعالجة الآلية للمعطيات في التشريع الجزائري فإن الاعتداءات على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب، وتتمثل السلوكات الإجرامية في هذه الاعتداءات في فعل عرقلة أو تعطيل والإفساد لنظام المعالجة الآلية للمعطيات عن أداء نشاطه العادي والمنتظم منه القيام به[2].

**التعطيل (العرقلة):** فالمشرع لم يشترط الوسيلة التي يتم بها فعل التعطيل، فقد تكون مادية أو معنوية سواء اقترنت بعنف أم لا ككسر الأجهزة المادية للنظام، أو تحطيم الأسطوانة وتكون معنوية إذا وقعت الكيانات المنطقية للنظام مثل البرامج والمعطيات بإتباع تقنيات إدخال برنامج فيروسي، أو استخدام قنابل منطقية تجعل النظام يتباطأ في أداء وظائفه إلى غيرها من التقنيات التي تلجأ إليها وتستغلها التنظيمات الإرهابية لتحقيق أهدافها الإرهابية باستعمال الانترنت.

[1] الاتفاقية العربية لمكافحة تقنية نظم المعلومات التي وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بالقاهرة بتاريخ 1432/01/15 هـ الموافق لـ 2010/12/21.

[2] أمال قارة، مرجع سابق، ص 113.

**الإفساد:** وهو كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

ومن صور الركن المادي في جريمة الإرهاب الالكتروني الاعتداءات العمدية على المعطيات المواد 3، 4، 8 من الاتفاقية الدولية لمكافحة الإجرام المعلوماتي لسنة 2001 وكذلك نص المادة 323 من قانون العقوبات الفرنسي بقولها:" كل من أدخل بطرق الغش المعطيات بنظام المعالجة الآلية للمعطيات أو محا أو عدل..."

وبالإضافة إلى ذلك نصت المادة 394 مكرر 2 من قانون العقوبات الجزائري على الاعتداءات العمدية بنصها:" يعاقب بالحبس من شهرين إلى ثلاث سنوات، وبغرامة من 100.00.00 دج إلى 500.00.00 دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"[1].

ومما سبق يتضح أن السلوك الإجرامي في جريمة الإرهاب الالكتروني يتجسد في صورتين، تتمثل الصورة الأولى في الاعتداءات العمدية على المعطيات الموجودة والتي تتجسد في أفعال ثلاث: الإدخال والمحو والتعديل، ولتوافر الركن المادي لهذه الجريمة لابد من توافر هذه الأفعال، إلا أنه لا يشترط توافرها مجتمعة بل يكفي توافر بعضها[2] .

ففعل الإدخال هو إضافة معطيات جديدة على الدعاية الخاصة سواء كانت خالية، أو موجود عليها معطيات من قبل، وأما فعل المحو فهو إزالة جزء من المعطيات المسجلة داخل النظام، وذلك بتحطيم الدعامة أو نقل أو تخزين جزء من المعطيات في ذاكرة مختلفة، وعن التعديل فهو تغيير

[1] الأمر رقم 66 /156 السالف الذكر.

[2] أمال قارة، مرجع سابق، ص 120.

المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، ويتحقق ذلك عن طريق برامج تتلاعب في المعطيات سواء بالمحو الكلي أو الجزئي وذلك بواسطة برامج الفيروسات– كما سبق توضيحها– .

وأما الصورة الثانية المميزة للسلوك الإجرامي في جريمة الإرهاب الالكتروني فتتمثل في المساس العمدي بالمعطيات خارج النظام، وقد نص المشرع الجزائري على هاتين الصورتين في قانون العقوبات بحيث تتعلق الأولى بحماية المعطيات من استعمالها في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، والثانية تتعلق بحماية المعطيات المتحصل عليها من هذه الاعتداءات وذلك من خلال نص المادة 394 مكرر 2 السالفة الذكر.

ويكمن الفرق بين هاتين الصورتين والمنصوص عليهما في نفس المادة (394 مكرر 2) في أن الصورة الأولى تكون فيها المعطيات وسيلة لارتكاب هذه الاعتداءات، فالحماية التشريعية في هذه الحالة تخصها قبل ارتكاب الاعتداءات، أما الصورة الثانية فتكون المعطيات هي المحصلة أو نتيجة لارتكاب الاعتداءات الماسة بالأنظمة والحماية التشريعية في هذه الصورة تهدف إلى الوقاية من ارتكاب جريمة أخرى[1]

وبالرجوع إلى التشريعات المختلفة كالتشريع الجزائري والفرنسي والعراقي وغيرها يستنتج أن السلوك الإجرامي في جريمة الإرهاب الالكتروني على اعتباره عنصر مهم من عناصر الركن المادي يمر بثلاث مراحل:

1. **الأعمال التحضيرية:** تعتبر هذه المرحلة أولى مراحل تنفيذ الجريمة، حيث يعد فيها الجاني العدة لتنفيذ الجريمة دون أن يرتكب أي عمل من أعمال التنفيذ كأن يحضر أجهزة كمبيوتر ويوصله بشبكة المعلومات، أو أن يجمع معلومات حول مواقع معينة مستهدفة من أجل إيجاد طريقة لاختراقها وقد لا يعاقب القانون على الأعمال التحضيرية في الجرائم البسيطة وفي الحالات العادية، إلا في حالة الجرائم الإرهابية والجرائم ضد أمن الدولة فإن الأمر يختلف، ففي هذه الحالة يمكن للقانون أن يجرم هذه الأعمال ويحدد لها عقوبة[2].

[1] محمد فريد قورة، نائلة عادل، مرجع سابق، ص 366 .

[2] عمار تيسير بجبوج، مرجع سابق، ص 124.

**2. أعمال بدء التنفيذ:** أو ما يعرف بالشروع، وفي هذه المرحلة يتجاوز الجاني الأعمال التحضيرية باتخاذ القرار والخطوة النهائيين نحو ارتكاب الجريمة، وفي هذه الحالة فان القانون يعاقب على هذه المرحلة مهما كان نوع الجريمة سواء كانت جريمة بسيطة أو إرهابية أو جرائم ضد امن الدولة ....

وقد نص المشرع الجزائري على الشروع في نص المادة 30 من قانون العقوبات الجزائري بقوله:" كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"[1].

أما فيما يتعلق بالجريمة الإرهابية فمن المسلم به أن جريمة الشروع فيها تفترض خيبة السلوك الإجرامي المرتكب من طرف الإرهابي وإيقافه أو خيبة أثره في تحقيق النتيجة الجرمية التي يهدف إلى تحقيقها وذلك بسبب لا دخل لإرادته فيها، ونصت الاتفاقيات الدولية والإقليمية على معاقبة الشروع في الجرائم الإرهابية، حيث نصت المادة 12 في فقرتها الأولى من القانون النموذجي للإرهاب الذي أعده مكتب الأمم المتحدة للجريمة والمخدرات على معاقبة أي شخص يشرع في ارتكاب إحدى جرائم الإرهاب، وتركت للمشرع الوطني تحديد العقوبة بمراعاة جسامة الجريمة[2]، ومن اجل ذلك تميل جميع النصوص العقابية في جميع دول العالم إلى اعتبار الجرائم التي من شأنها المساس بالأمن العام جرائم تامة، بغض النظر عن تحقق نتيجة السلوك الإجرامي أم لا، وفي هذا السياق نصت المادة 108 من قانون العقوبات الأردني على أنه:" يعد الاعتداء على أمن الدولة تاما سواء أكان الفعل المؤلف جريمة تاما أم ناقصا أم مشروعا فيه"[3]، وهذا بالنظر لما ينجم عن الجرائم الإرهابية وغيرها من الجرائم الماسة بأمن الدولة بالغة على الأمن من أخطار والاستقرار وسلامة المجتمع، فمن يشرع في ارتكاب جريمة إرهابية يعامل معاملة من يرتكب هذه الجريمة كاملة وهذا من اجل تحقيق الردع العام والخاص وعلى هذا الأساس يعتبر الشروع في الجريمة الإرهابية جريمة مستقلة وقائمة بذاتها[4] .

---

[1] الأمر رقم 156/66 السالف الذكر.

[2] أحمد فتحي سرور، مرجع سابق، ص 309.

[3] القانون رقم 16 لسنة 1960 المتضمن قانون العقوبات الأردني، والمعدل بموجب القانون رقم 12 لسنة 2010.

[4] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 111.

وتجدر الإشارة إلى أن التشريعات المتعلقة بمكافحة الإرهاب لم تجرم الأعمال التحضيرية في كل الحالات وهذا عملا بالقواعد العامة حيث أن القانون لا يعاقب على النوايا، غير أن التخطيط لارتكاب الجريمة الإرهابية تعتبر جريمة قائمة بذاتها ولا تعتبر شروع، كتولي قيادة جماعة تمارس الأعمال الإرهابية وتخطط له وكذلك المساهمة والاشتراك في هذا العمل[1].

ومن المسلم به أن الشروع في الجريمة الإرهابية الالكترونية –على اعتبارها موضوع الدراسة– يفترض خيبة السلوك الإجرامي الإرهابي وإيقافه أو خيبة أثره في تحقيق النتيجة التي يترجاها الإرهابي لسبب خارج عن إرادته، وفي هذا الشأن نصت الاتفاقيات الدولية والإقليمية على معاقبة الشروع في الجرائم الإرهابية حيث نصت المادة 12 فقرة 01 من القانون النموذجي للإرهاب الذي أعده مكتب الأمم المتحدة للجريمة والمخدرات على معاقبة أي شخص يشرع في ارتكاب إحدى جرائم الإرهاب تاركا للمشرع الوطني تحديد العقوبة مراعاة لجسامة الجريمة[2].

وبما أن جريمة الإرهاب الالكتروني تعتبر إحدى الجرائم الإرهابية، فهي الصورة المستحدثة لها حيث تغيرت وسيلتها لتواكب التطور التكنولوجي المذهل الذي عرفه العالم المعاصر فإنها تدخل ضمن نطاق تطبيق نص المادة سالفة الذكر.

وفي هذا الشأن نجد المشرع الأردني أيضا حذا حذو القانون النموذجي حيث اعتبر أن الاعتداء على امن الدولة يعتبر جريمة تامة سواء كان الفعل المكون للجريمة تاما أو ناقصا أم مشروعا فيه[3] وهذا نظرا لما يشكله هذا النوع من الجرائم من خطورة بالغة على الأمن والاستقرار وسلامة المجتمع وبالتالي يعامل من يشرع في الجريمة الإرهابية معاملة من يرتكب السلوك الإجرامي كاملا وهذا لتحقيق الردع العام والخاص، وقد أطلق الفقه الايطالي على هذه الحالة( أي المعاقبة على الشروع وكأنه جريمة تامة) تسمية الجرائم مبكرة الإتمام[4].

---

[1] المادة 87 مكرر3 من الأمر رقم 156/66 السالف الذكر.

[2] أحمد فتحي سرور، مرجع سابق، ص 309.

[3] المادة 108 من قانون العقوبات الأردني.

[4] عبد الفتاح مصطفى الصيفي، الاعتداء الواقع على أمن الدولة والأموال– قانون العقوبات اللبناني، دار النهضة العربية، بيروت، 1972، ص 18.

وعليه إذا كان لا يتصور شروع في الجريمة الإرهابية التقليدية على النحو الذي سبق وشرحناه فانه لا يتصور شروع في جريمة الإرهاب الالكتروني وذلك من ناحيتين، الأولى هو أن الإرهاب الالكتروني ما هو إلا شكل متطور وحديث للجريمة الإرهابية، فما تغير في جريمة الإرهاب الالكتروني سوى أن الوسيلة المستخدمة في هذه الجريمة تطورت وأصبحت وسيلة تقنية حديثة.

وأما الناحية الثانية هو أن جريمة الإرهاب الالكتروني هي في أصلها جريمة معلوماتية (الكترونية)، ففي الجريمة الالكترونية حتى الأعمال التحضيرية تعتبر جرائم في حد ذاتها، فشراء برامج الاختراق يعتبر عمل تحضيري ولكنه في نفس الوقت جريمة قائمة بذاتها[1].

3. **النشاط الإجرامي (الجريمة التامة):** بالوصول إلى هذه المرحلة يكون الجاني قد استنفذ كل المراحل السابقة من تفكير، ورغبة وأعمال تحضيرية، وبدء في التنفيذ إلى غاية إتمام الجريمة وتحقيق النتيجة التي يرجوها.

وتجدر الإشارة إلى أنه وبالإضافة إلى كل ما سبق فان التشريعات المتعلقة بالجريمة الإرهابية قد أضافت شرطا آخر بالنسبة للأفعال المكونة للسلوك الإجرامي ويتمثل في أن الأفعال السابقة وجب أن تكون تنفيذا لمشروع إجرامي إرهابي فردي أو جماعي[2].

المشرع العراقي أيضا حذا حذو المشرع الجزائري فيما يتعلق بالركن المفترض للجريمة الإرهابية وذلك من خلال نصي المادتين الأولى والثانية من قانون مكافحة الإرهاب العراقي[3]، وكذلك المشرع المصري الذي لم ينص على هذا الركن صراحة ولكنه يستنتج من عبارة " تنفيذا لمشروع إجرامي فردي أو جماعي"، وكان بذلك متأثرا بالمشرع الفرنسي من خلال المادة 706 من قانون الإجراءات الفرنسي[4].

ويرى الفقه أن الركن المفترض في الجريمة الإرهابية يتمثل في الدافع في ارتكاب هذه الجريمة سواء كان سياسيا أو دينيا أو طائفيا أو قوميا وعرقيا أو عسكريا أو اقتصاديا...

[1] عماد مجدي عبد الملك، مرجع سابق، ص 37.

[2] المادة 87 مكرر من قانون العقوبات الجزائري.

[3] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 93.

[4] أحمد محمد أبو مصطفى، مرجع سابق، ص 150.

وبالرجوع إلى الاتفاقية العربية لمكافحة الإرهاب نجدها تنص هي الأخرى على مصطلح "المشروع الإجرامي " لكنها لم تعرفه، إلا أن الفقه يرى أن المشروع الإجرامي هو هدف الجاني لارتكاب جريمة تتطلب وقتا من التخطيط والتروي قبل اقترافها، سواء اتخذ هذا المشروع طابع الفردية أو الطابع الجماعي، فالمشروع الإجرامي في الجريمة الإرهابية هو كل جهد أو نشاط يقوم به شخص لتحقيق غاية معينة مادية كانت أو معنوية ويستوي في ذلك أن كانت أغراض هذا المشروع تحقيق مكاسب مالية أو معنوية محضة كالعمليات الإرهابية التي تعبر عن التطرف الديني أو تقوم لأغراض انتقامية[1].

## ثانيا: النتيجة الجرمية.

يعرف الفقه النتيجة الإجرامية بأنها الأثر اللازم للفعل المجرم وتمس إما الأشياء أو الأشخاص وهي إما تعبر عن حقيقة مادية تحدث في العالم الخارجي كأثر للفعل الإجرامي، أو تعبر عن حقيقة قانونية لأنها لا يترتب عليها ضرر، لكنها تمس قيم المجتمع كالجرائم الشكلية، فالجرائم الشكلية ليس لنتيجتها وجود مادي أو ضرر مجتمعي فهذا النوع من الجرائم يعاقب عليها القانون وأن لم تنتج عليها نتيجة ضارة لأنها تمثل مجموعة مصالح يعاقب عليها القانون، أما النتيجة التي يتناولها المشرع كحقيقة قانونية ويطلق عليها النتائج القانونية، والتي تنقسم إلى جرائم الضرر كالقتل والسرقة والإرهاب وجرائم الخطر المحتمل كجرائم الغش التجاري[2].

وتجدر الإشارة أن بعض الفقه قسم نتائج الفعل الإجرامي إلى[3]:

- **نتيجة قانونية مجردة:** وتكون في الجرائم الشكلية أو ما يعرف بالجرائم غير ذات النتيجة، أنها تقصر على حماية قيم مجتمعية ومصالح وحقوق عامة، فهذه الجرائم ليس لها واقع مادي محسوس وملموس سوى حيازة محل الجريمة الذي نص عليه القانون، وعليه فانه لا يمكن حصول النتيجة الإجرامية في هذه الجرائم الشكلية .

[1] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 94.

[2] محمود عبد العزيز محمد، مرجع سابق، ص 196.

[3] نفس المرجع، ص 197.

وجريمة الإرهاب الالكتروني من حيث النتيجة تعتبر من جرائم الخطر التي لا يشترط فيها المشرع عناصر الركن المادي، من سلوك ونتيجة وعلاقة سببية، فالمشرع يفترض فيها الخطر المتمثل بنتيجتها، فبمجرد قيام السلوك الخارجي المحدد بنصوص القانون تقوم الجريمة ويتم العقاب عليها[1].

- **نتيجة مادية ملموسة محسوسة:** وهي تلك النتائج التي لها وجود مادي، وهو ما يعرف بالجرائم ذات النتيجة .

والنتائج الجرمية لابد أن تمس الحقوق والمصالح التي يحميها القانون والتي تتعلق بالأشخاص الطبيعية أو الاعتبارية سواء في أنفسهم أو في ممتلكاتهم، وكذا فيما يتعلق بالأموال العامة سواء كانت مملوكة على الإطلاق للدولة، أو كانت الدولة شريك فيها[2].

فالنتيجة الجرمية في الجريمة الإرهابية تتمثل في إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بالاتصالات أو بالمواصلات أو بالأموال العامة أو الخاصة أو بالمباني أو بالأملاك العامة أو الخاصة وذلك باحتلالها أو بالاستيلاء عليها أو منع أو عرقلة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها ...[3].

إلا أن الجرائم الإرهابية لا تعتبر جميعها من قبيل الجرائم الشكلية، فالقانون لا يتطلب لقيام الجريمة التامة تغيير في العالم الخارجي حتما كأثر للفعل المجرم، فقد يقوم الإرهابي بوضع متفجرات في مكان عمومي لكنها لا تنفجر، فهنا تخلفت النتيجة بسبب خارج عن إرادة الجاني ويعاقب عقوبة الجريمة التامة .

وتجدر الإشارة أن جميع الأعمال المنصوص عليها في المواد 87 مكرر إلى غاية 78 مكرر 11 من قانون العقوبات الجزائري معاقب عليها بصرف النظر على الضرر أو النتائج المترتبة عنها، فـــقد

[1] مصطفى سعد حمد خلف، جريمة الإرهاب عبر الوسائط الالكترونية –دراسة مقارنة بين التشريعين الأردني والعراقي مذكرة ماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، كانون الثاني 2017، ص 50.

[2] والمثال على ذلك المادة 119 قانون العقوبات المصري، والمادة 87 مكرر من قانون العقوبات الجزائري.

[3] محمود عبد العزيز محمد، مرجع سابق، ص 198.199.

اعتبرها المشرع جنايات بالنظر إلى خطورتها، أما مسالة ما هو المدلول الذي اخذ به المشرع هل هو مادي أم قانوني فقد مازال محل خلاف.

وبما أن جريمة الإرهاب الالكتروني تعتبر من الجرائم ذات النتيجة القانونية، فهي تعتبر من الجرائم المبكرة، لان المشرع يبادر في تجريمها في مرحلة السلوك ولا يتريث حتى تحقيق النتيجة وهذا يعتبر في حد ذاته ميزة تخص هذه الجريمة، كما تتميز أيضا بعدم التوازي بين ركنيها المادي والمعنوي، فيفترض في الجاني انه يقصد الأضرار بالمصلحة أو الحق الذي يحميه القانون[1].

وعموما تتمثل النتيجة الجرمية في جريمة الإرهاب الالكتروني في أمرين:

- وجود خطر عام
- حدوث الضرر

فالهدف من وراء جرائم الإرهاب سواء في صورته التقليدية أو المستحدثة (إرهاب الكتروني) هو إيجاد حالة من حالات الرعب وعدم الاستقرار في المجتمع، وحتى تتحقق حالة الخطر العام وجب أولا أن يقترن السلوك الجرمي بانتهاك حقوق الأفراد وحرياتهم فالأفعال الإرهابية تعد من جرائم الخطر التي تهدد المن الاجتماعي لما تبعثه من رعب في نفوس الآخرين فالاعتداء على حقوق الآخرين قد يكون على شكل تهديد بالقتل عن طريق البريد الالكتروني الذي يبعثه الإرهابي إلى الشخص المستهدف من العملية الإرهابية الالكترونية بدوافع إرهابية[2].

أما ثانيا وجب أن يخل هذا السلوك الإجرامي بالنظام العام، فيهدف الإرهابي من وراء أفعاله الإرهابية تعطيل وظائف وسبل الحياة، كشن هجوم الكتروني على مواقع للشرطة أو الجيش أو... بهدف إحداث اضطرابات تؤدي إلى النيل من النظام القانوني أو السياسي أو الإداري في دولة ما، أو إحداث فتنة طائفية عن طريق إنشاء مواقع متطرفة، وإما ثالثا فيجب أن يحقق هذا السلوك الإجرامي الضرر سواء كان هذا الضرر نفسي ومعنوي أو مادي[3].

[1] مصطفى سعد حمد مخلف، مرجع سابق، ص 51 .

[2] عصام عبد الفتاح عبد السميع مطر، مرجع سابق، ص 80.

[3] يوسف كوران، مرجع سابق، ص 88.

**ثالثا: العلاقة السببية.**

يقصد بالعلاقة السببية بين الفعل المجرم والنتيجة الصلة الموجودة بينهما، وتقوم هذه الرابطة السببية في جريمة ما عندما تكون النتيجة الواقعة محتملة الوقوع وفقا للسير العادي للأمور[1].

فللعلاقة السببية أهمية بالغة تكمن في كون الركن المادي في كل جريمة لا يكتمل كون وجود هذه العلاقة السببية، فبهذه العلاقة تتقرر المسؤولية الجنائية للجاني بشأن هذه الجريمة المرتكبة.

وعليه فإذا انتفت العلاقة السببية فان مسؤولية مرتكب الفعل تقتصر على الشروع إذا كانت النتيجة مقصودة، أما إذا كانت غير مقصودة فلا مسؤولية عليها، فعلاقة السببية عنصر من عناصر الركن المادي وشرط لازم لقيام المسؤولية الجزائية .

فالسببية علاقة بين سبب ومسبب ومن اجل ذلك تعتبر صلة رابطة بين ظاهرتين حسيتين ترتبطان على نحو ضروري لازم في تعاقب زمني يفيد أن احدهما سبب للآخر[2].

أما عن العلاقة السببية في جريمة الإرهاب الالكتروني فكما وضحنا سابقا أنها من جرائم الخطر ومن اجل ذلك فلا يشترط في هذه الجريمة وجود علاقة سببية بين فعل الفاعل والنتيجة، فيكفي أن يقوم الجاني بفعله فتقوم مسؤوليته دون أن نبحث في هذه العلاقة السببية.

وفي الأخير وكخلاصة على هذا العنصر نقول أن الركن المادي في جريمة الإرهاب الالكتروني تتنوع صوره وأشكاله، وهي تتوافر بتحقق إمكانية إيقاع الفعل باستخدام تقنية أنظمة المعلومات، وفي كل حالة يرتبط فيها النشاط موضوع الفعل بنطاق الكتروني يعتمد عليه شريطة تحقق ما يلي[3]:

- استخدام قدر كافي من العنف التهديدي، وفي الحقيقة فان العنف المقصود في هذه الجريمة وهو عنف معنوي، بمعنى ينظر إلى العنف كنتيجة لسلوك معنوي الكتروني، إذ يمكن لذلك

[1] يوسف كوران، مرجع سابق ، ص 89.

[2] مصطفى سعد حمد مخلف، مرجع سابق، ص 51.

[3] أسامة أحمد المناعسة، جلال محمد الزعبي، مرجع سابق، ص 323.

تصور عنف معنوي ظاهر في مدى قدرة الفاعل على استخدام تقنية أنظمة المعلومات بقدر كافي لإيقاع الضرر المقصود، أما التهديد بالعنف فأمر وارد جدا في ظل البيئة الالكترونية[1].

- أن يكون من شان هذا العنف أو التهديد به إيقاع الرعب بين الناس أو تعريضهم للخطر
- وأن يتبع هذا العمل تنفيذا لعمل فردي أو جماعي .

وعليه ومما سبق يمكن تصور أشكال السلوك المادي القادر على إظهار الإرهاب الالكتروني إلى حيز الوجود كجرائم مستوجبة العقاب ومن ذلك[2]:

1. استخدام العنف أو التهديد به وذلك بدافع تعريض أمن المجتمع للخطر أو الإخلال بالنظام العام، وهنا لا يشترط تحقيق النتيجة الضارة أو الإخلال فقط، بل يكفي احتمال وقوعه، كتلاعب الفاعل بأنظمة إدارة وتشغيل الإشارة الضوئية، أو اختراق الجاني لأنظمة ضخ الغاز عبر منشآت الدولة الحيوية، أو التهديد بتغيير مساره أو درجات الضغط فيه.
2. استخدام العنف أو التهديد باستخدامه بهدف إلحاق الضرر بالبيئة أو المرافق العامة ويكفي احتمال ذلك كالتلاعب بأنظمة المياه والكهرباء ومعدلاتها وجودتها وتوزيعها من خلال استخدام أنظمة المعلومات .
3. استخدام العنف أو التهديد باستخدامه بهدف الإضرار بالموارد الوطنية أو تعريضها للخطر أو استخدامه بهدف تعطيل أحكام الدستور والقوانين.
4. كذلك يمكن أن تكون صورة الركن المادي القيام بأية عملية مصرفية الكترونية داخلية أو خارجية تتعلق بإيداع الأموال لدى أحد البنوك من إحدى المؤسسات المالية التي تقوم ببعض النشاطات المالية كبنوك الصرافة، أو القيام بعملية تحويل أموال الكترونية لتلك الأموال بهدف تمويل جماعات أو منظمات إرهابية[3].
5. استخدام العنف أو التهديد باستخدامه بهدف تعطيل الاتصالات أو أنظمة الحاسوب أو بهدف اختراق شبكات تقنية أنظمة المعلومات أو التشويش عليها .

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، مرجع سابق ، ص 323.

[2] المادة 87 مكرر 12 من القانون 156/66 السالف الذكر.

[3] أسامة أحمد المناعسة، جلال محمد الزعبي، مرجع سابق، ص 324.

6. القيام بأي عمل الكتروني من شأنه تعريض نظام الحكم السياسي في أي دولة للخطر أو التحريض على مناهضته بعمل جماعي أو فردي، أو تغيير كيان الدولة الاقتصادي أو الاجتماعي أو أوضاع المجتمع الأساسية[1].

وتجدر الإشارة إلى أن القيام بأي عمل الكتروني أو التهديد به يجوز أن يعرض أمن المجتمع وسلامته للخطر، أو يخل بالنظام العام سواء كان هذا الفعل أو التهديد به ذو صلة بعمل فردي أو جماعي شريطة أن يقع ضمن نطاق التجريم .

ومن نطاق هذا التجريم المتعلق بالإرهاب الالكتروني:

- تجريم كافة أشكال وصور عمليات تمويل الإرهاب وجمع التمويل للعمليات الإرهابية بواسطة تقنية المعلومات.
- تجريم كافة أشكال وصور تسهيل الاتصالات بين الجماعات الإرهابية عبر تقنية نظم المعلومات، أو تجريم كافة صور وأشكال التدريب على الأعمال الإرهابية كنشر فيديوهات صناعة الأسلحة وكيفية القتال أو كيفية اختراق المواقع أو تدميرها.

وقد تنبه المشرعين حديثا لهذا الخطر ومثال ذلك المشرع الجزائري فنص في القانون 02/16 المعدل لقانون العقوبات الجزائري[2]، في مادته 87 مكرر 12 وذلك بقوله:" يعاقب بالسجن المؤقت من خمس سنوات (05) إلى عشر سنوات(10)، وبغرامة من 100.000 دج إلى 500.000 دج كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو ينظم إعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة"

[1] المادة 149 من قانون العقوبات الأردني رقم 16 لسنة 1960 والتي جاء فيها:" يعاقب بالأشغال الشاقة المؤقتة كل من أقدم على أي عمل من شأنه تعريض نظام الحكم السياسي في المملكة للخطر أو التحريض على مناهضتها وكل =من أقدم على أي عمل فردي أو جماعي بقصد تغيير كيان الدولة الاقتصادي أو الاجتماعي وأوضاع المجتمع الأساسية"

[2] القانون رقم 02/16 المؤرخ في 19 يونيو 2016 يتمم الأمر 156/66 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات الجزائري، الجريدة الرسمية عدد 37 للسنة الثالثة والخمسون، الصادرة في 22 يونيو 2016 م

أيضا المشرع الأردني يعتبر من المشرعين العرب السباقين في هذا الشأن حيث نص في المادة العاشرة (10) من قانون جرائم أنظمة المعلومات والتي تنص[1]:"كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو انشأ موقعا الكترونيا لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة".

ومن خلال نصي المادتين 78 مكرر12 من قانون العقوبات الجزائري والمادة 10 من قانون جرائم أنظمة المعلومات الأردني نستنتج ظهور السلوكيات الجديدة والمستحدثة والتي ارتبطت بتقنية المعلومات والاتصالات والتي تدعم صور الركن المادي لجريمة الإرهاب الالكتروني –التي سبق وان تعرضنا لها بشيء من التفصيل– وهذه السلوكيات تتمثل في:

- استخدام تقنية المعلومات أو الشبكات المعلوماتية لتسهيل القيام بأعمال وعمليات إرهابية.
- استخدام الشبكات المعلوماتية في إنشاء مواقع الكترونية لدعم تنظيم أو جماعة أو جمعية إرهابية أو استغلال هذه المواقع المنشأة للترويج لإتباع أفكار جمعية أو جماعة أو جمعية إرهابية أو لغرض تمويل هذه الجمعية أو الجماعة أو التنظيم الإرهابي.

هذا وقد أشارت الاتفاقية العربية لمكافحة تقنية نظم المعلومات[2] إلى العديد من السلوكيات التقنية المتعلقة بالإرهاب الالكتروني، وذلك في المادة الخامسة عشر منها (15) وتتمثل هذه السلوكيات في ما يلي:

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

[1] قانون رقم 30 لسنة 2010 المتضمن جرائم أنظمة المعلومات الأردني .

[2] الاتفاقية العربية لمكافحة تقنية نظم المعلومات لسنة 2010.

ومن أجل ذلك وجب على الدول الموقعة على هذه الاتفاقية تعديل تشريعاتها الداخلية بما يتماشى مع هذه الاتفاقية، بالإضافة إلى إضافة بعض السلوكيات التي يمكن أن تدرج تحت جرائم الإرهاب الالكتروني، والتي لابد من أن يتنبه المشرع لها ويدرجها ضمن نصوص تجريمية واضحة نظرا لخطورتها، ومن ذلك استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات لنشر طرق صناعة الأسلحة والمتفجرات، أو لوضع تصورات عن كيفية التخطيط أو التنفيذ لعمليات إرهابية معينة[1].

**الفرع الثاني: الركن المعنوي.**

إذا كان الركن المادي في أي جريمة يضم العناصر المادية لها أو يمثل مادياتها فإن الركن المعنوي يضم عناصرها النفسية، وذلك لأن الجريمة ليست كيانا ماديا بحتا قوامه الفعل أو السلوك المجرم وكذلك أثره، بل هي كذلك الكيان النفسي الذي قوامه العناصر النفسية المكونة لها أو ما اصطلح على تسميته بالركن النفسي أو المعنوي أو الشخصي للجريمة.

وقد اختلف الفقهاء في وضع تعريف محدد للركن المعنوي للجريمة، فمنهم من عرفه بأنه :" قوة نفسية من شأنها الخلق والسيطرة"، وقد استند هذا التعريف في الأصل إلى الإرادة وهي أحد مكونات الركن المعنوي للجريمة، وهناك من الفقهاء من عرفه بأنه:" الأصول النفسية لماديات الجريمة"، وهناك تعريف آخر للركن المعنوي مقتضاه أن الركن المعنوي هو القصد الإجرامي المتمثل في النية الإجرامية للجاني للقيام بالأفعال المادية المكونة للجريمة[2].

وسبق وأن توصلنا إلى أن جريمة الإرهاب الالكتروني جريمة عمدية شانها في ذلك شان جريمة الإرهاب التقليدي، كونها صورة من صوره الحديثة والمستحدثة بفعل التطور التكنولوجي الهائل الذي عرف العالم المعاصر، وعليه يشترط لقيام هذه الجريمة قيام القصد الجرمي ، العام والخاص.

ومن أجل ذلك قسمنا هذا العنصر إلى فرعين يتضمن الأول القصد الجرمي العام وأما الثاني القصد الجرمي الخاص.

[1] أسامة أحمد المناعسة، جلال محمد الزعبي، مرجع سابق، ص 327.

[2] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 165.

**أولا: القصد الجرمي العام.**

اختلف الفقه الجنائي في تعريفهم للقصد الجرمي، إلا أن هذه التعريفات بالرغم من اختلافاتها اتفقت من حيث مضمونها ومعناها، فجانب من الفقه ذهب إلى تعريف القصد الجرمي بأنه:" إرادة الخروج عن القانون بالقيام بعمل أو بالامتناع عن عمل"، كما عرفوه بأنه:" إرادة الإضرار بمصلحة يحميها القانون الذي يفترض العلم به عند الفاعل"[1].

كما عرف أيضا القصد الجرمي بأنه:" توجيه الفاعل إرادته إلى ارتكاب الفعل المكون للجريمة هادفا إلى تحقيق نتيجتها التي تحققت، أو أي نتيجة أخرى"[2].

والقصد الجرمي يمكن أن يكون بسيطا، كما يمكن أن يقترن مع سبق الإصرار،والذي يعرف بأنه التفكير المصمم عليه لارتكاب الجريمة قبل تنفيذها بعيدا عن ثورة الغضب أو أي انفعال أو الهيجان النفسي.

ويتحقق سبق الإصرار سواء كان قصد الفاعل أو الجاني من الجريمة موجها إلى شخص معين أو إلى شخص غير معين لكن الجاني وجده أو صادفه، وسواء كان ذلك القصد معلقا على حدوث أمر ما أو موقوفا على شرط[3].

ومن خلال هذه التعريفات للقصد الجرمي يتضح ان الركن المعنوي يقوم على عنصرين أساسيين وهما العلم والإرادة، ومن أجل ذلك قسمنا هذا العنصر إلى فرعين خصصنا الأول للعلم، وأما الفرع الثاني فقد خصصناه للإرادة .

**01- العلم.**

بما أن جريمة الإرهاب الالكتروني جريمة مصنفة من الجرائم العمدية التي افترض فيها المشرع علم مرتكبها وهذا لان كل المشرعين يعرفون القصد الجرمي بأنه إرادة الجاني ارتكاب الجريمة، ومعنى

[1] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق ، ص167.
[2] مصطفى سعد حمد مخلف، مرجع سابق، ص 77.
[3] نفس المرجع،ص 78.

ذلك أن اتجاه الإرادة لارتكاب الفعل المجرم يكون ملازم للعلم بجميع العناصر القانونية المكونة للجريمة[1].

والوقائع التي وجب على الجاني العلم بها حتى يعتد بعلمه يمكن حصرها في:

- **العلم بالواقعة المنتجة للنشاط:** وجب أن يكون الجاني على علم بان فعله يشكل اعتداء على حق يحميه القانون، فالتهديد الذي يرسله الإرهابي الالكتروني إلى شخص أو مجموعة أشخاص من شأنه أن يهدد استقرار هؤلاء الأشخاص ويهدد أمنهم .
- **توقع النتيجة:** أي أنه يجب أن يحيط علم الجاني علما أن سلوكه الإجرامي الإرهابي هو الذي أدى إلى حدوث النتيجة الجرمية، والتي تعتبر الأثر المباشر لسلوكه الإرهابي الآثم[2] فمثلا تدمير المواقع الخاصة بتنظيم الملاحة الجوية في دولة ما بهدف بث الرعب في الناس هو النتيجة الحتمية والمباشرة لفعل الاختراق الذي قام به الإرهابي .
- **توقع العلاقة السببية:** أي توقع كيفية وقوع النتيجة، فعندما يقوم الجاني بفعل مجرم ويريد تحقيق نتيجة معينة فانه يتصور ويتوقع حدوث النتيجة وفق كيفية معينة[3].

وبما أنه سبق وبينا أن الركن المادي لجريمة الإرهاب الالكتروني يشتمل على جريمة الدخول والبقاء غي المشروع في النظام فانه وعند الحديث عن الركن المعنوي لجريمة الإرهاب الالكتروني نقول إن جريمة الدخول والبقاء غير المشروعين كصورة من صور النشاط المادي لجريمة الإرهاب الالكتروني هي جريمة عمدية تتطلب قصدا جنائيا وذلك بنص المادة 394 مكرر من قانون العقوبات الجزائري حيث أن قولها :" كل من يدخل أو يبقى عن طريق الغش" فيه دلالة على أن الجاني له كامل العلم بأن دخوله وبقاؤه داخل النظام غير مشروع، وهو ما أخذ به المشرع الفرنسي من خلال نص المادة 323 فقرة أولى من قانون العقوبات الفرنسي.

وعليه ولتوافر القصد الجنائي في هذه الصورة لابد أن يكون الجاني على علم بكافة عناصر الجريمة، فهو يعلم أن الفعل الذي يقوم به ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه

[1] محمود نجيب حسني، مرجع سابق، ص 57.

[2] يوسف كوران، مرجع سابق، ص 97.

[3] عصام عبد الفتاح عبد السميع مطر، مرجع سابق، ص 98.

من معلومات وبرامج، وتتجه إرادته إلى فعل الدخول والبقاء داخل النظام مع علمه بعدم حقه في ذلك وان هذا الأمر يشكل جريمة.

ولا يتوافر القصد الجنائي إذا كان الجاني يعتقد أن فعل الدخول والبقاء في النظام الذي قام بهما مسموح به أي أنه مشروع، أو كان الجاني جاهلا بحظر الدخول والبقاء داخل النظام[1].

أما بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول إلى النظام حيث يقوم الجاني (أي الإرهابي في جريمة الإرهاب الالكتروني) باختراق الجهاز الرقابي الذي يحمي النظام، فهو يظهر من خلال الولوج دون وجه حق إلى النظام، وأن الدخول للنظام غير مرخص به.

وعليه ففي جريمة الإرهاب الإلكتروني يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أنه ليس له الحق في القيام بذلك، وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

كما يشترط لتوافر الركن المعنوي في هذه الصورة للنشاط الإجرامي في جريمة الإرهاب الالكتروني بالإضافة إلى القصد الجنائي العام نية الغش.

كما أن استخدام الإرهابي للمعطيات في ارتكابه لجريمته وذلك بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يكون عمديا، ويكون هذا الاستخدام عن طريق الغش ومن أجل ذلك يتطلب الأمر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش[2].

وعليه ومن كل ما سبق فان علم الجاني بموضوع الجريمة يعني علمه بمحل الحق المعتدى عليه، أي الحق الذي يحميه القانون ويقرر عقوبة على الاعتداء عليه ومن اجل ذلك ينتفي القصد الجرمي لدى الجاني بانتفاء هذا العلم.

[1] أمال قارة، مرجع سابق، ص 125.

[2] نفس المرجع، ص 126.

**02- الإرادة.**

الإرادة وهي احد عناصر القصد الجرمي وهي بمثابة نشاط نفسي يتجه إلى تحقيق غرض عن طريق وسيلة معينة، وهي بذلك ظاهرة نفسية تعتبر بمثابة المحرك لأنواع من السلوك ذات طبيعة مادية، تحدث في العالم الخارجي من الآثار ما يشبع به الإنسان حاجاته المتعددة"[1].

والإرادة تنصب على السلوك الإجرامي وعلى النتيجة المعاقب عليها، فيجب أن تتجه إرادة الجاني إلى تبني السلوك الإجرامي، فالإرادة هي حلقة الوصل بين الجريمة بوصفها واقعة مادية لها كيان خارجي وبين الإنسان الذي صدر عنه هذا السلوك وأراد تحقيق نتيجته[2].

ولأن الجانب الوجداني والنفسي في جريمة الإرهاب الالكتروني له أهمية كبيرة في عنصر الإرادة تكمن في جذب الأشخاص للقيام بتلك العمليات الإرهابية، ويمكن أن يكون هذا التأثير من خلال النشرات والرسائل التي يوجهها الإرهابي إلى الأشخاص ليتسنى لهم صحة ما يقومون به، وكذلك كل ما تقدمه تلك الجماعات الإرهابية من خلال وسائل الإعلام، فكل هذا من شأنه جعل هؤلاء الأشخاص يؤيدون ما تقوم به تلك الجماعات الإرهابية من أعمال عنف في المجتمع، وبذلك يتمكنون من إقناع الأشخاص بهذه الأعمال سواء من الناحية السياسية أو من الناحية الدينية....

ومما سبق فانه يثور التساؤل حول الإرادة الكاملة للشخص في توجيه نفسه الوجهة التي يريدها وما هو دور حرية الاختيار في توجيه هذه الأفعال؟.

وفي هذا الشأن يرى الفقهاء أن حرية الاختيار تعني:" مقدرة الجاني على تحديد الوجهة التي تتخذها إرادته اتجاها معينا، وتحديد الطريق الذي يسلكه بفعله، فلا يكفي أن يكون قادرا على أن يعلم بالجهات المختلفة التي يمكن أن تتخذها إرادته، بل يجب أن يكون في نفس الوقت قادرا أيضا على اختيار وجهة منها ودفع إرادته إليها"[3].

[1] يوسف كوران، مرجع سابق، ص 80.

[2] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 165.

[3] نفس المرجع، ص 167.

وجدير بالذكر أنه في الغالب ما لا تكون الإرادة حرة حرية مطلقة إذ ثمة عوامل من شأنها أن تضعف هذه الحرية، وبالتالي لا يملك الجاني السيطرة عليها وعندئذ سوف تنتفي حرية الاختيار في الغالب، أما لأسباب خارجية كالإكراه أو داخلية كالحالة العقلية أو النفسية.

ومن أجل ذلك ومن أجل أن يعتد القانون بالإرادة في جريمة الإرهاب الالكتروني وجب توافر شرطين اثنين:

### 1. أن تكون هذه الإرادة مميزة.

إن التمييز يعني المقدرة على فهم ماهية الفعل المرتكب وطبيعة الآثار المترتبة عليه بحيث تنصرف المقدرة إلى ماديات الفعل فتغلق كيانه وعناصره، كما تنصرف إلى آثاره وما يترتب عليه من خطورة على حقوق معينة يكفل المشرع حمايتها[1].

### 2. إرادة تحقيق الفعل الإجرامي.

لتحقيق هذا العنصر لا يكفي أن تتجه إرادة الجاني إلى القيام بالفعل المجرم بكافة عناصره، بل يجب فضلا على ذلك أن تتجه إرادته إلى تحقيق النتيجة وذلك في الحالات التي يتطلب فيها القانون تحقيق نتيجة معينة.

فالإرادة محرك نحو اتخاذ السلوك الإجرامي سلبيا كان أم ايجابيا ، فكلما تبين أن الجاني أراد ارتكاب الفعل المجرم وتحقيق النتيجة الضارة، توافر القصد الجرمي وقامت الجريمة المقصودة، أما إذا تبين أن الجاني أراد القيام بالفعل انو نتيجة فإن الإرادة في هذه الحالة توافرت دون قصد.

وفي حالة جريمة الإرهاب الالكتروني لا يمكن هذا التصور لأنها جريمة عمدية قوامها أن الجاني أراد القيام بالفعل كما أراد تحقيق النتيجة الضارة[2] .

[1] محمد صبحي نجم، شرح قانون العقوبات–القسم العام، دار الأوائل، عمان– الأردن، 2000، ص 250.
[2] نفس المرجع، ص 251.

**ثانيا: القصد الجرمي الخاص.**

يكتسب القصد الجرمي أهمية استثنائية في الجريمة الإرهابية، وفي الجريمة الإرهابية الالكترونية على وجه الخصوص، ومع أن معظم تشريعات العالم لا تهتم بمسالة القصد الجنائي الخاص لدى الجاني بل تركز كل اهتمامها بالقصد العام، إلا أن طبيعة الجريمة الإرهابية وخاصة الإرهابية الالكترونية غيرت هذه النظرة، وأعطت لفكرة القصد الجنائي الخاص أهمية كبرى، إذ أن هذا القصد هو من ميز الجريمة الإرهابية عن غيرها من الجرائم[1]، بل وإنه ميز حتى بين جريمة الإرهاب التقليدية وجريمة الإرهاب الالكترونية.

فجريمة الإرهاب سواء بشكلها العادي أو الالكتروني ما هي إلا جريمة عادية منصوص عليها في جميع التشريعات الجنائية الوطنية، إلا أن ميزتها هي وجود غاية تتعدى الأركان العامة للقصد الجرمي، فإرسال رسالة تهديد عبر البريد الالكتروني المرسلة لشخص معين تعتبر من قبيل الجريمة العادية إلا أنها اقترنت بغاية خاصة لدى الجاني وهي التخويف ونشر الرعب بين الناس وهو ما يميز الجريمة الإرهابية.

وعلى ذلك فان للجريمة الإرهابية الالكترونية قصدين قصد مباشر وقصير وهو اختراق المواقع وتدميرها أو التجسس من خلالها، أو تدمير أو إتلاف الأموال العامة، والثاني غير مباشر وبعيد وهو زرع الخوف والرعب في قلوب الناس بغية الوصول إلى أهداف وغايات إجرامية، فزرع الرعب هو العنصر الجوهري الكامن في الجريمة الإرهابية مهما كان نوعها ومنها الالكترونية[2].

وتجدر الإشارة إلى أن ما يساعد القاضي على الوصول إلى القصد الجنائي الخاص للجاني في الجريمة الإرهابية والمتمثل في زرع الرعب هو الوقوف على الظروف المحيطة بالجريمة والوسائل المستخدمة فيها وكذلك الأهداف المنتقاة والمرتبطة بالجو السائد، فكل هذه العناصر كفيلة بتحديد القصد الجنائي الخاص لدى الإرهابي وتمييزه عن غيره من الجناة[3].

---

[1] يوسف كوران، مرجع سابق، ص 96.

[2] محمد مؤنس محي الدين، الإرهاب في القانون الجنائي على المستويين الوطني والدولي، المكتبة الانكلو- مصرية مصر،(دون سنة نشر)، ص 96.

[3] يوسف كوران، مرجع سابق، ص 97.

ونقول أنه على الرغم من ارتباط الجرائم الإرهابية بأهداف سياسية أو اقتصادية أو حتى عسكرية أو جميع هذه الأهداف مجتمعة كقلب نظام الحكم أو الاستيلاء عليه بقوة أو الحصول على الأموال بغية تمويل العمليات الإرهابية، إلا أن هذه الأهداف قد تشترك مع جرائم أخرى كالجرائم السياسية مثلا وبالتالي فإن هذه الأهداف لوحدها لا تعتبر المعيار المميز للجريمة الإرهابية عن غيرها من الجرائم الأخرى، وبالتالي فان معيار زرع الرعب والتخويف هو ما يميز جريمة الإرهاب عن غيرها والتي ترتكب بأي وسيلة كانت (كالوسيلة الالكترونية محل دراستنا) .

## المطلب الثاني: الاتفاق والمساهمة الجنائية في جريمة الإرهاب الالكتروني.

نظرا للتداخل الكبير بين مفهوم المساهمة الجنائية في جريمة الإرهاب الالكتروني والاتفاق الجنائي فيها، كان من الواجب التعرف إلى مفهوم كل عنصر من أجل معرفة أوجه التشابه وتمييز نقاط الاختلاف بين المفهومين، وهذا من أجل الإحاطة بالجوانب الموضوعية لجريمة الإرهابية الالكترونية بدقة .

وعلى ذلك قسمنا هذا العنصر إلى فرعين خصصنا الأول للاتفاق الجنائي في جريمة الإرهاب الالكتروني، وأما الفرع الثاني فقد خصص للمساهمة الجنائية في جريمة الإرهاب الالكتروني.

### الفرع الأول: الاتفاق الجنائي في جريمة الإرهاب الالكتروني.

من خلال هذه العنصر سوف نتطرق أولا إلى مفهوم الاتفاق الجنائي ثم أركانه في عنصر ثاني.

#### أولا: مفهوم الاتفاق الجنائي.

تعد مسالة الاتفاق الجنائي من المسائل المختلف فيها في الفقه الجنائي الحديث، حيث انقسم الفقه بشأنه إلى قسمين:

_ يرى الاتجاه الأول بان الاتفاق الجنائي في سلوك مادي إجرامي يجب المعاقبة عليه[1].

[1] غسان ضياء المظفر، الاتفاق الجنائي، مجلة الحوار المتمدن، العدد 3621، 2012/01/28، منشورة في الموقع www.alhewar.org ، الاطلاع بتاريخ 2018/01/24، على الساعة 18:02 .

– أما الاتجاه الثاني فيرى أن الاتفاق الجنائي ليس سلوك مادي إجرامي وبالتالي لا يجوز فرض عقوبة عليه.

وبالرجوع إلى موقف بعض التشريعات من الاتفاق الجنائي، نجد أن المشرع العراقي –على سبيل المثال– نص على الاتفاق الجنائي بموجب المادة 55 من قانون العقوبات العراقي بقوله:" الاتفاق الجنائي هو اتفاق شخصين أو أكثر على ارتكاب جناية أو جنحة سواء كانت معينة أو غير معينة أو على الأفعال المجهزة والمسهلة لارتكابها متى كان الاتفاق منظما ولو في مبدأ تكوينه"[1] .

أما قانون العقوبات المصري فقد نص في المادة 48 من على أنه:" يوجد اتفاق جنائي كلما اتحد شخصان فأكثر على ارتكاب جناية أو جنحة ما أو على الأعمال المجهزة أو المسهلة لارتكابها .

ويعتبر الاتفاق جنائيا سواء أكان الغرض منه جائزا أم لا إذا كان ارتكاب الجنايات من الوسائل التي لوحظت في الوصول إليه .

كل من اشترك في اتفاق جنائي سواء أكان الغرض منه ارتكاب الجنايات أو اتخاذها وسيلة للوصول إلى الغرض المقصود منه يعاقب لمجرد اشتراكه بالسجن , فإذا كان الغرض من الاتفاق ارتكاب الجنح أو اتخاذها وسيلة للوصول إلى الغرض المقصود منه يعاقب المشترك فيه بالحبس .

وكل من حرض على اتفاق جنائي من هذا القبيل أو تداخل في إدارة حركته يعاقب بالأشغال الشاقة المؤقتة في الحالة الأولى المنصوص عنها في الفقرة السابقة وبالسجن في الحالة الثانية .

ومع ذلك إذا لم يكن الغرض من الاتفاق إلا ارتكاب جناية أو جنحة معينة عقوبتها أخف مما نصت عليه الفقرات السابقة فلا توقع عقوبة أشد مما نص عليه القانون لتلك الجناية أو الجنحة ويعفى من العقوبات المقررة في هذه المادة كل من بادر من الجناة بإخبار الحكومة بوجود اتفاق جنائي وبمن اشتركوا فيه من قبل وقوع جناية أو جنحة وقبل بحث وتفتيش الحكومة عن أولئك الجناة فإذا حصل الإخبار بعد البحث والتفتيش تعين أن يوصل الأخبار فعلا إلى ضبط الجناة الآخرين"[2] .

[1] القانون 111 لسنة 1969 المتضمن قانون العقوبات العراقي، مجلة الوقائع العراقية، عدد 1778 ، بتاريخ 1969/09/15 .

[2] قانون رقم 58 لسنة 1937 المتضمن قانون العقوبات المصري المعدل والمتمم.

المشرع السوري نص على الاتفاق الجنائي في المادة 260 منه وذلك بقوله:" المؤامرة هي كل اتفاق بين شخصين أو أكثر على ارتكاب جناية بوسائل معينة.. " فقد اعتبر المشرع الاتفاق الجنائي نفسه المؤامرة"[1] .

أما المشرع الكويتي فقد نص على الاتفاق في المادة 56 من قانون الجزاء الكويتي بقوله:" إذا أتفق شخصان أو أكثر على ارتكاب جناية أو جنحة ، واتخذوا العدة على وجه لا يتوقع معه أن يعدلوا عما اتفقوا عليه ، يعد كل منهم مسئولاً عن اتفاق جنائي ولو لم تقع الجريمة موضوع الاتفاق ....."[2] .

أما المشرع الجزائري فانه لم يعط تعريف للاتفاق الجنائي أو الجمعية، إلا انه لاكتساب الصفة الجرمية لهذا الفعل وجب انعقاد إرادتين أو أكثر للقيام بذلك، فالجمعية أو الاتفاق عبارتان تفيدان المعنى نفسه تقريبا، إلا أن الجمعية أكثر هيكلة من الاتفاق الذي يغلب عليه الطابع الفكري[3]، وقد نص المشرع الجزائري على الاتفاق في نص المادة 176 من قانون العقوبات الجزائري بقولها:" كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تألف بغرض الإعداد لجناية أو جنحة أو أكثر معاقب عليها ب....."[4].

وتجدر الإشارة إلى أن العديد من الدول لجأت إلى تجريم الاتفاق الجنائي في تشريعاتها باعتباره جريمة مستقلة،وهي بذلك تعاقب على الأعمال التحضيرية وهذا من قبيل القواعد الاستثنائية وخروج على القواعد العامة ويعتبر التشريع الجزائري في طليعة هذه التشريعات[5].

المشرع الفرنسي أيضا ذهب في نفس الاتجاه حيث نصت المادة (450-1) من الكتاب الرابع تحت عنوان "المشاركة في جمعية الأشرار" بقولها:" يشكل جمعيات الأشرار كل مجموعة أو اتفاق

[1] قانون رقم 148 لسنة 1949 المتضمن قانون العقوبات السوري المعدل.

[2] قانون رقم 16 لسنة 1960 المتضمن قانون الجزاء الكويتي.

[3] يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر، أطروحة دكتوراه في القانون الخاص، جامعة باجي مختار، عنابة، 2016، ص 92.

[4] القانون 156/55 السالف الذكر.

[5] رشيدة بوكر، مرجع سابق، ص 340.

تألف بغرض الإعداد لجنحة أو أكثر أو جناية أو أكثر معاقب عليها ب...."[1]، والواضح من هذه المادة أن المشرع الجزائري متأثر بالمشرع الفرنسي ومن أجل ذلك ذهب في نفس اتجاهه.

وكما سبق وأن تمت الإشارة أن الفقه الجنائي قد انقسم في شان الاتفاق الجنائي إلى اتجاهين فالجانب الذي يرى أن الاتفاق الجنائي وإن كان عزم إجرامي إلا أنه معاقب عليه، لا تعد استثناء على القاعدة التي تقضي "بعدم العقاب على مجرد العزم على ارتكاب الجرائم" وحجتهم في ذلك أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة المتفق عليها، وإنما يعاقب عليه في حد ذاته كجريمة تامة، وذلك لأنه في الاتفاق الجنائي يظهر العزم الإجرامي الجماعي لمظهر خارجي مادي، لأن كل عنصر في هذا الاتفاق يعلن عزمه إلى سائر الأعضاء فتتجه إرادتهم إلى ارتكاب الجريمة وبذلك يكون الاتفاق معلوما، ويمكن إثباته، هذا بالإضافة إلى أن الاتفاق الجنائي ظاهرة تهدد الأمن العام تهديدا فعليا، كما ان القانون يراعي في العقاب على الاتفاق الجنائي وجهة الجزاء، لأنه يعاقب على تكوين الاتفاق الجنائي، كما يراعي فيه جهة الوقاية فتكون نتيجته إحباط الاتفاق الجنائي، فيحال بين الجناة وبين تحقيق خططهم الإجرامية، وبالتالي يتم وقاية المجتمع من نشر الجنايات والجنح المتفق عليها[2].

في حين يرى أنصار الاتجاه الآخر أن الاتفاق الجنائي يعتبر من قبيل الأعمال التحضيرية للجريمة، فهي ترد إلى المرحلة النفسية، أي إلى مرحلة اتخاذ القرار وعقد العزم على ارتكاب الجريمة وبالتالي إذا صحت خطورة الاتفاق الجنائي تبريرا لمعاقبة المتفقين في هذه المرحلة المبكرة من المراحل التي تمر بها الجريمة لوجب على المشرع تجريم المرحلة التحضيرية للجريمة من باب أولى[3] .

حاول المشرع الجزائري تفادي الانتقادات الموجهة لأصحاب الرأي الأول، ولم يجرم مجرد العزم والتصميم على الاعتداء في جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، بل اشترط أن يكون هذا الاعتداء مجسدا في فغل أو عدة أفعال مادية، وقد ظهر موقف المشرع الجزائري هذا من خلال نص المادة 394 مكرر 5 بقولها:" كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل، أو عدة أفعال

[1] رشيدة بوكر، مرجع سابق ، ص 340.

[2] Linanatx AVIER et Allan HOLLANDE, pratique de droit informatique,4eme édition, Delmas,1998,p 239.

[3] رشيدة بوكر، مرجع سابق، ص 342.

مادية يعاقب بالعقوبات المقررة للجريمة ذاتها[1]، وبالتالي ومن خلال هذه المادة نلاحظ أن المشرع الجزائري لم يتوقف في التجريم عند المرحلة العقلية والنفسية بل رفعه إلى المرحلة المادية التي تتوسط العزم والبدء في التنفيذ.

وبما أن جريمة الاعتداء على نظم المعطيات تعتبر صورة من صور الإرهاب الالكتروني إذا كان ارتكابها جاء دافعا لتحقيق أهداف وأغراض إرهابية فإن أي اتفاق من أجل ارتكاب هذه الجريمة يعاقب مرتكبوه بنفس العقوبة المقررة لهذه الجريمة ذاتها (الإرهاب الالكتروني).

ومن خلال هذه المادة يلاحظ أن المشرع الجزائري حذا حذو المشرع الفرنسي الذي تطلب تجسيد العزم بأعمال مادية، وهو ما يستشف من نص المادة 323-4 التي تناولت النص على تجريم الاتفاق الجنائي في نطاق المعالجة الآلية للمعطيات[2].

ويرى بعض الفقه أن السبب الذي دفع المشرع الجزائري إلى عدم التوسع في تجريم الاتفاق وتحديد نطاق تجريمه في إطار الأعمال التحضيرية بدل من تجريم العزم أن المشرع الجزائري يعاقب على الاتفاق الجنائي معتمدا في ذلك على معيار خطورة الجريمة وجسامتها، حيث حدد في المادة 176 من قانون العقوبات[3] الجرائم التي يجوز فيها المعاقبة على الاتفاق، في حين أن الجرائم موضوع الاتفاق فيما يتعلق بالاعتداء على نظم المعالجة الآلية للمعطيات عبارة عن جنح معاقب عليها بأقل من خمس سنوات حبس[4] .

[1] قانون العقوبات الجزائري.

[2] عدلت هذه المادة بموجب المادة 45 من الفصل الثاني من القانون رقم 2004-575 المؤرخ في 2004/06/21 المتعلق بالثقة بالاقتصاد الوطني الفرنسي.

[3] تنص المادة 176 من الأمر 156/66 السالف الذكر على أنه: " كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تألف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر معاقب عليها بخمس سنوات حبس على الأقل ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل"

[4] رشيدة بوكر، مرجع سابق، ص 343.

## أركان الاتفاق الجنائي في جريمة الإرهاب الالكتروني.

إلى جانب أن جريمة الإرهاب الالكتروني هي جريمة إرهابية وتهدف إلى تحقيق أغراض إرهابية إلا أنها في ذات الوقت نوع من أنواع الجرائم الالكترونية، وبالتالي فإن أركان الاتفاق الجنائي في جريمة الإرهاب الالكتروني هي نفسها أركان الاتفاق الجنائي في الجريمة الالكترونية كأصل عام ويمكن استخلاص هذه الأركان من خلال نص المادة 394 مكرر 5 السالفة الذكر.

ومن أجل ذلك فإن أركان الاتفاق الجنائي في جريمة الإرهاب الالكتروني تتمثل في:

- **تعدد الجناة:** حيث يكون الاتفاق بين شخصين على الأقل ويتم ذلك بانعقاد الإرادات واجتماعها على ارتكاب جريمة الإرهاب الالكتروني، وحسب نص المادة 394 مكرر 5 فإنه لم يرد القيد على الحد الأقصى للتعدد بل اكتفت المادة بقولها "... كل من شارك في مجموعة أو اتفاق.." والأمر ذاته نصت عليه المادة 176 من قانون العقوبات الجزائري بقولها:" كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه"فإذا ارتكب الشخص العمل التحضيري المادي بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر، كما يجب أن تتجه هذه الإرادات إلى جرائم الاعتداء على نظم المعالجة الآلية للمعطيات[1]، ومن الأمثلة على ذلك اقتناء الإرهابيين برامج معدة خصيصا للاختراق نظم المعالجة الآلية للمعطيات، من أجل تبادل معلومات هامة لارتكاب جريمة إرهابية كالإعلان عن كلمة المرور لموقع استراتيجي لأمن الدولة أو رمز دخوله.
- **موضوع الاتفاق الجنائي:** حيث يستمد الاتفاق الجنائي صفته الإجرامية من موضوعه، ولم يكتف المشرع بالصفة الإجرامية أيا كانت بل حرص على وضع تحديد خاص للصفة الإجرامية لموضوع الاتفاق حيث جاء في نص المادة 394 مكرر 5 " بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم "، فيكفي أن يتفق الجناة على الاتفاق للإعداد لجريمة الإرهاب الالكتروني وحدها حسب هذا النص.

[1] مصطفى سعد حمد خلف، مرجع سابق، ص 92.
أمال قارة، مرجع سابق، ص 132.

كما لا يشترط أن تكون الجرائم المتفق عليها معينة، وفي هذا الشرط يكمن الفرق بين المساهمة الجنائية والاتفاق الجنائي، اذ يقوم الاتفاق حتى ولو كانت الجرائم موضوع الاتفاق غير محددة بل يكفي أن تكون من الجرائم الالكترونية[1]، كاتفاق شخص مع مجموعة إرهابية من أجل تعليمهم كيفية تصميم المعلومات والمواقع أو كيفية الاختراق فهنا يعاقب هذا الشخص على الاتفاق على الرغم من أنه قد لا يعلم ما هي الجرائم التي سوف يقوم بها هؤلاء الإرهابيين بالضبط .

- **المشاركة في الاتفاق:** لم يكتف المشرع الجزائري كغيره من المشرعين بتجريم الاتفاق فقط بل تعداه إلى تجريم فعل الاشتراك في مجموعة بهدف الاتفاق للإعداد لجريمة من الجرائم الماسة بنظم المعالجة الآلية للمعطيات ومنها جريمة الإرهاب الالكتروني موضوع الدراسة وقد وفق المشرع الجزائري في هذا الموقف وهذا بسبب أن الجرائم الالكترونية تتم عادة في إطار مجموعات وخاصة الإرهابية منها وهذا تحسبا لسرية الاتفاق وسهولته بين الإرهابيين في هذه الجريمة وإن لم تكن بينهم معرفة مسبقة أو اتصال مباشر.

وقد وسع المشرع في نطاق التجريم ليشمل المرحلة التحضيرية في هذا النوع من الجرائم لردع المجرمين وتخويفهم لارتكاب هذا النوع من الجرائم المستحدثة [2].

- **القصد الجنائي:** تقوم جريمة الاتفاق الجنائي في جريمة الإرهاب الالكتروني على عنصري العلم والإرادة .

**1. العلم.**

حيث يجب على كل فرد منضم للاتفاق الجنائي أن يعلم بالفعل موضوع الاتفاق الجنائي، وهذا العلم لا يعني معرفة الجريمة بالضبط بل المهم أن يعلم أنه يتفق من أجل ارتكاب جريمة من الجرائم الالكترونية، وعلى هذا الأساس من جهل موضوع الاتفاق لا يتم عقابه لأن القصد الجرمي غير متوافر لديه.

[1] رشيدة بوكر، مرجع سابق، ص 347.

[2] مصطفى سعد حمد خلف، مرجع سابق، ص 93.

**2. الإرادة.**

لا يكفي توافر عنصر العلم حتى تقوم جريمة الاتفاق الجنائي بل لابد من توافر الإرادة الجادة للشخص على الأقل للدخول أو الاشتراك فيه، بمعنى أن تتجه إرادة كل شخص من أشخاص الاتفاق إلى إتيان هذا الفعل المجرم، وأن يقوم كل شخص بالدور المسند إليه، وإذا كان عكس ذلك انتفى القصد الجنائي لجريمة الاتفاق الجنائي في جريمة الإرهاب الالكتروني[1] .

## عقوبة المشرع الجزائري للاتفاق الجنائي في جريمة الإرهاب الالكتروني.

كما سبق وأشرنا أن جريمة الإرهاب الالكتروني تعتبر من الجرائم المستحدثة التي تعتمد لقيامها على الوسائل التكنولوجية الحديثة ومن أجل ذلك صنفت أنها جريمة الكترونية فضلا عن أنها جريمة إرهابية، وأمام غياب النص الخاص بالاتفاق الجنائي في هذه الجريمة فإنه يسري عليها ما يسري على الاتفاق في الجريمة المعلوماتية .

وعلى هذا الأساس يمكن القول أن المشرع الجزائري جعل عقوبة الاتفاق الجنائي تتناسب وطبيعة الجرائم الواقعة على نظام المعالجة الآلية للمعطيات، وهذا خلافا لنص المادة 177 من قانون العقوبات الجزائري والتي نصت على أنه:" يعاقب على الاشتراك في جمعية الأشرار بالسجن المؤقت من خمس سنوات إلى عشر سنوات، وبغرامة من 500.000 دج إلى 1000.000 إذا تم الإعداد لارتكاب جنايات.

وتكون العقوبة من سنتين إلى خمس سنوات والغرامة من 100.000 إلى 500.000دج أذا تم الإعداد لارتكاب جنح .

ويعاقب منظم جمعية الأشرار أو من يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر سنوات إلى عشرين سنة وبغرامة من 1000.000 دج إلى 5000.000 دج"[2] .

---

[1] مصطفى سعد حمد خلف، مرجع سابق ، ص 94.

[2] الأمر رقم 156/66 السالف الذكر.

وعلى ذلك فمن خلال نص المادة 394 مكرر5 يلاحظ أن المشرع الجزائري تجاوب مع نصوص الاتفاقيات الدولية ومقررات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر، وما تضمنه القرار الصادر عن الأمم المتحدة الثامن عشر لمنع الجريمة ومعاملة السجناء المتعلق بالجرائم ذات الصلة بالكمبيوتر،والتي خلصت في مجملها إلى تجريم الاتفاق الجنائي[1].

وعليه فإننا نصل إلى نتيجة مهمة مفادها أن جريمة الاتفاق في جريمة الإرهاب الالكتروني معاقب عليها بنفس العقوبات المقررة لجريمة الإرهاب الالكتروني في التشريعات الوطنية ومنها قانون العقوبات الجزائري.

## الفرع الثاني: المساهمة في جريمة الإرهاب الالكتروني.

من المعلوم أن الجريمة قد ترتكب من طرف شخص واحد كما قد ترتكب من طرف أكثر من شخص، والجريمة الإرهابية من الجرائم التي في الغالب تتم من طرف أكثر من شخص واحد وذلك للعديد من الاعتبارات من بينها أن طبيعة هذه الجريمة والأهداف الآثمة التي تسعى إلى تحقيقها يتعذر على الشخص بمفرده القيام بها الأمر الذي يحتاج إلى تخطيط وتنظيم وتوزيع أدوار على الجناة.

وبالرجوع إلى القواعد العامة نجد أن المساهمة الجنائية أو كما يطلق عليها بعض الفقه الاتفاق الجنائي لا تتحقق إلا بتوافر شرطين اثنين:

- **تعدد الجناة:** وهو أن يقوم شخص بالتعاون مع غيره في تنفيذ الجريمة كالجريمة الإرهابية – محل دراستنا– سواء قاموا بنفس الفعل أو أنهم تقاسموا الأدوار، كما قد تتفاوت هذه الأدوار حسب طبيعتها إما أدوار رئيسية أم ثانوية[2].
- **وحدة الجريمة:** لا يكفي شرط التعدد لتقوم المساهمة الجنائية بل لا بد من تحقق شرط آخر لاكتمالها وهو وحدة الجريمة المرتكبة وتكون نتيجة التعاون المشترك بين الجناة، ووحدة الجريمة تعني وحدة ركنيها المادي والمعنوي:

[1] مصطفى سعد حمد خلف، مرجع سابق، ص 94.

[2] أمير فرج يوسف،(مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 115.

1. **الركن المادي:** وتعني وحدة الركن المعنوي تعاون الجناة على ارتكاب الفعل المكون للجريمة وتحقيق نتيجة واحدة متفق عليها من قبل الجناة.
2. **الركن المعنوي:** وهو العلاقة الذهنية التي تربط بين المساهمين في الجريمة الواحدة وتعني قصد التداخل في الجريمة لتحقيق نتيجتها الجرمية، فمتى قام قصد التداخل لدى كل المساهمين قامت الرابطة الذهنية بينهم.

## أولا: المساهمة الجنائية الأصلية في جريمة الإرهاب الالكتروني.

وتكون هذه الصورة من المساهمة عندما يقوم إرهابيين أو أكثر بأدوار أساسية في الجريمة الإرهابية، وهذا الدور قد يكون كافي لوحده لتحقيق النتيجة المرجوة من الجريمة دون المساهمة إلى المساهمة التبعية، وبالتالي فان هذا النوع من المساهمة يتعدد فيها المجرمون (الإرهابيون) في مرحلة التنفيذ المادي للجريمة، فهم يقومون بتنفيذ الدور الأساسي في تنفيذ ركنها المادي[1].

والملاحظ على اغلب التشريعات المكافحة للإرهاب لم تحدد المساهم الأصلي في الجريمة، تاركا ذلك للقواعد العامة في قانون العقوبات والمثال على ذلك قانون مكافحة الإرهاب المصري[2] والعراقي[3] وكذلك المشرع الجزائري في القسم الرابع مكرر المتضمن الجرائم الموصوفة بأعمال إرهابية أو تخريبية من قانون العقوبات لم ينص على المساهمة الجنائية في الجريمة الإرهابية الالكترونية وبالتالي يتم الرجوع في هذا الشأن للقواعد العامة المتعلقة بالمساهمة الجنائية .

ومعظم التشريعات الجنائية استقرت على أن الفاعل الأصلي للجريمة في المساهمة الجنائية من يقوم بالجريمة بمفرده أو بمعاونة الغير، أو أن يأتي عملا من أعمال التنفيذ المادي لها[4].

وقد نص المشرع الأردني في قانون منع الإرهاب الأردني في المادة السابعة فقرة واو(7/ و) على عقوبة المتدخل بنفس عقوبة الفاعل حيث نصت على انه يعاقب الشريك في أي جريمة من الجرائم

[1] عصام عبد الفتاح مطر، مرجع سابق، ص 119.

[2] قانون رقم 94 لسنة 2015 الصادر في 30 شوال 1436 هـ الموافق لـ 15 أغسطس 2015 م المتضمن قانون مكافحة الإرهاب المصري، الجريدة الرسمية عدد 33 مكرر، للسنة الثامنة والخمسون.

[3] المادة 6 من القانون رقم 13 لسنة 2005 المتضمن مكافحة الإرهاب العراقي ، الوقائع العراقية عدد 4009 بتاريخ 2005/11/09 ص 01.

[4] عصام عبد الفتاح مطر، مرجع سابق، ص 121.

المنصوص عليها في المادة 3 من نفس القانون بأي صورة من صور الاشتراك بما في ذلك التدخل في الجريمة أو التحريض عليها أو المساعدة في ارتكابها بعقوبة الأفعال الأصلية سواء ارتكبت الجريمة داخل المملكة أو خارجها، ويعتبر العمل الإرهابي تاما سواء أكان الفعل المؤلف له تاما أو ناقصا أو شروعا فيه[1].

وبالرجوع إلى نص الرابعة من قانون مكافحة الإرهاب العراقي نجدها تنص على أنه يعاقب المحرض والمخطط والممول وكل من مكن الإرهابيين في الجرائم الواردة في هذا القانون عقوبة الفاعل الأصلي[2]، ويبرر خروج المشرع العراقي عن القواعد العامة هو جسامة جريمة الإرهاب مهما كانت صورتها ، أي سواء كانت تقليدية أو الكترونية.

كما أن المشرع الجزائري عرف الفاعل الأصلي من خلال المادة 41 من قانون العقوبات بقولها:" يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي"[3].

فمن خلال هذه المادة يستنتج أن الفاعل هو كل شخص أتى بفعل مجرم قانونا أو ساهم في إتيانه سواء كان ذلك بالتحريض أو بالاشتراك على أن يقوم هذا الشخص بالدور الرئيسي، وقد يكون بصورة متعددة، وعليه فإن الفاعل هو من قام بارتكاب الجريمة وتحققت بأركانها المادية والمعنوية.

كذلك ومن خلال المادة 41 السالفة الذكر نجدها اعتبرت المحرض فاعل أصلي، وأن التحريض على ارتكاب الفعل المجرم يكون بأحد الوسائل المادية من قبيل المساهمة المباشرة، ويكون التحريض بالهبة أو الوعد أو التهديد أو بإساءة استعمال السلطة أو التحايل أو التدليس الإجرامي[4].

وعلى ذلك وبالرجوع للقواعد العامة فان المشرع الجزائري على غرار معظم مشرعي العالم اعتبر أن المساهمة الأصلية في جريمة الإرهاب الالكتروني أن يقوم الإرهابي بالركن المادي بمفرده أو بالمساهمة مع غيره على أن يقوم بالدور الأساسي ، كان يقوم شخص بتحريض آخر على إرسال

[1] مصطفى سعد حمد مخلف، مرجع سابق، ص59 .

[2] نفس المرجع، ص 61.

[3] القانون 156/66 السالف الذكر.

[4] القانون 156/66 السالف الذكر.

تهديدات عبر البريد الالكتروني إلى أشخاص معينين بهدف ترويعهم، ونشر الفزع والرعب في نفوس هؤلاء الأشخاص لخدمة أغراضهم الإرهابية، أو كأن يقوم إرهابيين فأكثر بتدمير مواقع الكترونية بهدف تعطيل شبكة المواصلات الجوية أو البحرية بهدف ترويع الأهالي وإثارة حالة من الفزع في دولة معينة[1].

## ثانيا: المساهمة الجنائية التبعية في الإرهاب الالكتروني.

يقصد بالمساهمة الجنائية التبعية في الجريمة الإرهابية بأنها كل نشاط يرتبط بالسلوك الإجرامي الإرهابي ونتيجته برابطة سببية دون أن يتضمن تنفيذا للجريمة أو القيام بدور رئيسي في ارتكابها[2] وعليه فان الصفة التبعية في المساهمة هي من تكسب سلوك الشريك الصفة غير المشروعة[3].

والمساهمة التبعية هي المساهمة التي يعدد فيها المجرمون في مرحلة قبل التنفيذ المادي للجريمة أي في مرحلة التفكير والإصرار على ارتكاب الفعل المجرم، وهم على ذلك لا يقومون بالدور الرئيسي أو الأساسي، بل يقتصر فعلهم على الدور الثانوي، ومن اجل ذلك يسمى هؤلاء الجناة بالشركاء، وإذا قام بهذا الدور شخص بمفرده يعرف بالشريك[4].

والشريك هو الذي ينفذ العمل الإجرامي، ولكنه ساهم في ارتكاب الجريمة، حيث نص المشرع الجزائري في المادتين 42 و 43 من قانون العقوبات على الشريك، حيث نصت المادة 42 على انه :" يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك"[5].

---

[1] مصطفى سعد حمد مخلف، مرجع سابق، ص61.

[2] محمود نجيب حسني، مرجع سابق، ص 227.

[3] ضيف الله بن شيب الجيلي، المساهمة التبعية في ارتكاب الجريمة الإرهابية وعقوبتها، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2009، ص 64.

[4] مقالة منشورة في الموقع: www.desconceils.com، تاريخ الاطلاع: 2014/03/11 على الساعة 18:10.

[5] قانون 156/55 السالف الذكر.

أما المادة 43 من نفس القانون فتنص على أنه:" يأخذ حكم الشريك كل من اعتاد أن يقدم مسكنا أو ملجأ أو مكانا للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص، أو الأموال مع علمه بسلوكهم الإجرامي"[1].

وعليه فان الشريك في جريمة الإرهاب الالكتروني حسب نصي المادتين 42 و 43 سالفتي الذكر يقوم بالأفعال التالية:

- **تقديم المساعدة:** أي تقديم العون لمرتكبي الجريمة على شرط أن تبقى في حدود الأعمال التحضيرية .
- **الأعمال المسهلة في الجريمة:**أي كل الأعمال التي من شأنها تسهيل الجريمة أمام الجناة.

وعلى ذلك تقتضي القواعد العامة في المساهمة التبعية توافر العناصر الآتية[2]:

- **العنصر المادي:** ويقصد به ارتكاب فعل من الأفعال المنصوص عليها كوسيلة من وسائل الاشتراك، وان يرتبط ذلك الفعل بالنتيجة غير المشروعة برابطة سببية عادية.

- فعل غير مشروع سواء في صورة تامة أو شروع معاقب عليه، وان يرتكب من طرف الفاعل أو المساهم الأصلي.

- وأن يتوافر قصد التدخل لدى الشريك.

وبناء على ذلك يمكن رصد أركان المساهمة التبعية في جريمة الإرهاب الالكتروني هي[3]:

-**الركن المفترض:** وهو وجود جريمة إرهاب الكتروني منصوص عليها قانونا وتستحق العقاب .

- **الركن المادي:** ارتكاب فعل من أفعال المساهمة التبعية المنصوص عليها قانونا .

- **الركن المعنوي:** قصد المساهمة التبعية أو الاشتراك.

---

[1] قانون 156/55 السالف الذكر.

[2] مقالة منشورة في الموقع: www.desconceils.com، تاريخ الاطلاع: 2014/03/11 على الساعة 18:10.

[3] إمام حسانين خليل، الجرائم الإرهابية في التشريعات المقارنة، الطبعة الأولى، مركز الخليج للنشر والتوزيع، القاهرة 2008، ص 05.

أما المشرع العراقي فقد حصر وسائل المساهمة الجنائية من محرض وشريك واتفاق ويلاحظ أن حصر وسائل الاشتراك له ما يبرره، نظرا لأن أفعال الاشتراك في ذاتها غير معاقب عليها إلا حينما يحقق الفاعل سلوكا غير مشروع وفقا لقاعدة تجريمية من قواعد القانون، فيكون من الضروري تحديد الأفعال التي يعاقب عليها لارتباطها بذلك السلوك حتى لا يترك الأمر لتقدير المحكمة[1].

فوفقا لنص المادة 47 من القانون العراقي فان الشخص لا يكتسب صفة الشريك في الجريمة إلا إذا اتخذ اشتراكه صورة من صور الاشتراك المنصوص عليها في القانون كالتحريض والاتفاق والمساعدة[2] .

وفي الأخير نقول انه من صور المساهمة الجنائية في جريمة الإرهاب الالكتروني أن يقوم تاجر بتزويد الإرهابيين بشبكة المعلومات ويكون عالما بالجريمة الإرهابية يكون بذلك مساعدا في هذه الجريمة .

[1] مصطفى سعد حمد مخلف، مرجع سابق، ص 60.

[2] سلامة مأمون، مرجع سابق، ص 245

## الفصل الثاني: المكافحة الإجرائية في جريمة الإرهاب الالكتروني.

إن التطور التكنولوجي في جميع مجالات الحياة جعل من هذا عصر يتميز بالتخصص والتميز والابتعاد عن العمومية الأمر الذي انعكس على مكافحة الجريمة الالكترونية وخاصة الإرهابية منها، وهو ما أوجب ضرورة استخدام التقنيات الالكترونية الحديثة والمتطورة في التحقيق الجنائي من أجل استخلاص الدليل واثبات جريمة الإرهاب الالكتروني كغيرها من الجرائم المعلوماتية.

وبناءا على ذلك فإننا نهدف من وراء هذا العنصر توضيح مختلف القواعد الإجرائية التي يتبعها المحققون في مجال الكشف عن جريمة الإرهاب الالكتروني والبحث عن حقيقة ارتكابها وملاحقة مرتكبيها وذلك في إطار اختصاص المحققين التي حددها لهم الدستور والقانون الموضوعي والإجرائي.

ومن أجل ذلك وللتعرض إلى هذا العنصر بشيء من التفصيل قسمنا هذا الفصل إلى مبحثين اثنين، تضمن المبحث الأول إثبات جريمة الإرهاب الالكتروني أمام الجهات القضائية كمرحلة حاسمة لمكافحة هذه الجريمة والحد منها، وكذلك سوف نتعرض من خلال هذا العنصر إلى أهم الصعوبات في إثبات هذا النوع من الجرائم.

وأما المبحث الثاني فتعرضنا من خلاله إلى القواعد الإجرائية لاستخلاص الدليل، بحيث سوف نتعرض إلى القواعد التقليدية والمستحدثة في استخلاص الدليل في جريمة الإرهاب الالكتروني .

## المبحث الأول: إثبات جريمة الإرهاب الإلكتروني.

بعد التطرق إلى طرق استخلاص الدليل من أجل إثبات جريمة الإرهاب الإلكتروني تأتي المرحلة الحاسمة والأخيرة وهي تقديم هذا الدليل إلى الجهاز القضائي بهدف الوصول إلى الحقيقة وتعتبر هذه المرحلة مسألة حاسمة متجسدة في عرض الأدلة على القاضي الجزائي بهدف تقييمه وإثباته بعد قبوله، ولا يكون الدليل مقبولا إلا بعد التيقن من مراعاة الحصول عليه بنصوص القانون.

والإثبات الجنائي بالأدلة الرقمية اعتبر من أهم المسائل التي تعرض لها المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات والذي عقد في "ريو دي جانيرو" بالبرازيل كما تعرضت لهذه المسألة الحلقة التمهيدية التي عقدت على المستوى الدولي في "فريبورج"[1].

وإثبات جريمة الإرهاب الإلكتروني ليست بالأمر السهل وهذا نظرا لوقوع هذه الجريمة ضمن بيئة رقمية، الأمر الذي أدى إلى ظهور معوقات كثيرة للأجهزة المختصة بالبحث والتحري والتحقيق في تطبيق القواعد الإجرامية التي نظمت مسألة استخلاص الدليل التقني، وهذا ما ينتج عنه نوع من الإعاقة لهذه الأجهزة وتصنف قيمتها في مكافحة جريمة الإرهاب الإلكتروني.

ومن أجل ذلك قسمنا هذا المبحث إلى مطلبين مطلب يتضمن:

حجة الدليل في إثبات جريمة الإرهاب الإلكتروني، ومطلب ثاني بعنوان: صعوبات إثبات جريمة الإرهاب الإلكتروني.

### المطلب الأول: حجية الدليل الرقمي في إثبات جريمة الإرهاب الإلكتروني.

الإثبات الجنائي هو نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقا لمعيار الحقيقة الواقعية، وذلك بشأن تأكيد اتهام ونفي اتهام آخر، أي أنه هو إقامة الدليل على وقوع الجريمة ونسبها إلى فاعل معين والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة ومن الواقعة المعروضة.

[1] بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه في القانون الجنائي والعلوم الجنائية، جامعة الجزائر1، 2015، ص209.

والقاعدة في مختلف التشريعات الجزائية يقوم على حرية الإثبات فلا قيد أو شرط على الإثبات في المواد الجنائية إلا أن تكون وسيلة الإثبات أو أن يكون الدليل قد تحصل عليه بطريقة مشروعة وهذا إعمالا لمبدأ الشرعية الإجرائية وذلك كما يلي:

## الفرع الأول: مشروعية الدليل التقني.

ويقصد بذلك أن يكون الدليل معترف به قانونا بحيث يجيز هذا الأخير للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة، وتحدد سلطة القاضي الجزائي في قبول الدليل التقني حسب نظام الإثبات السائد في كل دولة فالمشرع الجزائري تبنى مبدأ حرية الإثبات وفي هذه الحالة سلطة القاضي في قبول جميع الأدلة بأي طريقة من طرف الإثبات، إلا إذا نحى المشرع على عكس ذلك بموجب نص صريح[1].

وهو ما يستنتج من نص المادة 212 من قانون الإجراءات الجزائية الجزائري وذلك بقوله:" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".

وأهم ما يميز نظام الإثبات الحر أنه لا يرسم للقاضي طرق محددة للإثبات يتقيد بها فهو حر في تكوين قناعته في أي دليل يقدم إليه، وهو غير ملزم بتقديم تبريره لأسباب هذه القناعة من عدمها وفضلا عن ذلك فالقانون لم يضع لهم أي سؤال يشتمل على كل واجباتهم (هل لديكم اقتناع شخصي)[2].

وهناك العديد من الأسباب التي تبرر الأخذ بمبدأ حرية الإثبات أهمها أن هذا المبدأ بمثابة النتيجة الطبيعية و المنطقية لمبدأ قضاء القاضي بمحض اقتناعه الذاتي و الذي يستلزم بالضرورة منح الحرية للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها حتى يتسنى له أداء مهامه ويتمكن من إرساء العدالة بين المتقاضين.

[1] فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة – دراسة مقارنة، دار الثقافة، عمان– الأردن، 2006 ص 48.

[2] محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول، النظرية العامة، الطبعة الأولى الكتاب الجامعي، القاهرة، 1977، ص10.

كما أن الإثبات في الدعوى العمومية على وقائع قانونية مادية أو نفسية يصعب الحصول لها على دليل مسبق عكس الدعوى المدنية ولعل من أحد المبررات التي دفعت بالتشريعات الآخذة بهذا المبدأ هو ظهور الأدلة العلمية الحديثة و التي كشف عنها العلم الحديث في إثبات الجريمة و نسبتها إلى المتهم كالبصمة الوراثية A D N [1].

والأمر لا يختلف في الجزائر بالنسبة للدليل التقني حيث لم يتضمن القانون 09-04 السابق الذكر أية أوضاع خاصة بهذا الصدد و من ثم فان الدليل التقني سوف يكون مشروعا من حيث الوجود و ذلك على اعتباره من الأسباب العلمية الجدية في الإثبات الجنائي.

## النتائج المترتبة على مبدأ حرية الإثبات.

من أهم النتائج على هذا المبدأ:

**1/الدور الإيجابي للقاضي الجزائي:** وذلك في توفير الدليل التقني و عدم تقيده بما يقدمه أطراف الدعوى من أدلة وإنما يجب عليه بموجب سلطانه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات للتحقيق في الدعوى و الكشف عن الحقيقة الفعلية فيها، وهذا لأن الحقيقة لا تظهر من تلقاء نفسها وهكذا فإن القاضي الجزائي يجب أن يأمر باتخاذ الإجراء الذي يراه مناسبا و ضروريا للفصل في الدعوى بناء على طلبات الأطراف أو بموجب مقتضيات وظيفته ففي مواد الجنايات خول القانون الإجرائي الفرنسي لرئيس محكمة الجنايات بموجب نص خاص[2] سلطة تفويضية بمقتضاها يمكن أن يتخذ كافة الإجراءات التي يعتقد أنها ضرورية ومفيدة للكشف عن الحقيقة حيث لا قيد عليه سوى شرفه وضميره، وتطبيقا على ذلك فانه في جريمة الإرهاب الالكتروني يجب على القاضي الجنائي في سبيل الوصول للحقيقة أن يوجه أمرا إلى مزود خدمة الانترنت بتقديم المعطيات اللازمة التي تسمح بالتعرف على هوية المرسل والمرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها[3].

ومن أبرز مؤشرات ودلائل الدور الايجابي للقاضي الجزائري في البحث عن الدليل التقني في

[1] رشيدة بوكر، مرجع سابق، ص483.

[2] المادة 310 من قانون الإجراءات الجزائية الفرنسي.

[3] رشيدة بوكر، مرجع سابق، ص485.

جريمة الإرهاب الالكتروني السلطة التي منحها القانون للقاضي باعتراض الاتصالات السلكية واللاسلكية متى ما رأى ذلك ضروريا: –كما سبق وشرحنا في العناصر السابقة–

- الخبرة يجوز للقاضي الجزائي ندب الخبراء، وكذا إعلامهم ليقدموا إيضاحات عن التقارير المقدمة منهم، لما لها من دور كبير ومهم في مجال المساعدة القضائية فهي تعد من أقوى مظاهر تعامل قاضي التحقيق مع وقائع جريمة الإرهاب الالكتروني المعروضة عليه فللقاضي سلطة تعيين الخبراء وهذا حسب نص المادة 1/143 من قانون الإجراءات الجزائية بقولها: " لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب من النيابة العامة وإما من تلقاء نفسها أو من الخصوم".
- في مجال البحث عن الدليل في جريمة الإرهاب الالكتروني يلاحظ أن الخبرة التقنية تعد أخذ أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والانترنت خاصة أمام نقص المعرفة القضائية الشخصية لظاهرة تقنية المعلومات، وهذا الأمر جد صعب نظرا لاختلاف أساليب ووسائل الإرهاب الالكتروني من تدمير المواقع أو الاستيلاء عليها أو التجسس عليها.....الخ[1].

**2/الدور الايجابي للقاضي الجزائي في قبول الدليل التقني:** تعد هذه المرحلة ثاني مرحلة بعد توفير الدليل والبحث عنه وتقديمه من قبل جميع الأطراف (سلطة الادعاء، المتهم، أو القاضي) وعليه وعملا بمبدأ الشرعية الإجرائية التي يتحصل بها الدليل الجنائي بما يتضمنه من أدلة مستخرجة من وسائل الكترونية فلا يكون الدليل مقبولا في عملية الإثبات والتي يتم من خلالها إخضاعه للتقدير إلا إذا كان غير مشروعا أي انه استخلص بطرق منصوص عليها قانونا[2].

وفي هذا السياق تجدر الإشارة إلى أن طبيعة الدليل التقني لا تعبر عن قيمة أصلية بمجرد رفع محتواه على الانترنت، حيث يتواجد في كل مكان يتم استدعاؤه منه وذلك لأنه عندما يقوم المتهم بإزالة الدليل التقني عن بعد يكون ما تبقى منه نسخة فقط، يتم التوصل إليها من بعد بطريقة المراقبة الالكترونية أيضا، ومن أجل ذلك بحث مختلف المشرعين القانونيين هذا الأمر واعتمدوا على منطق افتراض أصالة الدليل التقني. فمثلا نص المشرع الأمريكي في قانون الإثبات في المادة 03/1003

[1] رشيدة بوكر، مرجع سابق، ص 486 .

[2] نفس المرجع، ص 487.

على أنه إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة فإن أية مخرجات طابع منها أو مخرجات مقروءة برؤية العين تبرز انعكاسا دقيقا للبيانات تعد بيانات أصلية أما عن المشرع الجزائري فلم يفصل في هذا النوع من المسائل[1].

ومن أجل التأكيد على ضرورة الحصول على الأدلة الالكترونية (التقنية) بطريقة شرعية وضعت مختلف الدساتير الوطنية الجزائرية وكذا القوانين الإجرائية نصوصا تتضمن ضوابط الشرعية الإجرائية الماسة بالحرية ومن ثم مخالفة هذه النصوص في استخلاص الدليل بصبغ هذا الدليل بلا مشروعية ولم يقتصر النص على مشروعية إجراءات الحصول على الدليل على الدساتير والقوانين الوطنية فحسب بل يتعدى ذلك إلى النصوص الدولية كالإعلان العالمي لحقوق الإنسان والمواثيق والاتفاقيات الدولية وقواعد النظام العام والآداب العامة السائدة في كل مجتمع بالإضافة إلى الاجتهادات القضائية[2].

ويترتب على مخالفة هذه النصوص وجمع الأدلة بطرق غير مشروعة البطلان والمشرع الجزائري في هذا الشأن تبع المشرع الفرنسي حيث نص على قاعدة استبعاد الدليل في مصطلح بطلان الإجراء وبالتالي عدم قبول الدليل بما في ذالك الدليل الرقمي المستمد من الوسائل الالكترونية المنصوص عنه طبقا للقاعدة ما بني على باطل فهو باطل، إلا أن هذا البطلان ليس مطلق في كل الحالات بل نسبي إذ يجوز تصحيحه بتنازل الأطراف الذين وقع في حقهم هذا البطلان وقد اختلف المشرع الجزائري عن نظيره الفرنسي في نطاق البطلان حينما قرر أن بطلان إجراءات الاستجواب والمواجهة بما فيها تلك التي يخضع لها المتهم المعلوماتي (الإرهابي في هذه الجريمة موضوع الدراسة) تكون باطلة ويمتد هذا البطلان على ما يتلوه من إجراءات، أما في بقية إجراءات التحقيق بخلاف إجراءات الاستجواب والمواجهة بما فيها المعاينة التقنية والتفتيش في البيئة الرقمية والضبط الرقمي فقد أعطى المشرع الجزائري لغرفة الاتهام قرار قصر البطلان الإجراء بعينه أو امتداده جزئيا أو كليا على الإجراءات اللاحقة له[3].

[1] رشيدة بوكر، مرجع سابق، ص 488.

[2] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة 2008 ص119.

[3] بن فردية محمد، مرجع سابق، ص277.

وتجدر الإشارة إلى أن أدلة الإثبات التقنية أو المستمدة من الوسائل الالكترونية في المسائل الجنائية تنقسم إلى أدلة براءة وأدلة إدانة، وإذا تم الحصول على أدلة الإدانة بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مشروع ومن ثم غير مقبول في عملية الإثبات لان قبول هذه الأدلة فيه مساس بالضمانات التي كفلها القانون لحماية حقوق المواطن او كرامته لا قيمة لها كما أن القواعد التي بينها المشرع لا أهمية لها متى ما أمكن إهدارها وعدم الالتزام بها فإذا تم الحصول على دليل تقني في جريمة الإرهاب الالكتروني وفق الطرق السابقة تم إبطاله وعدم إنتاج الإجراء الباطل للآثار المترتبة عنه[1].

على أنه في نظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بمقتضاه.

أما بخصوص دليل البراءة فقد وردت مسألة الأخذ به رأيان حيث يرى الاتجاه الأول أن المشروعية لازمة في كل دليل أكان إدانة أو براءة على أساس أن القضاء ليس له أن يقر قاعدة مفادها أن الغاية تبرر الوسيلة، وعليه فإن هذا الاتجاه يرى أن إثبات البراءة شانه شأن الإدانة لا يكون إلا من خلال طرق مشروعة فهو شرط أساسي في كل تشريع[2].

أما الاتجاه الثاني فيرى عكس ذلك أي أنه يرى أن مشروعية الحصول على الدليل تكون في حالة دليل الإدانة فقط دون البراءة على أساس أن الأصل في الإنسان البراءة ولا حاجة للمحكمة بان تثبت براءته، فكل ما تحتاجه هو التشكيك في إدانته، ويؤسس هذا الاتجاه رأيه على أن بطلان دليل الإدانة الذي استخلص من إجراء غير مشروع إنما شرع لضمان حرية المتهم فلا يجوز أن ينقلب هذا الضمان عكس مصلحته[3].

وأمام هذا الاختلاف بين الاتجاهين ظهر اتجاه ثالث (وسطي) مفاده أن أداة البراءة غير المشروعة يمكن قبولها في بعض الحالات، وهذا إذا كانت الوسيلة لا تصل إلى حد الجريمة وإنما

[1] نص المادة 191 من قانون الإجراءات الجزائية الجزائري.

[2] محمود نجيب حسني، مرجع سابق، ص492.

[3] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الثالث، دار النهضة العربية، القاهرة، 1980 ص388.

تتضمن مخالفة قاعدة إجرائية فقط، ففي هذه الحالة يمكن الاستناد إلى هذا الدليل دون إهداره[1].

ويرى جانب من الفقه أن الاتجاه الثاني هو الاتجاه الأقرب للصواب والذي يقصر المشروعية على دليل الإدانة دون البراءة وذلك لأنه لو تم التمسك بعدم قبول دليل البراءة لحجة انه غير مشروع فان ذلك قد يؤدي إلى نتائج وخيمة مفادها إدانة برئ، وفي هذه الحالة يتحمل المجتمع ضريبة عقاب بريء وإفلات مجرم من العقاب ولان التشريعات في جميع دول العالم من صنع البشر يعتريها فجوات وعيوب كثيرة نجد الكثير من الناس يستطيعون خرق هذه القوانين بحجة إتباع القانون نفسه وذلك بطرق غير مباشرة، ولذلك فالقوانين الوضعية مرشحة للتعديل والتجديد في أي وقت[2].

## الفرع الثاني: مصداقية الدليل الرقمي.

إذا كان المنحى الذي اعتمده المشرع الجزائري ينعكس من خلال نص المادة 212 من قانون الإجراءات الجزائية بقولها: "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي" ، وبناء على ذلك يصح للقاضي أن يؤسس اقتناعه على أي دليل، كما يصح أن يصدره تبعا لاطمئنانه.

إلا أن تطبيق ذلك على الدليل التقني قد يثير الكثير من الصعوبات وهذا بسبب الطبيعة الفنية للدليل التقني مما يسهل أمر العبث بمضمونه على نحو يحرف الحقيقة الأمر الذي لا يستطيع إدراكه إلا المختصون في هذا المجال مما يحتم على القاضي اللجوء للخبرة الفنية للبحث في مصداقية هذا الدليل التقني، وهذا ما يقوي قيمة الدليل من الناحية العلمية على نحو لا يحتمل العكس ومن أجل ذلك سوف نعالج اقتناع القاضي بالدليل التقني أو عدمه من خلال مايلي:

### أولا: الدليل التقني يعبر عن حقيقة علمية.

الفقه الفرنسي تناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشئة عن آلة أو تسجيل أو أجهزة التصنت، ومن اجل ذلك قضى في فرنسا بخصوص قوة المحررات الصادرة

[1] رشيدة بوكر، مرجع سابق، ص494.

[2] نفس المرجع، ص495.

عن الآلات الحديثة في الإثبات بأنه إذا كانت التسجيلات الممغنطة لها قيمة الدلائل التي يمكن الاطمئنان إليها، ويمكن أن تكون صالحة في الإثبات أمام القضاء الجزائي[1].

وعليه ومما سبق يتبين أن دور الخبراء تعاظم في إبداء خبراتهم الفنية بعدما زادت أهمية الدليل التقني في الإثبات، وهذا نظرا إلى أن الكثير من الجرائم التي ترتكب تقع على مسائل الكترونية معقدة وبالمقابل نجد أن نفس هذه التقنية العلمية توفر طرقا دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل يتمتع بقوة علمية شبه قاطعة يصعب إثبات عكسها.

وتجدر الإشارة إلى أن للخبرة دور هام يمتد حتى إلى البحث في مصداقية الدليل التقني، وعلى الرغم من أن الدليل التقني وبحكم طبيعته العلمية يمثل إخبارا صادقا عن الواقع باعتبارات علمية وموضوعية وحياده وكفاءته إلا أن هذا لا ينفي إمكانية العبث فيه من ناحية وصحة الإجراءات المتبعة في الحصول عليه من أجل ذلك تحتل الخبرة في هذه الحالة دورا مهما في التثبت من سلامة هذا الدليل.

وإن اتساع مساحة الأدلة العلمية واحتلالها هذا الدور المهم في الإثبات من الممكن أن ينقص من دور القاضي الجزائي في التقدير خاصة أمام غياب الثقافة المعلوماتية للقاضي الجزائي، ومن أجل ذلك تخوف بعض الفقه من أن يطغى هذا على نظام الإقناع للقاضي فيجعل للخبير القول الفصل ومن أجل ذلك وجب التعرض للنقاط التالية[2]:

## 1/ التقييم الفني للدليل التقني.

على الرغم من أن الدليل التقني له قيمة التدليلية من الناحية العلمية ويتوافر فيه المصداقية، إلا أن هذا لا ينفي إمكانية العبث فيه، كما يمكن أن يتحصل عليه بناء على إجراءات غير مشروعة وعلى ذلك يمكن أن يشكل في الدليل الرقمي من ناحيتين:

**الأولى:** إخضاعه للعبث للخروج به على نحو يخالف الحقيقة، ومن ثم فقد تقدم هذا الدليل معبرا عن واقعة معينة، وبالتالي قد صنع أساسا من اجل التعبير عنها خلافا للحقيقة وذلك بطريقة لا

[1] رشيدة بوكر، مرجع سابق، ص497.

[2] نفس المرجع، ص498.

يستطيع كشفها إلا الشخص المتخصص، فالتقنية الحديثة تمكن من العبث بالدليل التقني بسهولة ويسر بحيث يظهر وكأنه نسخة أصلية في تغييرها عن الحقيقة.

**الثانية:** على الرغم من أن نسبة الخطأ في الدليل التقني نادرة للغاية إلا أنها تبقى ممكنة، ويرجع الخطأ في الحصول على الدليل التقني لسببين، إما لخطأ في استخدام الآلة المناسبة في الحصول على الدليل التقني، وذلك بسبب الخلل في الشفرة المستخدمة أو بسبب استخدام مواصفات خاطئة، ويرجع سبب الخطأ في الحصول على الدليل إلى الخطأ في استخلاص الدليل، ويرجع ذلك إلى اتخاذ قرارات لاستخدام الأداة نقل نسبة صوابها 100% ويحدث هذا غالبا بسبب وسائل اختزال المعطيات أو بسبب معالجة المعطيات بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها[1].

ويخضع الدليل التقني أيضا لقواعد للحكم على قيمته التدليلية من الناحية العلمية كما هو الأمر في خضوعه لقواعد معينة تحكم طرق الحصول عليه وذلك يرجع للطبيعة الفنية لهذا الدليل فهناك وسائل تقنية من نفس طبيعة الدليل تمكن من فحصه للتأكد من سلامة وصحة الإجراءات المتبعة في الحصول عليه وذلك كما يلي[2]:

أ- **تقسيم الدليل التقني من حيث سلامته من العبث:** ويتم ذلك بعدة طرق:

- عن طريق الحاسب الآلي الذي يلعب دور مهم في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل الأمر الذي يساهم في كشف التلاعب بمضمون الدليل التقني وذلك عن طريق فكرة التحليل التناظري الرقمي الذي يقارن الدليل الرقمي المقدم للقضاء وبين الدليل الأصلي الموجود في الحاسب الآلي.
- عن طريق استخدام الخوارزميات فهي عبارة عن عمليات حسابية تستخدم للتأكد من سلامة الدليل الأصلي من العبث فيه.
- عن طريق ما يسمى بالدليل المحايد وهو دليل لا علاقة له بموضوع الجريمة إلا أنه يساهم في التأكد من سلامة الدليل التقني المقصود من حيث عدم حصول تعديل أو تغيير في نظام

[1] رشيدة بوكر، مرجع سابق، ص 499.

[2] طارق محمد الجميلي، الدليل الرقمي في مجال الإثبات الجنائي، مقالة مقدمة في المؤتمر المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس-ليبيا في الفترة الممتدة من 28-2009/10/29، ص26.

الحاسب الآلي.

ب- تقديم الدليل التقني من حيث سلامة إجراءات الحصول عليه: ويتم هذا التقييم بإتباع الإجراءات التالية[1]:

- إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المرجوة، وذلك إما عن طريق اجتياز السلبيات الزائفة حيث تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل التقني وأنه لا يتم إغفال معطيات مهمة عنه، أو عن طريق اختبار الايجابيات الزائفة حيث تخضع الأداة المستخدمة في الحصول على الدليل التقني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة.

وبذلك فمن خلال هذين الاختبارين يتم التأكد من هذه الأداة المستخدمة عرضت كافة المعطيات المتعلقة بالدليل التقني وفي ذات الوقت لم تضف إليها أي بيان جديد.

- الاعتماد على الدورات التي أثبتت البحوث العلمية كفاءتها في تقديم نتائج أفضل وذلك عن طريق البحوث المنشورة في مجال تقنية المعلومات التي تبين أهم الطرق السليمة التي وجب إتباعها في الحصول على الدليل التقني، الأمر الذي يساهم في مصداقية الأدوات المستمدة من تلك الأدوات[2].

## 2/ القيمة العلمية القاطعة للدليل التقني ومدى تأثيرها على اقتناع القاضي الجزائي

الدليل التقني دليل كباقي الأدلة الجزائية يخضع للمبدأ العام في الإثبات الجزائي، وهو حرية القاضي الجزائي في الاقتناع، فوزن الأدلة وتقديرها بالكيفية التي تمكنه من تكوين عقيدته في الدعوى المعروضة عليه، ولأنه ومع تعاظم دور الإثبات العلمي مع بروز الدليل التقني إلى حقل الأدلة الجنائية كأفضل دليل لإثبات الجرائم المستحدثة ومنها جريمة الإرهاب الالكتروني –موضوع الدراسة– أصبح القاضي الجزائي ملزم بان يتعامل مع هذا الدليل محاولا الموازنة بين نقص ثقافته المعلوماتية وبين

[1] رشيدة بوكر، مرجع سابق، ص501.

[2] طارق محمد الجميلي، مرجع سابق، ص 28.

شروط السلامة التي يتمتع بها الدليل التقني من العبث والخطأ من جهة أخرى.

ومن المعروف أن القاضي الجزائي يستمد قناعته من أي دليل تطمئن إليه نفسه ويسكن إليه وجدانه دون أي قيد يقيده في ذلك إلا ما قد تقتضيه عليه العدالة ذاتها من قيود، وبالتالي فان هذه الحرية الممنوحة للقاضي الجزائي في تقدير الأدلة المقدمة قررت له بالنظر إلى صعوبة الحصول على الدليل في المواد الجزائية[1].

وقد أكد المشرع الجزائري هذا المبدأ من خلال المادة 307 من قانون الإجراءات الجزائية[2] وكذلك نص المادة 212 من قانون الإجراءات الجزائية التي تنص على طرق الإثبات.

يلاحظ أن تأكيد المشرع الجزائري على هذا المبدأ جاء نتيجة لتأثره بالمشرع الفرنسي الذي نص على هذا المبدأ لأول مرة في المادة 342 من قانون التحقيقات الجزائية التي كانت تستلزم أن يكتب نص القناعة الوجدانية في قاعة المحكمة بأحرف بارزة وفي مكان ظاهر كي يستهدي بها المحلفون وتكون بمثابة شعار لمداولاتهم[3].

فالقانون لا يسال المحلفين عن الوسائل التي أدت إلى قناعتهم، ولا يرسم لهم قواعد يتعين عليهم الخضوع لها في تقدير مدى كفاية الدليل أو ملاءمته بل يسألهم فقط عن اثر هذه الأدلة على قناعتهم وان يبحثوا عنها في قرار ضمائرهم، ومن أجل ذلك يطرح عليهم سؤال واحد وهو: هل لديكم القناعة

---

[1] محمود نجيب حسني، مرجع سابق، ص412.

[2] تنص المادة 307 من قانون الإجراءات الجزائية الجزائري على أنه: "يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة.

**(إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير أو تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم:**

**هل لديكم اقتناع شخصي؟."**

[3] وقد الغي هذا النص بمقتضى قانون 1941/11/25 بحجة أن التعليمات التي كانت تتضمنها لا لزوم لها بعد ترسخ المبدأ وثبوته ومع ذلك فإن تطبيقه لم يختلف، لأن هذه المادة نقلت حرفيا في المادة 353 من قانون الإجراءات الجزائية الحالي الصادر سنة 1958 التي تنص" لا يطلب القانون من القضاة حسابا بالأدلة التي اقتنعوا بها ولا يفرض قاعدة خاصة تتعلق بتمام وكفاية دليل ما، وإنما يفرض عليهم أن يتساءلوا في صمت وتدبر وان يبحثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجحة ضد المتهم ووسائل دفاعه".

الوجدانية.

وإذا كان المشرع قد أقر هذا المبدأ لكي يطبق أمام قضاء الحكم أصلا إلا أن ذلك لا يعني أبدا أن نطاق تطبيقه مقصور على هذه المرحلة بل ويمتد أيضا إلى مرحلة التحقيق القضائي حيث أن هذا المبدأ ينطبق على قضاة التحقيق.

ومما سبق يمكن القول أن مبدأ الاقتناع الذاتي للقاضي الجزائي هو حجر الزاوية في الأحكام الجزائية في الجزائر وبقية الدول التي اعتنقت النظام اللاتيني وعلى هذا الأساس فان ظهور الدليل التقني بكل خصائصه المفروض أن لا يغير شيئا من هذا المبدأ ومن ثم فان الدليل التقني لا يحظى بقوة حاسمة في الإثبات استصحابا للأصل[1].

وفي الأخير ومما سبق عرضه بشان سلامة الدليل التقني من العبث والخطأ فانه لا يمكن أن يتنازع القاضي في قيمة ما يتمتع به من قوة استدلالية قد استقرت له وتأكدت من الناحية العلمية فحتى وإن كانت الإمكانية في التشكيك في سلامة الدليل التقني بسبب قابليته للعبث ونسبة الخطأ في إجراءا الحصول عليه، فتلك مسالة فنية لا يمكن للقاضي أن يقطع في شانهما برأي حاسم وان لم يقطع به أهل الاختصاص، وفي هذه الحالة يقتصر دور القاضي على الظروف والملابسات التي وجد فيها الدليل التقني فهي من يدخل في نطاق تقديره الذاتي فهي من صميم وظيفته القضائية بحيث يكون في مقدوره أن يطرح مثل هذا الدليل على الرغم من قطعيته من الناحية العلمية، إذا تبين بأنه لا يتفق مع ظروف الواقعة وملابساتها حيث تولد الشك لدى القاضي ومن لم يقضي في إطار الشك يعتبر لصالح المتهم[2].

وهذا يعني انه ليس بمجرد توافر الدليل التقني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدة لتقرير اقتناع القاضي بخصوصها مسألة غير مؤكدة[3].

[1] رشيدة بوكر، مرجع سابق، ص507.

[2] نفس المرجع، ص507،508.

[3] جميل عبد الباقي الصغير، مرجع سابق، ص22.

وعليه فإنه يمكن القول أنه مهما علا شأن الأدلة التقنية والفنية في هذا الإثبات إلا أن ذلك لا يؤثر في السلطة التقديرية للقاضي في تقدير هذه الأدلة فهذا الأخير يبقى هو المسيطر على هذه الحقيقة فهذه الأدلة تجعل الحقيقة العلمية حقيقة قضائية فحسب.

## ثانيا: الدليل التقني يعبر عن الحقيقة التي تهدف إليها الدعوى العمومية.

إن تأثير التطور العلمي والتكنولوجي لا يقف عند مضمون الدليل وإنما يجب أن يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل على المستوى القانوني ومن اجل ذلك وجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها وان تكون مطروحة أمام القاضي في الجلسة ضمن أوراق الدعوى لكي تتاح للخصوم إمكانية مناقشة هذا الدليل والرد عليه وان تكون يقينية.

### 1- مشروعية الدليل التقني.

صحيح أن القانون ترك للقاضي الجزائي الحرية في أن يكون قناعته من أي دليل مقدم له وبأية وسيلة يراها موصلة للحقيقة، إلا أن هذه الحرية ليست مطلقة بحيث يبني القاضي عقيدته على أي دليل يظفر به مهما كان مصدره أو وسيلة البحث عليه بل هو ملزم بان يكون الدليل الذي يستند عليه في حكمه مقبولا في الدعوى وهذا بعد أن يتيقن من مراعاة الدليل لقاعدة المشروعية باتفاقه مع النظام القانوني في مجمله، وذلك لان الخصوصية الجزائية تقوم على ضمان حرية المتهم لا على مجرد إثبات سلطة الدولة في العقاب، وبالتالي يتعين على القاضي إلا يثبت توافر هذه السلطة تجاه المتهم إلا من خلال دليل مستمد من إجراءات مشروعة احترمت فيها الحريات وأمنت فيها الضمانات التي رسمها القانون[1].

وتماشيا مع التوصية رقم 18 للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات يشترط في الدليل التقني الذي يؤسس عليه القاضي قناعته أن يكون مشروعا وغير مخالف للقواعد القانونية وللمبادئ القانونية العامة –على نحو ما شرحنا سابقا–.

[1] رشيدة بوكر، مرجع سابق، ص510.

## 2- وضعية الدليل التقني.

إذا ما تأكد القاضي من كون الأدلة محل التقدير مقبولة قانونا، عندئذ يستكمل هذا الضابط بوجود الدليل الذي سيقدره القاضي في أوراق الدعوى، طرحه في الجلسة وبحضور الخصوم ويتم مناقشتها، وهذا يقتضي عدم جواز القاضي أن يقضي استنادا على معلوماته الشخصية أو رأي غيره[1].

وقد أرست المادة 2/212 من قانون الإجراءات الجزائية هذا الضابط (أي وضعية الدليل) والذي يعني أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته وذلك احتراما لحقوق الدفاع، وبالتالي لا يجوز للقاضي أن يبني حكمه على دليل لا صلة له في الأوراق[2]، وكذلك ما نصت عليه المادة 2/427 من قانون الإجراءات الجزائية الفرنسي بقولها: "لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الخصوم"[3]

وبالتالي واستنادا لهذه النصوص وجب تدوين كافة إجراءات الاستدلال والتحقيق، وغاية ذلك حتى يكون الخصوم على بينة مما يقدم ضدهم من أدلة، وان تتاح لهم إمكانية مناقشتها والرد عليها[4]، ومن شان ضابط وضعية الدليل أن يحقق رقابة فعالة على جدية الأدلة التي تكون قد حصلت في مرحلة التحقيق فتعرض مجددا، وهو ما يتيح في المقابل مراقبة التقدير الذي كانت سلطة التحقيق قد خلصت إليه، فقد عبرت المحكمة العليا الجزائرية عن هذا الضابط في قرار لها صادر عن الغرفة الجزائية 1982/01/21 بقولها:"لا يمكن لقضاة الموضوع أن يؤسسوا قرارهم إلا بناء على الأدلة المقدمة لهم أثناء المرافعات والتي تم مناقشتها حضوريا"[5].

وبالتالي يمنع على القاضي الجزائي أن يأخذ بأدلة تقنية لم تكن قد عرضت أثناء المرافعات، ولم

---

[1] رشيدة بوكر، مرجع سابق، ص 511.

[2] المادة 2/212 "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات التي حصلت المناقشة فيها حضوريا أمامه".

[3] رشيدة بوكر، مرجع سابق، ص511.

[4] إبراهيم القماز، الشهادة كدليل إثبات في المواد الجزائية –دراسة قانونية ونفسية– الطبعة الأولى، علم الكتاب، القاهرة 1980، ص646.

[5] رشيدة بوكر، مرجع سابق، ص 512 .

يناقشها أطراف الدعوى.

### النتائج المترتبة على وضعية الدليل التقني.

ومن أهم النتائج المترتبة على هذا الضابط.

- عدم جواز قضاء القاضي استنادا على معلوماته الشخصية أو رأي غيره وهذا حماية للخصوم من أي تأثير خاطئ على القاضي، يكون ناتجا عما وصله من معلومات خارج إطار الدعوى وألا يكون قد جمع في شخصه صفتين متعارضتين وهما صفة القاضي وصفة الشاهد مما يترتب عليه بطلان الحكم.
- ضرورة التأهيل التقني والفني للقضاة فيتطلب من القاضي الجزائي أن يكون مؤهلا تأهيل فني وتقني على كيفية التعامل مع الدليل التقني، لأنه سيكون محلا للمناقشة الحضورية بين الأطراف عند الأخذ بها كأدلة إثبات في الدعوى الجزائية، فهذا التأهيل يضمن نجاح مهمة القاضي الذي تناط به مهمة المناقشة العلمية لهذه الأدلة والهيمنة على الدعوى الجزائية ويتحقق ذلك بعقد دورا تدريسية مكثفة لهؤلاء القضاة على كافة مستوياتهم ودرجاتهم في تقنية المعلومات.

### 3- يقينية الأدلة التقنية.

فالقاضي وهو يقدر الأدلة التقنية ويوازنها وجب عليه أن يصغي لما يمليه عليه وجدانه، دون أن يخضع في ذلك لرقابة المحكمة العليا، إلا أنه مع ذلك مقيد بضرورة تأسيس قناعته على الجزم واليقين لا على الظن والترجيح وذلك لاستبعاد قرينة البراءة اللصيقة بالمتهم استنادا إلى أن الأصل في الإنسان البراءة، وإذا كانت هذه الأحكام العامة التي تحكم التقنين في الأدلة الجزائية في الجزائر وفي الدول ذات الصياغة اللاتينية، فإن الأمر يختلف بالنسبة للدليل التقني، إذ يشترط أن يكون هذا الأخير يقيني حتى يمكن الحكم بالإدانة[1]، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من أدلة تقنية، وهكذا يستطيع القاضي من خلال ذلك وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من

[1] رشيدة بوكر، مرجع سابق، ص 513.

جرائم الاعتداء على نظم المعالجة الآلية إلى شخص معين من عدمه[1].

ويستطيع القاضي الوصول إلى هذا اليقين من خلال ما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، ويصل القاضي إلى هذا اليقين من خلال المعرفة الحسية التي تدركها الحواس، أو من خلال المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها[2].

**النتائج المترتبة على يقينية الأدلة التقنية:** ومن أهمها[3]:

- حتى يستطيع القاضي أن يستبعد قرينة البراءة اللصيقة بالإنسان فيجب أن يصل إلى درجة اليقين والقطع وذلك عن طريق المعارف الحسية والفعلية والمعلوماتية.
- يكون حكم الإدانة معيبا إذا ما تأسس على ترجيح ثبوت التهمة أو إذا كان قد بني على مجرد افتراضات أو استنتاجات تخمينية لا وجود لها في الواقع.

## المطلب الثاني: صعوبات إثبات جريمة الإرهاب الالكتروني.

إن جريمة الإرهاب الالكتروني تعتبر من الجرائم النظيفة، أي التي لا تترك أثارا ضد مرتكبيها وذلك لصعوبة اكتشاف دليل ثبوتها، فلا اثر فيه لأي دماء أو عنف، وإنما كل أدلتها مجرد أرقام وبيانات يمكن تغييرها أو محوها من السجلات المخزونة في ذاكرة الحواسيب الآلية، وليس لها اثر مادي خارجي، ومن هنا نقف على حقيقة الصعوبات التي تواجه كافة أطراف المنظومة الأمنية والقضائية في هذا الصدد التي تتجلى عندما تكون الجريمة واقفة على برامج الكمبيوتر وبياناته، أو بواسطتها، وذلك بالنظر إلى قلة الآثار المادية التي قد تنتج عن هذا النوع من الجرائم، وكثرة عدد الأشخاص الذين يترددون إلى مسرح الجريمة خلال المدة الفاصلة بين وقوع الجريمة والكشف عنها[4].

[1] هلالي عبد الله أحمد، مرجع سابق، ص90.

[2] نفس المرجع، ص 91.

[3] نفس المرجع، ص 87.

[4] أمين محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة–الإرهاب الالكتروني وطرق مواجهته، مرجع سابق، ص22.

ولأن صعوبة إثبات جريمة الإرهاب الإلكتروني ترجع إلى صعوبة إثبات الدليل التقني، و تكمن هذه الصعوبة في عاملين اثنين يتعلق الأول بالطبيعة التكوينية للدليل التقني، وأما الثاني يتعلق بالعامل البشري.

## الفرع الأول: المعوقات الخاصة بالطبيعة التكوينية للدليل التقني.

يقصد بالمعوقات الخاصة بالطبيعة التكوينية للدليل التقني المشاكل الداخلية فيه والتي تتعلق بالدليل تحديدا، و ذلك بسبب الطبيعة الرقمية ذات الفلسفة التابعة من تكنولوجيا المعلومات التي يتكون منها هذا الدليل سواء بسبب الطبيعة غير المركبة له، أو بسبب طبيعة الديناميكية أو خاصية بجزء وهذه المشكلات تعود على إجراءات جمة بالسلب حيث تضعف قيمتها إذا لم يتم إيجاد حلول بشأنها.

### أولا: الطبيعة غير المرئية للدليل الرقمي.

يتميز الدليل الرقمي بأنه دليل غير مرئي فهو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأرقام الثنائية(0-1) و التي لا تفصح عن شخصية معينة، و ما يخلفها الجاني من بيانات غير مرئية هي في الحقيقة بيانات مسجلة إلكترونية بكثافة بالغة وبصورة مرمزة وغالبا على دعائم و وسائط تخزين ممغنطة، لا يمكن قراءتها إلا عن طريق وسيلة إلكترونية مخصصة لذلك مثل الكمبيوتر[1].

كما أن الجاني لا يترك أي أثر يدل عنه مما يحول دون التعرف عليه و هذا يعد من أبرز المشاكل التي تواجه جهات التحري و التحقيق و كذا أثناء عرض الدليل على القاضي، بالإضافة إلى أن القرص الصلب محل الضبط يحتوي مزيجا من البيانات المختلطة فيما بينها و التي تكون كلها ذات صلة بالجريمة موضوع البحث، بمعنى يحدث أن هناك اختلاط بين الملفات المرئية و الملفات الدالة على ثبوت الجريمة مما يؤدي إلى إيثار مشكلة التعدي على الخصوصية، كما أن السبب في افتقاد الآثار التقليدية للجريمة المعلوماتية، والأمر الذي لاحظه جانب من الفقه مما دعائم إلى القول أن هناك بعض العمليات التي يجب إدخال بياناتها مباشرة في أجهزة الحاسب الآلي دون أن يتم تحديد ذلك عن طريق النقل من وثائق و مستندات ورقية و عليه في إدخال بيانات غير مطلوبة تكون مخرجات على حساب هوى المستعمل، و بهذا يقتضي الأمر توافر

[1] بن فردية محمد، مرجع سابق، ص 214.

الإمكانيات المادية والبشرية واستقطاب أجهزة الكفاءة المهنية المتخصصة في هذا المجال لكي يتم الاستعانة بها في كشف هذا النوع من الجرائم و ضبط الأدلة، ثم عرضها على القاضي وكل هذا مما يؤثر في مسألة قبول القاضي للدليل، يضاف إليه مسألة شكل قبول هذا الدليل غير المرئي، فهل يقبله بصورة مستخرج من طابعة أو مشاهدة فيديو من على القرص، أو من خلال شاشة الحاسوب، لكي يبني عليه حكمه بالإدانة أو البراءة[1].

## ثانيا: الطبيعة الديناميكية للدليل الرقمي

إن الأدلة الرقمية ذات الطبيعة ديناميكية فائقة السرعة إذ تنتقل عبر شبكات الاتصال بسرعة فائقة، وهذا يعني إمكانية تخزين المعلومات في الخارج على الخادم بواسطة شبكة الاتصال عن بعد وهذا ما قد يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط الأدلة الرقمية و البحث عنها لأنه يستلزم القيام بها خارج جهود الدولة في نطاق دولة أخرى حيث ارتكبت الجريمة أو جزء منها الأمر الذي يصطدم بمشاكل الحدود والولايات القضائية مما ينطوي عليه من مساس بسيادات الدول وهذه المشكلة تظهر بصورة واضحة أثناء اتخاذ إجراءات التفتيش لضبط هذه الجرائم، و منها جريمة الإرهاب الإلكتروني عندما يكون نظام المعالجة الآلية متصلا بنظم أخرى خارج الدولة، ويكون تفتيش هذه النظم ضروريا لكشف خفايا هذه الجريمة مثلا الإرهاب الإلكتروني[2].

مما سبق تجدر الإشارة إلى أن الحاجة تفرض الحصول على إذن الدولة التي يتم إجراء البحث في مجالها الإقليمي أو ابرم اتفاقيات و معاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي الذي يهدف إلى التقريب بين القوانين الجزائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود.

وتعد اتفاقية بودابست التي ابرمها المجلس الأوربي و المتعلقة بتقنية المعلومات الموقفة في 2001/11/23، و التي أيدتها الولايات المتحدة الأمريكية بقوة هي أول خطوة رئيسية في هذا الاتجاه

[1] بن فردية محمد، مرجع سابق، ص 214.

[2] رشيدة بوكر، مرجع سابق، ص 457.

ويمكن اعتبارها بداية لعمل وضع القواعد و المعايير التي يتوقع من البلدان الموقعة على الاتفاقية ومنهم الجزائر أن تتبعها و هذا في مجال جهودها في مكافحة مثل هذه الجرائم الخطيرة[1].

وقد خصصت اتفاقية بودابست الباب الثالث منها لدراسة التعاون الدولي، وهذا وقد نصت المادة 23 منها على ضرورة تعاون الأطراف فيما بينها وفقا لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المسائل الجزائية والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقوانين المحلية إلى أقصى مدى ممكن بغرض التحقيقات والإجراءات المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية، والبيانات المعلوماتية أو الجمع الأدلة ذات الشكل الالكتروني لمثل هذه الجرائم[2].

وفي هذا الصدد نجد أن المشرع الجزائري قد خصص الفصل السادس من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها للتعاون والمساعدة القضائية الدولية، وما يتبع ذلك من ضرورة أن تطلب الجزائر الدعم من الدول التي سبقتها في هذا المجال على غرار اتفاق التعاون بين الجزائر وفرنسا المتضمن التعاون الأمني والدعم التقني للشرطة الجزائرية لمحاربة المجرمين الالكترونيين، إذ يجب إذا اقتضت الضرورة وضع قانون يسهل هذا التعاون بين الجزائر والدول الأخرى[3].

### ثالثا: سهولة محو الدليل أو تعديله.

من أبرز الصعوبات التي يمكن أن تعترض عملية الحصول على الدليل الرقمي وبالتالي إثبات جريمة الإرهاب الالكتروني باعتبارها جريمة معلوماتية ونسبتها إلى المتهم بسهولة تعديل الدليل الرقمي أو محو وتدميره في فترة زمنية وجيزة[4]، وذلك كونه دليل غير مرئي فهو عبارة عن نبضات مغناطيسية، وبالتالي فإن هذه النبضات يمكن محوها بسهولة ويسر دون أن تترك أي اثر يذكر عكس الدليل المادي الذي يترك الكثير من الآثار اثر محاولة إزالته أو التخلص منه.

[1] رشيدة بوكر، مرجع سابق، ص 497.

[2] المادة 23 من اتفاقية بودابست لسنة 2001 .

[3] رشيدة بوكر، مرجع سابق، ص 458.

[4] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2001، ص 04.

كما أن الإرهابي الالكتروني يستطيع أن يدمره من بعيد و من أي منطقة بالعالم ويسهل عليه كثيرا أن يتنصل من الجريمة ويقطع كل صلته بها[1].

هذا ومن الصعوبات التي تعترض الإثبات الجنائي فيما يتعلق بالأدلة الرقمية أن الجاني يستطيع الدفع بأن الدليل الرقمي قد تم تعديله فبمجرد لمس مفاتيح لوحة المفاتيح يمكن تغيير البيانات المتعلقة بإدانة الشخص أو تبرئته لذلك فإن غالبية هذا النوع من الجرائم إما أن يقيد باسم مجهول لاستعمال أصحابها أسماء مستعارة، أو دخولهم إلى شبكة الانترنت من خلال مقاهي الانترنت مما يتعذر الوصول إلى الجناة الحقيقيين لتلك الجرائم، وعليه نجد القاضي يصعب عليه إدانة شخص دون أن يتأكد يقينيا بان هذا الشخص هو المذنب في ارتكاب الجريمة، ويرى جانب من الفقه حول ضرورة تدخل المشرع بإضافة حالة ارتكاب الجرائم المعلوماتية عموما ( منها الإرهاب الالكتروني كظرف استثنائي يسمح لرجال الضبطية القضائية القيام بضبط الأدلة عند وقوع الجريمة دون الحصول على إذن مسبق من النيابة العامة لتفادي مثل هذه الدفوع وللتأكد من أن هذا الدليل لم يتم التغيير فيه كتدبير الإرهابي لموقع الكتروني كان يجند من خلاله إرهابيين أخريين أو يعلم الغير كيفية صناعة الأسلحة و المتفجرات[2].

هذا وقد نصت اتفاقية بودابست في المادة 16 منها على ضرورة السماح لكل طرف لسلطاته المختصة أن تأمر أو تفوض بطريفة أخرى مزود الخدمة التحفظ على المعطيات المعلوماتية المحزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي[3].

والتحفظ على المعطيات بغير إجراء أولي أو تمهيدي يهدف إلى المحافظة على المعطيات قبل حذفها و فقدها، وهي المبررات التي حددتها المذكرة التفسيرية لاتفاقية بودابست والتي تدعو إلى اتخاذ هذا الإجراء كتالي[4]:

---

[1] Yam padova, un aperçu de la lutte contre la cybercriminalité en franc, revue de science criminelle et droit pénal compare, 03/02/2002, p 771.

[2] بن فردية محمد، مرجع سابق، ص 216.

[3] رشيدة بوكر، مرجع سابق، ص 459.

[4] هلالي عبد الله أحمد، ص 190.

1- قابلية المعطيات المعلوماتية للتلاشي، حيث تكون محلا للمحو أو التغيير سواء كان ذلك بواقع إجرامي أو غير ذلك، و ذلك في إطار الحذف الروتيني للمعطيات التي لم تعد الحاجة إليها.

2- في الغالب يتم ارتكاب جميع الجرائم المعلوماتية عن طريق نقل الاتصالات عبر نظم الحاسوب حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة مثل الفيروسات، فتحديد مصدر هذه الاتصالات يمكن أن تساعد في تحديد هوية مرتكبي الجريمة.

3- تأمين الدليل الرقمي من الضياع، حيث يتم نسخ الدليل على نشاط جنائي من قبل مزودي الخدمات، مثل المراسلة الالكترونية التي تم إرسالها أو استقبالها، و من ثم يمكن الكشف عن دليل جنائي للجرائم المرتكبة لمكافحة، المشرع الجزائري نص على التحفظ كسلطة قانونية لجرائم المستحدثة و منها جريمة الإرهاب الالكتروني و ذلك من خلال نص المادة العاشرة من القانون 09-04 لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال مكافحتها و ذلك حسب نص المادة العاشرة السالفة الذكر[1].

ويلاحظ انه بالرغم من أهميتها خاصة إذا تعلق الأمر بتتبع مصدر أو مكان وصول الاتصالات الالكترونية وبالتالي تحديد هوية الجناة إلا أن نطاق تطبيق هذه المادة لا يمتد إلى التحفظ على المعطيات وعليه إذا كان الأمر متعلق بحفظ معطيات سبق وجودها وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها فان السعي لدى مزود الخدمة بقصد التحفظ عليها يحتاج إلى غطاء من المشروعية يبرر له قيامه بذلك، وعلى ذلك يتعين على المشرع الجزائري أن يتدخل لسن قاعدة قانونية إجرائية ينظم فيها الوضع القانوني للتحفظ على المعطيات المخزنة تحت سيطرة مزود الخدمات وذلك على نحو ما فعلت به اتفاقية بودابست[2] -على ضوء ما تم شرحه-.

[1] نص المادة 10 من القانون 09-04 على أنه:" في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدات للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة .....".

[2] رشيدة بوكر، مرجع سابق، ص461.

### رابعا: صعوبة الحصول على الدليل الرقمي.

إن صعوبة الوصول إلى الدليل الالكتروني يعود إلى عدة أسباب أهمها صعوبة تتبع الجريمة وهذا راجع لوقت ارتكابها كون هذه العملية تمر عبر العديد من الحواسيب الآلية المنتشرة عبر العالم فكثير من هذه الأجهزة غير مصمم اليوم بعملية التتبع وأن يسهلها وهذا بسبب أن عنوان الانترنت يستقبل فقط عنوان الحاسب الآلي المتصل به مباشرة لا عناوين مصادر الاتصال وكذلك مسألة استخدام تقنيات التشفير من كلمات السر أو دس تعليمات خفية أو ترميزها بين الجماعات الإرهابية ...الخ، الأمر الذي يقلل من قدرات جهات التحقيق للوصول إلى الدليل.

وعليه فإن المسائل المثارة في هذا الإطار هو مدى سريان الحماية الفنية المعمول بها بموازاة الاطلاع غير المصرح به على الأوراق المختومة أو المغلقة لتمتد إلى نظام المعالجة الآلية للبيانات والمحمي فنيا ضد الاختراق ومن اجل ذلك يرى جانب من الفقه أن المادة 52 من قانون الإجراءات الجزائية المصري[1] والتي تقابلها المادة 58 من قانون الإجراءات الجزائية الاتحادي الإماراتي والتي تحضر اطلاع مأموري الضبط القضائي على الأوراق المختومة أو المغلقة الموجودة في منزل المتهم عند تفتيشه، فهل يطبق هذا الحضر على البيانات المخزنة كليا أو جزئيا؟

وهنا يرى جانب من الفقه يحضر الاطلاع لسببين[2]:

1- أن سبب حضر الاطلاع على الأوراق المغلقة هو حماية المشرع لحق الخصوصية المتمثل في رغبة صاحبها عدم اطلاع الغير عليها، بدليل انه اتخذ سبيل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها وهو غلقها أو ختمها، وذات العلة تتوافر في البيانات المعالجة آليا بحيث لا يمكن دون مفتاح الشفرة أو كود الدخول إلى نظام هذه البيانات.

2- المادتان 52، 58 سالفتي الذكر تصنعان قاعدة عامة بالنسبة للاطلاع على الأسرار التي حصنها صاحبها ضد الاطلاع غير المصرح به أيا كان وعاء هذه الأسرار يستوي أن يكون وعاء تقليدي كالأوراق أو حديث كالأقراص المرنة والممغنطة.

---

[1] نص المادة 52 "إذا وجد في منزل المتهم أوراق مختومة أو مغلقة بأي طريقة فلا يجوز لمأمور الضبط القضائي أن يفضها"

[2] بن فردية محمد، مرجع سابق، ص217.

المشرع الألماني بدوره ذهب في نص المادة 110 من قانون الإجراءات الجزائية إلى قصر الاطلاع على النائب العام وحده دون رجال الضبطية القضائية وأن مهمتهم في هذا الجانب هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية.

وفي اعتقاد الباحث أن هذا الرأي هو الصائب حتى يتم المحافظة على خصوصية الحياة الخاصة من جهة وتحقيق المصلحة العامة وملاحقة الجناة من جهة أخرى، وهذا الإجراء يحقق نوع من التوازن.

## الفرع الثاني: الصعوبات المتعلقة بالعامل البشري.

تتعدد صعوبات الإثبات الجنائي الرقمي في جريمة الإرهاب الالكتروني على ضرورة تعاون الأطراف من خلال تطبيق وسائل التعاون الدولي في المسائل الجنائية بغرض التحقيقات في الإجراءات الجنائية المتعلقة بالجرائم المعلوماتية أو بجمع الأدلة الالكترونية[1].

### أولا : البعد عن مسرح الجريمة

إن جريمة الإرهاب الالكتروني كغيرها من الجرائم المعلوماتية تتم عن بعد وعبر شبكة الانترنت حيث لا يتواجد الفاعل دوما في مسرح الجريمة، ومن ثم تتباعد المسافات بين الفاعل والنتيجة، وقد لا تقف هذه المسافات عند حدود دولة واحدة بل تمتد إلى نطاق دولة أخرى مما يصعب كشفها وملاحقة مرتكبيها.

كما أن القاضي قد لا يكون مختص بالحكم فيها، بالإضافة إلى أن الجناة في الغالب ما يستخدمون أسماء مستعارة، كما قد يدخلون إلى الشبكة عن طريق مقاهي الانترنت[2].

وتعتبر مسألة تخفي الجاني وبعد مكان ارتكاب الجريمة مسألة عويصة تتميز بها الجرائم المعلوماتية وخاصة جريمة الإرهاب الالكتروني، ومن أجل ذلك أوصى مجلس الدولة الفرنسي في

[1] المادة 22 من اتفاقية بودابست لسنة 2001.

[2] بن فردية محمد، مرجع سابق، ص 221.

تقريره المتعلق بالانترنت والشبكات الرقمية بضرورة التزام مقدمي الخدمات الوسيطة التعاون مع جهات التحقيق عن طريق إمدادها بالبيانات الشخصية الخاصة بالعملاء المشتركين لديهم[1] .

وهذا الأمر أكدته اتفاقية بودابست في مادتها 18 وذلك بضرورة إلزام مقدمي الخدمات البيانات والمعلومات التي بحوزتهم من أجل المساعدة في تحديد هوية الشخص المطلوب (الإرهابي).

أما في ألمانيا نجد أن الفقه الألماني يشكك في إمكانية الدخول إلى أنظمة تقنية المعلومات لدى الحاسبات الأخرى الموجودة في الخارج بغرض ضبط الدليل الرقمي، لأن اتخاذ هذا الإجراء دون موافقة الدولة المعنية يعد انتهاكا لسيادتها.

ولأجل مواجهة هذه المعضلة قامت العديد من الدول بعقد العديد من المعاهدات والاتفاقيات الثنائية والجماعية بهدف التقريب بين القوانين الجنائية الوطنية من أجل الحصول واثبات هذا النوع من الأدلة العابرة للحدود الوطنية .

فاتفاقية بودابست قامت بتخصيص الباب الثالث للتعاون الدولي حيث نصت المادة 23 منها على ضرورة تعاون الأطراف من خلال تطبيق وسائل التعاون الدولي في المسائل الجنائية بغرض التحقيقات والإجراءات الجنائية المتعلقة بالجرائم المعلوماتية أو لجمع الأدلة الالكترونية.

## ثانيا: إحجام المجني عليه عن التبليغ عن الجريمة الالكترونية.

وخاصة جريمة الإرهاب الالكتروني وهذا بسبب الطبيعة الخاصة بالجريمة المعلوماتية التي تجعلها نثير الكثير من المشكلات وأبرزها صعوبة اكتشاف هذه الجرائم وكثيرا ما تكتشف هذه الجرائم عن طريق الصدفة، كما انه وفي الجزائر بالذات نلاحظ قلة في القضايا الأمنية والقضائية المنشورة والمتعلقة بالجريمة الالكترونية ويكمن السبب في ذلك إلى كون هذه الجرائم تكون في الغالب مجهولة ومستترة وتتم في بيئة رقمية لا تترك وراءها أي اثر خارجي وذلك عن طريق تلاعب الفاعل غير المرئي في النبضات أو الذبذبات الالكترونية التي تسجل المعلومات عن طريقها، فلا يلاحظها المجني عليه ولا يدري حتى بوقوعها كأن يقوم الإرهابي بإدخال فيروس إلى موقع معين يستهدفه فيظل هذا

[1] بن فردية محمد، مرجع سابق، ص 221.

الفيروس كامنا إلى غاية اللحظة المحددة فيقوم بتدمير الموقع وتخريب، وفي أغلب الأوقات حتى إذا اكتشف المجني عليه ذلك يعمد إلى التستر والصمت ولا يعترف بأنه ضحية لهجمة الكترونية إرهابية[1].

هذا وقد أجريت دراسات في فرنسا دلت على أن الجريمة المعلوماتية التي تم اكتشافها لم تمثل إلا 1%، فدراسة هذه الظاهرة برمتها يزيد من صعوبة هذه الجرائم وإثباتها، الأمر الذي عبر عنه علماء الإجرام بمصطلح "الرقم الأسود" وهو ما يعيق رسم البيانات الجنائية السليمة لمواجهة الجرائم المعلوماتية وخاصة جريمة الإرهاب الالكتروني[2].

وقد ذهب آخرون إلى رفض تعاون الجهات الأمنية، ويسعون بدلا من ذلك إلى محاولة تجاوز آثارها حتى ولو كانت الوسيلة هي مكافأة المجرم، وقد أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في "ريوديجانيرو" بالبرازيل في الفترة من 4-9 سبتمبر 1994 بضرورة تشجيع المجني عليهم على الإبلاغ عن هذا النوع من الجرائم فور وقوعها، وهو ما أوصى به المجلس الأوروبي وهذا بهدف تخفيض الرقم الأسود للجرائم المعلوماتية[3]

ويرى جانب من الفقه أن طرق وصول خبر الجريمة المعلوماتية إلى سلطات الضبط ترتبط بعدة تدابير منها قدرة الرصد الأمني ومدى جاهزية سلطات الضبط والتحقيق، كما تعتمد على قدرة ومدى وعي المواطنين[4].

أما في الولايات المتحدة الأمريكية فقد طالبت من أجل تفعيل عملية إبلاغ الضبطية القضائية بان تتضمن القوانين المتعلقة بجرائم الحاسب والمعلومات نصوص تلزم موظفي الجهة المجني عليها بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال إلا أنه عند عرض هذا الاقتراح على لجنة خبراء المجلس الأوروبي قوبل بالرفض لسبب قانوني مؤداه أن الضحية (المجني عليه) سوف تصبح متهمة ولذلك وردت اقتراحات بديلة منها الالتزام بإبلاغ جهة خاصة وتشكل أجهزة

[1] رشيدة بوكر، مرجع سابق، ص471.

[2] حسين محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الانترنت، رسالة دكتوراه في القانون –كلية الحقوق– جامعة عين شمس،2000، ص148.

[3] Hans G.Nilsson, computer crimes and other crime against 1 information technology within the working programmer of the council of Europer R I D P Vol.64 1 st et 2 end tremesters 1993,p121,124.

[4] بن فردية، مرجع سابق، ص224.

خاصة بتبادل المعلومات وكذلك إصدار شهادة امن خاصة تمنح بعد مراجعة دقيقة من هيئة ويتعين على هذا الأخير إبلاغ الشرطة بما تكتشفه من جرائم/ وفي هذا الإطار استحدثت الصين شرطة متخصصة لملاحقة الاختراقات الالكترونية حيث أسس أحد الأقاليم الصينية أول وحدة بوليسية لمراقبة استخدامات شبكة الانترنت، كما أن الشرطة الدولية (الانتربول) بدأت تهتم بمكافحة جرائم الانترنت وأنشأت لديها فرقة خاصة لهذا الغرض وهي على اتصال دائم بفرق مكافحة الجريمة المعلوماتية في أوروبا والولايات المتحدة الأمريكية[1].

### ثالثا: نقص خبرة سلطات الاستدلال والتحقيق والحكم.

تختلف الجرائم المعلوماتية ومنها جريمة الإرهاب الالكتروني باعتبارها الجريمة الأخطر عن غيرها من الجرائم المادية الأخرى، في أن عملية ضبط الأدلة فيها عملية تقنية بحتة تتطلب إتباع استراتيجيات خاصة ومهارة وذكاء فائقين كونها في مواجهة تقنيات الحاسب الآلي، ويقابل ذلك نقص الخبرة لدى رجال الضبطية القضائية وأجهزة العدالة الجنائية، فيما يتعلق بثقافة الحاسوب، والإلمام بعناصر الجريمة المعلوماتية وكيفية التعامل معها على الأقل في البلدان العربية نظرا لأن تجربة الاعتماد على الحاسوب وتقنياته جاءت متأخرة عن أوروبا وأمريكا، ومن هنا تظهر الدعوة في مجال تأهيل المحققين ورجال العدالة بصفة عامة.

كما أن الكثير من الدول أصبحت تعتمد على رجال الشرطة المتخصصين في المعلوماتية ورغم ذلك تبقى صعوبة مواجهة الجرائم المعلوماتية قائمة واستنباط الدليل الرقمي وهذا راجع إلى التطور المذهل الذي تشهده العالم الرقمي وانتشار الحواسيب في الأماكن العامة والخاصة[2].

والأمر الذي يزيد من الصعوبة في هذا الإطار افتقار شبكة الانترنت إلى الرقابة وضوابط التدقيق والمراجعة فضلا عن كون هذا النوع من الجرائم عابرا للحدود فكثير ما تفشل جهات التحقيق في تعقب الجاني، بل وان جهة التحقيق في حد ذاتها يمكن أن تدمر الدليل بخطأ منها أو نتيجة إهمال وهذا الأمر حدث كثيرا في الولايات المتحدة الأمريكية حيث جاء في توصية المجلس الأوروبي رقم

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة 2007، ص117.

[2] بن فردية محمد، مرجع سابق، ص226.

95 /13 بتاريخ: 1995/09/11 في شأن مشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسوب وإعداد برامج خاصة في مجال تأهيل العاملين في مجال العدالة الجنائية[1].

وفي نفس الإطار أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريوديجانيرو بالبرازيل بين 4-9 سبتمبر 1994 بضرورة تدريب الجهات القضائية الخاصة بالتحقيق والحكم في ذلك النوع من الجرائم والتقنية المستحدثة فيها، ونظرا لانتشار التقنية الرقمية في شتى نواحي الحياة وما ارتبطت به من قيام جرائم متناسبة معها حتم على أجهزة الشرطة في إطار جمع الاستدلالات وكذلك الأمر بالنسبة للقضاة وهذا للسعي دوما إلى تطوير أسلوب الكشف عن الجريمة والتيقن من الدليل الرقمي ونسبته إلى الجاني وإنشاء برامج ودورات تخصصية وتدريب أفرادها على تعلم التقنية الرقمية[2].

ومما تقدم في هذا العنصر يمكن أن نلخص أهم الصعوبات التي تعترض إثبات جريمة الإرهاب الالكتروني فيما يلي:

1- **البعد الدولي:** يجري النفاذ إلى أنظمة الحاسوب في احد البلدان ويتم التلاعب بالبيانات في بلد آخر وتسجل النتائج في بلد ثالث، هذا فضلا على انه يمكن تخزين أدلة الجريمة الالكترونية في جهاز حاسوب موجود في بلد غير الذي ارتكب فيه المجرم فعله، بالتالي يستطيع المجرم الالكتروني إخفاء هويته، ونقل المواد من خلال قنوات موجودة في بلدان مختلفة في قارات مختلفة قبل الوصول إلى المرسل إليهم، نتيجة القدرة على التنقل الكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة بحيث تقع الجريمة في عدة دول وتحكمها عدة

[1] بن فردية محمد، مرجع سابق، ص227.

[2] هشام فريد محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط- مصر، 1994، ص21.

قوانين وقواعد معنية بذلك مما يشكل تحديا أمام الجهات القضائية في تطبيق القانون ويزيد من صعوبة التحقيق فيها[1].

2- مهارة التخزين الالكتروني للمعطيات التي يجعلها غير مرئية وغير مدركة بالعين المجردة.

3- تشفير البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال.

4- سهولة محو الأدلة في زمن قصير.

ومن أجل هذا فإن إعداد رجال الضبطية القضائية وكذا القضاة من أجل البحث عن أدلة الإثبات للجريمة الالكترونية يكتسي أهمية بالغة في عالم المعلومات وشبكات الكمبيوتر القائم على تقنية الاتصالات والتوصيلات والوسائط الالكترونية، وهذا لأن سلطة البحث والتحري والتحقيق لا تستطيع تطبيق الإجراءات التقليدية على جريمة الإرهاب الالكتروني بالخصوص، ومن أجل ذلك وجب تدريب وتكوين كل من رجال الضبط القضائي وكذا القضاة في ميدان الرقمية على نحو ما تم توضيحه سابقا[2].

## المبحث الثاني: القواعد الإجرائية الخاصة باستخلاص الدليل .

تنقسم هذه القواعد إلى قواعد تقليدية متبعة في كافة الجرائم وقواعد مستحدثة أو حديثة دعت إليها ضرورة مكافحة الجرائم المستحدثة التي ترتكب باستخدام تقنية المعلومات ومنها وأهمها وما يعنينا -في هذه الدراسة- جريمة الإرهاب الالكتروني.

ومن أجل ذلك قسمنا هذا المبحث إلى مطلبين اثنين خصص مطلب إلى القواعد التقليدية ومطلب أخر خصص إلى القواعد المستحدثة.

[1] أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة- الإرهاب الالكتروني وطرق مواجهته، بحث مقدم في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، خلال الفترة 2-4 /2014/09 ، عمان- الأردن، ص23.

[2] نفس المرجع، ص 23.

## المطلب الأول: القواعد التقليدية الخاصة باستخلاص الدليل.

يشكل تقديم البلاغ في جريمة الإرهاب الالكتروني أهمية بالغة كغيره من الجرائم بل يمكن القول إن الأهمية تزيد نظرا لطبيعة الجريمة وهذا للإحجام عن الإبلاغ عن هذا النوع من الجرائم في مجتمعاتنا العربية خاصة، فقد تحجم الكثير من الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك عن الكشف عن هذه الجريمة حتى بين موظفيها وتكتفي باتخاذ الإجراءات الإدارية الداخلية فقط دون إبلاغ السلطات المختصة تجنبا للأضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[1] والاهم حتى لا ينتشر الرعب بين الناس.

وتعقب تلقي البلاغ أو الشكوى سرعة الانتقال لمسرح الجريمة لبدء إجراءات المعاينة، وتختلف المعاينة في جريمة الإرهاب الالكتروني عنها في الجريمة الإرهابية التقليدية، حيث تثير البيئة الرقمية الكثير من القضايا المتعلقة بكيفية إجرائها.

### الفرع الأول: الخبرة والمعاينة .

تعتبر البلاغات والشكاوى وسيلة يتم بواسطتها نقل نبأ وقوع الجريمة إلى الضبطية القضائية وبعدها يمكن للضبطية القيام بإجرائي المعاينة والخبرة من أجل ذلك لا يحق لضباط الشرطة القضائية رفض البلاغات وعدم قبوله، ومن أجل ذلك سوف نتعرض إلى تلقي البلاغات والمعاينة ، وبعدها سوف نتعرض للخبرة القضائية.

#### أولا: تلقي البلاغات والمعاينة.

بعد أن يتلقى ضباط الشرطة القضائية البلاغ يسارعون في القيام بالمعاينة بغية الوصول إلى الأدلة الضرورية للكشف على الحقيقة ومن أجل ذلك زاد اهتمام الفقهاء ورجال القانون بأمر البلاغات.

#### تلقي البلاغات.

تناول العديد من الفقهاء وخبراء البحث الجنائي تعريف البلاغ، فالبعض عرفه بأنه ما يصل إلى علم رجال الضبط القضائي من معلومات حول واقعة يعتبرها القانون جريمة وهناك من عرفه بأنه

[1] خالد حازم الإبراهيمي، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية " الانترنت"– دراسة مقارنة ، (دون دار نشر)، (دون مكان نشر)، 2014، ص208.

إخبار السلطات المختصة بالتحقيق عن جريمة وقعت أو على وشك الوقوع وإن هناك أدلة أو قرائن على وجود نية اتفاق أو عزم على ارتكابها، أو وجود شك أو خوف من أنها ارتكبت[1] .

كما يعرف البلاغ أيضا أنه ذلك الإجراء الذي يقوم به الشخص لم يلحقه ضرر من الجريمة لإيصال نبئها إلى العدالة، أو ذلك الاتصال الأول الذي يقوم به الفرد لدى المصالح المختصة[2].

وبالتالي يختلف البلاغ عن الشكوى كون هذه الأخيرة تكون من المجني عليه أو من المتضررين من الجريمة، ويقصد بها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشان جرائم معينة حضر المشرع تحريكها قبل تقديمه هذا البلاغ[3] .

ويتطلب القانون في البلاغ في الجريمة الإرهابية الالكترونية شكلا معينا حاله في ذلك حال البلاغ في كافة الجرائم، وهدف المشرع من ذلك حتى لا يتهرب الأفراد من التبليغ[4] .

وعلى ذلك فإن التبليغ يكفي أن يكون مستوفي بيانات على نوع الحادثة وتحديد المجني عليه ووقت وقوع الجريمة، وبيانات الإصابات والأسباب والدوافع لارتكاب الجريمة، وتحديد شخص المتهم .

كما يقدم البلاغ كتابة أو شفاهة بمعرفة من المجني عليه أو أحد الشهود أو بمعرفة الجاني نفسه عندما يبلغ بالجريمة، ويسمى في هذه الحالة بالبلاغ المادي .

كما قد يقدم البلاغ بواسطة البريد أو البرق أو التليفون أو الصحف، ويسمى البلاغ المعنوي، كما قد يقدم البلاغ عن طريق الانترنت بواسطة البريد الالكتروني، ويسمى في هذه الحالة بالبريد الرقمي وهناك من يرى أنه يمكن إرسال البلاغ عبر البريد الالكتروني للجهة المختصة[5].

وجدير بالذكر أن افتقاد بيان واحد أو بعض البيانات لا يمنع تحرك الضبطية القضائية للقيام بأعمال التحري والاستدلال .

---

[1] رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي، القاهرة، 2005، ص 263.

[2] خالد حازم الإبراهيمي، مرجع سابق، ص 211.

[3] Jean Paul, masseron manuel, Pratique de la procédure policière, préface de robe, poplawsky, paris, 1946, p 16,17.

[4] بغدادي جيلالي، التحقيق –دراسة مقارنة– نظرية تطبيقية، الطبعة الأولى، الديوان الوطني للأشغال التربوية الجزائر، 1999، ص 24.

[5] خالد حازم الإبراهيمي ، مرجع سابق، ص 211.

ويجب لتحريك الدعوى الجزائية اتهام شخص محدد بارتكاب الجريمة، كما أن مضمون البلاغ لا يلزمه محكمة الموضوع، ولكن العبرة بما تقتنع به المحكمة مما تستخلصه من فهم الواقعة[1] .

وللتبليغ عن الجرائم أهمية بالغة تكمن في مساعدة السلطات في مكافحتها والحد منها وخاصة الخطيرة منها كجريمة الإرهاب الالكتروني، كما يعتبر التبليغ سلوك حضاري تقاس بها درجة الحس المدني لدى الأمم[2].

ونظرا لأن جريمة الإرهاب الالكتروني جريمة خطيرة ومخيفة فالغالب أن التبليغ عنها يتم بطريقة رقمية (الكترونية) نظرا للخوف الذي قد يعتري المبلغ، حيث يقدم البلاغ عبر الانترنت مما يمكن الضبطية القضائية من ربط البيانات المدونة به (البلاغ)، بنظام برمجي مرتبط بقاعدة معلوماتها الرقمية ليقدم المعلومات عن المكان والأشخاص الوارد ذكرهم في البلاغ، ورصد التحريات الكاملة حول الواقعة وأشخاصها والتوصل إلى الخطوات التي اتخذها المجني عليه قبل وقوع الجريمة إلى وقت حدوثها .

كما يتم جمع المعلومات عن الجاني والمجني عليه، وكل من ارتبط مع الواقعة الإجرامية التي تكفل القيام بسير أعمال الاستدلال، والتحقيق[3].

وعلى الرغم من عدم اشتراط القانون أن يكون الشخص مصدر البلاغ معلوما لدى الجهات المختصة حتى تتمكن الضبطية من فحص البلاغ، إلا أنه إذا تعلق الأمر ببلاغ رقمي، إن هذا الأخير يقيد بقواعد علم الحاسب وشبكة الانترنت للقائمين على التحريات الفنية بجهات الضبط استخدام الوسائل التقنية الحديثة لتتبع مصدر البلاغ على الشبكة ومن ثم الشخص المبلغ[4].

وكلما كان البلاغ دقيقا كلما ساعد رجال الضبطية القضائية فإذا كانت الوقائع تشكل جريمة الإرهاب الالكتروني يبدأ وضع التصور المبدئي لخطة التعامل مع الواقعة المرتكبة من حيث تجهيزات الانتقال إلى مسرح الجريمة والخطة التي سوف يتم التعامل بمقتضاها في الكشف عن تفاصيل الواقعة

[1] خالد حازم الإبراهيمي ، مرجع سابق، ص 211.

[2] العيش فضيل، شرح قانون الإجراءات الجزائية، مطبعة البدر، الجزائر، 2008، ص 101.

[3] خالد حازم الإبراهيمي ، مرجع سابق، ص 214.

[4] عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي– المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، (مكان النشر غير موجود)، (سنة النشر غير موجودة) ص836.

وتحديد نوع الخبرة المتطلبة للعمل في الواقعة، ورجال البحث المفترض انتقالهم لمحل الواقعة وأدوارهم في إجراء معاينة محل الواقعة[1].

وأهم الأسئلة الاسترشادية التي يمكن لضباط الشرطة القضائية أن يجيب عليها إذا تعلق الأمر بالبلاغ الرقمي محل المعاينة كنوع من تسهيل المهمة للوصول إلى الجاني في اقرب وقت ممكن، كأن يتأكد هل المبلغ يوجد لديه نظام IDS (نظام اكتشاف الهجوم أو الاعتداء) ومصدره، وهل الجاني مازال على اتصال بشبكة الانترنت أم قطع اتصاله بعد ارتكاب جريمته، هل يوجد متهم واضح ومحدد وهل النظام المعلوماتي محل الواقعة مؤمن أم لا.... الخ من الأسئلة الاسترشادية[2] .

**المعاينة والمعاينة الرقمية.**

يجب أن يتم الانتقال بعد تلقي البلاغ إلى مسرح الجريمة المعلوماتية مع مراعاة استغلال الوقت خلال عملية الانتقال في تحليل الإجابات التي أوردها المجني عليه قبل الانتقال، وإمكانية تحليلها حتى يتم الاستعداد بالأدوات اللازمة لمعاينة مسرح الجريمة كما يتم خلال هذه الإجابات تحديد الخطوات التي يجب اتخاذها عقب الوصول لمسرح الجريمة وتحديد خطة لدور كل عضو من أعضاء فريق الضبطية المتجهة للمعاينة[3].

ويقصد بالمعاينة هو ذلك الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء أو أشخاص والفحص الدقيق لكافة المحتويات، بهدف كشف مخلفات وآثار الجاني بالمكان، وهذه المحتويات والمخلفات هي التي تشير إلى شخصيته أو شركائه، وما قد يفيد في إثبات الجريمة وتوضيح قدر من الاستنتاجات المنطقية تشكل الأساس الذي تقوم عليه عملية التحقيق والبحث التالية[4].

كما يقصد بالمعاينة رؤية مجال ارتكاب الوقائع الجنائية واثبات حالتها بالشكل الذي تركه به الجاني عقب ارتكاب الجريمة، كما تنصرف إلى فحص جسم المجني عليه والمتهم واثبات ما يوجد بهما من آثار[5].

---

[1] خالد حازم الإبراهيمي ، مرجع سابق، ص216.

[2] Bruce Middletion, Cyber crime investigator's field guide auevbach publication, New-York, 2000, p1,2.

[3] خالد حازم الإبراهيمي ، مرجع سابق، ص2017.

[4] هشام فريد رستم، مرجع سابق، ص223.

[5] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الجزء الثاني، دار النهضة العربية، القاهرة، 1995، ص640.

وتقتضي المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة ورفع الآثار المتعلقة بها كالبصمات و الدماء وغيرها مما يفيد التحقيق، والمعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة ، ووضع الشهود و المتهم والمجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص.

يثور التساؤل هنا عن مدى إمكانية معاينة الجريمة المعلوماتية ، وهذا لأننا نصطدم بالعقبة الأساسية أمام معاينة الجريمة المعلوماتية التي ترتكب داخل الفضاء المعلوماتي أو السيبراني، فالمحقق في هذه الحالة يتعامل مع بيئة مليئة بالنبضات الالكترومغناطيسية والبيانات المخزنة داخل نظام معلوماتية شديدة الحساسية ولا يتعامل مع أوراق أو أسلحة أو أشياء قابلة للربط وهو ما يؤكد القواعد الإجرائية التقليدية سنت لتواجه سلوكاً ماديا يرتكب بواسطة آلات وأدوات قابلة للربط والتحريز ولا يمكن لها أن تواجه مثل هذه الجرائم .

وتجدر الإشارة إلى أن المعاينة تصعب وتختلف في الجرائم التي تستخدم فيها التقنيات الرقمية كالإرهاب الالكتروني حيث أن هذا النوع من الجرائم يندر فيها أن يتخلف عن ارتكابها أثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها مما يعرض الآثار الناجمة عنها إلى المحو أو التلف[1].

وإذا كانت المعاينة في الجرائم بصفة عامة تجاوز وجودها مجرد الرؤية والمشاهدة وعدم اعتمادها على مجرد حاسة النظر، فقد عرفه بعض الفقه بأنها إثبات مادي ومباشر لحالة الأماكن والأشخاص ذات الصلة بالحادث عن طريق رؤيتها أو فحصها فحصا حسيا مباشرا، أي أنها إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبها[2]، فإن معاينة مسرح الجريمة المعلوماتية، يختلف، فهو يقصد به معاينة الآثار التي يرتكبها مستخدم الشبكة المعلوماتية أو الانترنت

[1] طه أحمد طه، التحقيق الجنائي وفن استنطاق مسرح الجريمة، منشأة المعارف، الإسكندرية، 2000، ص20.

[2] عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهرة، 1993 ص373.

وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب والانترنت[1].

ويلاحظ أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جداً فيما تحتويه من معلومات مثل صفحات المواقع المختلفة Web Pages والبريد الإلكتروني E-mail ، الفيديو الرقمي digital Video ، الصوت الرقمي Digital audio ، غرف الدردشة والمحادثة Digital Logs of Synchronous Chat Sessions ، الملفات المخزنة في الكمبيوتر الشخصي Files Stored On Personal Computer ، الصورة المرئية Digitized Still Images، الدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات Computer Logs from An Internet service Provider (I S P).

ولم تهتم معظم التشريعات الجنائية المعاصرة بتعريف مسرح الجريمة أو وضع معايير ثابتة لتحديد نطاقه المكاني كما هو الشأن بالنسبة للتفتيش بل أن هذا التحديد لم يحظ كثيراً باهتمام الفقه والقضاء الجنائي على نفس النحو الذي حظي به التفتيش فمعظم التشريعات تعبر عن مسرح الجريمة بمحل الواقعة .

## مسرح ارتكاب الجريمة المعلوماتية.

تدور معظم تعريفات رجال الفقه على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها بحيث يتخلف فيه آثار ارتكابها .

ويرجع عدم الاهتمام بتعريف مسرح الجريمة وتحديد معالمه المكانية على وجه مفصل إلى اعتبارين[2] :

**الأول** : أن معظم القوانين الجنائية لا ترتب عادة آثار قانونية بالبطلان أو الانعدام على تجاوز الحدود المكانية لما هو معروف بمصطلح " مسرح الجريمة " عند إجراء المعاينة تاركاً للمحقق أو القائم بالمعاينة تقدير دائرة نشاطه الإجرائي في المعاينة داخل محيط اختصاصه الوظيفي حسبما يراه وفقاً لما تقتضيه مصلحة التحقيق طالما أن التوسع الميداني في هذا الإجراء ليس فيه مساس بخرق مستودع سر الغير في مسكنه أو محله الخاص وليس فيه خروج على قواعد الاختصاص .

[1] خالد حازم الإبراهيمي، مرجع سابق، ص224.

[2] خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي ، الإسكندرية، 2009، ص 166.

**الثاني:** أنه لا تثور عادة بشأن تحديد المجال الميداني لمسرح الجريمة منازعة أو جدل بين الخصوم في الدعوى الجنائية ( الدفاع أو الاتهام ) أو طلب بطلان الإجراء تأسيساً على تجاوز هذا النطاق المكاني وذلك فيما لم تتناوله التشريعات بتفصيل أو تحديد كما هو الشأن بالنسبة للتفتيش الذي يمثل مساساً بحرمة الأفراد ومستودع أسرارهم ومن ناحية أخرى فالمعاينة إجراء واجب من إجراءات التحقيق تفرضه القوانين على رجال الضبط والتحقيق بمجرد علمهم بوقوع الجريمة أو تبليغها إليهم وبالتالي فلا يجوز لأي خصم أو طرف أن يعترض على إجراء معاينة مسرح الجريمة أو على طريقة أو أسلوب تنفيذها أو مجالها الميداني إذ أن المعاينة تستهدف التعرف على أبعاد الجريمة وأركانها وظروفها وكشف الحقيقة بشأنها وليست إجراء موجه ضد شخص معين ماساً بحرمة مستودع سره حتى ينشأ له حق الطعن فيه بالبطلان .

ومن جانب آخر فقد تكون معاينة مسرح الجريمة أول إجراء يقوم به المحقق بعد تلقي البلاغ أو إخطاره به وذلك في ظروف قد لا يكون فيها عنصر الخصوم أو المتهمين قد ظهر بعد بهذه الصفة على ساحة التحقيق ، وذلك بخلاف التفتيش الذي لا يجري إلا في مواجهة شخصية وجه إليها الاتهام وإذا تناول التفتيش مكاناً فهو مستودع السر الذي يلزم أن يكون معيناً على وجه التحديد التعين النافي للجهالة ، وهو ما اهتمت به التشريعات والفقه والقضاء وأحاطته بضمانات كافية[1] .

ويمكن تعريف مسرح الجريمة بأنه " هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة ومركزها بحيث تكون ميداناً لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند ارتكاب الأفعال المؤثمة جنائياً والتي تدخل في عداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها "[2].

ويدخل في عداد ذلك الملحقات المتصلة التي تكون مع المكان وحدة واحدة وهذا النطاق المكاني يكتسب صفة مسرح ارتكاب الجريمة من واقع احتوائه على مركز وقوعها بداخله ووجود آثار ومخلفات ارتكابها أو احتمال وجود ذلك .

[1] خالد ممدوح، معاينة مسرح الجريمة الالكتروني، مقالة منشورة على الرابط:
ttps://kenanaonline.com/users/KhaledMamdouh/posts/81659، تاريخ الاطلاع 2018/08/14 على الساعة 14:21 .

[2] خالد ممدوح، (فن التحقيق الجنائي في الجرائم الإلكترونية)، مرجع سابق، ص 167.

ويجب أن تكون هذه المواقع ميداناً لأنشطة الجاني الذي ارتكب الجريمة وحده " أو الجناة من الفاعلين الأصليين عند تعددهم " ومارسوا أفعالاً تضفي عليهم هذه الصفة وذلك بارتكاب كل أو بعض الأعمال التنفيذية للجريمة أو الشروع فيها .

المعاينة في مسرح الجريمة الرقمي تنقسم إلى قسمين أولهما هو معاينة المكونات المادية للأجهزة التي تم بها ارتكاب الواقعة، كالحاسوب ومكوناته المختلفة وهذه المكونات المادية لها طابع مادي محسوس للأدلة المادية وتنطبق عليها القواعد نفسها المتعارف عليها في المعاينة التقليدية للأدلة المادية وأما القسم الثاني فهو المتمثل في المكونات المنطقية للواقعة الإجرامية المرتكبة.

ومن أمثلة هذه المكونات برامج الحاسب الآلي بأنواعها المختلفة مثل برامج التشغيل والتامين ومعالجة البيانات ... الخ وبيانات المعالجة الآلية باستخدام الحاسب بأشكالها المتعددة مثل النصوص والصور والفيديو ....الخ وكذلك النظم التي يتم اتصال الحواسيب الشخصية وشبكات الحاسب من خلالها بشبكة المعلومات الدولية، وهي التي تجعل من معاينتها مختلفة عن معاينة الأدلة المادية[1] .

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهارات هذه التقنية ، مثل القدرة على استخدام برامج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الإجرامي، لأن ذلك لا يكون متاحاً في جميع الأنظمة المعلوماتية، أما الخبير ففي هذه الحالة يجب أن يكون ملماً بمهارات تحليل البيانات و مهارات التشفير cryptanalysis skills التي تتيح له فك الرموز استعادة البيانات الملغية .

ولما كانت الجرائم ترتكب عبر الشبكة الدولية فقد نصت المادة 23 من الاتفاقية الدولية للإجرام الالكتروني[2] على أن (تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وكذلك بشأن الحصول على الأدلة في الشكل الإلكتروني لمثل هذه الجرائم) كما نصت المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على : أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير

[1] خالد حازم الإبراهيمي، مرجع سابق، ص224، 225.

[2] الاتفاقية الأوربية لمكافحة جرائم تقنية المعلومات (بودابست) لسنة 2001.

المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله. كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة .

ومما سبق يلاحظ أن المعاينة في جريمة الإرهاب الالكتروني تكون بقسميها المادي والرقمي وهذا لأنها جريمة تقليدية ولكنها ارتكبت بوسيلة رقمية (أي تكنولوجيا حديثة).

هذا ويرى جانب من الفقه أن المعاينة في مسرح الجريمة الرقمي لا يكتسي نفس أهمية المعاينة في مسرح الجريمة التقليدي، ويرجع ذلك إلى عدم تخلف أثار مادية عن الجرائم التي تتم باستخدام الحواسيب الآلية وشبكة الانترنت، وأيضا عدم القدرة على حصر الأفراد الذين ترددوا على مسرح الجريمة الرقمي لطول الفترة الزمنية الفاصلة بين ارتكاب الجريمة واكتشافها، وذلك مما يفتح المجال أمام التغيير أو العبث بالآثار المادية أو زوالها، وهو ما يدفع بالشك حول الآثار المادية المتولد عنها[1].

وعليه ترتبط كل من المكونات المادية والمنطقية لمحل المعاينة للواقعة المرتكبة باستخدام الحاسب وشبكاته بعضها بالبعض ارتباطا وثيقا وبالتالي يجب أن تتم المعاينة في الجريمة الإرهابية الالكترونية للأدلة المادية بالشكل الذي يتفق والحرص على عدم إتلاف أو تعديل وضياع الأدلة المنطقية ومن أجل ذلك يستحب أن تجري المعاينة من طرف ضابط شرطة قضائية له خبرة في هذا المجال وأن تكون هناك نماذج معدة مسبقا لهذا النوع من المعاينة مستوفاة البيانات المطلوبة مثال ذلك إصابة صفحة ويب، إجراء تعديل في قاعدة البيانات للمجني عليه قصد الإضرار به أو قصد نشر الرعب بين الناس أو استخدام احد التصميمات لتدمير قاعدة بيانات منطقية، وفي هذه الحالة – موضوع الدراسة– استخدام الحاسب الآلي وشبكة الانترنت في جريمة تقليدية (الإرهاب)، أو إجراء تعديلات في المعلومات الخاصة بالتسليح أو قواعد البيانات العسكرية[2].

[1] جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2002 ص29.

[2] وليد عاكوم، التحقيق في جرائم الحاسوب،مداخلة ألقيت في الملتقى العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، المنعقد بأكاديمية شرطة دبي(ا.ع.م) في الفترة من(28/26 أفريل 2003).

وفي الأخير حتى تكون المعاينة في جريمة الإرهاب الالكتروني فعالة ونتيجة لأثارها وجب إتباع مجموعة من الخطوات قبل التحرك والانتقال إلى مسرح الجريمة ومنها[1]:

1- توفير معلومات مسبقة عن مكان الجريمة، وعن نوع وعدد الأجهزة المتوقع مداهمتها وشبكتها لتحديد إمكانية التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات.

2- إعداد خريطة للموقع الذي تتم الإغارة عليه وإعداد خطة للهجوم على ذلك المكان.

3- الحصول على الاحتياجات الضرورية من الأجهزة وبرامج صلبة ولينة للاستعانة بها في الفحص والتشغيل.

4- تامين التيار الكهربائي بحيث لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

5- إعداد فريق تفتيش من المختصين وإعداد الأمر القضائي اللازم للقيام بالتفتيش.

أما عند الوصول إلى مسرح الجريمة فوجب القيام بالخطوات التالية:

- تصوير شاشة الحاسب الآلي.
- عدم نقل أي مادة معلوماتية من مسرح الجريمة، قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أية مجالات لقوى مغناطيسية (ممرات مغناطيسية) يمكن أن تسبب في محو البيانات المسجلة.
- البحث عن خادم الملف لتعديل حركة الاتصالات[2].
- التحفظ على محتويات سلة المهملات والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.
- الاستعانة بأهل الخبرة.

## ثانيا: الخبرة القضائية في جريمة الإرهاب الالكتروني.

من أجل معرفة دور الخبرة في إثبات جريمة الإرهاب الالكتروني وجب أن نتعرض إلى الخبرة في إثبات الجرائم الالكترونية بصفة عامة وهذا لأن جريمة الإرهاب الالكتروني نوع من الجرائم الالكترونية، كما أن المشرع لم يخصها بأي نصوص خاصة في هذا الشأن.

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات- دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013، ص 219.

[2] هشام محمد فريد رستم، مرجع سابق، ص 60 ،61.

تقدم الخبرة عونا كبيرا للقضاء ولجميع جهات المختصة بالدعوى الجنائية من خلال أداء مهمتها التي بدونها يستحيل الوصول إلى رأي بشأن المسائل الفنية، والتي من خلالها يمكن التوصل إلى ظهور الحقيقة المبنية على حقائق علمية فنية والذي يعتبر العنصر المميز لها عن غيرها من إجراءات الإثبات.

**القواعد القانونية التي تحكم الخبرة القضائية في الجرائم المعلوماتية.**

مع التطور السريع للجرائم الالكترونية يصعب على المختصين مواكبتها واستيعابها بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم[1] .

وإن أهم صعوبة تواجه الخبرة هي تكوين الخبير المناسب للاستعانة به، باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصة بتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية[2]، فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال الجريمة المعلوماتية بشكل خاص أن يتمتع بشروط خاصة، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادة ودراسات عليا في فرع التخصص، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفية من أجل مواكبة كل جديد يطرأ على تخصصه لأداء مهمته ، فيتطلب من الخبير أن يكون ملما بالجوانب الفنية والتقنية، ومنها الملحقة به وكلمات المرور وأكواد التشفير...الخ لمعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية، وأيضا طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة لذلك، وكذلك المواضيع الرقمية المحتمل أن تتواجد فيها أدلة الإثبات والصور أو الأشكال التي تتخذها وأيضا الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة والكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب على ذلك إتلافها، كما يتعين على الخبير المعلوماتي التمكن من تحويل أدلة الإثبات غير

[1] عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، طبعة الثانية، دار النهضة العربية القاهرة، 2001، ص 392.

[2] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس، 2004، ص 1034.

المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها[1]

وتجدر الإشارة إلى أن الخبير قد يكون سببا لفقدان الأدلة لعدم التخصص الدقيق في المسألة التي تطلب ضرورة الخبرة وقد تحتاج إلى أكثر من خبير، كما يجب أن يكون الخبراء في مجال الأدلة الرقمية على وعي تام بأن أي خطأ في التفسير يؤدي إلى إتلاف أو محو الدليل الرقمي كحالة الخطأ في طريقة الحصول على الدليل الرقمي أو عدم تحريز الأدلة ، كما قد يتم إتلاف الأدلة بسبب خطأ الخبراء والجهة المجني عليها.

## القواعد الفنية التي تحكم الخبرة القضائية في الجرائم المعلوماتية.

تتمثل القواعد الفنية للخبرة أساسا في الوسائل الفنية التي يستعين بها الخبير المعلوماتي من أجل إظهار الحقيقة وتقدير عمله ودوره في العمل على حفظ الأدلة الناجمة عن الخبرة التقنية.

### 01-وسائل الخبير في اكتشاف الدليل الإلكتروني.

وتتمثل في الوسائل المادية والإجرائية كالتالي:

**- الوسائل المادية .**

وهي الأدوات الفنية للنظم المعلوماتية التي يمكن أن تستخدم في ارتكاب الجرائم وأهمها عنوان برتوكول الانترنت IP والبريد الإلكتروني وبرامج المحادثة، ويقصد بعنوان الانترنت المسؤول عن تراسل كم من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ويشبه عنوان البريد العادي حيث يسمح للشبكات بنقل الرسالة وهو يوجد بكل جهاز إلكتروني مرتبط بالانترنت ويتكون من أربعة أجزاء وهي المنطقة الجغرافية، مزود الخدمة الحاسبات الآلية المرتبطة، والرابع يقوم بتعيين الحاسب الآلي الذي تم الاتصال به[2]

وتوجد أكثر من طريقة يمكن من خلالها معرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، مثل ما يستخدم في حالة العمل على نظام تشغيل Windows حيث يتم كتابة WINPCFG في أمر التشغيل فيظهر مربع حوار فيه عنوان IP على أنه عنوان الانترنت، وقد يتغير في كل اتصال شبكة الانترنت .

[1] عبد الله حسين على محمود، مرجع سابق، ص 395 .

[2] خالد ممدوح الإبراهيمي، مرجع سابق، ص 304.

أما في حالة استخدام برامج المحادثات كأداة للجريمة، فإنه يجب تحديد هوية المتصل حتى ولو لم يدون معلوماته في خانة المرسل، وذلك بشرط أن تكون المعلومات التي وضعها أثناء إعداد بريد إلكتروني صحيح

إلى جانب العنوان هناك ما يعرف بالبروكسيProxy ، يعمل البروكسي كوسيط بين الشبكة ومستخدميها وأيضا كمزود طلبا من المستخدم البحث عن صفحة ما ضمن ذاكرة المحلية والمتوفرة، لذلك يتحقق البروكسي في حالة تنزيل الصفحة من قبل، وبالتالي يقوم بإرسالها إلى المستخدم دون حاجة الرجوع إلى الشبكة العالمية، أما إذا لم يتم تنزيلها فيتم إرسال طلب إلى الشبكة العالمية، وفي هذه الحالة يقوم البروكسي كمزود زبون ويستخدم أحد عناوين IP ،كما يمكن لمزود البروكسي أن يحتفظ بتلك العمليات خاصة لإجراء الإثبات بواسطة فحص تلك العمليات المحفوظة به[1].

أما الوسيلة المادية الأخرى فتتمثل في نظام كشف الاختراق ، يرمز له بأحرف IDS وهذه البرامج تقوم بمراقبة وتحليل بعض العمليات التي تحدث على أجهزة الحاسب الآلي أو الشبكة، من أجل البحث عن إشارات تفيد وجود مشكلة في الحاسوب أو الشبكة، وذلك من خلال تحليل مجموعة من البيانات أثناء انتقالها عبر الشبكة ببعض ملفات التشغيل التي تختص بتسجيل الأحداث فور وقوعها في الحاسب الآلي أو الشبكة، ومقارنة النتائج بمجموعة الاعتداءات الواقعة على الأنظمة المعلوماتية والتي يطلق عليها مصطلح التوقيع، بالتالي إذا تم اكتشاف النظام لوجود توقيع من التوقيعات يقوم بإنذار مدير النظام بطرق عديدة وفورية، حيث يقوم نظام كشف الاختراق بتسجيل البيانات محل الاعتداء في سجلات الحاسوب الخاصة لهذا الغرض.

- **الوسائل الإجرائية.**

من بين الوسائل الإجرائية نجد ما يلي:

**01-اختفاء الأثر.**

إن المسجلات التي يتم نشرها في المواقع الخاصة بالمخترقين تشير دائما بنصائح مختلفة من بينها قم بمسح آثارك trachs your Cover وفي حالة عدم مسح المخترق لأثاره يقبض عليه، حيث يتقصى على الأثر بطرق عديدة سواء بواسطة البريد الإلكتروني الذي تم استقباله أو بتتبع أثر الجهاز

[1] خالد ممدوح الإبراهيمي، مرجع سابق، ص 305 .

الذي تم استخدامه للقيام بالاختراق، وحتى لو تمت عملية الاختراق بشكل صحيح وسليم إلا أنه يمكن القبض عليه كونه لم يقم بمسح أثاره.

**02- الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته.**

من المفروض على المحقق في حالة إجرائه للتحقيق في جريمة معلوماتية ما، أن يقوم بالإطلاع على النظام المعلوماتي ومكوناته من شبكات وبرامج، وعملياته كقاعدة المعطيات وإدارتها ومعرفة النظام والمستفيدين والإجراءات منها إجراء أمن العاملين وكذلك عليه الإطلاع على أسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية كمراقبة المستفيدين والبرامج وتسجيل الوقائع[1].

**03- الاستعانة بالذكاء الصناعي.**

من الممكن الاستعانة بالذكاء الصناعي في جمع الحقائق والأسباب والفرضيات التي يستخلص منها النتائج عن طريق معاملات حسابية يتم تحليلها بالحاسب الآلي وفقا لبرامج صممت لأجل ذلك حيث أن تقنيات الحاسب الآلي أثبتت نجاحها وتمكنها من جمع أدلة جنائية وتحليلها واستنتاج الحقائق منها[2] .

**- عمل الخبير المعلوماتي وأساليبه .**

تقتصر مهمة الخبير على التحقيق في الدعوى وإبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية، وعليه لجمع الأدلة حول الجرائم السالفة الذكر بمعرفة الخبير المعلوماتي، يجب مراعاة القواعد الفنية المتعارف عليها في مجال الخبرة المعلوماتية، وبالتالي يمكن للخبير إتباع الخطوات التالية في عمله[3]:

1. **مرحلة ما قبل التشغيل والفحص:** يجب على الخبير أن يقوم بوضع نسخة أو نسخ مطابقة للأصل لوسائط التخزين المضبوطة كالقرص الصلب للقيام بعملية الفحص المبدئي وحماية الأصل من الفقدان أو التلف، وعليه التأكد من صلاحية النظام للتشغيل ومدى مطابقة محتوى الأحراز المضبوطة أثناء التحقيق بما هو مدون عليها كما يقوم بتسجيل محتوى البيانات المضبوطة كالطرز والنوع...الخ

[1] خالد ممدوح الإبراهيمي، مرجع سابق، ص 305.

[2] نفس المرجع، ص308 .

[3] محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006 ، ص 254.

2. **مرحلة التشغيل والفحص:** يقوم الخبير في هذه المرحلة باستكمال تسجيل البيانات التي لم يتم ضبطها من خلال قراءة جهاز الحاسب الآلي، ويحدد أنواع البرمجيات كبرامج النظام برامج التطبيقات وأي من البرامج له علاقة بموضوع الجريمة التي تحقق المعالجة فيها الصور في جرائم التزييف أو التعديل أو التلاعب... الخ مع إبراز إذا كانت مستندات أو معلومات لها دلالة بموضوع الجريمة كبصمات الأصابع في جرائم التزوير ووجود رسائل تهديد في جرائم القتل وغيرها، وكذلك ينبغي عليه اكتشاف المستندات أو النصوص المخبأة داخل الصور ، وأن يقوم بتحويل الدليل الرقمي إلى مكونات مادية بواسطة طباعة الملفات أو تصوير محتواها أو وضعها وعاء حسب نوع البيانات المكونة، ويجب أن يقوم باسترجاع الملفات التي تم محوها على الأصل عن طريق استخدام أحد برامج استعادة البيانات بالنسبة للملفات والسجلات المعطلة أو التالفة وذلك باستخدام برنامج Professional all 4 Recover Eassyوالعمل على تخزين السجلات أو البيانات والقيام بنسخ طبق الأصل من الأقراص أو الأسطوانات لفحصها.
3. **مرحلة تحديد مدى ترابط الدليل المادي والدليل الرقمي:** يتم في هذه الخطوة فحص الدليل المادي المضبوط مع الدليل المستخرج من جهاز الحاسب الآلي والربط بينها ليصبح الدليل موثوق ويقيني حتى يتسنى قبوله أمام المحكمة[1] .

4. **تدوين النتائج وإعداد تقرير:** يقوم الخبير بتقديم تقرير موقعا منه لما توصل إليه من نتائج من بداية إجرائه للخبرة، وغالبا ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة وغيرها، ويقدم الملف إلى جهة التحقيق أو جهة الحكم .

ويتطلب لحفظ الأدلة داخل جهاز الحاسوب معرفة دقيقة لصحة البيانات الواردة في الحاسب الآلي وهذا ما يستلزم من الخبير التقني ضرورة الكشف بداية على نطاق محتوى صحة حركة الحاسب الآلي من وجود شك في صحة الأدلة المستفادة، خاصة حالة وجود الخلل أو العطب مثل الفيروس ومثل هذا الاتجاه نجد التشريع الإنجليزي، حيث تتم عملية حفظ الأدلة داخل جهاز الحاسوب بأساليب عديدة منها استخدام الحفظ العادي وأهمها القيام بعمليات حجز الحاسوب على الدليل الموضوع فيه

[1] محمد حسين منصور، مرجع سابق، ص 255.

ذلك أن الدليل الرقمي هو ملف يحتوي على معطيات رقمية تبين مظهرا معلوماتيا محددا غير قابل للتحويل إلاَ بقيام تعديلات أو تغييرات رقمية على البيانات المذكورة .

فعملية حفظ الأدلة الرقمية تتطلب من الخبير التقني القيام بمعرفة موقع الانترنت أو المعلومات التي تشكل الجريمة، كجرائم السب والقذف في غرف المناقشة أين يتم العودة إلى ذاكرة الخادم ليقوم بربط الغرف حتى يتم التوصل إلى تحديد موضوع السب والقذف وتاريخه، أما في حالة كون الجريمة من جرائم النشر عبر الانترنت، فيتم اللجوء مباشرة إلى ذاكرة الحاسب الآلي المستخدم، وبالتالي تستدعي عمليات حفظ الأدلة من الخبير أن يقوم باستخدام البرمجيات للقيام بحفظ الأدلة الرقمية كما أنه ملزم أن يقوم بعرض الأدلة على المحكمة أو جهات التحقيق[1] .

## مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة المعلوماتية.

باعتبار أن القاضي قد يستخدم خبير استشاري بشكل غير رسمي في المجال الرقمي ذلك ما قد يشكل صعوبة ويعيق إجراءات التحقيق وأكثر من ذلك قد تكون وجها من أوجه البطلان، كون أن بعض القوانين تخول للمتهم دون سلطة التحقيق أو الاتهام الاستعانة بخبير استشاري، لأنه قد لا يجد القاضي خبيرا في مجال تكنولوجيا المعلومات ضمن قائمة جدول الخبراء، هذا ما يستدعي من المشرع التدخل من خلال تضمين نصوص قانونية التي تسمح بالاستعانة بالخبرة الاستشارية من طرف جهة التحقيق والاتهام في المجال المعلوماتي دون التقيد بخبراء الجدول المعتمدين[2].

ولقد نظم قانون الإجراءات الجزائية الجزائري نصوص خاصة بالأحكام المتعلقة بالخبرة بالنسبة للجريمة التقليدية من المادة (143 إلى المادة 156) منه ، ورغم عدم تضمين نصوص خاصة تتعلق بالخبرة الرقمية، وكذلك نقص الخبرة في مجال تكنولوجيا المعلومات، إلا أنه هناك إمكانية تطبيق الأحكام المتعلقة بالخبرة في الجرائم الناشئة عن الحاسب الآلي، فبات الأمر على القاضي أن يكون ملما بالأمور الفنية، باعتباره يشرف ويراقب أعمال الخبرة، كما أنه يحدد المواضيع التي تتطلب الاستعانة بالخبرة، غير أن هذا الأمر غير متوفر في الدول النامية، وبالتالي تدريب كوادر الأجهزة الضبطية والقضاة في مجال الخبرة الرقمية تكاد تكون ضرورة لا غنى عنها[3].

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص 1044، 1045.

[2] نفس المرجع، ص 892 .

[3] المواد من 143 إلى 156 من قانون الإجراءات الجزائية الجزائري.

وعليه في الأخير يمكن القول أن جريمة الإرهاب الإلكتروني كغيرها من الجرائم المعلوماتية هي جرائم ذو طبيعة غير مادية، هذا ما أدى بإجراءات التحقيق الجنائي فيها لا تزال محل خلاف فقهي وقضائي، وبالأخص إجراءات التفتيش والضبط عن بعد والمعاينة وكذا غياب وجود الخبير المعلوماتي المتخصص في المجال الرقمي وغيرها من إجراءات التي تثير العديد من المشكلات التي تعيق التحقيق، باعتبار أن الدليل المراد استنباطه يكون خفيا غير مرئي وأكثر من ذلك فقدان الدليل لأثاره سواء بالتلاعب أو التغيير أو الحذف، لكون الجريمة المعلوماتية مجهولة لا تصل إلى علم سلطات التحقيق والاستدلال، وهذا راجع إلى عدم اكتساب المهارة والمعرفة وعدم الخضوع لتدريبات التي تسمح للقضاة وضباط الشرطة القضائية بمواجهة تقنيات الحاسب الإلكتروني المتطورة وكذا عدم استعانتهم بخبراء مختصين في مجال التحقيق، وهذا ما ينعكس سلبا على نفسية المحقق والمجتمع وإيجابا على نفسية الجاني، كونه على ثقة بأن السلطات التحقيق المختصة غير قادرة على إيجاد الدليل ضده وهذا ما يشجعه أكثر على ارتكاب جرائم كثيرة وخطيرة، لذا فإن متابعة إجراءات التحقيق في مجال الجريمة المعلوماتية، تحتاج إلى الأمن المعلوماتي ولرجال الضبط القضائي والقضاة المتمكنون في الأمور الفنية، والتي لن يتسنى تحقيقها إلا عن طريق التدريب والتأهيل في المجال التقني المعلوماتي[1] .

## الفرع الثاني: التفتيش في جريمة الإرهاب الالكتروني.

من المعلوم أن التفتيش هو إجراء من إجراءات التحقيق يهدف إلى التوصل إلى أدلة مادية تتعلق بالجريمة الجاري جمع الاستدلالات والتحقيق بشأنها أي أن التفتيش ما هو إلا وسيلة للحصول على دليل مادي يساهم في بيان وظهور الحقيقة.

والتفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش التقليدي المتعارف عليه في القواعد الإجرائية العامة من حيث شروطه وموضوعه.

وعلى الرغم من تعدد التعريفات التي أضفاها الفقه على التفتيش إلا أن هذه التعريفات تجمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة ونسبتها إلى المتهم تحقق وقوعها في محل يتمتع بحرمة وذلك وفقا للضمانات والقيود القانونية المقررة[2].

[1] عمر أبو بكر بن يونس، مرجع سابق، ص892.

[2] رشيدة بوكر، مرجع سابق، ص394.

بالرجوع إلى التعريف السابق يتبين أن التفتيش ما هو إلا وسيلة للإثبات المادي، ذلك لأنه إجراء يستهدف ضبط أشياء مادية قد تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليه ارتكابها، وبناء على ذلك يعد تفتيش نظام المعالجة الآلية (التفتيش الرقمي) من اخطر المراحل حال اتخاذ الإجراءات الجزائية ضد مرتكب جرائم الاعتداء على نظام المعالجة الآلية، لكون محل التفتيش هو نظام المعالجة الآلية محل استفسار فقهي متزايد مع الزمن فيما يخص الجانب غير المادي له فهو لا يعدو أن يكون إلا معلومات الكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي[1].

وفي هذا الشأن يرى جانب من الفقه أن المصطلح الواجب إطلاقه على عملية البحث عن أدلة الجريمة المرتكبة في العالم الافتراضي (الإلكتروني) "الولوج أو النفاذ" باعتباره المصطلح الدقيق بالنسبة للمصطلحات المعلوماتية، بينما مصطلح التفتيش يعني البحث أو القراءة أو التفحص، والتدقيق في البيانات وبالتالي فهو مصطلح تقليدي أكثر[2] وهناك من يستخدم المصطلحين معا بغرض التنظيم والتنسيق بين المفاهيم التقليدية والحديثة وهذا ما يستشف من المادة 19 من الاتفاقية الأوروبية لمكافحة جرائم تقنية المعلومات بقولها في فقرتيها الأولى والثانية والتي جاء فيها:

1. يجب على كل طرف أن يتبني الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من اجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة مشابهة:

أ- لنظام معلوماتي أو لجزء منه وكذلك للبيانات المعلوماتية المخزنة فيه وعلى أرضيته.

ب-بدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية.

يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل التأكد مما إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معين أو جزء منه وفقا للفقرة (1) بند (أ) وأنها تملك أسباب للاعتقاد بان البيانات التي تسعى إليها مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضه وان هذه البيانات يمكن الوصول إليها بشكل قانوني سواء من خلال النظام الآلي أو من خلال كونها مهيأة من اجله، وان هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريقة مشابهة لنظام آخر[3].

[1] رشيدة بوكر، مرجع سابق، ص 394.

[2] نبيلة هبة هروال، مرجع سابق، ص223، 224.

[3] الاتفاقية الأوروبية لمكافحة جرائم تقنية المعلومات لسنة 2001.

## أولا: طبيعة التفتيش الالكتروني في جريمة الإرهاب الالكتروني.

ويتنازع الفقه الحديث حول مدى اعتبار النفاذ أو الولوج إلى النظم المعلوماتية نوعا من التفتيش وذلك كمايلي:

### الاتجاه الأول.

يجسده مشروع قانون الحاسوب المعدل من قبل وزارة العدل الإسرائيلية لمواجهة قصور قواعد التفتيش والضبط التقليدية للتطبيق على هذا النوع من الجرائم، وذلك بإضافة عبارة جديدة إلى نص المادة التي تنظم ذلك التفتيش والضبط وهي عبارة "أو مادة معالجة بالحاسب" إلى جانب الأشياء التي يرد عليها ذلك الإجراء.

وقد وضح المشروع بأنه يقصد من تلك العبارة برامج الحاسب الآلي وبياناته[1].

ومن الدول التي قامت بسن تشريعات جزائية حديثة قادرة على مواجهة التقنية الإجرامية التي صاحبت الحاسب الآلي وشبكة الانترنت وأفردت جانبا كبيرا من تلك القوانين والتشريعات لبحث مسألة التفتيش و الضبط المملكة المتحدة وذلك من خلال قانون إساءة استخدام الحاسب الآلي سنة 1990 إذ نص على إجراءات تفتيش نظم الحاسب الآلي في جرائم الولوج غير المصرح به في نظام دون إذن طالما كان هدف الولوج ارتكاب أفعال غير مشروعة فإن التفتيش ممكن لكن بإذن قضائي[2].

الولايات المتحدة الأمريكية أيضا سنت تشريعات حديثة وذلك من خلال القوانين الإجرائية الفدرالية بشأن جرائم الكمبيوتر إذ نظمت إجراء التفتيش والضبط في بنية الحاسب الآلي في القسم 642USC200، وكذلك فرنسا من خلال المادة 19 من اتفاقية بودابست المشار إليها سابقا، حيث تهدف هذه المادة إلى تحديث وتناغم التشريعات الداخلية المتعلقة بالتفتيش وبضبط البيانات المعلوماتية المخزنة بهدف تجميع أدلة تسهل تنقيبات أو إجراءات جنائية معينة، فكل تشريع داخلي يتعلق بالإجراءات الجنائية يقرر سلطات للتفتيش وضبط الأشياء المادية، ومع ذلك في غالبية الدول فإن البيانات المعلوماتية المخزنة لا تعتبر في حد ذاتها كأشياء مادية، وبالتالي لا يمكن الحصول عليها أو ضبطها لأغراض التفتيش والتحري أو في جرد جنائي بنفس طريقة الأشياء المادية، لكن على الأقل

[1] هشام فريد رستم، مرجع سابق، ص66.

[2] نبيلة هبة هروال، مرجع سابق، ص226.

يمكن ضبط حاملة البيانات، أي الدعامة التي تم تخزين البيانات عليها عليها، وعليه فإن هدف هذه المادة هو إقامة سلطة مساوية أو معادلة خاصة بالبيانات المخزنة[1].

وتجدر الإشارة فيما يتعلق بعملية البحث عن المعلومات المعلوماتية فإن كثيرا من عناصر التفتيش التقليدي تبقى مستمرة في البيئة التكنولوجية الجديدة، ومن ذلك جمع البيانات يتم خلال الفترة الزمنية للتفتيش وانه يعتمد على بيانات موجودة في هذه الفترة، وبما أننا بصدد التفتيش في جريمة الإرهاب الالكتروني فهي تطبق عليها شروط الجريمة الإرهابية وبالتالي فان التفتيش فيها لا يتقيد بوقت معين وهذا كما سبق واشرنا أن جريمة الإرهاب الإلكتروني في صورة مستحدثة للجريمة الإرهابية وتقنية المعلومات المستخدمة كوسيلة فيها لن تخرجها على طابعها الإرهابي كما أن شروط الحصول على إذن قانوني مكتوب لا يختلف بين التفتيش التقليدي والإلكتروني[2]، وهذا حسب المادة 64 من قانون الإجراءات الجزائية الجزائرية.

**الاتجاه الثاني.**

ويستند أنصار هذا الاتجاه إلى عمومية نصوص التفتيش للتوسع في تفسيرها من أجل مد حكمها إلى البيانات المخزنة آليا في الأنظمة المعلوماتية، ونموذج هذا الاتجاه يمكن رصده في محيط الفقه الكندي، عندما توسع في تفسير المادة 487 قانون عقوبات كندي إلى حد يسمح بتفتيش وضبط بيانات الحاسب غير المخصوصة وإن كان في الحقيقة وحتى الآن يتم ضبط الركيزة أو الوعاء المادي للبيانات كالأقراص والاسطوانات الممغنطة[3] .

ومن أجل الموازنة بين الاتجاهين يرى بعض الفقه أن التشكيك في الطبيعة المادية للبيانات الإلكترونية على النحو الذي جاء به الاتجاهان السابقان إلى محاولة إزالة أو تجنبه قد لا يكون له ما يسوغه ذلك أن تمييزا معمقا لأسباب تكنولوجية وقانونية يجب أن يقام بين المعلومات من جهة والبيانات المعالجة الكترونيا من جهة ثانية، فأولهما ليس شيئا ماديا وإنما هو عملية أو علاقة تقوم بين

[1] هلالي عبد اللاه أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست، الطبعة الثانية، دار النهضة العربية القاهرة، 2013، ص206،207.

[2] نفس المرجع ، ص208.

[3] هشام فريد رستم، مرجع سابق، ص67.

ذهن بشري وبعض أنواع المثيرات وهي مع تجسيدها ماديا في وعاء أو ركيزة تحتويها تنتقل إلى الغير بواسطتها من طبيعة معنوية مؤكدة ومن ثم فلا سبيل أن يرد عليها تفتيش أو ضبط[1].

أما بيانات المعالجة الكترونيا فهي نبضات أو ذبذبات الكترونية وإشارات أو موجات كهرومغناطيسية قابلة لأن تسجل أو تخزن على وسائط معينة ويمكن نقلها وبثها وحجبها واستغلالها وإعادة إنتاجها، كما يمكن أيضا تقديرها كميا من بين المبدأ وقياسها فهي إذا ليست شيئا معنويا كالحقوق والآراء والأفكار، بل هي شيء له في العالم الخارجي المحسوس وجود مادي، وقد وصفتها محكمة جنح بروكسل أشياء محسوسة ومادية ومن لم يصبح أن يرد التفتيش في الضبط عليها[2].

ويبدو أن المشرع الجزائري يميل إلى هذا الاتجاه، حيث انه واستجابة لهذه التغييرات أجاز تفتيش المعطيات والمعلوماتية وذلك بموجب المادة 05 من القانون 64/09 لسنة 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بجرائم بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أجازت هذه المادة للسلطات القضائية المختصة وكذا لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، في الحالات المنصوص عليها في المادة 04 من هذا القانون كتوفر المعلومات عن احتمال اعتداء على منظومة معلوماتية[3]

وفي حالة جريمة الإرهاب الالكتروني فالاعتداء يهدد النظام العام والدفاع الوطني وكذلك يمس بأمن الدولة حيث أجازت لها الدخول بغرض التفتيش أو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذلك التغيرات إذ قام بتعديل نصوص التفتيش، حيث قام بإضافة عبارة "المعطيات المعلوماتية" في المادة 94 من قانون الإجراءات الجزائية وذلك بموجب المادة 42 من القانون 645-2004 المؤرخ في 2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي لتصبح المادة .. كما يلي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة، وهو ما صرحت به المادة 19 من الاتفاقية الأوروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش النظم في إطار الإجراءات الجزائية – كما سبق وأشرنا إليها– وفي حالة كان نظام المعالجة الآلية مزودا بنظام حماية يمنع من ولوجه دون تدخل القائم على المنظومة أو لا يمكن الدخول دون مساعدته فما مصير التفتيش في هذه الحالة؟

[1] هشام فريد رستم، مرجع سابق، ص 68.

[2] نبيلة هبة هروال، مرجع سابق، ص228.

[3] رشيدة بوكر، مرجع سابق، ص398.

في هذا الشأن تباينت الآراء فهناك رأي يرفض إجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي، ويختصر في ذلك تجسيد في قاعدة معروفة ومستقرة أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته إذ من حقه الالتزام بالصمت دون أن يفسر صمته ضد مصلحته ومن التشريعات الحديثة التي اعتنقت هذا الاتجاه التشريع الياباني الذي يمنع على الأجهزة المختصة إكراه مالك نظام المعالجة الآلية على الإفصاح عن كلمة المرور وقد نص قانون الإجراءات الجزائية البولندي على ذات الأمر[1]

أما الاتجاه الآخر فقد ذهب إلى القول بأنه وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه إلا أن ذلك لا ينبغي أن يكون حائلا دون إجباره على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة، متى كانت هذه المعلومات بحوزته، قياسا على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته. وتجدر الإشارة أن معظم التشريعات الحديثة أخذت بالرأي الأول على أساس أن أمر الإدلاء أمر معنوي ولا يمكن قياسه على تسليم المفتاح لأنه أمر مادي كما أنه في حالة الإدلاء قد يتذرع المتهم بالنسيان مثلا وقد اخذ المشرع الجزائري بالاتجاه الأول وهو ما يستنتج ضمنا من خلال نصوص قانون الإجراءات الجزائية الجزائري[2].

وعلى خلاف ذلك يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلا بتقديم بعض معطيات المرور للتمكن من تحديد المصدر أو مكان الوصول للاتصالات[3] .

والسبب في ذلك أن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافا للوضع بالنسبة للمتهم[4].

---

[1] رشيدة بوكر، مرجع سابق، ص389.

[2] تنص المادة 100 من قانون الإجراءات الجزائية الجزائري بما يلي:" يتحقق قاضي التحقيق عند مثول المتهم لديه أول مرة من هويته ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر في عدم الإدلاء بأي إقرار وينوه عن ذلك التنبيه في المحضر فإذا أراد المتهم بأن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور، كما ينبغي للقاضي أن يوجه المتهم بأن له الحق في اختيار محام عنه، فإن لم يختر له محاميا عين له القاضي محاميا من تلقاء نفسه إذا طلب منه ذلك وينوه عن ذلك بالمحضر كما ينبغي للقاضي علاوة على ذلك أن ينبه المتهم إلى وجوب إخطاره بكل تغيير يطرأ على عنوانه ويجوز للمتهم اختيار موطن له في دائرة اختصاص المحكمة"

[3] المادة 10 و11 من القانون 04/09 سابق الذكر.

[4] رشيدة بوكر، مرجع سابق، ص401.

والتفتيش في نظام المعالجة الآلية مثلما يتم عن قرب –على نحو ما شرح سابقا– من الممكن أن يكون عن بعد، وذلك نتيجة لطبيعة التكنولوجيا الرقمية التي تسمح بتوزيع المعلومات التي تحتوي على أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش وان ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية المحاذية للتفتيش، وقد يكون الموقع الفعلي للشبكات داخل اختصاص قضائي آخر أو حتى في بلد آخر، وفي هذا الشأن يثور التساؤل حول أثر تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، وفي هذه الحالة نكون أمام فرضيتين[1]:

**الفرضية الأولى: اتصال نظام المتهم بنظام آخر موجود في مكان آخر داخل الدولة.**

– في هذه الحالة هل يقتصر التفتيش على جهازه فقط؟ أم يمتد؟

على الرغم من أن معظم التشريعات الإجرائية الحديثة لم تنص على هذه الحالة إلا أن كل من المشرع الفرنسي والمشرع الجزائري قد حسما هذه المسألة، فالمشرع الفرنسي قام بتعديل قانون الإجراءات الجزائية وذلك بموجب القانون رقم: 239–2003 بشأن الأمن الداخلي[2] ،حيث عدل المادة 1/57 بموجب المادة 17 منه والتي أجازت لرجال الضبط القضائي الدخول من الجهاز الرئيسي على المعلومات التي تهم عملية البحث والتحري[3].

المشرع الجزائري بدوره تأثر بالمشرع الفرنسي، حيث نص في المادة 5 فقرة 2 من القانون 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه : " في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة (حالة التفتيش) إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك .

[1] رشيدة بوكر، مرجع سابق، ص 401.

[2] صدر هذا القانون في 18 مارس 2003.

[3] المادة 17فقرة أولى من قانون الإجراءات الجزائية الفرنسي 239–2003 "يجوز لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية وفي إطار التفتيش المنصوص عليه الحضور عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي تتم فيها التفتيش عن المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي أخر بما أن هذه المعطيات يتم الدخول إليها أو تكون متاحة انطلاقا من النظام الرئيسي.

كما تسمح الاتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001[1] للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش[2].

**الفرضية الثانية: اتصال نظام المتهم بنظام موجود في مكان آخر خارج الدولة.**

يحدث كثيرا في جريمة الإرهاب الالكتروني أن تكون المعلومات غير المشروعة مخزنة في نظام معالجة آلية خارج إقليم الدولة حيث يقوم الإرهابيون بهذا الأسلوب بغية إعاقة الوصول إلى الدليل ومن أجل ذلك قام المشرع الجزائري بإجازة تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، حيث أجازت المادة 5 فقرة 03 من القانون المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الحصول على المعطيات المبحوث فيها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني أو التي يمكن الدخول غليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل[3].

المشرع الفرنسي سبق المشرع الجزائري في أخذه بهذا الاتجاه حيث أجاز بموجب المادة 17 فقرة 02 من قانون الأمن الداخلي رقم 2003/239 لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم فنصت:"إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني وانه يمكن الدخول إليها أو أنها متاحة انطلاقا من النظام الرئيسي، فإنه يمكن الحصول عليها من طرف ضابط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية.

كما أن المجلس الأوروبي أصدر توصيات تجيز أن تمديد تفتيش الكمبيوتر إلى الشبكة المتصلة بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة.

وقد نصت التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات على انه "لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة

[1] المادة 19 فقرة 2 من ذات الاتفاقية.

[2] خالد ممدوح الإبراهيمي، مرجع سابق، ص203.

[3] رشيدة بوكر، مرجع سابق، ص403.

مادامت مرتبطة بشبكة واحدة وأن تضبط المعطيات المتواجدة فيها، مادام أنه حتى وإن كانت هناك إمكانية التفتيش عن بعد إلى إقليم بلد أجنبي لما لهذا الإجراء من أهمية في التمكن من الحصول على الدليل التقني عن بعد وفي مدة زمنية قد تكون قصيرة جدا.

إلا أن هذا الأمر يستلزم بالضرورة التوصل إلى اتفاق دولي في هذا الإطار لما في ذلك من اختراق مباشر لهذه المواقع على مستوى الدول كافة وبالتالي فهذا الإجراء (الاختراق) عابر للحدود وإلا أعتبر هذا الإجراء تهديدا لسيادة الدول الأجنبية[1].

المادة 32 من الاتفاقية الأوروبية بشأن جرائم تقنية المعلومات نصت على إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكة تابعة لدولة أخرى دون علمها في حالتين:

- إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.
- والثانية إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش[2].

## ثانيا: شروط التفتيش في جريمة الإرهاب الإلكتروني.

بما أن المشرع الجزائري على غرار معظم المشرعين لم يحدد الشروط المتعلقة بالتفتيش في جريمة الإرهاب الإلكتروني وبما أن هذه الجريمة تعد من الجرائم الإلكترونية (المعلوماتية) وعلى ذلك سوف نرجع إلى القواعد العامة الخاصة بالتفتيش في الجريمة الإلكترونية.

ونظرا لما يشكله التفتيش من اعتداء على حرمة الحياة الخاصة أحاطته أغلب القوانين بمجموعة من الشروط والضمانات.

### الشروط الموضوعية.

يقصد بها مجموع الضوابط اللازمة لإجراء تفتيش صحيح، وتتمثل في السبب، المحل، السلطة المختصة بالقيام به.

- **سبب التفتيش.**

والمقصود به الدافع أو المبرر المقتضى لإجرائه ويتحقق هذا السبب بوقوع جريمة الإرهاب الإلكتروني، واتهام أشخاص معينين بارتكاب هذه الجريمة المعلوماتية أو الاشتراك فيها ووجود دلائل على وجود محل الجريمة في المكان أو لدى الشخص المراد تفتيشه ووجود غاية معينة من وراء

[1] خالد ممدوح الإبراهيمي، مرجع سابق، ص205.
رشيدة بوكر، مرجع سابق، ص 404.
[2] اتفاقية بودابست لسنة 2001.

إجرائه، وعليه فإنه يشترط لإجراء التفتيش أن تكون الجريمة الإرهابية قد وقعت فعلا، فلا يجوز إجراء التفتيش بحثا عن أدلة لجريمة مستقبلية، وإن كان هناك احتمال في أنها سوف تقع فعلا، وذلك لأن التفتيش إجراء خطير يمس بحرية الأشخاص وحرمة حياتهم الخاصة[1].

ويشترط في التفتيش في جريمة الإرهاب الإلكتروني إذن التفتيش وبما أن جريمة الإرهاب الإلكتروني تعتبر جريمة معلوماتية فهي بذلك تشكل اعتداء على نظم المعالجة الآلية[2].

كما يشترط لتحقيق سبب التفتيش في جريمة الإرهاب الإلكتروني اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها، بحيث يشترط وجود دلائل قوية وكافية لتوجيه الاتهام إلى شخص أو أكثر، فلا يجوز انتهاك حرماتهم أو حياتهم الخاصة دون وجود دلائل نرجح ارتكابهم هذه الجريمة الإرهابية.

ويقصد بالدليل في هذه الحالة استنتاج واقعة مجهولة من أخرى معلومة وهذا الاستنتاج يكون على سبيل الاحتمال والرجحان[3] .

وقد استخدم قانون الإجراءات الجنائية الفدرالي الأمريكي السبب المحتمل إذ نص على أنه: "يصدر قاضي محكمة الولايات أمر التفتيش للبحث عن شخص أو الاستيلاء على الأشياء إذا كان هناك سبب محتمل لذلك".

وهذا التعبير استخدم في التعديل الرابع للدستور الأمريكي الذي نص على عدم جواز القبض أو تفتيش الأشخاص وانتهاك حرمة منزلهم ما لم يكن بناء على سبب معقول، كما استند أيضا المشرع المصري نفس اللفظ أو التعبير في المادة 237 من قانون العقوبات المصري[4].

كما يلزم أن يسبق التفتيش تحريات جدية تسوغ الأمر به، إذ لا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش مجرد وقوع جريمة الإرهاب الإلكتروني، واتهام شخص معين أو أكثر بارتكابها بل يجب أن تتوفر لدى سلطة التحقيق أسباب كافية انه يوجد في مكان ما أو لدى الشخص المراد

[1] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية،2011، ص117.

[2] القانون رقم 04/09 المؤرخ في أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] السيد محمد حسن الشريف، النظرية العامة للإثبات الجنائي، دار النهضة العربية، القاهرة،2002، ص133.

[4] سامي جلال فقي حسين، مرجع سابق، ص122.

تفتيشه أو لدى غيره أدوات استخدمت في جريمة الإرهاب الالكتروني أو أشياء متحصله كأن تكون مستندات الكترونية[1].

**- محل التفتيش.**

ويقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سر والسر الذي يحميه القانون وهو ذلك الذي يستودع في محل له حرمة، أما محل التفتيش في جريمة الإرهاب الالكتروني هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال[2].

وقد أطلق بغض الفقه على عملية البحث عن أدلة الجريمة في الجرائم الإلكترونية ومنها الإرهاب الالكتروني –كما سبق أن أشرنا بالولوج أو النفاذ لأنها أكثر دقة من مصطلح التفتيش[3].

ويشترط في فقه المحل أن يكون معينا تعيينا نافيا للجهالة، بمعنى أن يتم تحديد المكان المراد تفتيشه بدقة سواء كان مكانا واحدا أو عدد من الأماكن[4]، ولكي يتم التفتيش على هذا المجال فإنه ينبغي الإشارة أن هذه الأخيرة لا تكون قائمة بذاتها بل يكون موضوعه في مكان كالمسكن أو المكتب أو أن تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال[5].

**- السلطة المختصة بالتفتيش.**

من المعلوم أن التفتيش إجراء من إجراءات التحقيق الابتدائي والذي يمس حقوق وحريات الأفراد ونتيجة لذلك كان المشرع الجزائري في معظم دول العالم حريص لإسناد هذا الإجراء إلى جهة قضائية من أجل ضمان هذه الحقوق والحريات وقد حددها المشرع بقاضي التحقيق وإذا كان الأمر أن يقوم هذا الأخير بإجراء التفتيش بنفسه إلا أنه يمكن لضابط الشرطة القضائية أن يقوم بذلك استثناءا وذلك في حالة كان الفعل المجرم جناية أو جنحة داخل منزل واستدعاؤهم من قبل صاحبه لإجراء التحقيق، أو أن هذه الجريمة متلبس بها في جريمة الإرهاب الالكتروني قد تكون متلبس بها، ومثال ذلك أن يكون ضابط الشرطة القضائية في أحد مقاهي الانترنت فيلاحظ حركة غريبة للعمل على الانترنت من قبل أحد أعضاء الانترنت فيتدخل لمراقبته عن طريق حاسوب آخر فيجده يقوم بالإبحار على تلك الشبكة

[1] رشيدة بوكر، مرجع سابق، ص408.

[2] نفس المرجع، ص 408.

[3] خالد حازم، مرجع سابق، ص294.

[4] سامي جلال فقي حسين ، مرجع سابق، ص129.

[5] رشيدة بوكر، مرجع سابق، ص408.

للتجسس على مواقع الدفاع الوطني الجزائرية أو انه يقوم بإرسال رسائل تهديد لفئة معينة من الناس بغية نشر الرعب والفزع كما يمكن أن يقوم ضابط الشرطة القضائية بإجراء التفتيش في حالة الإنابة من قبل قاضي التحقيق المختص[1].

وفي حالة الإنابة وجب أن يحدد في إذن الندب بالتفتيش المكان والشخص والأشياء المراد تفتيشها وضبطها كتحديد الحاسوب وبرامج الاختراق وبرامج الفيروسات ....الخ

وتجدر الإشارة أن أغلب التشريعات بما فيها المشرع الجزائري لم يقدم حل حول إمكانية تفتيش كل الملفات بإذن واحد أم يلزم إذن لكل ملف؟.

ويرى بعض الفقه أنه وجب على المشرع الجزائي أن يتدخل بالنص لهذه الإشكالية وينص صراحة على جواز التفتيش لكل الملفات المتواجدة في نظام المعالجة الآلية بسببين أن القانون يجب أن يتكيف مع الواقع[2].

**الشروط الشكلية.**

بالإضافة إلى الشروط الموضوعية للتفتيش هناك شروط شكلية وجب مراعاتها عند ممارسة هذا الإجراء:

- **الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الرقمية.**

حيث يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان على سلامة الإجراء وصحة الضبط[3].

إلا انه وفي الجريمة محل دراستنا وبالنسبة للمشرع الجزائري وكذلك الفرنسي لم يشترط هذا الإجراء الشكلي أثناء التفتيش[4].

وكذلك المشرع الفرنسي وهذا الموقف لمعظم مشرعي العالم يتماشى والطبيعة الخاصة لهذه الجرائم من حيث كونها ذات طبيعة تقنية محضة استمدتها من البيئة التقنية التي ترتكب فيها والتي

[1] المواد: 138، 139، 140، 141، 142، من قانون الإجراءات الجزائية الجزائري.

[2] رشيدة بوكر، مرجع سابق، ص413.

[3] نبيلة هبة هروال، مرجع سابق، ص265.

[4] الفقرة الثانية من المادة 45 من قانون الإجراءات الجزائية الجزائري.

أثرت بدورها على الأدلة التي يمكن الاعتماد عليها في إثبات هذا النوع من الجرائم فاكتسبت هي الأخرى طبيعة خاصة من حيث سرعة تعديلها والتلاعب فيها في اقل من ثانية وهو ما يقتضي الإسراع في استخلاصها قبل فقدانها[1].

- **وقت التفتيش.**

حيث قيد المشرعون في معظم الجرائم إجراء التفتيش في ميقات زمني معين حيث يعد الميقات الزمني لإجراء التفتيش من الأمور المهمة جدا والتي تساعد في الحصول على الدليل المعلوماتي في الجرائم المعلوماتية من عدمه، وذلك لأنه من السهل جدا إتلاف الدليل المعلوماتي ومحوه من قبل وصول السلطات المختصة بالتحقيق لذلك كلما كان التفتيش في وقت قريب بعد ارتكاب الجريمة كانت فرضية الحصول على الأدلة أكبر وفي هذا الشأن اختلفت التشريعات الإجرائية في تنظيمها لذلك فمثلا التشريع الجزائي العراقي لم يحدد في النصوص المتعلقة بالتفتيش وقتا معينا لإجراء التفتيش وبالتالي يجوز إجراؤه في أي وقت وفي أي مكان وهو نفس الاتجاه الذي أخذ به المشرع المصري[2].

أما كل من المشرعين الفرنسي والجزائري قد اتجها إلى حصر التفتيش المتعلق بالمنازل ولم يتركا الأمر لتقدير القائم بالتفتيش فقد حدد المشرع الجزائري ميقات التفتيش من الساعة 5 صباحا إلى الساعة 8 مساءا إلا أنه وفي حالات جريمة الإرهاب الالكتروني لا يوجد ضابط لوقت التفتيش وهذا لخطورة الجريمة فهي جريمة إرهابية باستخدام نظام معالجة المعطيات حسب المادة 47 في فقرتها الثالثة وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فانه يجوز إجراء التفتيش والمعاينة في كل محل سكني، في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص.

وجدير بالذكر أن في استثناء بعض المشرعين ومنها المشرع الجزائري حظر التفتيش ليلا إدراكا منه بالطبيعة المميزة لهذه الجرائم وخصوصيتها من حيث أنها يمكن ارتكابها في أي وقت وأن أدلة الإدانة فيها سهلة المحو والتدمير وأنها غير مرئية وبالتالي فإن تأخير التفتيش في الموعد القانوني قد

[1] رشيدة بوكر، مرجع سابق، ص415.

[2] سامي جلال فقي حسين، مرجع سابق، ص164.

يعرقل السير الطبيعي لمجريات التحقيق، كما أن هذه الضمانات بذات تتضاءل أهميتها مع ظهور ما يسمى بالتفتيش عن بعد ( أي التفتيش من مكتب الضبطية باستخدام برامج خاصة تعتمد في طابعها قاعدة التفتيش عن الجريمة) أو التفتيش المباشر والذي يمكن أن يتم في أي وقت[1].

- **محضر التفتيش.**

إن التفتيش في جريمة الإرهاب الالكتروني كغيره من الإجراءات في باقي الجرائم يستلزم بالضرورة تحرير محضر يثبت فيه ما تم من إجراءات وعلى ذلك فان هذا المحضر يستوجب القواعد العامة في المحاضر عموما بحيث وجب أن يكتب باللغة الرسمية وان يشتمل على ساعة وتاريخ التحرير والتوقيعات المتعلقة بمحرره....الخ، وعليه فان المحاضر المتعلقة بالتفتيش في جريمة الإرهاب الالكتروني تستلزم أيضا ضرورة إحاطة القائم بالتفتيش بتقنية المعلومات فضلا على استعانته في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش بشخص يرافقه يكون متخصص في الحاسوب والانترنت[2].

وأما عن ضابط الدليل التقني باعتباره النتيجة الطبيعية للتفتيش وهنا الضبط هو وضع اليد على شيء يتصل بالجريمة–محل الدراسة– ويفيد في كشف الحقيقة عنها وعن مرتكبها[3]،فالأدلة المضبوطة في جريمة الإرهاب الالكتروني ذات طبيعة معنوية يتمثل في المعلومات كالمراسلات والاتصالات الالكترونية[4].

المشرع الجزائري تدخل لاستكمال ما تبقى من فراغ تشريعي في المنظومة التشريعية وذلك بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث استحدث المادة 06 منه والتي تنص على انه "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين

[1] رشيدة بوكر، مرجع سابق، ص 417.

[2] نبيلة هبة هروال ، مرجع سابق، ص263.

[3] هشام محمد فريد رستم، مرجع سابق، ص419.

[4] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، 2006، ص218.

الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية....."[1].

المشرع الفرنسي بدوره قام بإدخال تعديلات على قانون الإجراءات الجزائية الفرنسي وذلك بموجب قانون الأمن الداخلي رقم 239 لسنة 2003 حيث استحدث الفقرة 03 من المادة 01/67 التي تنص على انه:"المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعامات التخزين المعلوماتية هذه يتعين تحريرها في أحراز مختومة وفقا للشروط المنصوص عليها في هذا القانون[2].

وتجدر الإشارة أن فرنسا من الدول الموقعة على اتفاقية بودابست لعام 2001 حيث نصت هذه الأخيرة على الضبط في الفقرة الثالثة من المادة 19 منها في القسم الرابع "من سلطة طل دولة طرف أن تتخذ الإجراءات التالية: أن تضبط نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وان تحافظ على سلامة تلك المعلومات المخزنة[3].

أما عن ضبط الأدلة المادية فلا تثير أي إشكال ويتم الرجوع في ضبطها للنصوص التقليدية.

## المطلب الثاني: الإجراءات المستحدثة في استخلاص الدليل.

نظرا لما أحدثته الثورة التكنولوجية من تعقيدات فيما بتعلق باستخلاص الدليل الالكتروني، الأمر الذي يؤدي إلى إفلات العديد من المجرمين وخاصة الإرهابيين من العقاب، وعلى ذلك كان يجب على التشريعات المختلفة أن تتطور وتطور استخلاص الدليل الجنائي وذلك من خلال تكريس قواعد قانونية إجرائية غير تقليدية تتناسب والطبيعة التقنية لهذه الجرائم.

وقد تفطنت معظم التشريعات لهذه المسالة ومنها المشرع الفرنسي وأيضا المشرع الجزائري الذي جاء بالقانون 22/06 المؤرخ في 2006/12/20 فاستحدث الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان: "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" فأجاز بموجبه لوكيل

[1] القانون 09-04 سالف الذكر.

[2] رشيدة بوكر، مرجع سابق، ص 420.

[3] اتفاقية بودابست 2001.

الجمهورية أن يأذن باعتراض الاتصالات السلكية واللاسلكية وبعدها جاء بالقانون 04/09 بشان الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فاستحدثت بموجبه إجراءين المراقبة الالكترونية وحفظ المعطيات المتعلقة بحركة السير[1].

## الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الاعتراض والتسجيل والالتقاط والتسرب هي عدة تسميات يمكن اختصارها في مصطلح "المراقبة" والتي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو أحاديث أو مراسلات مكتوبة أو مسموعة أو مرئية، نتيجة لاشتباه في تصرفات غير قانونية وذلك بصورة لا يحس معها الغير لمباشرتها بطابع السرية الذي يكتنفها[2].

### أولا: الاعتراض.

قد اغفل معظم المشرعين ومنهم المشرع الجزائري مسالة تعريف الاعتراض واكتفى بتنظيم هذه العملية ولا يعتبر هذا الأمر تقصيرا في التشريعات وإنما ترك هذا الأمر (إعطاء تعريف للاعتراض) للفقه[3].

وفيما يتعلق بالجريمة الإرهابية الالكترونية فقد انعقد بشأنها اجتماع للجنة الخبراء البرلماني الأوروبي بستراسبورغ والذي انعقد بتاريخ: 2006/10/06 وذلك لبحث حول أساليب التحري والتقنية وعلاقتها بالأفعال الإرهابية عرفت اعتراض المراسلات بأنها: "عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجريمة[4].

[1] رشيدة بوكر، مرجع سابق، ص440.

[2] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة 01، عدد 33، جوان 2010، ص254.

[3] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية الإسكندرية، 2009، ص138.

[4] رشيدة بوكر، مرجع سابق، ص442.

وقد أجازت المادة 65 مكرر 05 من قانون الجزاءات الجزائية الجزائري لوكيل الجمهورية بان يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وعلى ذلك يستشف من نص هذه المادة أن المقصود باعتراض المراسلات اعتراض تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين الاستقبال والعرض[1].

ويمكن تعريف الاعتراض بأنه رصد إشارات إلكترومغناطيسية في الأنظمة المعلوماتية أو تحليلها بغية استخراج المعلومات المفهومة والمقروءة منها[2]

وقد أجازت اتفاقية بودابست للجرائم الالكترونية ومنها جريمة الإرهاب الالكتروني –موضوع الدراسة– الاعتراض الشرعي لكل أشكال النقل الالكتروني للبيانات، سواء تم عبر التلفون أو الفاكس أو البريد الالكتروني ....الخ

وتشمل الاتصالات محل الاعتراض محتوى غير المشروع أو دليل على الأفعال الجرمية الخطيرة التي يعرفها القانون الداخلي لكل دولة طرف في الاتفاقية[3].

مما يستوجب اعتراض المراسلات الالكترونية المتبادلة عبر الحاسب الآلي أيضا لدرء خطر الجريمة وملاحقة الجناة، وهو ما نص عليه المشرع الجزائري في المادة 658 مكرر سالفة الذكر حيث أجاز المشرع وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية والقيام بإجراء التفتيش والحجز داخل منظومة معلوماتية في إطار إذن من السلطة القضائية[4].

وعليه وحسب نص المادة 11/08 من القانون 03/2000 المتعلق بالبريد والمواصلات السلكية واللاسلكية فكل مراسل أو إرسال أو استقبال علامات أو إشارات، كتابات، صور أو أصوات أو

[1] قانون الإجراءات الجزائية الجزائري.

[2] يزيد بوحليط، مرجع سابق، ص188.

[3] جميلة محلق، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار –عنابة عدد 42 ، جوان 2015، ص178.

[4] نفس المرجع، ص178.

معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي إذا كان الحال كذلك فكل إشارة أو كتابة أو صورة أو صوت مهما كانت وسيلة الاتصال يضل حان يكون محلا للاعتراض[1].

ومن خصائص اعتراض المراسلات حتى يتأتى الهدف المرجو من ورائها ومن أهم هذه الخصائص:

1- اعتراض المراسلات يتم دون علم صاحب الشأن ودون رضاه.

2- الإجراء( الاعتراض) يمس بحق الشخص في السرية ويعتبر هذا الإجراء بمثابة الاستثناء على هذا الحق الدستوري وهذا بهدف السير الحسن للتحريات والتحقيقات والحفاظ على الأمن العام وهذا لما يقدمه إجراء الاعتراض من مساعدة للجهات القضائية والأمنية للوصول إلى أدلة ومعلومات كانت تعتبر شخصية ولا يمكن المساس بها تحت ذريعة الحريات الشخصية.

3- إن الدليل الذي يسعى إلى الحصول عليه من وراء الاعتراض هو دليل غير مادي فيبعث من عناصر شخصية مما يصدر عن الغير من أقوال وأحاديث يقنع القاضي بطريقة غير مباشرة تفيد في الكشف عن الجريمة، فتعتبر الأحاديث دليل معنوي غير مادي، وعلى ذلك فإن هدف اعتراض المراسلات هو التقاط الأدلة المعنوية بغية تأكيد أدلة الاتهام[2].

4- يتم الاعتراض بواسطة أجهزة قادرة على التقاط الأحاديث وهو الأمر الذي دعته ضرورة التطور التكنولوجي والتقني فمثلا في جريمة الإرهاب الالكتروني –موضوع دراستنا– وجب استعمال أجهزة اعتراض ذات تقنية واسعة قادرة على التقاط الأحاديث الصوتية بدقة وجودة عالية وهذا لما تشكله الجريمة من قلق رهيب في أوساط المجتمع[3].

ومما سبق يمكن القول أن فعل الاعتراض يمكن أن يقع داخل منظومة معلوماتية واحدة أو بين نظامين متصلين سواء شبكة داخلية( وهي شبكة انترنت داخلية تستخدم ذات التقنية، لها سرعات مختلفة وكلما بعدت المسافة عن مصدرها قلت سرعتها، فهي شبكة صغيرة بحيث تسمح للأعضاء

[1] قانون رقم 03/2000 مؤرخ في: 05 جمادى الأولى عام 1421 ﻫ الموافق لـ 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية واللاسلكية، جريدة رسمية، عدد48، ص03، (2000/08/06).

[2] ياسر الأمير فاروق، مرجع سابق، ص165.

[3] نفس المرجع، ص165.

المسجلين بمنظمة أو مؤسسة أو أي كيان تنظيمي آخر الذي يستخدم البروتوكولات نفسها مثل: IMAP.SMTP. HMP. IP. TCP بمزاياها متعددة كسرعة تبادل البيانات، مما أدى إلى انخفاض تكاليف الإدارة وإمكانية الوصول إلى المحتوى والخدمات وارتفاع مستوى الحماية الذي لا يمكن مقارنته بمستوى الحماية الموجود على شبكة الانترنت العادية[1].

كما قد يكون عن طريق شبكة الانترنت كما هو الشأن في البريد الالكتروني إذ يغطي النظام المعلوماتي كافة أنواع الاتصالات الالكترونية مثل شبكة ( WIFI ) وهي نظام مفتوح من السهل اعتراضه باستعمال وسائل الكترونية، ويتم ذلك عن طريق اعتراض خط سير البيانات الالكترونية، أو قطع بث واستقبال بيانات تقنية المعلومات باستعمال وسائل فنية توفرها تكنولوجيا الإعلام والاتصال[2].

### ثانيا: تسجيل الأصوات.

ويقصد به تسجيل أحاديث التي تدور بين المتهمين الإرهابيين والحديث هو الكلام الذي له دلالة مفهومة سواء كان هذا الكلام موجها لجمهور الناس أو لفئة محددة منهم وبأي لغة، حتى ولو كان يدور بالشفرة، إذ أن هذه الأخيرة في حقيقتها لغة[3].

وعلى ذلك فإن تسجيل الأصوات هو النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت، والتعرف على مضمونه.

فالتسجيل الصوتي المتخذ كوسيلة للتحري عن جريمة الإرهاب الالكتروني يشمل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، فهذا الإجراء يهدف إلى متابعة المحادثة أو المكالمات الهاتفية ومعاينتها، فهو يعني من ناحية مراقبة المكالمات ومن ناحية أخرى التصنت عليها، ويكفي مباشرة إحدى هاتين العمليتين لقيام عملية تسجيل

[1] يزيد بوحليط، مرجع سابق، ص 189.

[2] نفس المرجع، ص 189.

[3] سمير الأمين، مراقبة التلفون والتسجيلات الصوتية والمرئية، الطبعة الثالثة، دار الكتاب الذهبي، القاهرة، 2000 ص43.

الأصوات التي تعتمد على وضع رقابة على الهواتف ونقل الأحاديث وتسجيلها التي يتم عن طريقها أو بوضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، وقد يتم أيضا عن طريق التقاط إشارات لاسلكية أو إذاعية التي يجريها ضباط الشرطة القضائية بغرض الاستعانة به في التحري والبحث والإثبات الجنائي[1].

وتجدر الإشارة أن مختلف التشريعات لم تعرف التسجيل الصوتي مثل المشرع الفرنسي، وكذلك المشرع الجزائري الذي أشار إلى هذا الإجراء من خلال نص المادة 65 مكرر/02 " 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"[2].

وعلى ذلك فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجزائية نظرا لأنها لم تسجل في شان دعوى جنائية حركتها السلطات القضائية بقصد الوصول إلى الحقيقة كما يخرج عن نطاق البحث تسجيل الأحاديث التي لا تتضمن اعتداء على حق من يتم تسجيل حديثه كما في حالة تسجيل الأحاديث التلفزيونية أو الإذاعية أو الصحفية متى تم ذلك بموافقة المعني[3].

ولسلامة التسجيل الصوتي وجب التأكد أولا من أن الصوت يخص المتهم (أي الإرهابي في هذه الجريمة) وأن هذه الشريط لم يتعرض إلى عملية مونتاج[4].

كما يجب تفريغ هذه التسجيلات في أحراز مختومة، بحيث تعتبر هذه الأحراز المختومة بمثابة أدلة مادية[5].

وقد اختلفت الآراء حول الطبيعة القانونية لعملية تسجيل الأصوات، فاعتبرها البعض أن لها علاقة كبيرة بعملية التفتيش حيث تهدف هي الأخرى إلى كشف الحقيقة مثلها مثل التفتيش، في حين

---

[1] مقني بن عمار بوراس عبد القادر، التنصت على المكالمات الهاتفية واعتراض المراسلات كآلية للوقاية من جرائم الفساد، مداخلة مقدمة للملتقى الوطني حول الآليات القانونية لمكافحة الفساد، جامعة ورقلة، في الفترة من 2-2008/12/3، ص14.

[2] قانون الإجراءات الجزائية الجزائري .

[3] حسين المحمدي البوادي، الوسائل العلمية الحديثة في الإثبات الجنائي، الإسكندرية، 2005، ص47.

[4] سمير الأمين، مرجع سابق، ص38.

[5] المواد 18 و45 من قانون الإجراءات الجزائية الجزائري.

يرى البعض الآخر أن تسجيل الأصوات ينشأ عن ضبط الوسائل التي تتضمن حديث كتابي وأن التسجيلات الصوتية تتضمن حديث شفوي، إلا أن هناك فرق واضح بين عملية ضبط الوسائل وتسجيل الأصوات، تكمن في كون ضبط الرسائل تعتبر أدلة مادية إلا أن التسجيلات الصوتية ليست بأدلة مادية ولا تقبل الضبط بالمعنى القانوني فالطبيعة القانونية للتسجيلات الصوتية تكمن في أنها إجراء من نوع خاص فهي مستقلة عن عملية التفتيش وكذا ضبط الرسائل، وهذا الموقف أحق به المشرع الجزائري[1].

**ثالثا: التقاط الصور.**

التقاط الصور إجراء مستحدث جاءت به التشريعات محاولة منها بمكافحة الجرائم المستحدثة ومن بينها جريمة الإرهاب الإلكتروني، ويقوم هذا الإجراء أساسا على استخدام الكاميرات أو أجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة أشخاص مشكك في أمرهم على الحالة التي كانوا عليها وقت التصوير لغرض استخدام محتوى الفيلم كمادة إثبات ودليل مادي، أو بمعنى آخر مادة مرئية في المحاكم لضمان اتخاذ الإجراءات الوقائية لضبط المجرمين أو المشتبه فيهم، واستخدام الكاميرات يمكن أن يكون علنا أو خفية، وهذا أمر مألوف في المؤسسات المصرفية كالبنوك والمصارف وهذا بسبب تزايد الجرائم في عصرنا، فهذا الإجراء يربط الأشخاص في زمان ومكان في وقت واحد وخاصة مع التطور التكنولوجي والعلمي أصبح بالإمكان استخدام وسائل حديثة وذات تقنية جيدة تساعد على التقاط الصور بجودة عالية فهناك أجهزة تعمل بالأشعة تحت الحمراء تلتقط صور الأشخاص ليلا بصورة دقيقة وواضحة، حيث تستخدم هذه الأجهزة لنقل الصوت والصورة بشكل رائع ملفت للانتباه، بحيث تمكن ضابط الشرطة القضائية من سماع ورؤية ما يدور في حياة المشتبه فيه طوال مدة التحري والبحث.

وبالرجوع للمشرع الجزائري نجده لم يكتف بالسماح لقاضي التحقيق تسجيل الأصوات، بل مكنه أيضا من إمكانية التقاط الصور وهذا بموجب المادة 65 مكرر5 من قانون الإجراءات الجزائية

[1] ياسر الأمير فاروق، مرجع سابق، ص 182.

الجزائري، والتي سمحت لقاضي التحقيق أن يمد الكاميرات إلى الأماكن الخاصة التي تعد مستودعات أسرار المعنيين بالمراقبة[1].

وبالنظر إلى طبيعة اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراءات استثنائية نص عليها المشرع في بعض الجرائم، فقط والتي ظهرت حديثا، وذلك رعاية للمصلحة العامة، ومن أجل ذلك وجب توافر العديد من الشروط قبل اتخاذها وهذا لما تحمله في طياتها من اطلاع على أسرار الحياة الخاصة للآخرين، بحيث وجب أن تقوم بها سلطة مختصة بحيث يكون دائما تحت وقاية قاضي التحقيق، كما يجوز أن تتم هذه الإجراءات في أي ميقات وفي أي مكان، دون الحاجة إلى قيود لا زمنية ولا مكانية والقيد الوحيد الذي يرد على هذا اتخاذ الإجراءات اللازمة لضمان احترام كتمان سر المهنة ويتفرع عنه احترام سرية المراسلات والمحادثات الهاتفية بين المحامي وموكله مثلا[2].

هذا وإن كل من القائم والمشرف على هذه الإجراءات لا يترتب عليه أي مسؤولية جنائية ولا مدنية وهذا حسب المادة 65 مكرر 5 قانون الإجراءات الجزائية.

وتجدر الإشارة إلى أن اللجوء إلى هذه الإجراءات يكون في حالة الضرورة والتي يقدرها ويقررها قاضي التحقيق في جميع الأحوال (المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائرية).

عن قيام الضبطية القضائية بهذه الإجراءات من اعتراض للمراسلات وتسجيل الأصوات والتقاط الصور لا يعني أن الجهة المعنية كالنيابة العامة وقضاة التحقيق أو الحكم مجبرة على الآخذ بها، بل هي عميل كباقي الأعمال وفي هذا الشأن استوجب المشرع الجزائري في المادة 65 مكرر 9، تحرير محضر على كل عملية اعتراض وتسجيل مراسلات وكذا عمليات وضع الترتيبات التقنية والتقاط الصور ويذكر في المحضر تاريخ وساعة بداية ونهاية العملية وتودع في ملف والسلطة التقديرية لهذه السلطات وذلك للأخذ بها واستبعادها[3].

[1] فوزي عمارة، مرجع سابق، ص 238.

[2] نفس المرجع، ص 239.

[3] يقدح دارين، هنوني نصر الدين، الضبطية القضائية في القانون الجزائري، دار هومة، الجزائر، 2009، ص80.

## الفرع الثاني: التسرب والمراقبة الالكترونية.

أمام التطور الهائل الذي عرفه عصرنا الحاضر خاصة في المجال التكنولوجي والمعلومات صار من الضروري التفكير في آليات جديدة لمواجهة المستجدات في الجرائم وخاصة وأن الجرائم المستحدثة اختلفت أنواعها وصورها، الأمر الذي جعل مختلف تشريعات العالم تبنت نصوص قانونية مستحدثة تتماشى وهذه الجرائم بهدف مكافحتها والأمر لم يقتصر على التشريعات الوطنية فالمنظمات الدولية وفي مقدمتها الأمم المتحدة انتقلت بكثير من برامجها وسياستها الجنائية إلى التحدي للجريمة بشتى أنواعها وخاصة الجرائم المستحدثة وعلى رأسها جريمة الإرهاب الإلكتروني وهذا لكون نشاطات هذه الجرائم تتم بصورة خفية وبتخطيط محكم تجعل منفذيها غير معروفين.

وقد بين المشرع الجزائري الأسلوب تنفيذا للالتزامات المترتبة على الدولة الجزائرية في هذا المجال، ومن ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته لمكافحة الجرائم المستحدثة من بينها جرائم الاعتداء على نظم المعالجة الآلية عملية التسرب [1] كإجراء علاجي والمراقبة الالكترونية كإجراء وقائي.

### أولا: مفهوم عملية التسرب.

يقصد بعملية التسرب القيام بمراقبة المشتبه في ارتكابهم جناية أو جنحة بإيهام المتسرب لهؤلاء الأشخاص أنه فاعل معهم أو شريك لهم أو خاف، وقد عرفه المشرع الجزائري في نص المادة 65 مكرر 12 من قانون العقوبات بقوله:قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف"[2].

وبالرجوع إلى نص المادة 65 مكرر من قانون العقوبات الجزائري نجد أن التسرب إجراء يجوز في جرعة الإرهاب الإلكتروني حيث أن هذه الأخيرة جريمة مستحدثة تنتمي إلى الجريمة الإرهابية من

[1] قانون الإجراءات الجزائية الجزائري.

[2] الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري.

حيث الطبيعة والهدف وإلى الجريمة المعلوماتية من حيث الوسيلة المستخدمة في ارتكابها ومن أجل ذلك فهي ضمن النطاق الذي حدده المشرع الجزائري.

ومن خلال تعريف عملية التسرب يمكن القول أن التسرب عملية معقدة تتطلب أن يتدخل العون المكلف بالعملية في اتصال بالأشخاص المعنيين ويربط معهم علاقات ضيقة ويحافظ على السر المهني لغاية تحقيق الهدف النهائي للحماية، فهي تطالب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها والذي يكون أحيانا ضرورة لقبوله[1].

وفي جريمة الإرهاب الإلكتروني يمكن تصور عملية التسرب في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشر في كيفية قيام أحد الإرهابيين اختراق الشبكات أو تدمير مواقع وبث فيروسات، أو كيفية تصنيع الأسلحة مستخدما في ذلك أسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منهم حول كيفية اقتحام الإرهابي لموقع أو تدميره[2].

التشريع الفرنسي بدوره تطرق إلى هذا الإجراء كغيره من معظم تشريعات العالم واعتمدها كأسلوب من أساليب التحري للبحث عن الدليل حيث نص عليها في قانون الإجراءات الجزائية الفرنسية من خلال 7 مواد[3].

ومما سبق يمكن القول أن التسرب عملية منظمة يحضر لها بدقة تامة ستهدف أوساطا معينة قائمة على دراسة مسبقة لها بحيث يتم الوقوف على أدق خصوصياتها وتفاصيلها بهدف معرفة طبيعة عملها وكيفية تحركها من الناحية البشرية والمادية، ويقوم بها ضابط الشرطة القضائية أو إحدى أعوانه تحت مسؤوليته بمراقبة الأشخاص في ارتكابهم لإحدى الجرائم المنصوص عليها في المادة 65 مكرر– ومن بينها المجموعة موضوع الدراسة– ولا يجوز لهذا الإجراء إلا في حالة الضرورة التي تتطلبها إجراءات كالبحث والتحري والتي يقدرها قاضي التحقيق دائما.

[1] رشيدة بوكر، مرجع سابق، ص 434.

[2] نفس المرجع، ص 434.

[3] المواد من 706/81 إلى غاية 706/87 قانون الإجراءات الجزائية الفرنسي.

كما أن عملية التسرب لا يجوز قانونا مباشرتها إلا بإذن من قاضي التحقيق بعد إخطار وكيل الجمهورية أو وكيل الجمهورية[1].

## شروط صحة عملية التسرب:

بما أن عملية التسرب تعتبر ممارسة غير مألوفة لضابط الشرطة القضائية أو العون كما أن هذا الإجراء يعتبر من أخطر الإجراءات بما فيه من انتهاكات لحرمة الحياة الخاصة للمتهم، من أجل ذلك أحاطه المشرع بمجموعة من الضمانات أو الشروط كما يلي:

- **شروط شكلية:**

من أهم الشروط الشكلية الواجب توافرها في التسرب:

**1/ صدور إذن قضائي في الجهة المختصة لإصدار إما وكيل الجمهورية أو قاضي التحقيق.**

وذلك بعد إخطار وكيل الجمهورية، وفي ذلك حماية للحقوق الأساسية المكرسة دستوريا وعليه لا يمكن بأي حال من الأحوال أن يقوم ضابط الشرطة القضائية بالعملية بمفرده دون المرور بالجهاز القضائي وهذا ما يستنتج من المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري[2].

**2/ أن يكون مكتوب.**

لما كان الأمن في العمل الإجرائي الكتابة فيجب أن يكون إذن التسرب مكتوب وإلا كانت العملية باطلة فيجب أن يكون إذن التسرب مكتوب وإلا كانت العملية باطلة وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري.

وإذا صدر هذا الإذن في إطار الإنابة القضائية ينبغي مراعاة الشروط الشكلية والموضوعية للإنابة القضائية التي نصت عليها المادتين 138 من قانون الإجراءات الجزائية الجزائري والتي تنص:" يجوز لقاضي التحقيق أن يكلف بطريق الإنابة القضائية أي قاضي من قضاة محكمته أو أي

[1] محمد حزيط، مذكرات في قانون الإجراءات الجزائية، دار هومة، الجزائر، 2005، ص172 .

[2] رشيدة بوكر، مرجع سابق، ص 435.

ضابط من ضباط الشرطة القضائية المختص بالعمل في تلك الدائرة أو أي قاضي من قضاة التحقيق بالقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم.

ويذكر في الإنابة القضائية نوع الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه.

ولا يجوز أن يؤمر فيها إلا باتخاذ إجراءات التحقيق المتعلقة مباشرة بالمعاقبة على الجريمة التي تنصب عليها المتابعة".

أما المادة 139 من نفس القانون فتنص:" يقوم القضاة أو ضباط الشرطة القضائية المنتدبون للتنفيذ بجميع السلطات المخولة لقاضي التحقيق أن يعطي بطريق الإنابة القضائية تفويضا عاما .

ولا يجوز لضباط الشرطة القضائية استجواب المتهم أو القيام بمواجهته أو سماع أقوال المدعي المدني "

**3/ ذكر اسم الضابط المشرف على العملية وهويته كاملة.**

**4/ المدة المطلوبة لعملية التسرب[1].**

حسب نص القانون فإن مدة التسرب لابد أن لا تتجاوز أربعة أشهر، ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية وفي نفس الوقت أجاز القانون للقاضي الذي رخص بإجراءاتها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة لها[2].

[1] رشيدة بوكر، مرجع سابق، ص 435.

[2] المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري والتي تنص:" يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان.

تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.

ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر

يمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية

ويجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل المدة المحددة

= تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب"

وبالنسبة للعون المتسرب فيمكن أن يواصل نشاطه غير القانوني الوارد في نص المادة 65 مكرر 14[1]، من قانون الإجراءات الجزائية الجزائري، مع إعفائه من المسؤولية الجزائية لمدة لا تتجاوز 4 أشهر على أن يخطر القاضي مصدر الرخصة في أقرب الآجال، أما إن لم يتمكن العون المتسرب من إيقاف نشاطه خلال المدة المذكورة في ظروف تضمن أمنه يمكن للقاضي أن يرخص بتمديدها لمدة 4 أشهر أخرى.

**5/ إبعاد إذن التسرب خارج ملف الإجراءات .**

وذلك إلى غاية الانتهاء من العملية، حفاظا على السرية المطلوبة التي حصرها المشرع بين القاضي الآمر بها وضابط ش.ق المشرف على العملية وكذا العون المتسرب.

**6 / وجود تقرير مسبق محرر من طرف الضابط عن الجريمة**

ويكون بشكل مفصل لاطلاع القاضي بشكل تام على ظروف القضية ومتطلباتها.

- **شروط موضوعية[2]:**

تتمثل الشروط الموضوعية في التسبيب، بحيث يعتبر هذا الإجراء كباقي الأعمال القانونية، يجب أن يكون أساسه التسبيب(م 65 مكرر 15)، وكذلك وجب أن تكون هذه الجريمة ضمن نطاق المادة (65 مكرر 5.

[1] المادة 65 مكرر 14 من قانون الإجراءات الجزائية الجزائري:" يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرب والأشخاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جزائيا، القيام بما يأتي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال"

[2] قانون الإجراءات الجزائية الجزائري.

**آثار التسرب.**

التسرب كغيره من الإجراءات بعد صدور الإذن الخاص به من طرف الجهاز القضائي يباشر العون المتسرب عمله حسب المقتضيات المطلوبة منه ومن ثم هناك آثارا ستترتب عن ذلك منها.

**1/ تسخير الوسائل المادية والقانونية.**

وفقا لنص المادة 65 مكرر 14 من قانون الإجراءات الجزائية الجزائري على أنه يمكن:

- اقتناء الحيازة أو نقل أو تسليم أو إعطاء مواد أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستخدمة في ارتكابها.
- وكذا استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.
- وعلى ذلك يمكن للعون المتسرب استعمال الأموال المتحصل عليها من ارتكاب الجرائم المذكورة بنص المادة 65 مكرر 5 قانون الإجراءات الجزائية الجزائري ومن ثم نقل، تسليم وإيواء .....الخ.

أما بخصوص الوسائل القانونية فالمقصود منها توفير الوثائق الرسمية إن كان هناك ضرورة ولذلك كاستخراج بطاقة تعريف أو رخصة سياقة أو بطاقة رمادية وبالتالي يحتاج إلى جهاز خاص لتزوير الوثائق الرسمية دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة[1].

**2/ الإعفاء من المسؤولية.**

الأعمال التي يقوم بها المتسرب هي أعمال في حقيقتها غير مشروعة، وتستوجب العقاب لكن بالنظر إلى ضرورات التحقيق ومقتضياته في الجرائم المذكورة سابقا ومنها جريمة الإرهاب الإلكتروني، أدخل المشرع الجزائري عملية التسرب ضمن أسباب الإباحة باعتبار أن القانون إذن بذلك وهذا حسب نص المادة 39 من قانون العقوبات الجزائري[2] الأمر الذي يجعل العون المتسرب معفى من المسؤولية

[1] رشيدة بوكر، مرجع سابق، ص 437.

[2] تنص المادة 39 في فقرتها الأولى من قانون العقوبات الجزائري على أنه: " لا جريمة :
1. إذا كان الفعل قد أمر أو أذن به القانون"

الجزائية وأيضا استنادا إلى نص المادة 65 مكرر12 في فقرتها الثانية من قانون الإجراءات الجزائية بقولها: "يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم".

بل وإن المشرع يحدد أيضا من نطاق هذا الإعفاء لظروف أمنية للمتسرب حتى بعد انقضاء المدة المحددة في رخصة التسرب أو في حالة تقرر وفق عملية التسرب المادة 65 مكرر 17 من قانون الإجراءات الجزائية الجزائري[1].

**3/ إحاطة عملية التسرب بالسرية التامة.**

حتى تحقق عملية التسرب الأهداف والنتائج المرجوة منها وجب إحاطتها بالسرية التامة، ومن أجل ذلك حدد المشرع جزاءات عقابية مشددة في حالة إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية بل إن المشرع وسع من دائرة الحماية لتشمل أسرة العون المتسرب.

وتتراوح هذه العقوبات من سنتين إلى 20 سنة حبس وغرامة من 50.000دج إلى مليون دينار حسب الحالات الثلاثة المذكورة في المادة 65 مكرر 16 من قانون الإجراءات الجزائية.

وعليه يبقى العون والضابط المتسرب في سرية تامة، كما أن المادة 65 مكرر 18 من قانون الإجراءات الجزائية منعت سماع العون المتسرب وإجازة سماع للضابط المشرف على العملية بوصفه شاهدا[2].

## ثانيا: مراقبة الاتصالات الإلكترونية.

نظرا لكثرة الجرائم التي تقع ضمن الفضاء الافتراضي (الإلكتروني)، الذي يتم فيه تبادل المعلومات الرقمية وتجري عبره كل أنواع المعاملات والخدمات الإلكترونية، الأمر الذي يجعل السلطات العمومية غير قادرة على التحكم فيها بطرق الرقابة التقليدية، ومن أجل ذلك كان لزاما على التشريعات أن تكرس إطار قانوني أكثر فعالية في مواجهة وخطورة جرائم المعلوماتية المستحدثة

[1] يزيد بوحليط، مرجع سابق، ص 267.

[2] رشيدة بوكر، مرجع سابق، 480.

كجريمة الإرهاب الإلكتروني بحيث تكون هذه التشريعات منتمية للقواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة وللتنقل السريع لتحديد مصدرها والتعرف على مرتكبيها، وأهم هذه القواعد، وهو ما يخدم موضوع دراستنا هو المراقبة الإلكترونية.

## مفهوم المراقبة الإلكترونية

يقصد بالمراقبة الإلكترونية نظام الرقابة الوقائية عبر الوسائل الإلكترونية ويعد من بين أحد آليات واستراتيجيات مكافحة جرائم الاعتداء على نظم المعالجة الآلية والوقاية منها على اعتبار أن الفضاء الافتراضي الذي نحن جزء منه هو أرضية لشبكات عديدة من الجرائم، ومنها وأهمها وأخطرها جريمة الإرهاب الإلكتروني[1].

وتعرف المراقبة في مجال المعلوماتية بالمراقبة الالكترونية(la cyber-surveillance) ويقصد بها مراقبة شبكة الاتصالات أو ذلك العمل الذي يقوم به المراقب باستخدام التقنية الالكترونية لجميع البيانات والمعلومات حول المشتبه به، سواء كان شخصا أو مكانا أو شيئا حسب طبيعته، وذلك مرتبط بالزمن لتحقيق غرض أمني ولأي غرض آخر.

وعليه فالمراقبة الالكترونية كأصل وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه يقوم بها شخص يسمى ب:"المراقب الالكتروني" وهو في العادة من ضباط الشرطة القضائية، يتميز بالكفاءة التقنية العالية في مجال المعلوماتية التي تتماشى مع نوع الجريمة، يستخدم في ذلك التقنية الالكترونية، كأن يراقب نشاط أحد الإرهابيين الالكترونيين، أو يقوم بنسخ البريد الالكتروني لمراقبة اتصالات المشتبه به عند إرساله أو استقباله للبريد الالكتروني[2].

ويعتبر المشتبه فيه في إطار تنفيذ إجراء المراقبة الالكترونية عادة، هو شبكة الانترنت وحاسوب الشخص الذي أساء استعمالها، فتتم مراقبة اتصالاته الالكترونية المشتبه فيها والتي تتم عن طريق الانترنت، وبما أن إجراء المراقبة الالكترونية يستند إلى مبررات أسسها الوقاية ومكافحة الجرائم المعلوماتية وخصوصا الجرائم الإرهابية منها فإنها إجراء شرعي لا يتم اتخاذه إلا بناءا على أمر من

[1] رشيدة بوكر، مرجع سابق، 480.

[2] ربيعي حسين، المراقبة الالكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 01-2016 لسنة 2016، ص 417.

السلطات القضائية المختصة، وبجملة من الضمانات القانونية التي تحمي حق الفرد في الخصوصية المعلوماتية .

وعلى الرغم من ذلك فقد أشارت المستشارة العليا للأمم المتحدة المكلفة بترقية حقوق الإنسان "نافي بلاي" في تقرير لها حول نشاطات المراقبة الالكترونية ومدى تعارضها مع المبادئ الأساسية المتعلقة بحقوق الإنسان إلى ارتفاع عدد الهيئات المكلفة بتنفيذ هذا الإجراء حول العالم، وهو ما يفسر ازدياد عدد حالات المراقبة الالكترونية للحياة الخاصة للأفراد وتعارضها مع المبادئ الأساسية لحقوق الإنسان[1].

كما أشار السيد "فرانك لاراي" في تقريره A/HRC/23/40 باعتباره المكلف الخاص من قبل هيئة الأمم المتحدة بترقية وحماية حرية التعبير إلى ضرورة احترام الإجراءات الشرعية في مجال ممارسة المراقبة الالكترونية للاتصالات من أجل ضمان هذه الحقوق الأساسية بعدما لا حظه من خروقات عديدة في مجال التعسف في اللجوء إلى إجراءات المراقبة الالكترونية إما دون مبرر حقيقي أو دون استيفاء الضمانات القانونية اللازمة[2].

وتعسف الدول في اللجوء إلى إجراء المراقبة الالكترونية للاتصالات عبر الشبكات مرده زيادة وتنامي عدد الهيئات الحكومية والخاصة والتي تمارس إجراءات المراقبة الالكترونية، فقد أحصت منظمة "صحفيون بلا حدود" في تقريرها الذي أعدته في سنة 2014 تحت عنوان "أعداء الانترنت" بمناسبة إحيائها فعاليات اليوم العالمي لمحاربة الرقابة على شبكة الانترنت، ويرتكز نشاطها إما على حذف بعض المعلومات أو حجزها أو تغييرها، وقد صنف هذا التقرير ثلاث هيئات تشكل أكبر تهديد على الحق في الخصوصية وتنتهك حرمة الحياة الخاصة عبر الشبكات.

[1] ربيعي حسين، مرجع سابق، ص 418.

[2] .Macdonald Raegen- liberté sur internet et droit a la vie privée protection des données a caractère personnel et respect des formes l égales – Rapport présenté pour la Conférence des ministres du conseil de l'Europe responsable des medias et de la sécurité de l'information – Belgrade-Serbie- le 7 – 8 Novembre 2013-p 08 disponible sur internet – date de consultation 01 /11/2015. lien directe:
http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/MCM(2013)008_Rapport_MacDonald_fr.pdf.

ومن الأمثلة على الأساليب الحكومية المنتهجة في مجال اللجوء السري للمراقبة الالكترونية ما قامت به الصين سنة 2006 حينما صرح الوزير المكلف بالأمن العام لديها عن إطلاق مشروع تحت اسم "الدرع الذهبي" من خلال تفعيل نظام شامل للمراقبة الالكترونية، وكذلك ما حدث سنة 2009 حينما حاولت الحكومة الصينية فرض تثبيت برنامج تجسس يعرف ب:" السد الأخضر" على كل الحواسيب التي تسوق داخل الصين الأمر الذي يمكنها من بسط سيطرتها على كل أنشطة مستخدمي النظام المعلوماتي في الصين غير أن هذا الطلب قوبل بالرفض من قبل منظمة التجارة العالمية[1].

أما اتفاقية بودابست والتي أبرمت أساسا من أجل مكافحة الإجرام المعلوماتي وخاصة الجرائم الالكترونية الخطيرة ومنها الإرهاب الالكتروني فقد نادت بالمراقبة الالكترونية في المادة 21 تحت عنوان "اعتراض معطيات المحتوى والتي نصت على ما يلي: يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل سلطاته المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي المكنات التالية:

أ. جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.

ب. إلزام مقدم الخدمات، في نطاق قدراته الفنية المتوافرة على:

1. على أن يجمع أو يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه.

2. أن يمنح السلطات المختصة عونه ومساعدته من أجل تجميع أو تسجيل في الوقت العقلي البيانات المتعلقة بمحتوى اتصالات معينة على أرضية منقولة عن طريق نظام معلوماتي..." [2].

وهذا ما أكد عليه المشرع الجزائري بموجب المادة من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما يلي: "مع مراعاة الأحكام القانونية التي نصت على سرية المراسلات والاتصالات، يمكن بمقتضيات حماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقوانين المنصوص عليها في قانون الإجراءات جزائية

[1] ربيعي حسين، مرجع سابق، ص 419.

[2] اتفاقية بودابست للإجرام الالكتروني لسنة 2001.

وفي هذا القانون، وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها..."[1]

وفي هذا الإطار نجد اتفاقية بودابست قد ميزت بين نوعين من المعطيات المعلوماتية محل الاعتراض، إلى معطيات متعلقة بالمرور ومعطيات متعلقة بمحتوى الاتصال.

فبالنسبة للنوع الأول عرفته المادة الأولى بأنه: "كل البيانات التي تعالج الاتصالات التي تمر عن طريق نظام معلوماتي، والتي يتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال مع تعيين المعلومات التالية:

أصل الاتصال، مقصد الاتصال، أو الجهة المقصورة بالاتصال في السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال، نوع الخدمة.

أما بالنسبة للنوع الثاني فهي المعطيات المتعلقة بالمحتوى فلم يأت تعريف بها في الاتفاقية لكنها تشير إلى المحتوى الإخباري للاتصال بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال فما عدا المعطيات المتعلقة بالمرور[2].

وما قيل بشأن اتفاقية بودابست يقال بالنسبة للمشرع الجزائري حيث وأنه بالرجوع إلى القانون رقم 09-04 السابق الذكر، نجده يفرق بين اعتراض المعطيات المتعلقة بالمحتوى وتجميع المعطيات المتعلقة بحركة السير من وجهة نظر مزدوجة للشروط القانونية التي ينبغي بداية أن تكون متوافرة من أجل الإذن تمثل هذا الإجراء والجرائم التي يمكن اللجوء حيالها، فقد أشار بشكل معياري في عناوين هاذين الإجراءين إلى تجميع المعطيات المتعلقة بحركة السير تحت مسمى "حفظ المعطيات المتعلقة بحركة السير" وهذا من خلال المادة الحادية عشر (11) من القانون 09-04 السالف الذكر، وتجميع المعطيات المتعلقة بالمحتوى تحت مسمى "مراقبة الاتصالات الإلكترونية" من خلال نص المادة الرابعة من نفس القانون[3].

[1] قانون رقم 04/09 مؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد 47، الصادرة في 16 غشت 2009، ص6.

[2] رشيدة بوكر، مرجع سابق، ص 368.

[3] نفس المرجع، ص 368.

ولم يتطرق المشرع الجزائري إلى تعريف مراقبة الاتصالات الإلكترونية شأنه في ذلك شأن أغلب التشريعات، واكتفى بتحديد مفهوم الاتصالات الإلكترونية بقوله: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[1].

أما قانون البريد والاتصالات الإلكترونية الفرنسي لسنة 1980 فقد عرف الاتصالات الإلكترونية بقوله "كل انتقال أو إرسال أو استقبال لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي.

الفقه تصدى لتعريف المراقبة الإلكترونية- كما سبق وأشرنا- بقوله هي مراقبة شبكة الاتصالات، كما عرفها بأنها العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية بجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض آخر[2].

ويستنتج من خلال هذين التعريفين أن المراقبة الإلكترونية تعتبر من بين التدابير الماسة بحق الإنسان في سرية مراسلاته واتصالاته الخاصة وما يتفرع عنها من حق سرية مراسلاته الإلكترونية ومن ثم وجب تحديد استخداماتها في إطار استخدامها في نطاق الاتصالات المنطوية على خطورة التهديدات المحتملة بالنظر إلى أهمية المصالح المعنية، وفي هذا الإطار حددها المشرع الجزائري فيما كانت هناك معلومات كافية عن احتمال اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الانتماء الوطني أو للوقاية من الأفعال الموصوفة بجرائم إرهابية أو تخريبية أو الجرائم الماسة بأمن الدولة[3] .

كما أن التقنية المستخدمة في هذه المراقبة الإلكترونية حققت نجاحها الأمر الذي أكدته التجارب في الولايات المتحدة الأمريكية، وهذا لأن هذه المراقبة تقي مجموعة من الأجهزة المتكاملة مع

[1] المادة 2 فقرة "و"من القانون 09-04 السابق الذكر.

[2] رشيدة بوكر، مرجع سابق، ص 370.

[3] المادة الرابعة فقرة أ و ب من قانون 09-04 السابق الذكر.

بعضها بغرض تشغيل مجموعة من البيانات الداخلة وفقا لبرامج موضوع سبقا للحصول على النتائج المطلوبة، وبالتالي فهي رصد مبكر للاعتداءات المحتملة وخاصة الإرهابية[1].

## مشروعية مراقبة الاتصالات الإلكترونية.

إن الحماية الجزائية للاتصالات السلكية واللاسلكية بما فيها التي تمر عبر الوسائل الإلكترونية أصبح أمر حتمي ومؤكد، وإذا كان المشرع قد أباح مراقبة الاتصالات الإلكترونية إذا اقتضت ضرورة الوقاية من الجرائم وأهمها جريمة الإرهاب الإلكتروني محل دراستنا، فإن إحاطة المراقبة ببعض الضمانات القانونية الفعالة يعد أمرا ضروريا لحماية الحرية الفردية ولحماية حق الإنسان في سرية اتصالاته ومن أهم هذه الضمانات[2]:

1/ أي تم تعيين هذا الإجراء وحتى سلطة القضاء وبإذن منه قبله وخلاله وبعده فالجهاز القضائي هو وحده المختص عموما بإصدار هذا الإذن ويعد ذلك ضمانة لازمة لمشروعية الاعتراض على الاتصالات الإلكترونية، وهو الأمر الذي أعد عليه المشرع الجزائري في المادة الرابعة من القانون 09-04 السابق الذكر وذلك في فقرتها الأخيرة بقولها: "...لا يجوز إجراء عملية المراقبة في المادة المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة".

2/ أن تدعو إلى هذا الإجراء حالة الضرورة القصوى في ضابط الوقاية من وقوع بعض الجرائم يعتبر السند الشرعي المبرر للمراقبة ومن قبيل ذلك أن تكون هناك معلومات كافية تنذر باحتمال اعتداء جماعة إرهابية على منظومة معلوماتية على نحو ينشر الرعب والفزع بين الناس، أو بتهديد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو هناك معلومات أكيدة على وقوع اعتداء على أمن الدولة، وفي هذه الحالة يتم الترخيص بالمراقبة الإلكترونية[3].

3/ يراعي استخدام المراقبة الإلكترونية في نطاق ضيق للغاية للوقاية من عدد محدود من الجرائم، وهي التي تمس حقوق ذات أهمية كبيرة، لاعتبارات يقدرها المشرع الأمر الذي نصت عليه

[1] رشيدة بوكر، مرجع سابق، ص 370.

[2] نفس المرجع، ص 374.

[3] المادة 04 من القانون 09-04 السابق الذكر.

صراحة المادة 04 من القانون 09-04، والتي حددت الحالات التي يجوز فيها المراقبة وعلى سبيل الحصر، ومن هذه الحالات الجريمة الإرهابية والتخريبية حسب الفقرة "من المادة الرابعة وذلك بقولها:

"أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة"، وهذا لأن هذه الجرائم الإرهابية تمس أهم المجالات الحيوية المرتبطة ارتباطا وثيقا لكيان الدولة والاقتصاد الوطني وأمن المجتمع وسلامته.

ويعتبر إجراء المراقبة الإلكترونية الذي أقره المشرع الجزائري بموجب القانون 09-04 من أهم جهود المشرع الجزائري في الوقاية من جريمة الإرهاب الإلكتروني ومكافحتها في المجال الإجرائي وهذا نظرا لخطورة هذه الجريمة على سلامة المجتمع وأمنه.

## آليات ووسائل تنفيذ المراقبة الالكترونية.

تعتبر المراقبة الالكترونية وسيلة فعالة في مراقبة نشاط الأفراد المشتبه فيهم في إطار التحريات والتحقيقات القضائية عن الجرائم المعلوماتية وخاصة الإرهابية منها، على الرغم من أنها إجراء يتعارض مع الحق في الخصوصية المعلوماتية، كما أنها إجراء يسمح بالوقاية من الجرائم المعلوماتية التي من شأنها المساس بمجالات الأمن والنظام العام والدفاع الوطني والتي تصنف عادة في خانة الجرائم الإرهابية.

إن اللجوء إلى ها الأسلوب يستوجب من القائمين على تنفيذه الإلمام بالمعرفة الدقيقة بمجال النظم المعلوماتية، والحيل والأساليب الإجرامية لارتكاب الجرائم المعلوماتية بالإضافة إلى معرفة الآليات القانونية لضمان شرعية هذا الإجراء الذي يكتسي طابعا خاصا في العالم الرقمي، وهو ما يدفعنا إلى التساؤل حول طبيعة هذا الإجراء والوسائل والأساليب المستعملة من أجل تنفيذه[1].

ويتم تنفيذ المراقبة الالكترونية من خلال استهداف الاتصالات الالكترونية التي يجريها المشتبه فيه من خلال استعماله لأي وسيلة الكترونية إما في شكل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها تمت عن طريق وسيلة الكترونية.

[1] ربيعي حسين، مرجع سابق، ص 419.

وتنصب إجراءات المراقبة الالكترونية على جملة المعلومات والبيانات المتداولة عبر النظم المعلوماتية، والتي تعرف بالمعطيات المتعلقة بحركة السير، وقد تكون هذه المعطيات والبيانات إما ساكنة أو متحركة ويمكن تعريفها بأنها:" أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصال، توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي تسلكه والوقت وتاريخ وحجم ومدة الاتصال"[1] .

ويتولى عادة ضباط الشرطة الذين ينتمون إلى وحدات مختصة في الوقاية ومكافحة الجرائم المعلوماتية مهام تنفيذ إجراء المراقبة الالكترونية بناء على إذن من وكيل الجمهورية أو قاضي التحقيق، غير أن هذا الإجراء لا يمكن له أن يتم إلا من خلال جهود مزودي الخدمة بالانترنت أو مقدمي الخدمات الذين يمكن تعريفهم بأنهم:" أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات، أو كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال[2] .

ويحق للقائمين بتنفيذ إجراء المراقبة الالكترونية أن يطلبوا من مقدمي الخدمات تزويدهم بالمعلومات المتعلقة بالاتصالات الالكترونية التي يجريها المشتبه فيه إما من خلال :

- **الأمر بالتحفظ المعجل على البيانات** : ويقصد به التحفظ على بيانات معلوماتية مخزنة في حوزة أو تحت سيطرة مزودي الخدمات في انتظار اتخاذ إجراءات قانونية أخرى بشأنها كالتفتيش ويتضح أن الهدف من هذا الإجراء هو الاحتفاظ بالبيانات المعلوماتية المخزنة لدى مزودي الخدمة بالانترنت قبل حذفها من قبلهم بعد انقضاء مدة الحفظ والتي حددها المشرع الجزائري بسنة واحدة حسب نص المادة 11 من القانون 04/09 السالف الذكر.

ويعتبر هذا الإجراء بالنسبة لغالبية الدول سلطة قانونية جديدة مستحدثة كليا، فهو أداة للتنقيب على أثار الجرائم المعلوماتية في إطار مكافحتها أو الوقاية منها نظرا للأسباب التالية[3]:

1. قابلية البيانات المعلوماتية للتلاشي فمن السهل التلاعب بها وتغيير محتواها وبالتالي فقدان عناصر إثبات الجريمة.

[1] المادة 2 الفقرة هـ من القانون 04/09 السالف الذكر

[2] المادة 2 الفقرة د من القانون 04/09 السالف الذكر.

[3] ربيعي حسين، مرجع سابق، ص 421.

2. ارتكاب غالبية الجرائم المعلوماتية بواسطة النظم المعلوماتية أو بواسطة نظم الاتصالات وبالتالي تحديد هوية المرسل والمرسل إليه يساعد في الكشف عن مرتكب الجريمة.
3. استعمال مضمون هذه الاتصالات كدليل إثبات.

- **تقديم بيانات معلوماتية متعلقة بهوية المشترك:** حيث أصبحت غالبية التشريعات تجيز للجهات المختصة في إطار أداء مهامها المتعلقة بالوقاية ومكافحة الجرائم المعلوماتية حق الاطلاع على البيانات الشخصية للمشترك من خلال تقديم طلب لمزودي الخدمات بالانترنت من أجل مدهم بها[1].

ويشير مصطلح المشترك إلى عديد الطوائف منهم الشخص الذي يدفع مقابل الخدمة، والعميل الذي يدفع مسبقا نظير الخدمات والشخص المستفيد من الخدمة مجانا والشخص المخول له استخدام حساب المشترك، وتعتبر من قبيل بيانات المشترك،هويته عنوانه البريدي، رقم هاتفه، بيانات فاتورته أو بياناته الشخصية المدرجة في العقد[2] .

أما المراقبة الالكترونية الواردة على البيانات الالكترونية فهي التي تعرف اعتراض المراسلات الالكترونية وتجميع المراسلات في الوقت الفعلي لمرور البيانات، وهو إجراء يتم عن طريق سلطة مختصة أو عن طريق مزودي الخدمات –كما سبق بيانه– حيث يقصد بها "اعتراض وتجميع البيانات أثناء بثها ولي الحصول عليها في شكل بيانات الكترونية مخزنة[3].

وتعتبر البيانات المستهدفة تلك المتعلقة بالاتصالات في فترة الإنتاج ولحظة نقلها عبر الاتصال وهو ما يفسر مصطلح " الوقت الفعلي " ، وتكون البيانات هنا في شكل غير مادي يتم نقلها في شكل ذبذبات صوتية أو الكترونية، مع العلم أن هذه العملية لا تشوش على تدفق البيانات بحيث تصل

[1] المادتين 10 و11 من القانون 04/09 السالف الذكر، وكذلك نص المادة 43–9 من القانون 719–2000 الخاص بحرية الاتصالات.

[2] هلالي عبد اللاه أحمد، (المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 230،231.

[3] بوعناد فاطمة الزهرة، مكافحة الجريمة إلالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول مركز الدراسات القانونية، الجزائر، 2013، ص 72.

الشخص المرسل إليه، وبدلا من ضبطها ماديا فإنه يتم تسجيلها ونسخها أثناء فترة نقلها والبيانات التي يتم اعتراضها .

وتجدر الإشارة أن بعض الدول تلجأ إلى استصدار قوانين خاصة تبيح لها إجراء المراقبة الالكترونية خارج نطاق الضمانات القانونية التي توفرها القوانين وعلى رأسها الدستور، ففي سنة 2013 صدر في فرنسا قانون تحت اسم "la loi de la programmation militaire"، بحيث تجيز نص المادة 20 منه إمكانية مراقبة الاتصالات الهاتفية وعبر شبكة الانترنت في الوقت الفعلي لمرور البيانات دون إذن أو إشراك لأي قاضي وذلك بهدف البحث عن معلومات استخباراتية تتصل بالأمن القومي بهدف حماية الاقتصاد الوطني والوقاية من الأعمال الإرهابية[1].

وفي الجزائر تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال سنة 2009 وذلك بتاريخ 05 أوت بموجب القانون 09-04 السالف الذكر حيث جاء في نص المادة 13 تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم، وبعد ست سنوات كاملة صدر المرسوم الرئاسي رقم 15- 261 [2] .

وبينت الفقرة الثانية من المادة الرابعة من المرسوم 15-261 مهام الهيئة التي تتمثل في:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

[1] ربيعي حسين، مرجع سابق، ص 421 .

[2] المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53 8 أكتوبر 2015.

– ضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية[1].

– العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[2].

– تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال .

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال .

– المساهمة في تحديث المعايير القانونية في مجال اختصاصها[3].

وتجتمع الهيئة بناءا على استدعاء من رئيسها أو بناءا على طلب احد أعضائها إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه حيث يتم تزويدها بقضاة وضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني كما يمكن لها الاستعانة بأي خبير أو أي شخص يمكن تعيينه في أعمالها شرط التزامهم بالسر المهني وواجب التحفظ وخضوعهم لإجراءات التأهيل .

[1] إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، مقالة منشورة في موقع وكالة الأنباء الجزائرية، الأربعاء 14 ديسمبر 2016، على الرابط: www.aps.dz/sante.science، تاريخ الاطلاع 2018/09/03 على الساعة 19:31.

[2] المادة 14 من القانون رقم 09-04 السالف الذكر.

[3] المواد 2 و 3 من المرسوم الرئاسي رقم 15-261 السالف الذكر.

في إطار الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب والمساس بأمن الدولة تكلف الهيئة بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية تحت سلطة قاض مختص يتم ذلك بوضع وحدة مراقبة واحدة أو أكثر تزود بالوسائل والتجهيزات التقنية الضرورية تتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط من الشرطة القضائية أو أكثر ينتمي إلى الهيئة .

لا يمكن أن يشارك في عملية مراقبة الاتصالات الالكترونية إلا أعضاء الوحدة أو الوحدات التي أوكلت لها السلطة القضائية هذه المهمة كما يتخذ مسئول الوحدة أثناء سير العملية كل التدابير اللازمة بالاتصال مع المسئولين المعنيين في الهيئة من اجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة .

ويتم حفظ المعلومات المستقاة أثناء عملية المراقبة خلال حيازتها من الهيئة بالإضافة لتسجيل الاتصالات الالكترونية التي تكون موضوع مراقبة وتحرر وفق الشروط والأشكال المنصوص عليها قانون خاصة في إطار قانون الإجراءات الجزائية إذ تسلم التسجيلات والمحررات إلى السلطات القضائية ومصالح الشرطة القضائية المختصة حيث تحتفظ دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع، إذ يجب عدم استخدام المعطيات والمعلومات التي تستلمها أو تجمعها الهيئة لأية أغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1] .

وفي إطار ممارستهم لوظائفهم أو بمناسبتها يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعين للهيئة طبقا للتشريعات المعمول بها بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم انه يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الالكترونية .

من جهة أخرى في حال معاينة أفعال يمكن وصفها جزائيا تخطر الهيئة النائب العام المختص للقيام بالمتابعات المحتملة إذ يمكن في هذا الصدد أن تطلب الهيئة مساعدة موظفين مختصين من

[1] آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتروني بالجزائر، مداخلة في الملتقى الدولي حول "الإجرام السيبراني –المفاهيم والتحديات، في الفترة 11–2017/04/12 ، جامعة 08 ماي 1945 قالمة– الجزائر ، ص8.

الوزارات المعنية في مجالات تكنولوجيات الإعلام والاتصال حيث يتم رفع تقارير فصلية عن نشاطات الهيئة من قبل رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية .

في إطار ضمان قيام موظفو الهيئة بمهامهم في أحسن الظروف يستفيد مستخدمو الهيئة من حماية الدولة من التهديدات أو الضغوط أو الاهانات مهما تكن طبيعتها التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم

باستثناء الحالات السابقة لا يمكن أن يتم استيراد أو اقتناء أو حيازة أو استعمال وسائل وتجهيزات تقنية لمراقبة الاتصالات الالكترونية إلا الهيئة أو عند الاقتضاء سلطة ضبط الاتصالات السلكية واللاسلكية أو المؤسسة العمومية المكلفة بشبكات الاتصالات[1].

وتمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني و الأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة الإلكترونية منها 30 بالمائة على مواقع التواصل الاجتماعي[2]، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الالكتروني اغلبها خاصة بتهديدات إرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب الكتروني تمت إحالتهم على القضاء[3].

وقد استطاع الجيش الالكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا كما تمكن من فك شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيسبوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها

[1] آمال بن صويلح، مرجع سابق، ص 9.

[2] الجزائر تبحث تحصين مؤسساتها من هجمات الإرهاب الالكتروني"، جريدة البلاد، على الموقع: www.elbilad.nd/article65620، 2017/01/25 على الساعة 23:11.

[3] آمال بن صويلح، مرجع سابق، ص 9.

معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب اتصالات محلية و دولية[1].

[1] آمال بن صويلح، مرجع سابق، ص 10.

## خلاصة الباب الأول.

لقد بات الفضاء الالكتروني وسيلة مفضلة وفعالة تعمد التنظيمات الإرهابية عل إتباعها والاعتماد عليها بطرق معينة غير مشروعة تمكنها من تحقيق أهدافها وتجنيد اكبر عدد ممكن من الشباب والنساء وحتى الأطفال في صفوفها، فحسب تقديرات وإحصائيات منظمة الأمم المتحدة تعتبر الجرائم الالكترونية عموما من جرائم القرن القادم ذلك لارتفاع نسب ارتكابها و كثرة أعداد مرتكبيها وأهمية وحساسية أهدافها المتمثلة في إلحاق أضرار بالأشخاص والممتلكات والمساس بالأنظمة المعلوماتية والبنى التحتية الحيوية.

فمما سبق يتبين أن جريمة الإرهاب الالكتروني أصبحت فعلا من أخطر الجرائم التي تهد كيان الدول والمجتمعات على السواء، فعلى الرغم من أن جريمة الإرهاب الالكتروني تتم عن طريق استخدام تقنية المعلومات، كما أن الإجراءات المتبعة في التحري بشأنها وكشفها وملاحقة مرتكبيها هي نفسها الإجراءات المتبعة في إثبات الجرائم المعلوماتية عموما، إلا أن ذا الأمر لا يخرج جريمة الإرهاب الالكتروني أبدا عن طبيعتها كونها جريمة إرهابية ترتكب من أجل تحقيق أغراض وأهداف إرهابية، كما أنها ترتكب بهدف القضاء على أمن واستقرار الدول وزعزعة نظامها السياسي، فالفرق بينها وبين جريمة الإرهاب التقليدي هو أن جريمة الإرهاب الالكتروني تتم بطريقة أكثر دقة واحترافية كما أنها تجنب الإرهابيين التكاليف الباهظة والأخطار الكبيرة لأنها جريمة صعبة الاكتشاف والإثبات ولا تعرف حدود معينة شأنها في ذلك شأن جميع الجرائم المعلوماتية.

كما يمكن أن نستخلص من خلال هذا الباب أن جريمة الإرهاب الالكتروني من خلال أركانها القانونية تشترك مع الجريمة المعلوماتية في الركن المادي كون الوسيلة المستخدمة في جريمة الإرهاب الالكتروني وسيلة معلوماتية أو الكترونية .

وتشترك مع الجريمة الإرهابية في الركن المعنوي، أي أن القصد الجنائي لمرتكبيها هو تحقيق أغراض إرهابية وتخريبية .

هذا بالإضافة إلى أن المشرع الجزائري كغيره من معظم مشرعي العالم أدرج جريمة الإرهاب الالكتروني ضمن الجرائم الإرهابية واعتبرها جريمة إرهابية مستحدثة.

# الباب الثاني:

## الآليات الإقليمية والدولية في مكافحة جريمة الإرهاب الالكتروني.

## الباب الثاني:الآليات الإقليمية والدولية في مكافحة جريمة الإرهاب الالكتروني.

تتمثل الآليات الدولية في تلك المساعي والجهود المبذولة من قبل المنظمات الدولية للقضاء على ظاهرة الإرهاب بمختلف أشكالها منها جريمة الإرهاب الالكتروني، فالمجتمع الدولي لم يكن باستطاعته مكافحة هذه الجريمة الخطيرة إلا بعد دراسات ولقاءات متعددة جمعت أعضاء المجتمع الدولي، وبذل جهود كبيرة في هذا المجال، ومنذ أن تأسست هيئة الأمم المتحدة أخذت على عاتقها مهمة الحفاظ على السلم والأمن الدوليين، وقد كان لها الفضل الكبير في دعوة الدول إلى عقد اللقاءات والمؤتمرات لدراسة ظاهرة الإرهاب وإبرام الاتفاقيات بشأن مكافحتها ، والتي على أساسها تم تعديل العديد من تشريعات الدول الوطنية من أجل تجريم الإرهاب، وبالتالي فقد ساهمت بشكل كبير في الوقاية من الإرهاب ومكافحته من خلال الدور الذي لعبته الجمعية العامة ومجلس الأمن في الميدان، هذا دون أن ننسى دور منظمة الشرطة الجنائية الدولية، وهي منظمة دولية متخصصة في ميدان قمع الجريمة بمختلف صورها، فمنذ نشأتها عملت على إيجاد الأساليب الناجحة في ميدان تخصصها، وخاصة أمام هذا التطور التكنولوجي المذهل والذي صاحبه ارتفاع كبير في الجرائم الالكترونية وخاصة جريمة الإرهاب الالكتروني التي تعتبر أكثر فتكا وخطورة بالمجتمعات المختلفة.

إن المنظمات الدولية لوحدها لم تستطع مكافحة الجريمة الإرهابية، بل هناك المنظمات الإقليمية والتي ساهمت بدورها في تفعيل آليات وقائية وردعية لمحاربة ظاهرة الإرهاب كمنظمة الدول الأمريكية والاتحاد الأوروبي، دون أن ننسى الدور العربي في مكافحة ظاهرة الإرهاب بمختلف صورها ومنها الإرهاب الالكتروني كصورة مستحدثة ومعقدة .

ومن أجل كل هذا قسمنا هذا الباب إلى فصلين خصصنا الأول إلى الآليات الإقليمية في مكافحة الإرهاب الالكتروني، وأما الثاني الآليات الدولية في مكافحة الإرهاب الالكتروني

## الفصل الأول: الجهود الإقليمية في مكافحة الإرهاب الالكتروني.

لم تقتصر الجهود الدولية في مكافحة الإرهاب الالكتروني على المنظمات العالمية بل كان للمنظمات الإقليمية أيضا دور في مهم وفعال في مكافحة الإرهاب الالكتروني، فقد كان للاتحاد الأوروبي دور في تكريس قواعد تشريعية وأخرى أمنية وقضائية في مكافحة الإرهاب بشكل عام فلم يغفل حتى عن الإرهاب الالكتروني، كما أبرمت منظمة الدول الأمريكية العديد من الاتفاقيات حاولت من خلالها مسايرة أحكام المنظمات العالمية والقرارات الأممية في مجال مكافحة الجريمة الإرهابية .

وعلى الصعيد العربي كان لجامعة الدول العربية الدور البارز في مكافحة جميع أشكال الإرهاب ومنها جريمة الإرهاب الالكتروني حيث عملت على وضع خطة عملية من خلال المبادرات التي قام بها مجلس وزراء الداخلية العرب والهيئات التابعة له بهدف التقليص من حدة الإرهاب، فقد عملت الجامعة على عقد المؤتمرات والملتقيات التي نتج عنها العديد من التوصيات التي أثرت في العالم بأسره، كالسياسة الوقائية من خطر الإرهاب والتي أخذت بها الولايات المتحدة الأمريكية في سياستها في مكافحة الإرهاب، وكذلك إدراج جميع الفئات في المجتمع لوضع سياسة محكمة في مجال التصدي للجرائم الإرهابية بمختلف أشكالها وأنماطها.

ولم تقتصر جهود المنظمات الإقليمية في مكافحة الإرهاب عند حد إبرام المعاهدات بل كان لها الفضل كذلك في بعض الآليات العملياتية والتنديد بالجرائم الإرهابية وخاصة بعد أحداث 11 سبتمبر 2001 حيث تعرضت الولايات المتحدة الأمريكية لهجمات إرهابية بوسيلة مستحدثة وظهر ما يعرف بالإرهاب الالكتروني.

كما رفضت هذه المنظمة للاضطرابات السياسية والصراعات العسكرية التي تعيشها معظم دول العالم من جراء هذا الخطر الداهم حيث أصبحت الجريمة الإرهابية ترتكب بسهولة بعد الانتشار الواسع لشبكة الانترنت، وبخطورة أقل بالنسبة للإرهابي وفتكا كبير بالنسبة لأثاره التي تلحق بضحاياه وبالتالي كانت الإجراءات المتخذة في النطاق الإقليمي لمواجهة الإرهاب الالكتروني تتماشى مع الإجراءات على النطاق العالمي بل وتكملها .

ومن أجل توضيح هذا الأمر أكثر قسم هذا الفصل إلى مبحثين اثنين، خصص الأول لدور المنظمات الغربية في مكافحة الإرهاب الالكتروني، وأما الثاني فهو مخصص لدور المنظمات العربية في مكافحة الإرهاب الالكتروني.

## المبحث الأول: دور المنظمات الغربية في مكافحة الإرهاب الالكتروني.

بعد أحداث الحادي عشر من سبتمبر من سنة ألفين وواحد تعرضت كل من القارة الأمريكية والقارة الأوربية إلى العديد من الهجمات الإرهابية الشرسة، فكانت دول هاتين القارتين مسرحا لصور مختلفة من الجرائم الإرهابية وخاصة جريمة الإرهاب الالكتروني التي نشرت الفزع والرعب الشديدين وسط المجتمع الأمريكي والأوربي، بسبب الدمار المادي والخسائر في الأرواح، الأمر الذي غير طبيعة الآليات الدولية في مجال مكافحة الإرهاب حيث اعتبر المجتمع الدولي الإرهاب بمثابة العدوان الذي يفتك بالأمن والسلام في العالم ويجب مكافحته بمختلف الوسائل فكان من الضروري على المنظمات الإقليمية اعتماد إجراءات من شأنها التخفيف من آثار هذه الظاهرة لتكون مساندة ومكملة بذلك للأحكام والقرارات الأممية.

كما أن ظهور تنظيمات إرهابية جديدة مستخدمة لوسائل تقنية حديثة في جرائمها الإرهابية ك"داعش" التي ضربت وهددت جميع الأنظمة السياسية في العالم، زاد من مخاوف المجتمع الدولي ودفع بالكثير من الدول التكتل من أجل الالتزام بوضع تدابير من شأنها الحد من زحف الإرهاب ومنع انتشاره حيث أبرمت منظمة الدول الأمريكية اتفاقيات خصت بها مكافحة الاعتداءات التي تصيب الأفراد وجميع أعمال الابتزاز المرتبطة بالإرهاب وجرائمه، بالإضافة إلى وضع آليات خاصة تمنع تمويل الإرهاب، كما كان للاتحاد الأوربي نفس الدور في هذا الشأن، حيث كرست الاتفاقية التي أبرمها الإتحاد الأوربي في مجال مكافحة الإجرام المعلوماتي بما في ذلك جريمة الإرهاب الالكتروني دور كبير في تكريس الآليات الواجب اتخاذها من أجل الحد نمن استغلال الجماعات الإرهابية لشبكة الانترنت كما حدث في أحداث 2001/09/11 في الولايات المتحدة الأمريكية، وبعدها دعوة المجتمع الدولي إلى ضرورة الالتزام باستحداث آليات وقائية تضمنتها اتفاقية 2005 التي ورد فيها تدابير الوقاية من الإرهاب .

ولمزيد من التفصيل قسمنا هذا المبحث إلى مطلبين، مطلب مخصص للدور الأمريكي ومبحث مخصص للدور الأوروبي في مكافحة الإرهاب الإلكتروني.

## المطلب الأول: الدور الأمريكي في مكافحة الإرهاب الإلكتروني.

ومن خلال هذا العنصر سوف نتعرض إلى كل من منظمة الدول الأمريكية، وأيضا دور مجموعة الدول الثمانية في مكافحة الإرهاب الالكتروني .

### الفرع الأول: منظمة الدول الأمريكية.

منظمة الدول الأميركية منظمة إقليمية تضم دول الأمريكيتين الشمالية والجنوبية في إطار الأمم المتحدة، وتسعى إلى خلق نوع من التضامن والتقارب والتعاون بين الدول الأعضاء فيها.

بدأت محاولات تأسيس هيئة تجمع بلدان القارة الأميركية عام 1889، وعقد أول مؤتمر دولي بهذا الشأن بمشاركة 18 من دول القارة ما بين أكتوبر 1889 وأبريل 1890 في العاصمة الأميركية واشنطن بدعوة من الولايات المتحدة الأمريكية.

وتم خلال هذا المؤتمر الاتفاق على تأسيس "الاتحاد الدولي لجمهوريات أميركا للتوزيع الجيد وتوزيع المعلومات التجارية" الذي تحول لاحقا إلى "اتحاد بلدان أميركا."[1]

واستبدل هذا المكتب باسم "اتحاد عموم أميركا التاسع" الذي انعقد في عاصمة كولومبيا "بوغوتا" ودخل الميثاق الأساسي للمنظمة حيز التنفيذ في ديسمبر/كانون الأول 1951، ثم عُدّل في فبراير 1970 واتخذ اسم "الأمانة العامة لمنظمة الدول الأميركية" OAS.

ويبلغ عدد أعضاء منظمة الدول الأميركية 35 عضوا من البلدان المستقلة في أميركا الشمالية والجنوبية، إضافة إلى 69 دولة لديها عضوية "مراقب" بينها الاتحاد الأوروبي، كالتالي[2]:

1. الأرجنتين وانضمت سنة 1948 .
2. بوليفيا وانضمت سنة 1948.
3. البرازيل وانضمت سنة 1948 .
4. تشيلي وانضمت سنة 1948 .
5. كوستاريكا وانضمت سنة 1948[1].

[1] منظمة الدول الأمريكية، منشور في موقع ويكيبيديا: https://ar.wikipedia.org، تاريخ الاطلاع 2018/07/01 على الساعة 16:46.

[2] نفس المرجع

6. جمهورية الدومينيك وانضمت سنة 1948.
7. الإكوادور وانضمت سنة 1948.
8. السلفادور وانضمت سنة 1948.
9. غواتيمالا وانضمت سنة 1948 .
10. هايتي وانضمت سنة 1948 .
11. هندوراس وانضمت سنة 1948.
12. كولومبيا وانضمت سنة 1948.
13. كوبا وانضمت سنة 1948.
14. المكسيك وانضمت سنة 1948.
15. نيكاراغو وانضمت سنة 1948.
16. بنما وانضمت سنة 1948.
17. باراغواي وانضمت سنة 1948.
18. بيرو وانضمت سنة 1948.
19. الأوروغواي وانضمت سنة 1948.
20. فنزويلا وانضمت سنة 1948.
21. الولايات المتحدة الأمريكية 1948.
22. بابادوس وانضمت سنة 1967.
23. ترينيداد وتوباغو وانضمت سنة 1967
24. جامايكا وانضمت سنة 1969.
25. غرينادا وانضمت سنة 1975.
26. سورينام وانضمت سنة 1977.
27. دومينيكا وانضمت سنة 1979[2].
28. سانت لوسيا وانضمت سنة 1979.
29. أنتيغوا وباربودا وانضمت سنة 1981.

[1] منظمة الدول الأمريكية، مرجع سابق.

[2] نفس المرجع

30. سانت فينسنت والغرينادين وانضمت سنة 1981.
31. باهاماس وانضمت سنة 1982.
32. سانت كيتس ونيفيس وانضمت سنة 1984.
33. كندا وانضمت سنة 1990.
34. بليز وانضمت سنة 1991.
35. غيانا وانضمت سنة 1991.

وتعمل المنظمة من خلال عدة هيئات وآليات، في مقدمتها الجمعية العمومية التي تضع السياسات الكبرى في جلساتها السنوية، وتستطيع جميع الدول الأعضاء أن تشارك في هذه الجمعية ولكل منها صوت واحد.

وهناك أيضا مجلس الاجتماع التشاوري لوزراء الخارجية الذي يعالج المشكلات الملحة خاصة تلك المتعلقة بشؤون الدفاع وحفظ السلام في القارة الأميركية.

ويعتبر الممثلون الدبلوماسيون للدول الأعضاء في واشنطن أعضاء في هذا المجلس الذي يشرف على أمانة عامة تعد الخطط من أجل جلسات الجمعية العمومية ولمكاتب المنظمة الإدارية عبر البحار. وينتخب الأمين العام للمنظمة من قبل الجمعية العمومية ومأموريته تدوم خمس سنوات. وتعزز المؤتمرات المتخصصة التعاون بين دول المنظمة.

كما تتوفر منظمة الدول الأميركية أيضا على مجلس دائم يوجد مقر رئاسته في العاصمة الأميركية واشنطن، وهو الهيئة التنفيذية للمنظمة، وتمثل جميع الدول الأعضاء في هذا المجلس.

وانطلاقا من الشعار الرسمي للمنظمة "ديمقراطية من أجل السلام والأمن والتنمية"، تتلخص أهدافها في نشر وترسيخ الديمقراطية بالبلدان الأعضاء، والدفاع عن مبادئ حقوق الإنسان، وتكريس مقاربة أمنية متعددة الجوانب، ودعم التعاون الإقليمي بين بلدان المنظمة[1].

وتنص "معاهدة بوغوتا" على ضرورة حل الخلافات بين البلدان الأعضاء بالطرق السلمية، من خلال الوساطة والتحقيق والمصالحة والمبادرات الحسنة والتحكيم، وفي حال فشل هذه الوسائل يتم

[1] منظمة الدول الأمريكية، مرجع سابق

اللجوء إلى محكمة العدل الدولية بلاهاي، كما ينص ميثاقها على أن أي عدوان ضد أي بلد أميركي يعتبر عدوانا ضد جميع هذه البلدان.

واعتمدت المنظمة عام 2013 اتفاقيتين جديدتين تهدفان إلى حماية الجماعات المستضعفة في الأمريكتين بمن فيها النازحون في المنطقة، وهما "اتفاقية البلدان الأميركية لمكافحة العنصرية والتمييز العنصري"، و"اتفاقية البلدان الأميركية لمكافحة جميع أشكال التمييز العنصري والتعصب"[1].

ومن أهم الأحداث التي مرت على المنظمة أنه في بداية عام 1962 صوتت المنظمة لصالح قرار طرد حكومة كوبا من العضوية، لكن كوبا ظلت عضوا في المنظمة على الرغم من أن حكومتها لا تستطيع أن تشارك في أنشطتها، ثم صوتت المنظمة عام 2009 على عودة كوبا إلى صفوفها.

وفي عام 1965 دفعت الثورة في جمهورية الدومينيكان بالمنظمة إلى تأسيس قوتها العسكرية الأولى والتي شاركت فيها ست دول من أميركا اللاتينية مع الولايات المتحدة. وعملت هذه القوات بالاشتراك مع لجان المنظمة على إعادة النظام في هذه الجمهورية.

وفي عام 1969 عملت منظمة الدول الأميركية على التدخل السريع لوضع نهاية لغزو هندوراس الذي استمر خمسة أيام من قبل قوات السلفادور.

وركزت المنظمة خلال سبعينيات القرن العشرين بشكل أساسي على موضوع حقوق الإنسان في الدول الأعضاء، واستفسرت لجنة حقوق الإنسان التابعة للمنظمة عن أعمال الإبعاد السياسي، وأجرت تحقيقات في مجال انتهاكات حقوق الإنسان بعدة بلدان أعضاء، كما نشرت اللجنة تقاريرا عن الاحتيال في الانتخابات، والاعتقال غير القانوني، والتعذيب، والأعمال الوحشية الأخرى.

اتهمت المنظمة بتراجع نفوذها خلال ثمانينيات القرن العشرين بسبب ما وُصف بالتدخل المتزايد من وكالات دولية أخرى في شؤون دول أميركا الجنوبية، من بينها صندوق النقد الدولي والبنك الدولي[2].

ونظرا للدور الذي تلعبه هذه المنظمة في تأمين ذاتي جماعي على القارة الأمريكية وبعث سياسة التعاون الإقليمي، وحل النزعات الدولية بالطرق السلمية والحد من فعالية الأسلحة وإبرام اتفاقيات إقليمية في مجال مكافحة الإرهاب، اتخذتها مرجع قانوني لها، وقامت بتعديل تشريعاتها على أساس

[1] منظمة الدول الأمريكية، مقالة منشورة في موسوعة الجزيرة فضاء من المعرفة الرقمية، متوفرة في الموقع: http://www.aljazeera.net.تاريخ الاطلاع 2018/07/22 على الساعة: 23:26 .

[2] نفس المرجع.

تطور الجريمة الإرهابية، فهي تسعى إلى مكافحة هذه الجريمة مهما كانت صورتها أو الوسيلة المرتكبة بواسطتها.

كان دور منظمة الدول الأمريكية معتمدا على قرارات وأحكام منظمة الأمم المتحدة في مجال مكافحة الإرهاب، فقد قامت باعتماد الآليات المنبثقة عن المؤتمرات الدولية، وعن توصيات الجمعية العامة وقرارات مجلس الأمن في هذا الشأن، حيث كان لها في مكافحة جريمة الإرهاب اتفاقية لمحاربة الاعتداءات ضد الأفراد، وهي مستمدة من اتفاقية "جنيف" لسنة 1937، والمتعلقة بمكافحة الجرائم ضد الأشخاص المتمتعين بالحماية الدولية واتفاقيات الأمم المتحدة لمحاربة الاعتداءات الإرهابية ضد الأفراد لسنة 1977.

كما أخذت منظمة الدول الأمريكية على عاتقها وضع إجراءات لمحاربة تمويل الإرهاب الذي تعتبره الركيزة الأساسية في مكافحة الإرهاب في الوقت الراهن وخاصة الإرهاب الالكتروني فتمويله يتم بالوسائل والشبكات، وهذا تماشيا مع قرار مجلس الأمن رقم 1373 لسنة 2001 السالف الذكر[1] والذي جاء بعد اعتداءات 11 سبتمبر 2001 على الولايات المتحدة الأمريكية، وظهور نوع جديد من الإرهاب عرف بالإرهاب الالكتروني.

## أولا: جهود المنظمة في مكافحة الإرهاب قبل أحداث 11 سبتمبر 2001 .

كانت منظمة الدول الأمريكية سباقة في مجال إبرام الاتفاقيات الإقليمية، حيث تم إعداد مشروع اتفاقية لمحاربة الاعتداءات الإرهابية الموجهة ضد الأشخاص سنة 1971، التي دخلت حيز التنفيذ سنة 1973، وقد أطلق عليها اتفاقية واشنطن، وأعقبتها اتفاقية أخرى في نيويورك سنة 1979، إضافة إلى ذلك الاتفاقيات الثنائية التي كانت تعتمد عليها هذه الدول خاصة الولايات المتحدة الأمريكية التي كانت على رأس هذه المنظمة الإقليمية كاتفاقية مكافحة الإرهاب مع السودان سنة 2000، بالإضافة إلى مشاركة الدول الأعضاء في المنظمة في العديد من المؤتمرات وصادقت على جميع المواثيق الدولية المتعلقة بمكافحة الجريمة الإرهابية[2].

[1] ساعد الهام حورية، مرجع سابق، ص 93.

[2] نفس المرجع، ص 94.

## 01- اتفاقية واشنطن لمنع وقمع الإرهاب ضد الأشخاص وجميع أعمال الابتزاز المرتبطة به لسنة 1971.

قامت منظمة الدول الأمريكية بتكليف اللجنة القانونية على مستوى الجمعية العامة بتاريخ 02 فيفري سنة 1971 بإعداد اتفاقية لحماية أعضاء البعثات الدبلوماسية من الاعتداءات الإرهابية ، وقد تمت الموافقة على هذه الاتفاقية ودخلت حيز التنفيذ سنة 1973 وسميت باتفاقية "منع وقمع الأعمال الإرهابية ضد الأشخاص وكذلك أعمال الابتزاز المرتبطة بها ذات الأهمية الدولية"[1].

وتعتبر هذه الاتفاقية الأولى من نوعها التي تناولت وسائل مكافحة الجرائم الإرهابية ضد الأشخاص المكفولين بالحماية الدولية، في الفترة التي ارتفع فيها معدل جرائم الخطف واحتجاز الدبلوماسيين، وتحتوي على ديباجة وثلاثة عشر مادة، وجاءت جميعها تدين الأفعال الإرهابية خاصة خطف الأشخاص المشمولين بالحماية الدولية والسلب المرتبطة بهذه الجرائم.

ولم تعرف هذه الاتفاقية جريمة الإرهاب، بل اكتفت فقط بتحديد الجرائم محل المتابعة الجزائية من خلال نص المادة الثانية منها، حيث يتعلق الأمر بالقتل والخطف والاعتداءات الأخرى الموجهة ضد حياة وسلامة الأشخاص ذوي الحماية الدولية، وأفعال الابتزاز المرتبطة بها، حيث يتعين على الدول الأعضاء في منظمة الدول الأمريكية اتخاذ جميع التدابير التي من شأنها حماية هذه الفئة من الأشخاص في حال تعرضهم للجرائم المنصوص عليها في هذه الاتفاقية.

ولم يرد تعريف الإرهاب في التشريعات الإقليمية المبرمة على مستوى منظمة الدول الأمريكية لهذا السبب قام مجلس المنظمة بإعداد دراسة تفسيرية للاتفاقية تعرض فيها لمسالة التعريف، واعتبر الفعل الإرهابي الذي ارتكب بهذه الصفة في تشريعات الدولة التي وقع فيها الفعل أو التي يتواجد فيها المتهم، أو تلك التي تختص بمحاكمته، وفي غير هذه الأحوال فانه يقصد بالإرهاب كل فعل ينتج عنه رعب أو فزع بين سكان الدولة أو قطاع منهم، وبالتالي هذا التحديد يمنح الاختصاص للتشريعات الوطنية لتحديد الفعل الإرهابي.

[1] سامي حامد عياد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية، 2008 ص 363.

فإذا تمكنت هذه التشريعات من تحديد الفعل الإرهابي كان لها ذلك، بينما إن لم تستطع فتأخذ بعامل الرعب والفزع في تحديد إذا ما كان الفعل يندرج ضمن سياق الإرهاب أولا بالإضافة أن الاتفاقية ذكرت بعض الأفعال التي اعتبرت مجالا للعنف والرعب[1] .

وتضيف أحكام المادة الثامنة من الاتفاقية على حتمية الدول الأعضاء اعتماد ما يلزم من إجراءات لمنع التحضير لهذه الجرائم فوق أراضيها وحماية هؤلاء الأشخاص من جميع الاعتداءات ذات الطابع الدولي[2].

وتجدر الإشارة أن الاتفاقية سالفة الذكر لم تتعرض إلى الجرائم الإرهابية التي تمس الأموال بالإضافة إلى ذكر الخطف وليس اخذ الرهائن للتمييز الموجود بينهما في المجال الفقهي والقضائي لكن الأمر يتعلق بحماية الأشخاص الدبلوماسيين، فلا يتصور خطف الدبلوماسي بعيدا عن الاحتجاز من أجل الابتزاز كطلب الفدية، وخاصة أن مضمون الاتفاقية اشترط بأن يكون الخطف ذو صفة دولية.

وعموما فان الاتفاقية في مجملها تخص الأشخاص الذين تتولى الدولة حمايتهم طبقا لأحكام القانون الدولي، والجدير بالذكر أن هذه الحماية لا تمتد إلى عائلة الدبلوماسيين.

وحسب نص اتفاقية واشنطن فان الدولة تلتزم بمحاكمة المتورطين في الجرائم الإرهابية في حال رفضت تسليمهم للدولة الطالبة، وحينها تلتزم الدولة التي رفضت طلب التسليم تطبيق اختصاصها القضائي طبقا لنص المادة الخامسة من الاتفاقية، والتي تتضمن على ضرورة تأسيس الدول الأعضاء اختصاصها القضائي في مجال الجرائم المشمولة بهذه الاتفاقية في حال رفضها التسليم، وهذا كله إعمالا للمبدأ القاضي بعدم إفلات المجرم من العقاب، مع إبلاغ الدولة طالبة التسليم بهذا الإجراء[3].

### 02- اتفاقية مناهضة اخذ الرهائن في نيويورك.

جمعت هذه الاتفاقية الدول الأعضاء في منظمة الدول الأمريكية في نيويورك سنة 1979، ومن خلالها اعترفت جميع دول المنظمة أن مسألة اخذ الرهائن جريمة دولية تشكل خطرا على المجتمع الدولي، وهذا نظرا لخطورتها ومساسها بالحقوق والحريات الفردية المكرسة في المواثيق الدولية، وأهمها

[1] ساعد الهام حورية ، مرجع سابق، ص 95.

[2] إمام حسانين عط الله، الإرهاب- البنيان القانوني للجريمة، دار المطبوعات الجامعية، الإسكندرية، 2004، ص 768.

[3] ساعد الهام حورية ، مرجع سابق، ص 95.

ميثاق الأمم المتحدة كالحق في الحياة، والسلامة الجسدية، حيث تندد الدول الأعضاء في منظمة الدول الأمريكية بشدة ضد اختطاف الأشخاص أو ما يعرف في القوانين الدولية باختطاف الرهائن، فقد ورد في نص المادة الأولى من اتفاقية أخذ الرهائن لسنة 1979 عبارة " يطلق عليها رهينة" أي أن الشخص المخطوف حسب هذه الاتفاقية تلحق به تسمية رهينة[1].

وقد عرفت المادة الأولى من اتفاقية نيويورك عملية الاختطاف بقولها:" أنه قبض الشخص على شخص آخر يطلق عليه رهينة، أو يحتجزه، أو يهدد بقتله أو إيذائه، أو استمرار احتجازه، من أجل إكراه طرف ثالث، سواء كانت دولة أو منظمة دولية أو حكومية، أو شخصا طبيعيا، أو اعتباريا أو مجموعة من الأشخاص على القيام أو الامتناع عن القيام بعمل معين كشرط صريح أو ضمني للإفراج عن الرهينة، ليس هذا وحسب بل إن المادة السابقة جرمت في فقرتها الثانية الشروع وجميع أعمال المساهمة في ارتكاب الأفعال المنصوص عليها في الفقرة الأولى من نفس المادة[2].

بالإضافة إلى أن تطبيق أحكام هذه الاتفاقية لا يتوقف على الأفراد فقط بل يمتد إلى الدولة، إذا كانت طرف في الجريمة فبموجب نص المادة الثانية فان هذه الدولة الخاطفة تتعرض إلى عقوبات حسب طبيعة وخطورة الأفعال المرتكبة، حيث تنص:" تعتبر كل دولة طرف الجرائم المنصوص عليها في المادة الأولى، جرائم يعاقب عليها بعقوبات مناسبة تأخذ بعين الاعتبار الطبيعة الخطرة لهذه الجرائم"[3].

والواضح من نصوص هذه الاتفاقية أنها تسري على وقت السلم فقط، فلا تسري أحكامها إذا ارتكبت أثناء النزاعات المسلحة المنصوص عليها في اتفاقية جنيف لسنة 1949 والبروتوكولات المكملة لها خاصة البروتوكول الإضافي الأول لسنة 1977 المتعلق بحق الشعوب في تحقيق مصيرها، والتحرر من السيطرة الاستعمارية، ونظم الحكم الاستبدادية حيث تعترف ضمن أحكام المادة 12 منها بحق الشعوب في تقرير مصيرها طبقا لأحكام ميثاق الأمم المتحدة والمواثيق الدولية[4].

كما وجب أن نشير إلى أن أحكام اتفاقية نيويورك الخاصة بأخذ الرهائن لا تسري إلا على جرائم الاختطاف التي ترتكب في نطاق الإرهاب الدولي، فلا يمكن تطبيق أحكامها على الجرائم المرتكبة

[1] ساعد الهام حورية ، مرجع سابق، ص 96.

[2] اتفاقية مناهضة أخذ الرهائن الموقعة في 1979/12/18 في نيويورك.

[3] نص المادة الثانية من نفس الاتفاقية سالفة الذكر.

[4] ساعد الهام حورية ، مرجع سابق، ص 97.

داخل إقليم الدولة من طرف شخص من نفس الجنسية، وكانت الرهينة أيضا من نفس الجنسية، ففي هذه الحالة يكون القانون الواجب التطبيق، أو الأولى بالتطبيق هو قانون دولة الشخص( أي قانونها الوطني).

وعليه مما سبق، فانه وحتى تطبق الدولة قانونها الداخلي على الخاطف إذا كان جنسيته من جنسية الدولة وهي نفسها جنسية المخطوف وجب عليها أن تسعى وتعدل تشريعها الداخلي بما يتماشى وهذه الحالة.

كما أن اتفاقية نيويورك لسنة 1979 والتي أبرمتها منظمة الدول الأمريكية من اجل مناهضة أخذ الرهائن تدعو إلى تكريس مبدأ التعاون القضائي فيما يخص التسليم والمساعدات القضائية المتبادلة وأن مرتكب الفعل وجب أن يقدم للمحاكمة على الفعل بوصفه جريمة من جرائم الإرهاب الدولي، مع ضرورة الأخذ بسياسة التعاون الدولي الأمني بين السلطات المختصة بإنفاذ القانون للحد من جرائم اختطاف الأشخاص واستعمالهم كرهائن، للضغط على الدول والمنظمات الدولية مهما كانت طبيعتها بهدف تحقيق أغراضهم الدنيئة[1].

## ثانيا: جهود منظمة الدول الأمريكية لمكافحة الإرهاب بعد أحداث 11 سبتمبر 2001.

في الاجتماع الاستثنائي الذي عقدته لجنة مكافحة الإرهاب في نيويورك، في 6 آذار 2003 تعهّدت المنظّمات الإقليمية في جميع المناطق، وخصوصًا منظّمة الدول الأميركية تقاسم خبراتها في إطار التعاون الإقليمي لمكافحة الأنشطة الإرهابية.

كما سلمت بأنها تضطلع بدورٍ فريد لمساعدة أعضائها على تنفيذ القرار 1373 وبالتالي إذكاء الوعي في مكافحة الإرهاب على الصعيدين الإقليمي والقطري، وذلك بالتعاون مع منظّمة الطيران المدني الدولي، والمنظّمة الدولية للشرطة الجنائية (الانتربول)، والمنظّمة البحرية الدولية، ومفوّض الأمم المتحدة السامي لشؤون اللاجئين، ومنظّمة الجمارك العالمية.

وفي أثناء الاجتماع الخاص للجنة مكافحة الإرهاب ومنظّمة الدول الأميركية/لجنة البلدان الأميركية لمناهضة الإرهاب الذي عقد في واشنطن، في 7 تشرين الأول 2003 التزمت الدول الأعضاء التعاون الإقليمي، سواء بمعناه السياسي والتضامني أم على المستوى التنفيذي.

[1] ساعد الهام حورية ، مرجع سابق، ص 97.

وفي سياق مكافحة تمويل الجماعات الإرهابية داخل أميركا وخارجها، تعهّدت الولايات المتحدة تقديم الدعم الفني لدول المنظّمة الأميركية، ومراقبة أنشطة المنظّمات الإرهابية المالية داخل أميركا وخارجها، وتجميد أرصدتها وأصولها الثابتة.

كما قرّرت المنظّمة التعاون الدولي لمكافحة تمويل الإرهاب، وتمت صياغة تسع توصيات خاصة بتمويل الإرهاب، أُضيفت إلى التوصيات الـ40 الموجودة حاليًا لمكافحة غسل الأموال، وذلك في إطار مجموعة العمل المالي الدولية (GAFI) وفريق العمل للشؤون المالية (FATF)[1].

وقد أبرمت منظمة الدول الأمريكية اتفاقية إقليمية لتجريم ورفض جميع وسائل الدعم المادي والمعنوي للتنظيمات الإرهابية وهي اتفاقية منع تمويل الإرهاب من أجل منع الإرهاب والتصدي له وقمعه، وقد دخلت حيز التنفيذ سنة 2009 ، وتضمنت هذه الاتفاقية النص على أن جرائم الإرهاب تمثل تهديدا للسلم والأمن الدوليين[2] مهما كان شكلها أو وسيلة ارتكابها.

وقد حاولت الدول أعضاء منظمة الدول الأمريكية مسايرة ميثاق الأمم المتحدة خاصة أحكام القرار RES01/10revocorr1/023 الذي تضمن "تقوية التعاون في نصف الكرة الأرضية من أجل منع ومحاربة الإرهاب والقضاء عليه"، جاء فيها تبني الإجراءات المنصوص عليها في الاتفاقية الدولية لمنع الإرهاب لسنة 1999[3].

### أولا: نطاق تطبيق الاتفاقية.

لما اجتمعت الدول الأعضاء في منظمة الدول الأمريكية في نيويورك عمدت إلى تحديد الجرائم موضوع الملاحقة الجزائية على أحكام ومبادئ المواثيق الدولية التي أبرمت في هذا المجال تضمنتها المادة الثانية على سبيل الحصر، ويتعلق الأمر باتفاقية مكافحة الاستيلاء غير المشروع على الطائرات المبرمة بلاهاي في 16 ديسمبر 1970، واتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني في مونتـريـال في 23 سبتمبر 1971 واتفاقية منع الجرائم المرتكبة ضد الأشخاص المتمتعين بالحماية الدبلوماسية في نيويورك سنة 1973، بالإضافة إلى اتفاقية الحماية المادية للمواد النووية التي تم التوقيع عليها في فيينا في 03 مارس 1980، وبروتوكول قمع أعمال

[1] إلياس أبو جودة، الإرهاب والجهود الدولية والإقليمية في مكافحته، مجلة منشورات الجيش اللبناني، العدد 91، 15 كانون الثاني 2015، بيروت– لبنان، ص 09.

[2] محمد سيد عرفة، تجفيف مصادر تمويل الإرهاب، أكاديمية نايف للعلوم الأمنية، الرياض، 2009، ص 156.

[3] ساعد الهام حورية ، مرجع سابق، ص 98.

العنف غير المشروع في المطارات التي تخدم الطيران المدني الدولي، الملحق باتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة الطيران المدني التي تم التوقيع عليها في مونتريـــال في 24 فيفري 1988.

كما اعتمدت الجرائم الواردة ضمن اتفاقية قمع الأعمال غير المشروعة الموجهة ضد سلامة المنشآت الثابتة الموجودة على الجرف القاري، والذي تم إقراره في روما في 10 مارس 1988، وتلك المنصوص عليها في الاتفاقية الدولية لقمع الهجمات الإرهابية بالقنابل التي أقرتها الجمعية العامة للأمم المتحدة سنة 1977، والاتفاقية الدولية لمنع تمويل الإرهاب لسنة 1999 .

ومما سبق يتضح أن منظمة الدول الأمريكية تسعى إلى مكافحة جميع أشكال وصور الجرائم الإرهابية، ومهما كانت وسيلة ارتكابها، لأنه مهما اختلفت هذه الوسيلة يبقى الهدف والغاية من الجرائم الإرهابية واحدة لا تتغير.

## ثانيا: الإجراءات الواجب اتخاذها في مجال منع تمويل الإرهاب.

في سبيل منع تمويل الإرهاب ومهما كان شكله وصورته أو وسيلة ارتكابه دعت الدول الأعضاء في منظمة الدول الأمريكية من خلال اتفاقية منع تمويل الإرهاب لسنة 2009 إلى اتخاذ جملة من التدابير اللازمة لمنع تمويل الإرهاب، حيث دعت الدول الأعضاء إلى اتخاذ تشريعات وطنية تتماشى وأحكام هذه الاتفاقية، وذلك بإقامة خطة وطنية شاملة للإشراف على البنوك والمؤسسات المالية الأخرى وسائر الكيانات التي يشتبه أنها تقوم بتمويل الأنشطة الإرهابية، من حيث وجوب التعرف على العملاء، وحفظ السجلات وتقديم التقارير على أية تحويلات مالية مشتبه فيها أو غير مألوفة بالإضافة إلى مراقبة حركة انتقال الأموال أو حركة الشيكات والحوالات وسائر أشكال انتقال القيم المادية، مع وضع ضمانات لحماية قانونية على هذه الإجراءات لضمان استخدام هذه المعلومات بشكل قانوني صحيح حتى لا تكون عائقا أمام حركة انتقال رؤوس الأموال بشكل مشروع، ومنح القدرة لأجهزة تطبيق القانون بالقدر الذي يسمح لها ممارسة المهام المنوطة بها، وعلى تبادل المعلومات دوليا ووطنيا، طبقا للشروط المنصوص عليها في قوانينها الداخلية[1].

وفي هذا الإطار يجب على هذه الدول إنشاء وحدة للاستخبارات المالية تعمل كمركز وطني لجمع وتحليل ونشر المعلومات المتعلقة بغسيل الأموال وتمويل الإرهاب.

[1] ساعد الهام حورية ، مرجع سابق، ص 99.

في المجال نفسه تقوم كل دولة بإبلاغ السكرتير العام للمنظمة بالإجراءات المتخذة وعلى حجز ومصادرة الودائع أو الموارد التي تم بها تمويل الجماعات الإرهابية بالإضافة إلى تضمين التشريعات الوطنية جريمة تبييض الأموال.

بالإضافة على ذلك وضع حزام أمني عبر الحدود لمراقبة حركة تنقل الإرهابيين ومنع الاتجار بالأسلحة وقمع عمليات تزوير وثائق السفر والهوية مع احترام حرية الأشخاص وتسهيل التجارة وربطت بين إجراءات منع تمويل الإرهاب وغسيل الأموال للعلاقة الوطيدة بين الجريمتين[1].

**ثالثا: الدعوة لتكريس مبدأ التعاون الدولي والتشاور بين الدول الأعضاء.**

دعت هذه الاتفاقية الدول الأعضاء إلى تجسيد مبدأ التعاون الدولي في المجال الأمني والقضائي وعدم رفض التسليم بحجة الطابع السياسي للجريمة، كما تضمنت المادة 12 رفض منح حق اللجوء السياسي أو إضفاء صفة لاجئ للإرهابيين مع منع التمييز العنصري ووجوب احترام الحقوق الأساسية لكل دولة طرف في الاتفاقية.

بالإضافة إلى تطوير وسائل التدريب ووسائل التعاون التقني بين الدول الأطراف بموجب أحكام المادة 16 على المستويات القومية والثنائية والإقليمية وشبه الإقليمية، وكذلك وفي إطار منظمة الدول الأمريكية، بالإضافة إلى تطوير برامج مناسبة للتعاون التقني والتدريبي مع المنظمات الدولية والإقليمية الأخرى التي تطبق إجراءات تتماشى مع أهداف هذه الاتفاقية.

وقد شهد نموذج التعاون الذي تمثّله مجموعة العمل GAFI توسعًا متناميًا في السنوات الأخيرة ليشمل منظمات إقليمية شبيهة، وذلك أيضًا بهدف ضمان التطبيق العالمي للمعايير التي صاغتها ولإحداث تناغم بين التشريعات الوطنية المختلفة في هذا الاتجاه.

وقد أنشئ أخيرًا العديد من المراكز الإقليمية في أميركا للتدريب والتكوين وتبادل الخبرات، بهدف تعزيز أواصر التضامن في مكافحة الإرهاب[2].

في نفس السياق تنص المادة 17 على تشجيع الدول الأطراف التعاون الواسع بين الجهات المعنية بمكافحة الإرهاب داخل منظمة الدول الأمريكية مثل لجنة مكافحة الإرهاب[3].

---

[1] ساعد الهام حورية ، مرجع سابق، ص 100.

[2] إلياس أبو جودة، مرجع سابق، ص 09.

[3] تنص المادة 17 من اتفاقية منظمة الدول الأمريكية لمنع تمويل الإرهاب:" التعاون عبر منظمة الدول الأمريكية.

كما تقوم الدول الأطراف بعقد اجتماعات دورية للتشاور فيما بينها بموجب المادة 18 من الاتفاقية سالفة الذكر والتي تنص على أنه:" التشاور بين الدول الأطراف.

1. تقوم الدول الأطراف بعقد اجتماعات دورية للتشاور فيما بينها وبغرض تسهيل ما يلي:
أ- التطبيق الكامل لهذه الاتفاقية ، والأخذ في الاعتبار القضايا الهامة التي تقررها الدول الأطراف .

ب – تتبادل الدول الأطراف المعلومات والخبرات فيما بينها بشأن الوسائل والطرق الفعالة لمنع وتعقب ، والتحري عن الإرهاب ومعاقبة مرتكبيه.

2. يدعو السكرتير العام لعقد اجتماع للتشاور للدول الأطراف بعد تسلمه الوثيقة العاشرة للتصديق وبدون الاتكاء على هذا ، تقوم الدول الأطراف بعقد اجتماعات تشاورية إذا كان هناك ضرورة لذلك.

3. يجب أن تطلب الدول الأطراف من الجهات المعنية بمكافحة الإرهاب داخل منظمة الدول الأمريكية تسهيل عملية التشاور المشار إليها في الفقرات السابقة وان تمدها بالوسائل المساعدة الأخرى التي تتعلق بتنفيذ هذه الاتفاقية.

ومن خلال هذه المادة يتضح أن الدول الأعضاء تجتمع للتشاور في القضايا والأحداث المهمة ومن خلال ذلك تتبادل الدول المعلومات والخبرات فيما بينها بشان الوسائل والطرق الفعالة لمنع والتعقب والتحري عن الإرهاب وتعقبه مهما كانت وسيلته وخاصة لو كانت شبكة الانترنت، ومعاقبة مرتكبيه.

إن اتفاقية منظمة الدول الأمريكية لمنع تمويل الإرهاب لسنة 2009 وان كانت تهدف إلى تجفيف جميع مصادر تغذية الإرهاب ماديا إلا أنها تدعو إلى حصر الفعل الإرهابي في مجموعة الاتفاقيات التي أبرمت بشأنه، فمن الصعوبة بما كان حصر السلوك الإرهابي في إطار جرائم الإرهاب، وهذا لأن التطور الذي يشهده العالم بأسره في الوقت الراهن جعل من جريمة الإرهاب الالكتروني من أخطر الجرائم الإرهابية وهذا نظرا لسهولة ارتكابها وصعوبة ملاحقة مرتكبيها ومعاقبتهم وخطورتها على العالم بأسره.

---

= تشجع الدول الأطراف التعاون الواسع بين الجهات المعنية بمكافحة الإرهاب داخل منظمة الدول الأمريكية مثل لجنة مكافحة الإرهاب فيما بين الدول الأمريكية ، وفي أمور تتعلق بأهداف وغايات هذه الاتفاقية".

## الفرع الثاني: دور مجموعة الدول الثماني (G 8) في مكافحة الإرهاب الالكتروني .

قبل أن نتعرض إلى جهود منظمة الدول الثماني في مجال مكافحة كل أنواع الإرهاب ومنها جريمة الإرهاب الالكتروني وجب أولا أن نوجز لمحة على تأسيس المنظمة ونشأتها .

### أولا: نشأة المنظمة[1].

ظهرت مجموعة الدول الثماني أو نادي الكبار للوجود سنة 1976، وكانت في بداية الأمر تضم سبعة دول فقط وهي: الولايات المتحدة الأمريكية- ألمانيا- كندا- ايطاليا- اليابان- فرنسا- بريطانيا وبعد ذلك انضمت روسيا كعضو ثامن بمناسبة انعقاد قمة "برمنجهام" سنة 1998.

فبعد الأزمة النفطية في عام 1973 وفترة الركود الاقتصادية التي تبعتها ظهر مفهوم تجمع للدول الأكثر تصنيعاً، وفي عام 1974 أنشأت الولايات المتحدة المجموعة في تجمع غير رسمي للمسؤولين الاقتصاديين من الولايات المتحدة الأمريكية والمملكة المتحدة، وألمانيا الغربية واليابان، وفرنسا[2].

أما في سنة 1975 ، دعا الرئيس الفرنسي " فاليري جيسكار ديستان" زعماء حكومات ألمانيا الغربية، وإيطاليا، واليابان، والمملكة المتحدة، والولايات المتحدة الأمريكية إلى قمة في" رامبوليت" أين أتفق الزعماء الستة على تنظيم اجتماع سنوي تحت رئاسة متناوبة، مشكلين بذلك مجموعة الستة .

وفي السنة التالية انضمت كندا إلى المجموعة بناء على توصية الرئيس الأمريكي" جيرالد فورد" وأصبحت تعرف بمجموعة السبعة، ويمثل الاتحاد الأوربي من قبل رئيس الاتحاد الأوربي وزعيم الدولة التي تتولى رئاسة مجلس الاتحاد الأوربي وحضر كل الاجتماعات منذ أن تمت دعوته من قبل المملكة المتحدة في عام 1977.

بعد انتهاء الحرب الباردة بتفكك الاتحاد السوفيتي سنة 1991 ،أصبحت روسيا الدولة الوريثة الشرعية لهذا الاتحاد، وبداية بقمة نابولي عام1994 ، دعي المسئولون الروس لحضور هذا التجمع بصفة مراقب مع زعماء مجموعة السبعة بعد انتهاء القمة الرئيسية عرفت هذه المجموعة بمجموعة السبعة زائد واحد، وبمبادرة رئيس الولايات المتحدة" بيل كلينتون" انضمت روسيا بشكل رسمي

[1] مجموعة الثماني G8، منشورة في موقع ويكيبيديا: https://ar.wikipedia.org/wiki، تاريخ الاطلاع 2018/07/03 على الساعة 19:18.

[2] نفس المرجع.

إلى المجموعة في عام1997 ، وأصبحت تدعى بمجموعة الثمانية (G8)[1] ، وتشكل المجموعة منتدى للحوار والاستشارة المتبادلة بين الدول الأكثر تصنيعا في العالم.

وفي أول الأمر أنشئت هذه المنظمة من أجل التعاون المتبادل بينها في المجالات السياسية والاقتصادية، بل تعدتها إلى التحديات الإستراتيجية والقانونية ومكافحة الإرهاب وقضايا الصحة والبيئة والانتشار النووي والتنمية المستدامة.

ويجتمع قادة منظمة مجموعة الثماني مرة كل سنة للتباحث في القضايا ذات الطابع الاقتصادي والأمني للدول الثمانية الأكثر تصنيعا وقوة اقتصادية في العالم، ويتخذون إجراءات هامة في هذا المجال[2] .

ونظرا للطابع غير الرسمي لهذه المجموعة مكنها من تطوير مجالات التعاون بصورة فعالة ومكيفة فيما بينها، ولتطبيق التزامات المجموعة المتخذة من قبل قادتها تجرى اجتماعات تقنية حول المسائل المعالجة، واجتماعات وزارية تضم وزراء العدل والداخلية والخارجية والمالية والبيئة[3].

## ثانيا: جهود المجموعة في مكافحة الإرهاب الالكتروني .

تناولت مجموعة الثماني على نحو منظّم الموضوعات الرئيسة المتعلّقة بالإرهاب على المستوى السياسي وبكل أنواعه، وخصوصًا في القمم الأخيرة (جان- إيطاليا 2001، كاناناسكيس- كندا 2002 أيفيان- فرنسا 2003، سي أيلاند- الولايات المتحدة 2004، غلين إغلز- بريطانيا 2005، سان بطرسبرغ -روسيا 2006، هيليغيندام- ألمانيا 2007، هوكايدو- اليابان 2008، أكيلا -إيطاليا 2009، ماسكوكا- كندا 2010)[4].

وتم التركيز على معالجة الأسباب التي تؤدي إلى استمرار ظاهرة الإرهاب، منها انتشار أسلحة الدمار الشامل، والمشاكل الاجتماعية، والنزاعات الداخلية في الشرق الأوسط وأفريقيا.

وتم وضع برنامج عمل لحماية الموارد والمحطات النووية، وتقديم المعونات التقنية وزيادة المساعدات المالية، ومعالجة الفقر والمشاكل الصحية في الدول الفقيرة.

---

[1] مجموعة الثماني G8، مرجع سابق

[2] شبلي مختار، مرجع سابق، ص 280.

[3] إلياس أبو جودة، مرجع سابق، ص 8.

[4] نفس المرجع ص 8 .

أما على مستوى الخبراء، ومن أجل القضاء على الشبكات والمنظّمات الإرهابية، فقد أنشئت هيئتان متخصصتان:

### أولا: مجموعة ليون.

أنشأت مجموعة ليون سنة 1995، على اثر انعقاد مؤتمر "هاليفكس"، من أجل فحص الجوانب القانونية والتقنية، وإصدار توصيات واقتراح خطط عمل لمواجهة الجريمة المنظمة العابرة للأوطان في كل صورها، كالإرهاب والاتجار غير المشروع بالأشخاص[1].

وانبثق عن هذه المجموعة ثلاث مجموعات عمل فرعية تعني بالتعاون القضائي والتعاون العملياتي، وإجرام الإعلام الآلي، كالإرهاب الالكتروني الذي أصبح الشغل الشاغل لكل المنظمات المكافحة لظاهرة الإرهاب والتصدي إليها بكل الوسائل المتاحة.

وتترأس فرنسا مجموعة العمل الفرعية المعنية بالتعاون القضائي في المجال الجنائي كما استحدث ضمن هذه المجموعة لجنة تدرس قضايا الهجرة غير الشرعية.

### ثانيا: مجموعة روما (لجنة مكافحة الإرهاب).

بما أن جرائم الإرهاب شكلت أولى انشغالات الدول الأعضاء في المجموعة، كان لابد من اتخاذ إجراءات للمواجهة الفعالة ضد كل مظاهر الإرهاب.

ونشأت مجموعة روما بعد أحداث 11 سبتمبر 2001 ، وتتشكل من نخبة من الخبراء تمثل مخبرا من الأفكار والمشاريع، وتقديم مقترحات فعلية في مجال التعاون الشرطي والقضائي، بالتنسيق مع جهود الأمم المتحدة واللجنة التي أنشأتها لمكافحة الإرهاب بكل مظاهره وصوره.

وفي الوقت الحاضر تشكل مجموعة روما هيئة عمل لمناقشة وتطوير الرهانات والاستراتيجيات ذات الصلة بالأمن العمومي، خاصة في مجال مكافحة الإرهاب والجريمة المنظمة.

وتعدّ مجموعة روما منتدى لتبادل المعلومات وتحليلها ودراستها، ولدعم مبادرات التشاور والتعاون في مكافحة الإرهاب والجريمة المنظّمة[2].

وتقوم بصياغة المقترحات لتتم الموافقة عليها على المستوى السياسي (رؤساء الحكومات – وزارات الخارجية – وزارات العدل والداخلية)، بالإضافة إلى صياغة أفضل الممارسات والتوجيهات

[1] شبلي مختار، مرجع سابق، ص 281.

[2] نتائج وتوصيات قمة مجموعة الثماني بمادلينا– أكيلا– ايطاليا، 2009، موقع قمة مجموعة الثماني www.g8italia2009.it:، تاريخ الاطلاع: 2018/07/04 على الساعة 23:22.

لاتخاذ إجراءات فعالة من جانب الهيئات المتخصصة متعدّدة الأطراف، مثل منظّمة الطيران المدني الدولي والمنظّمة البحرية الدولية.

أما فريق عمل مكافحة الإرهاب، فيقوم بتنسيق المساعدات الفنية والمالية المقدَّمة إلى الدول الفقيرة في الشرق الأوسط وأفريقيا والأكثر عرضة للتهديد الإرهابي.

وقد خُصِّص مبلغ 20 مليار دولار لمدة عشر سنوات بهدف تنفيذ خطة عمل تعالج جميع القضايا التي تهدّد الأمن والسلم الدوليين، كمسألة الإرهاب، والجريمة المنظّمة، وتجارة الأسلحة الخفيفة والمخدرات، ومشكلة الفقر والفساد.

ويعمل أيضًا على مراقبة المصادر المالية التي تموّل المجموعات الإرهابية وتجميدها بالتعاون مع الدول والمصارف والمؤسسات المالية الدولية، كما يتخذ التدابير اللازمة لحماية وسائل النقل البرية والبحرية والجوية من الأعمال الإرهابية، من خلال رفع معايير سلامة بنى هذه الوسائل التحتية وتحسين إجراءات مراقبة المطارات والمرافئ ومحطات السكك الحديدية، وتسهيل تبادل المعلومات.

ومن بين الاتجاهات الأخرى، المهمة التي تنتهجها أعمال مكافحة الإرهاب، تبرز مسألة تأمين وثائق السفر وتطبيق التكنولوجيات الجديدة في هذا المجال.

ويضمّ الفريق دول مجموعة الثماني، كما توجّه الدعوة إلى المشاركة في أعماله إلى دول أخرى مانحة (هي حتى اليوم سويسرا وأستراليا وإسبانيا)، فضلاً عن منظمات دولية معنية ومنظمات إقليمية وذلك وفق الموضوع الذي يعالج في الاجتماعات المختلفة.

وفي تنفيذها الأعمال الداخلة في تكليفها، ترمي اللجنة إلى دعم عمل لجنة مكافحة الإرهاب التابعة للأمم المتحدة، عبر تعزيز التنسيق وتقديم الدعم التقني اللازم لمكافحة الإرهاب، وفي هذا السياق، تطالب روسيا اليوم بتفعيل التعاون الدولي لمواجهة المجموعات الإرهابية المتطرفة في العراق وسوريا[1].

والجهود الأمريكية في مكافحة الإرهاب الإلكتروني لم تقف عند المنظمات السالفة الذكر فحتى منتصف التسعينات كانت هناك ثلاث استراتيجيات لحماية البنية التحتية للمعلومات في الولايات المتحدة الأمريكية تتضمن الفعل العسكري "التدخل"، الحلول الفنية لتأمين الأنظمة "الاستعداد"، بناء الوعي "المعلومات"

[1] شبلي مختار، مرجع سابق، ص 281.

في حين جاءت السياسات الحكومية الخاصة بمكافحة هجمات الفضاء الالكتروني وتعزيز الأمن الالكتروني متنوعة في مراحل تنفيذها، وبعضها كان قويا بينما كانت الأخرى مجرد اقتراحات، وجاءت بأشكال وصور متنوعة تراوحت بين إتباع سياسة تنظيمية خاصة بالبنية التحتية للمعلومات لتضمين تلك الإجراءات الخاصة بالأمن الالكتروني في الجهود العامة لمكافحة الإرهاب

وفي سنة 1996 إنشاء " لجنة حماية البنية الحساسة" " Commission of critical infrastructure protection" (CCIP)، وأجرت هذه اللجنة سلسلة دراسات وأبحاث تناولت كل النقاط الحساسة في الأمن القومي الأمريكي، وخصوصا في مجال التكنولوجيا، فوجدت أن المعادلة التي تجمع قطاعات الكهرباء والاتصالات والكمبيوتر هي من الركائز الضرورية لسكان الولايات المتحدة الأمريكية وأمن نظامهم العام وتفوقهم على سائر الأمم.

رأت لجنة حماية البنية الحساسة أن هذه المعادلة كهرباء+ اتصالات+ كمبيوتر معرضة جديا لتهديدات الحرب الرقمية، كما أعطت تعريفا للتهديدات الممكنة ضمن هذا الأسلوب فقالت:" المصادر التي يعتمد عليها من يريد القيام بهجوم رقمي متوافرة ومنتشرة بين عامة الناس، وتتألف من جهاز كمبيوتر ونقطة اتصال بالانترنت"[1] .

في فترة حكم الرئيس "بيل كلينتون" تسلل الخوف إلى نفوس الأمريكيين نتيجة سقوط الولايات المتحدة الأمريكية في أيدي هاكرز وإرهابيين دوليين، واعتبر "بيل كلينتون" أن هجوم حرب المعلومات يمكن أن يكون جزءا من عملية عسكرية تقليدية، أو يمكن للعدو المتوقع استخدام المعلومات بوصفها طلقة تحذير لتهديد الولايات المتحدة الأمريكية حتى تستجيب بالعدول عن موقف معين في سياستها الخارجية، أو بوصفها جزءا من عملية إرهابية محدودة.

ومن النقاط التي وضعت باعتبارها أهدافا محتملة لهذا الخطر نظام الاتصالات أو شبكة الكمبيوتر، حيث تعتمد القوات العسكرية الأمريكية على نظم النقل التجارية لنقل الجنود والتي تعتمد بدورها على شبكات الكمبيوتر للتحكم في الماكينات وفي الاحتياط، وفي عملية التنسيق والتموين وبذلك يكون في مقدور جهة خارجية عرقلة القوات الأمريكية.

وكذلك تعتمد نظم الطوارئ على البرامج الإذاعية التجارية والانترنت التي تساعد في التنسيق والمتابعة.

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 370.

ويمكن استهداف نظم وحواسيب شركات معينة لها أهمية خاصة في إنتاج الأسلحة الأمريكية، أو في حركة التعبئة، وهناك البنوك والمؤسسات المالية التي تكون عرضة للتلاعب بالبيانات المسجلة، إما بجمع المعلومات بغرض المساومة أو بزرع معلومات خاطئة.

وفي سنة 1997 أصبح ضعف العسكرية الأمريكية في مواجهة هجمات الاتصالات واضحا عندما أطلق قائد القوات المشتركة تدريبا سمي ب "الملتقى المناسب" لقياس قدرات الكمبيوتر الدفاعية.

وقد أثبتت الدراسات أن هذا التدريب يثبت أن لصوص الكمبيوتر المحترفين "الهاكرز" يمكنهم تعطيل محولات الطاقة في تسع مدن أمريكية، ومنع خدمات الطوارئ المحلية من الاستجابة لهذه الأزمة، واستغلوا في ذلك انشغال الحكومة بهذه الأحداث ليتجولوا وبكل حرية داخل موقع البنتاغون محدثين الدمار، وتعطيل أوامر القيادات العليا للبنتاغون[1].

ويعتبر أول تحرك في إستراتيجية الولايات المتحدة الأمريكية في مكافحة الإرهاب الالكتروني تكليف الرئيس بيل كلينتون الجنرال المتقاعد " روبرت ث.مارش" لدراسة التهديدات الخارجية التي تواجه نظم المعلومات والبنية التحتية مثل وسائل النقل ومولدات الطاقة.

تم الاعتراف بحجم التهديدات التي تواجه الأمن القومي الأمريكي، وعين بيل كلينتون منسقا دوليا لتأمين وحماية البنية التحتية ومكافحة الإرهاب، وفي فيفري سنة 1998 وضعت وزارة العدل الأمريكية مركز حماية البنية التحتية تحت تصرف مكتب التحقيقات الفيدرالي لمتابعة أي هجوم إرهابي على نظم المعلومات.

وفي شهر مارس من نفس السنة بدأ البنتاغون في التحري عن أخطر الهجمات الالكترونية على أنظمة الكمبيوتر الأمريكية والتي سميت ب "متاهة ضوء القمر" .

واقتحمت مجموعة من الهاكرز أو ما يعرف بلصوص الكمبيوتر والشبكات الخاصة بوكالة الفضاء الأمريكية "ناسا" البنتاغون وهيئات حكومية أخرى وجامعات ومراكز أبحاث وعلى إثرها سرقوا آلاف الملفات التي تحتوي على أبحاث فنية وعقود ووسائل أخفاء المعلومات وبيانات غير سرية لكنها مهمة وجوهرية تتعلق بأنظمة البنتاغون لتخطيط الحروب.

ومنذ اكتشاف هذه الجريمة الخطيرة انخرطت هيئة الاستخبارات الأمريكية في اكبر مجال تحقيقي استخباراتي في مجال الاتصالات الالكترونية ، وبعد ثلاث سنوات من العمل تبين أن الهجمات تم

[1] Information Security, Emerging Cyber Security Issues Threaten Federal information systems, Washington, GAO,2005, p 72,73.

توجيهها من خلال سبعة مواقع روسية على الانترنت، وبناءا على ذلك أبلغت واشنطن هذه النتائج لموسكو وزودتها بأرقام الهواتف التي صدرت منها هذه الهجمات.

إلا أن الحكومة الروسية كان ردها بأن أنكرت تماما وجود هذه الأرقام بالخدمة من الأساس، وظل الهجوم مستمرا، وأنشأ هؤلاء اللصوص ما أسموه "بالأبواب الخلفية" التي يمكن عن طريقها معاودة الدخول للمواقع التي اقتحموها مسبقا وسرقة بيانات إضافية[1] .

وعلى الرغم من الدمار الذي سببته "متاهة ضوء القمر" للمواقع المستهدفة إلا أنها لا تعدو أن تكون مجرد بداية للأخطار القديمة .

حينئذ بدأ القادة العسكريون يدركون أن خسارة المعارك الالكترونية بداية ستقوي بشكل متزايد قدرة أي دولة على خوض هذا النوع من المعارك والحروب، فلن يساوي مشروع الدفاع الصاروخي المليارات التي ستنفق على إقامته إذا ما دمرت الهجمات الرقمية برامجه التكنولوجية وبنيته التحتية[2].

في أكتوبر سنة 1999 تم البدء في تدريب آخر أطلق عليه "نجم القمة" لإجراء تجارب على الدروس المستفادة من تدريب "الملتقى المناسب"، وفي هذا التدريب هاجم لصوص الانترنت أنظمة القوى التي تغذي عددا من القواعد العسكرية الأمريكية وأربكوا أنظمة الطوارئ في محطات الطاقة السابق ذكرها بسيل من المكالمات عن طريق الكمبيوتر، مما دفع إلى إنشاء العديد من المبادرات الخاصة من الهيئات التي تقدم تقارير عن تبادل المعلومات والتحذيرات ومراكز داخل الولايات المتحدة الأمريكية وفي الخارج.

وقررت الإدارة الأمريكية في عهد الرئيس بيل كلينتون بدء خطوات تنفيذية لمكافحة ظاهرة الإرهاب الالكتروني.

في سنة 2000 صدرت مسودة اتفاق عالمي حول الجريمة والإرهاب الالكتروني من جامعة "ستانفورد" والتي عرفت فيما بعد ب "خطة ستانفورد" التي شملت العديد من النقاط حول هدف الوصول إلى تعاون دولي أوسع في مقاومة هجمات الفضاء الالكتروني، وذلك على اعتبار أن الإرهابيين والمجرمين يستغلون نقاط الضعف في القوانين، وخاصة مع التطور المستمر في التكنولوجيا وجمود الأطر القانونية الحالية في مواجهة الأخطار والهجمات.

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 372.

[2] نفس المرجع، ص 372.

وقد تم تكوين مسودة الخطة من تسعة خبراء من جامعة ستانفورد بالولايات المتحدة الأمريكية سنة 2000 وذلك من خلال مؤتمر دولي تم عقده في ديسمبر سنة 1999 بنفس الجامعة، وذلك بدعم من مؤسسة "هوفر"، التجمع من أجل البحث في أمن المعلومات والسياسة CRISP، مركز الأمن الدولي والتعاون CISAC، جامعة ستانفورد، بالإضافة إلى دعم كل من منظمات المجتمع المدني والشركات ورجال الصناعة والأكاديميين من العديد من دول العالم، وقد كانت تلك المسودة إضافة مهمة للتوصل إلى الاتفاقية الأوربية للجريمة الالكترونية في سنة 2000 [1]

وتقترح المادة 12 من هذه الخطة إقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات العمل على دعم التعاون حول الأمن الالكتروني في كل دول العالم، وروح هذه الاتفاقية مستمدة من المنظمة الدولية للملاحة الجوية والاتحاد الدولي للاتصالات .

كما أن مركز الدفاع الالكتروني الذي أنشأه حلف الناتو ربما يمثل نموذجا مهما، وتم إنشاء المركز العالمي للاستجابة للطوارئ بما يجعله شبيها بالمنظمات الدولية الأخرى كالنظام القانوني للجرف القاري في إطار القانون الدولي للبحار.

زاد الاهتمام العالمي بمسألة مكافحة الإرهاب الالكتروني بعد أحداث الحادي عشر من سبتمبر سنة 2001 التي أعقبها التوصل إلى اتفاقية الاتحاد الأوربي حول الجريمة الالكترونية"اتفاقية بودابست 2001"، فبعد هذه الأحداث وضع البنتاغون خطة بعنوان "خريطة طريق لعمليات المعلومات"، وهي تستهدف مراقبة الانترنت والتعامل معها بوصفها "منظومة سلاح معادية" .

في أكتوبر سنة 2001 تم عقد اجتماع ضم خبراء التقنية العالية وخبراء العديد من الشركات العالمية العاملة في تكنولوجيا المعلومات الأمنية، وعين الرئيس "بوش" "ريتشارد كلارك" أول مستشار خاص بالأمن القومي، وتم إنشاء مكتب الأمن للفضاء الالكتروني، وإدراكا منها لخطورة هذا التهديد طلبت الإدارة الأمريكية ما يقارب 4.5 بليون دولار لحماية البنية التحتية، وعمل مكتب التحقيقات الفدرالي على زيادة تحقيقاته حول الأمن المعلوماتي لتصل إلى ما يقرب الألف تحقيق، وتشكل لجنة متابعة على مدار الساعة[2].

[1] مضمون المسودة بالتفصيل متوافر على الرابط:
.http//www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm

[2] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 373.

من جميع الأحداث السابقة ذكرها أدركت الإدارة الأمريكية على نحو فعلي قدرة تنظيم القاعدة في مجال التكنولوجيا عندما وجدت قواتها أجهزة كمبيوتر محمول مع أعضاء تنظيم القاعدة في أفغانستان وعلى الرغم من عدم استخدام هذه الأجهزة في العمليات الإرهابية بصورة مباشرة، فإنها استخدمت في الاتصال والتنسيق للهجمات وتلقي الأوامر وإرسال الرسائل، وأظهر تنظيم القاعدة تطورا بارعا في كيفية استخدام الانترنت، فكان اكتشاف الرسائل الالكترونية "لخالد الشيخ محمد" بمثابة نقطة البداية للوصول إلى اعتقاله، الذي اعتبرته الاستخبارات الأمريكية أكبر عمل في الحرب ضد القاعدة.

في يوليو 2002 أجرت الولايات المتحدة الأمريكية عملية محاكاة للتعرض لهجوم من الفضاء الالكتروني سميت "بيرل هاربر الالكتروني" وجاء إنشاء "لجنة حماية البنية الحساسة" في الولايات المتحدة الأمريكية لتؤسس مجموعة خاصة تتناول جوانب الإرهاب الالكتروني أطلقت عليها اسم "مركز حرب المعلومات" الذي يضم نحو ألف موظف وبينهم مجموعة تعمل على مدار أربع وعشرين ساعة في اليوم مناوبة للرد على أي تطورات أو استفسارات وتم إنشاء المركز القومي للبنية التحتية NIPC مركز تحليل وتبادل المعلومات ISACS برنامج حراسة البنية التحتية INFRAGARD، .... وغيرها من المبادرات[1].

وعلى مدار التسعينات أصبح هذا المركز من أهم مراكز حرب المعلومات في العالم الغربي، إلا أن تطوير المركز واجه الكثير من العراقيل أهمها: تشابك صلاحيات التحقيق بين CIA ومكتب التحقيق الفيدرالي FBI .

من الجهود الأمريكية في مكافحة الإرهاب الالكتروني من خلال المشاريع مثل مشروع "أيشلون" وهو مشروع قام بالاشتراك مع الدول الأوروبية للتجسس على رسائل الانترنت والمكالمات الهاتفية في العالم ومشروع "كارنيفور" وغيرهما، مع وجود تشابك واضح في الصلاحيات بين تلك الأجهزة ، فكان مكتب FBI مكلفا بمتابعة التهديدات داخليا، وكذلك استخبارات الجيش، بينما كانت تعمل CIA في مواجهة القضايا الخارجية، وانتشرت في أجهزة الأمن الأمريكية المختلفة وحدات خاصة بالإرهاب الالكتروني، إلى جانب قيام جهاز FBI بملاحقة المخترقين والقراصنة على أنواعهم، وتقوم أجهزة الخدمات السرية بملاحقة الإرهاب الالكتروني في حالات الصرف الآلي والتحويلات المالية عبر الانترنت والنصب والاحتيال والتنصت.

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 374.

أما سلاح الجو الأمريكي فأسس "فرق هندسة الأمن الالكتروني"، ومحاولة اختراق أنظمة وشبكات عسكرية، واستطاعت هذه الفرق اختراق 30 % من شبكات الأجهزة العسكرية في العالم[1] .

ومع كل الجهود السابقة ظهرت مخاوف من تعرض أنظمة التحكم الإشرافي في الحصول على البيانات SCADA، للانتهاك عندما تستخدم شبكة الانترنت للمراقبة والتحكم في العمليات الإنتاجية من مواقع بعيدة، والتي تستخدم في مجموعة واسعة من الصناعات وأنشأت الولايات المتحدة الأمريكية وزارة الأمن الداخلي في صيف سنة 2003 والتي تركز دورها في الحماية من الأخطار التي تأتي من الجبهة الداخلية، وذلك في إطار الحرب على الإرهاب، أصبحت المخابرات والرقابة عنصرا حيويا في تلك الحرب، ولكن مع تزايد المخاوف الأمريكية من تصاعد التهديدات الالكترونية عالميا.

إلى جانب الخوف المتزايد من تعرض البني الحساسة لهجوم الكتروني، وذلك للعمل على إيجاد فرصة لتعزيز الأمن الالكتروني ليكون مستعدا لصد أي هجوم مرتقب من المخترقين والقراصنة والإرهابيين، وكذلك ضد المدونات الالكترونية التي تنشر معلومات مزيفة.

وتقع الولايات المتحدة الأمريكية في عدة إشكاليات للمواجهة من أهمها الاعتماد على السوق الحرة في عملية تأمين الشبكات، كذلك مسألة الاختيار مابين الاحتكار والحماية فطبيعة المواجهة الأمنية تتطلب قدرة عالية على التحكم، ولكن السعي نحو مكافحة الاحتكار والقطاع الخاص أفقد الولايات المتحدة الأمريكية القدرة على السيطرة الأمنية عليها، كما أن قانون الهجرة الذي يمنع شركات تكنولوجيا المعلومات من تعيين كوادر أجنبية أدى إلى تكلفة عالية فيما يخص قطاع الأمن، مما أثر على عائدات تلك الشركات، إلى جانب السيطرة على الموظفين الذين يعملون في القطاع الخاص تشكل عبئا أمنيا إضافيا ولعل تردد الولايات المتحدة الأمريكية في صفقة تولي شركة إماراتية إدارة ستة موانئ مبعثه القلق الأمني بما كان قد يتضمن خروجها جزئيا عن ممارسة سيطرتها الأمنية، لذا فإن هناك حساسية خاصة تجاه القطاع الخاص في قطاعات معينة ، وفي ظل أهمية تشجيع الاستثمارات والتزامات اتفاقيات التجارة الدولية[2].

[1] مقالة منشورة في موقع الجزيرة السعودية متوافرة على الرابط:
http//www.al-jazirah.com.sa/evillage/30112002/hk.htm، بتاريخ 2007/07/12 ، تاريخ الاطلاع 2015/07/13 على الساعة 04:43 .

[2] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 374.

في 2007 اجتمع ممثلو المركز القومي مع مسؤولين حكوميين في الولايات المتحدة الأمريكية وفي الخارج من استراليا– كندا– الدانمارك– فرنسا– ألمانيا– إسرائيل– اليابان– النرويج– سنغافورة– السويد– المملكة المتحدة– وبعض الدول الأخرى للبحث في مسائل حماية البنية التحتية مع نظرائهم ويتصل مركز المراقبة في المركز القومي لحماية البنية التحتية بمراكز المراقبة لعدد من الدول.

كما دأبت بعض الدول على اختبار دفاعاتها في مقابل هجمات الكمبيوتر فيما يمثل إجراء مناورات داخلية لاختبار قدراتها على الدفاع، بل أن هناك حتى مناورات مشتركة فشاركت قوات حليفة من بريطانيا وفرنسا وبلجيكا والولايات المتحدة في الفترة من 3 إلى 05 أكتوبر من سنة 2007 في مناورات أطلق عليها اسم " وايكومب واريبور" واستهدفت إحباط هجوم عنكبوتي على أوروبا والعالم وشاركت في العملية العسكرية نحو 150 طائرة مقاتلة وهيلكوبتر متطورة، بالإضافة إلى قواعد إسناد أرضية.

كما أفاد بيان أن الهدف هو تنسيق الدفاع عن العالم الحر في منطقة معادية تتعرض للأطباق الالكترونية، وتمنع الأسلحة المختلفة من الاتصال فيما بينها وتنفيذ مهامها، وفي ذلك تتزعم الولايات المتحدة الجهود الغربية في الحرب الالكترونية، ومكافحة أي هجمات معادية قد تتعرض لها، والعمل على الحفاظ على تفوقها العسكري وسيطرتها على الفضاء الالكتروني، وتخصيص ما يصل إلى 5% من ميزانيتها العسكرية للإنفاق على تطوير شبكات الأمان الالكترونية في الداخل والخارج[1] .

في 03 أغسطس 2006 أقر مجلس الشيوخ الأمريكي اتفاقية مجلس أوروبا الخاصة بالجريمة الالكترونية، وهي اتفاقية متعددة الأطراف لمواجهة مشكلات الجرائم المتصلة بالكمبيوتر ولجمع الأدلة الالكترونية.

في أغسطس سنة 2007 تم عقد مؤتمر بهدف تجنيد قراصنة الكمبيوتر في الحرب على الإرهاب، وذلك بمشاركة مؤسسات أمنية أمريكية، حيث شارك 6000 من القراصنة ومحترفي الكمبيوتر في هذا المؤتمر، والذي هدفت الولايات المتحدة الأمريكية من ورائه مشاركتها جهودها في مكافحة الإرهاب الالكتروني، وتبادل المعلومات مع أشخاص من خارج المؤسسات الأمنية، وذلك على أمل أن تكسب محترفي الكمبيوتر حلفاء في مجال الأمن الرقمي وخاصة مع إدراكها أن المرحلة

[1] بول روجرز، حماية أمريكا ضد الإرهاب عبر الانترنت، مقالة منشورة في موقع وزارة الخارجية الأمريكية، متوافرة على الرابط: http//usinfo.state.gov/journals/itps/1101/ijpa/focus4.htm.تاريخ الاطلاع 2018/07/13 على الساعة 19:32.

المقبلة من مكافحة الإرهاب والجريمة ستتطلب الاستعانة بأذكى العقول التقنية لخوضها، وأن هذه العقول ستوفر مبالغ ضخمة تضطر الحكومة الأمريكية لدفعها إلى القطاع الخاص.

وتجري الولايات المتحدة الأمريكية مناورات سنوية لاختبار مدة جاهزيتها للهجمات الالكترونية عبر حواسيب آمنة في مركز الخدمة السرية في واشنطن فقامت الولايات المتحدة بإنشاء قيادة عسكرية للدفاع عن الفضاء الالكتروني سنة 2009، وبعد تولي الرئيس "أوباما" تم استحداث منصب حديد في البيت الأبيض هو مساعد الرئيس لشؤون الانترنت، وذلك بعد عجز وزارة الأمن الداخلي في مواجهة تهديدات الإرهاب الالكتروني .

وحذت روسيا حذو الولايات المتحدة الأمريكية في مكافحة الإرهاب الالكتروني وسعت لصياغة مقترحات تهدف إلى تشديد العقوبات على استخدام الإرهابيين لشبكة الانترنت وكذا اتخاذ التدابير الصارمة لإيقاف انتشار أفكار الإرهاب والتطرف، واقترح احد الخبراء الروس إلى إنشاء جهاز للأمن على غرار جهاز الأوروبول للشرطة الأوربية- كما سوف نوضح في العنصر الآتي- يكلف بالحراسة ومراقبة الانترنت، بما فيها عمليات التحايل والقرصنة التي تتعرض لها في المستقبل[1] .

وتعد الولايات المتحدة الأمريكية من أكثر الدول التي يقوم فيها بأنشطة تخريبية باستخدام الكمبيوتر كما أن أغلب البرامج التخريبية أمريكية الأصل، فضلا عن أن الشركات الأمريكية توفر استضافة المواقع الالكترونية، وتوجد في الولايات المتحدة الأمريكية عصابات تشكل حلقات معقدة ذات خبرة تقنية عالية وهناك منافسة عنيفة في عالم الجرائم التقنية مما يخفض من أسعار البيانات المالية المسروقة، كما تأتي الولايات المتحدة الأمريكية على رأس قائمة الدول التي تشهد أنشطة شبكات أجهزة "البوت"، وهي أجهزة كمبيوتر يتم التحكم بها عن بعد، ويتم بتشغيلها لتقوم بنشر برامج متطفلة مزعجة غير مرغوب فيها وتجري أعمالا تخريبيا، ويحدث ذلك دون علم صاحب الجهاز الأصلي مع ظهور رسائل الكترونية غير مرغوب فيها

من ضمن الجهود الأمريكية أيضا في هذا الشأن عمليات التنسيق بين مكتب التحقيقات الفيدرالي الأمريكي والشرطة البريطانية من أجل إنشاء قاعدة بيانات دولية، هدفها الإيقاع بمن يصنفونهم إرهابيين ومجرمين، هذا وقد أنشأت دول التحالف(أمريكا- بريطانيا- كندا- نيوزلندا) ضد الإرهاب مجموعة عمل(كونسورتيوم) للمعلومات الدولية من أجـــل التخطيط لاستراتيجياتها في مجـال مكافحـــة

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 377.

الإرهاب الالكتروني والجريمة المنظمة، وبموجب البرنامج المقترح يتم تبادل صور قزحيات العين وراحات الأيدي وبصمات أصابع المطلوبين ومعلومات شخصية أخرى بين أجهزة الأمن في الدول الأربع، ويتوقع أن تحتوي شبكة المعلومات المشتركة في هذا الإطار بيانات تتعلق بملايين المشبوهين ويهدف البرنامج إلى تشجيع البحث المتقدم من تبادل المعلومات على نطاق دولي، ما يؤسس لمنبر تقني لتبادل المعلومات الشخصية عن الإرهابيين والمجرمين المطلوبين.

وقد خصصت وزارة الأمن الداخلي الأمريكي 5.12 مليون دولار عام 2004 للأمن الرقمي، وفي سنة 2005 وصلت إلى 5.17 مليون دولار، و15 مليون دولار سنة 2006 وسنة 2007، وهذا التزايد يعكس خطة أمنية إستراتيجية ضد الإرهاب الالكتروني[1] .

## المطلب الثاني: الدور الأوروبي في مكافحة الإرهاب الالكتروني.

اجتهدت الدول الأوربية في مكافحة الإرهاب بعد الأمم المتحدة ، وكان الاتحاد الأوروبي متصدراً في هذا الجانب بالنظر لتقدم دوله في مجال تقنية المعلومات من جانب ومشاركة هذه الدول في الجهود الدولية لمكافحة الإرهاب تحت مظلة الأمم المتحدة مما جعلها هدفاً للتنظيمات الإرهابية .

وكان التحاق سائر المنظمات الإقليمية متأخراً بهذه الجهود ولم يكن الإرهاب الالكتروني في أجندتها لمحدودية اعتمادها على الشبكة الدولية للمعلومات وانشغال دولها بهموم وتحديات اكبر إلا أنها مع ذلك نصت في كل اتفاقياتها على أنها تسعى إلى مكافحة جميع أشكال وصور الإرهاب.

بالإضافة إلى الاتحاد الأوربي، يوجد أيضا الحلف الأطلسي على اعتباره المظلة الأمنية لأوروبا وكذلك المنظمات الأوربية المتخصصة والتي تميزت بطابع العالمية فيما بعد والتي بذلت جهود محمودة في مجال مكافحة الإرهاب الالكتروني.

ومن أجل ذلك قسمنا هذا المطلب إلى ثلاثة فروع، فرع أول ونتعرض فيه لجهود الاتحاد الأوربي في هذا المجال، وأما الفرع الثاني فيكون لجهود الحلف الأطلسي والفرع الثالث فقد خصص لجهود المنظمات المتخصصة في مكافحة الإرهاب الالكتروني.

### الفرع الأول: جهود الاتحاد الأوروبي في مكافحة الإرهاب الالكتروني.

كثيرا ما بذل الاتحاد الأوربي جهودا كبيرة من اجل مكافحة جريمة الإرهاب والوقاية منها، وسخر لهذا الشأن إمكانيات بشرية ومادية كبيرة، وهذا بعد الاعتداءات الإرهابية الكثيرة والمتتالية على دوله

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 378.

الأعضاء، بل وعلى العالم بأسره، ومن اجل ذلك اتخذ الاتحاد الأوربي جملة من الإجراءات حتى تنعم القارة الأوربية بالأمن والسلام والاستقرار، ومن أجل تحقيق هذه الأهداف اتبع الاتحاد الأوروبي إستراتيجية شملت أربعة محاور وهي: الوقاية– الحماية– المتابعة– الرد[1].

وفي إطار الحماية من الجرائم الإرهابية بمظاهرها المختلفة عملت دول الاتحاد الأوربي على محاربة كل العوامل التي أدت إلى نشوء الإرهاب واستفحاله في المجتمعات وذلك بسد منابع التجنيد أمام المنظمات الإرهابية، كما سعت إلى وضع سياج امني لحماية الحدود ووسائل النقل والمنشآت الحساسة، وتتبع حركة الإرهابيين والتنسيق في الميدان القضائي من اجل ضمان محاكمة الإرهابيين كما التزمت دول الاتحاد الأوروبي بوضع الوسائل الأمنية للرد على الضربات الإرهابية، كما أبرمت العديد من الاتفاقيات في هذا الشأن.

هذا وتجدر الإشارة أن الاتحاد الأوروبي عمل على تجسيد الآليات الأممية في الميدان من خلال ما اتخذه من إجراءات تشريعية، واستحداث هيئات قضائية وأمنية كانت لها الفعالية في وضع تدابير لحماية القارة الأوربية[2].

ونظرا لتعاظم تطور الإرهاب وتطوره بتطور تكنولوجيا المعلومات ووصوله إلى صورته الحديثة والمتمثلة في الإرهاب الالكتروني زاد ذلك من جهود الاتحاد الأوربي في مكافحة الإرهاب وكانت من أهم هذه الجهود إبرام اتفاقية بودابست لسنة 2001.

### أولا: اتفاقية بودابست لمكافحة الإرهاب الالكتروني.

يعتبر الإرهاب الالكتروني من أخطر أنواع الإرهاب في حاضرنا، حيث أصبحت الجماعات الإرهابية كثيرا ما تستغل مواقع الانترنت في تجنيد الإرهابيين والدعاية لأنشطتها الإجرامية، وتدمير المواقع بغرض نشر الرعب والفزع وإلحاق الشلل بأجهزة الدولة الحيوية– على نحو ما تم شرحه سابقا– ولتفاقم خطر هذه الظاهرة حاولت الدول الأوربية إيجاد آلية تشريعية تكون سند قانوني للتصدي لجرائم الحاسوب بما في ذلك الإرهاب الالكتروني.

[1] ساعد الهام حورية، مرجع سابق، ص 102.

[2] نفس المرجع، ص 101.

وتعتبر اتفاقية بودابست لسنة 2001 والتي دخلت حيز التنفيذ سنة 2004 مكسب تشريعي هام لجميع الدول ومرجعية لتعديل القوانين الداخلية، كما انضمت إليها فيما بعد الولايات المتحدة الأمريكية بالتصديق على أحكامها سنة 2006، وكذلك كندا وجنوب أفريقيا.

وتعد اتفاقية بودابست الاتفاقية الوحيدة المتعددة الأطراف التي تتناول بالتفصيل الإجراءات الواجبة التطبيق في مجال جرائم الانترنت ومنها جريمة الإرهاب الالكتروني، وهي بمثابة دعوى لجميع دول العالم للتفاعل والتعاون ضد الإجرام الالكتروني، والذي يعرف اليوم أنماطا مختلفة من الاعتداءات، وتم تعديلها ببروتوكول إضافي سنة 2003 بستراسبورغ[1].

## 01-التعريف بالاتفاقية وعلاقتها بمكافحة الإرهاب الالكتروني.

بتاريخ 20 نيسان 2001 تقدمت اللجنة الأوربية لمشكلات الجريمة CDBC بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت فيما بعد في بودابست سنة 2001 وعرفت بالاتفاقية الأوربية لمكافحة الجرائم الالكترونية .

وتتكون هذه الاتفاقية من مقدمة وأربعة فصول، تضمنت المقدمة استعراض لأهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود إرشادية وتوجيهية وتدابير إقليمية ودولية، وأما الفصل الأول فتضمن تغطية للمصطلحات الأساسية، والثاني اشتمل على الإجراءات المتعين على الدول الأعضاء اتخاذها على المستوى الوطني، وأما الفصل الثالث من الاتفاقية فقد نص على التعاون الدولي[2].

ومما سبق يتضح أن هذه الاتفاقية تقدم ولأول مرة إطار لتحديد قائمة جرائم الكمبيوتر وأنماطها وطوائفها، إذ انه وعلى الرغم من الجهود التشريعية والتدابير الإقليمية والدولية على مدى السنوات الماضية لم تتوفر على رؤية شاملة أو إطار واضح يحدد قائمة الجرائم أو بينت أسس التقسيم، وهي الميزة الايجابية التي تمتعت بها هذه الاتفاقية، وبالرجوع إلى المعيار التي اعتمدته، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة، فالطائفة الأولى التي نصت عليها الاتفاقية، والتي أطلقت عليها الجرائم التي تستهدف سرية وسلامة المعلومات، وهي في الحقيقــة الجرائــم التي يلعب الكمبيوتـر فيها

[1] ساعد الهام حورية ، مرجع سابق، ص 105.

[2] عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية 2011، ص 175.

دور الهدف، أي الجرائم التي تستهدف معطيات الكمبيوتر بذاتها سواء لجهة الوصول إليها أو الاطلاع عليها أو إفشائها أو تحريرها أو إتلافها، وهي المعطيات في مراحل المعالجة والتخزين والنقل بواسطة أجهزة الكمبيوتر ووسائل الاتصال وشبكات المعلومات.

وأما الطائفة الثانية من هذه الاتفاقية وهي الجرائم التي أطلقت عليها الاتفاقية الجرائم المرتبطة بالكمبيوتر، وهي الجرائم التي يلعب الكمبيوتر فيها دور الوسيلة، أي الأداة المستخدمة لارتكاب جرم تقليدي[1] .

ومن خلال هذه التقسيم يتضح أن جريمة الإرهاب الالكتروني تدخل ضمن الطائفة الثانية فهو جريمة تقليدية اعتمدت على الكمبيوتر وشبكة الانترنت كوسيلة لتحقيق أهدافها الدنيئة.

أما الطائفة الثالثة وهي طائفة الجرائم المرتبطة بالمحتوى، فهي الجرائم التي يلعب فيها الكمبيوتر دور البيئة الجرمية، وقد ربطتها الاتفاقية بجرائم المواد لا أخلاقية المتصلة بالأطفال، أو المتعلقة بهم إلا أن الاتفاقية لا تنص على بقية أنماط الجرائم المرتبطة بالمحتوى كالمقامرة والجرائم المرتبطة بالمخدرات.

وأما الطائفة الرابعة والأخيرة فهي المتعلقة بجرائم الملكية الفكرية، فهو نص مكمل لقواعد الحماية الجزائية في هذا الحقل المقرر وطنيا ودوليا.

والملاحظ أن الطائفة الرابعة قد ركزت على شخص الجاني، ومدى الدراسات التقنية التي يتمتع بها بخصوص النظم المعلوماتية، ومن هذا المنطلق جاء تعريف الجريمة الالكترونية بأنها تلك التي يقوم بها شخص لديه إلمام خاص بتقنيات الحاسب ونظم المعلومات.

وبما أن جريمة الإرهاب الالكتروني –كما سبق وأشرنا– تنتمي إلى الطائفة الثانية التي تعول على الحاسب الآلي كوسيلة لارتكاب الجريمة التقليدية حتى تصبح جريمة الكترونية فإن هذا الرأي لم يسلم من النقد[2]، وذلك لأن التعويل على الحاسب الآلي كوسيلة لارتكاب الجريمة حتى يمكن نسبها إلى طائفة الجرائم الالكترونية ينطوي على الكثير من التوسع غير المقبول، وهذا لأن تعريف الجريمة يستوجب الرجوع إلى الأفعال المكونة لركنها المادي وفقا للنموذج القانوني الذي حدده المشرع، فقانون العقوبات يركز اهتمامه على الأفعال التي يقترفها الجاني، لا على الوسائل التي ارتكبها الجاني، كما

[1] عماد مجدي عبد الملك،مرجع سابق، ص 176.

[2] هلالي عبد اللاه أحمد،( المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست )، مرجع سابق، ص 112.

أن مجرد استخدام جهاز الكمبيوتر لا يضيف شيئا جديدا إلى السلوك الإجرامي حتى توصف بالجريمة المعلوماتية[1].

إلا أننا وكباحث في هذا الموضوع لا نشاطر هذا الرأي وهذا لان استخدام الوسيلة الحديثة من حاسب آلي وشبكة الانترنت يضيف جديدا إلى السلوك الإجرامي من أنه يصبح أكثر يسرا وأكثر تطورا إلا أن هذه الوسيلة لا تغير من طبيعة الجريمة كما هو الحال في جريمة الإرهاب الالكتروني فهي تبقى جريمة إرهابية لكن وسيلة ارتكابها تطورت فقط.

كما يلاحظ على اتفاقية بودابست أنها جعلت من الاستيلاء على البيانات في إطار مفهوم الجرائم التي تستهدف السرية وسلامة توافر المعلومات، وفي ذات النطاق يمكن إدخال أنماط مختلفة لجرائم البريد الالكتروني والتراسل الالكتروني، وكلاهما وسيلتان تعتمدهما جريمة الإرهاب الالكتروني، ولقد ابتعدت عن الوصف الفرعي أو التفصيلي لأنماط السلوك الإجرامي أو الصور التي تتخذها الجريمة الواحدة أو التي تندرج في نطاق الجريمة الواحدة، وهذا مسلك ايجابي في نظر البعض من الفقهاء والباحثين على اعتبار أن توصيف السلوك في الغالب يتصل بالوسائل الالكترونية المتبعة في ارتكاب الجريمة.

أما ما يتعلق بجرائم الخصوصية حسب ذات الاتفاقية أو بشكل أدق لجرائم التي تستهدف البيانات الشخصية في مراحل الجمع والمعالجة والاستخدام والنقل، فإن الإطار العام للنصوص الموضوعية لم يميز نوع المعطيات، وأما إذا كانت بيانات تتصل بالشخص أو بمصالح اقتصادية أو مالية أو مسائل أمنية أو غير ذلك، وهذه الصورة أيضا تخص جريمة الإرهاب الالكتروني، ولعل هدف هذه الاتفاقية في هذا الشأن لتعميم حماية المعطيات بكافة أنواعها[2] إضافة إلى أن مسائل حماية البيانات الشخصية والخصوصية تحظى بتنظيم تشريعي قائم ومتميز عن التنظيم التشريعي لجرائم الكمبيوتر، إذ أن هذا الموضوع يغطى بواسطة الاتفاقية الأوربية لحماية البيانات الشخصية، وبقائمة طويلة من التشريعات الوطنية، والأدلة الإرشادية في نطاق أوربا.

أما عن الحديث حول النصوص الإجرائية فإنها تتخذ الأهمية القصوى في هذه الاتفاقية وذلك أن التدابير التشريعية الإجرائية لم تكن بمستوى التدابير التشريعية الموضوعية التي تعتبر مغيبة إلى اليوم في

[1] هلالي عبد اللاه أحمد،( المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست )، مرجع سابق، ص 113.

[2] عماد مجدي عبد الملك، مرجع سابق، ص 176.

الجزء الأكبر من دول الاتحاد الأوربي، فيما يتعلق بالقواعد الإجرائية الخاصة بجرائم الكمبيوتر والانترنت وفي هذا الشأن تمثل أحكام الاتفاقية قواعد عامة وتوجيهات تتطلب تحديدا منضبطا من المؤسسات التشريعية لدى وضع القوانين الوطنية فالاتفاقية حاولت أن تؤكد على حقيقة أن جرائم الكمبيوتر والانترنت تنطوي على الخصوصية في ميدان الإثبات والتحري والضبط والتفتيش والمقاضاة والاختصاص، ولهذا سعت الاتفاقية لتقديم معايير لضبط هذه العناصر من أجل انسجام الحلول الإجرائية، وقد منحت هامشا للدول الأعضاء لاتخاذ التدابير المختلفة، أو على الأقل حلولا بديلة أو أخرى غير ما تضمنته[1].

وعن التعاون الدولي لمكافحة الجرائم الالكترونية والتي من ضمنها جريمة الإرهاب الالكتروني فقد جاءت اتفاقية بودابست بأحكام أكثر تفصيلا، باعتبار الاتفاقية نفسها هي الأداة التشريعية الرئيسية التي ستحكم مسائل التعاون الدولي في أنشطة المكافحة.

وتجدر الإشارة أن أبرز ما تنطوي عليه مسائل التعاون الدولي يتمثل بالقواعد المتعلقة بتسليم المجرمين، والإنابة القضائية ومسائل الضبط والتفتيش وتحريز الأدلة خارج الحدود، ولقد كانت الأحكام التي تضمنتها الاتفاقية في هذا الميدان[2] .

ويرى بعض الفقه الجنائي انه على الرغم من التمسك بمقتضيات السيادة الوطنية إلا أنه وفيما يخص الجرائم الالكترونية بالذات لا يمكن مواجهتها دون قواعد مخصوصة تنظم المسائل الحساسة والمهمة، بل ويمكن أنها القواعد التي سوف تحمي السيادة الوطنية باعتبارها تنطبق على كافة الدول الأعضاء ضمن المعايير الموضوعية المقررة في الاتفاقية، وبشكل يحول دون تدخلات لصالح طرف دون آخر، وهذا في ظل اختلا موازين القوى وسيدة إرادة المتحكمين بمصائر الشعوب والدول[3].

## 02- الإجراءات التي اتبعها الاتحاد الأوروبي لمكافحة الإرهاب الالكتروني.

مارس الإتحاد الأوربي دوراً مهماً في مجال التصدي لجريمة الإرهاب الالكتروني عبر إقراره العديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات .

[1] عماد مجدي عبد الملك، مرجع سابق، ص 173.

[2] هلالي عبد اللاه أحمد،( المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست )، مرجع سابق، ص 243.

[3] عماد مجدي عبد الملك، مرجع سابق، ص 178.

ففي عام 1981 وقعت اتفاقية تحت مظلة المجلس الأوربي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية، كما صدر عن المجلس الأوربي العديد من القواعد التوجيهية في مجال جرائم الحاسب الآلي تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم كالغش المعلوماتي وسرقة الأسرار المخزنة وتضمنت هذه القواعد عددا من الإجراءات الفنية التي يتوجب اتخاذها لحماية نظم المعلومات من كل أشكال الانتهاك .

في عام 1980 جرى توقيع معاهدة مجلس أوربا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات ذات الطابع الشخصي والتي سرى مفعولها في أكتوبر عام 1985 وانطوت على توجيهات بصدد وجوب توفير قواعد تكفل حماية البيانات الشخصية من مخاطر المعالجة الآلية[1].

فضلا عن ذلك فقد صدر عن مجلس أوربا العديد من التوصيات لحماية البيانات الحاسوبية ولاسيما التوصية بالرقم (R81/1) بشان تنظيم البيانات الطبية المعالجة آليا في بنوك المعلومات وكذا البيانات الخاصة بحماية البحوث العلمية .

ولا يمكن التغاضي كذلك عن جهود السوق الأوربية المشتركة في مجال إصدار القرارات المعنية بحماية الفرد في مواجهة التطور التقني للمعلوماتية كما حصل في الأعوام 1979 و1982، وإذا كانت الحماية الأوربية للبيانات الشخصية لم تتوج حتى الآن ، إلا أنه صدر إرشاد أوربي في 11 آذار عام 1996 يتعلق بالحماية القانونية لقواعد البيانات واعتبار برامج الكومبيوتر ضمن مجال المؤلفات الفكرية الواجب حمايتها .

وقد شملت هذه الحماية التركيب والتصميم أي حماية محتواها من الاقتطاع أو الاستعمال له أو لأي جزء منه وذلك بمجرد أن يتطلب تحضير وإعداد المحتوى من واضعي القاعدة توظيفا ذا طابع اقتصادي مهم نوعا وكما .

يضاف إلى ذلك الجهود التي قامت بها منظمة التعاون الاقتصادي والتنمية في مجال إرساء مبادئ حماية الخصوصية بشأن البيانات الشخصيــة والتي اهتمت بشكل عملي بحمايــة الخصوصيــة

[1] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، بحث مقدم إلى جامعة كربلاء، 1437 هـ/ 2016 م ، ص 29.

عبر الحدود والتي تبلورت على شكل قواعد إرشادية تم تبنيها رسميا من قبل مجلس المنظمة في أيلول 1980 تحت عنوان "قواعد أوسيد الإرشادية بشان حماية الخصوصية ونقل وتدفق البيانات الشخصية"[1] .

غير أن الحدث الرئيس الذي توج جهود الإتحاد الأوربي – كما تم توضيحه في العنصر السابق– في هذا المضمار قد تمثل بإصدار اتفاقية شاملة تتعلق بجرائم الحاسب في اجتماع المجلس بستراسبورغ في عام 2000 تضمن الدعوة إلى حماية مجتمعاتها من الجرائم الرقمية ووضع التشريعات الملائمة لمكافحتها بالنص على تجريم الأفعال التي تشمل إتلاف قواعد البيانات ووظائف الحاسب الآلي وأنظمته أو التزوير فيها أو الاحتيال وعقوبة المتسبب بذلك أو حتى الشروع في مثل هذه الجرائم والمساهمة فيها وضمان التعاون الدولي في مجال التحقيق وتبادل المعلومات لتحقيق الأمن المعلوماتي.

وقد سبق وتمت الإشارة إلى أن اتفاقية بودابست لسنة 2001 تضمنت 48 مادة اشتملت على الإجراءات القانونية التي من شأنها المحافظة على الإطار الشرعي للفضاء الالكتروني، إذ تدعو إلى وضع نظام تعاون دولي يتميز بالسرعة والفعالية في التنفيذ وتضمين التشريعات الوطنية التدابير اللازمة لمحاربة هذا النمط من الإجرام والتحكم في المواقع الالكترونية الخاصة بالجماعات الإرهابية حيث تضمن المواد من 10 إلى 21 من نفس الاتفاقية على القواعد الإجرائية المتعلقة بالجريمة الالكترونية ومنها الإرهاب الالكتروني كما يلي:

1. سرعة التحفظ على بيانات الكمبيوتر المخزنة.
2. إجبار مقدمي الخدمات على التزويد بالمعلومات المطلوبة.
3. تفتيش وحجز بيانات الكمبيوتر المخزنة.
4. التجميع الفوري لبيانات الكمبيوتر وإمكانية اعتراض هذه البيانات.

وزيادة على ذلك نصت المادة 22[1] على ضرورة تضمين التشريعات الوطنية الآليات القانونية اللازمة لتأسيس اختصاص الدولة القضائي على الجرائم المشمولة بهذه الاتفاقية والتنسيق فيما بينها

[1] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي،مرجع سابق، ص 30.

من أجل تكريس مبدأ التعاون القضائي، فالمادة 22 وضعت القواعد القانونية التي بموجبها يتأسس الاختصاص القضائي للدولة في حالة ارتكاب جريمة من الجرائم في نطاق هذه الاتفاقية سواء في إقليم الدولة، أو على متن إحدى السفن أو الطائرات التي ترفع علمها، وكذلك على كل جريمة مرتكبة من طرف مواطنيها إذا كان معاقب عليها في القوانين الداخلية للدولة التي ارتكب الفعل في إقليمها، أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي لأية دولة.

وقد تم تعديل المادة 22 طبقا لأحكام بروتوكول بستراسبورغ لسنة 2003 المتعلق بتكملة أحكام اتفاقية مجلس أوربا لحماية المعطيات الآلية للكمبيوتر أو محاربة الإجرام الافتراضي.

كما نصت الاتفاقية على ضرورة التشاور بين الدول الأعضاء حول الاختصاص القضائي الأكثر ملاءمة في حالة تعدد طلبات التسليم.

ويتضح مما سبق أن الهدف الأساسي من الإجراءات المنصوص عليها ضمن أحكام هذه الاتفاقية هو ضمان حماية سريعة للبيانات المخزنة في الكمبيوتر حول جرم ما لتسهيل عملية التحقيق والوصول إليها في أية دولة من الدول الأعضاء في الاتفاقية، خاصة وأن الجرائم الالكترونية والتي من ضمنها الإرهاب الالكتروني من الصعب التحقيق فيها والوصول إلى مرتكبيها[2].

وحاليا يعتزم الإتحاد الأوربي وضع خطة جديدة يقوم بموجبها بتفتيش أجهزة الكومبيوتر عن بعد لمكافحة الجريمة الرقمية .

وستشجع هذه الخطة تبادل المعلومات بين قوات الشرطة الالكترونية لملاحقة ومقاضاة المجرمين بعد أن توجه تحذيرات حول الأخطار المحدقة تلحقها إنشاء فرق تحقيق تعمل عبر الحدود وترخص

[1] نصت المادة 22 من اتفاقية بودابست على انه:" تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الاختصاص بشأن أي جريمة تنص عليها هذه الاتفاقية، وذلك عندما ترتكب الجريمة في إقليمها أو على متن السفن ترفع علم الطرف أو على متن إحدى الطائرات المسجلة بموجب قوانين ذلك الطرف، أو من جانب أحد مواطنيها إذا كانت الجريمة معاقب عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأية دولة"

[2] ساعد الهام حورية، مرجع سابق، ص 107.

استخدام دوريات افتراضية لملاحقة المجرمين وضبط بعض النواحي في الانترنت وذلك في مسعى لضمان احترام قوانين حماية المعلومات أثناء جمعها وتبادلها[1].

## ثانيا : اتفاقية أوروبا للوقاية من الإرهاب لسنة 2005 .

في إطار الجهود الأوروبية في مكافحة الإرهاب مهما كانت أشكاله وصوره ويعتبر الإرهاب الالكتروني أخطر هذه الصور، اعتمد المجلس الأوروبي في 16 و17 كانون الأول 2004 إجراءات منها تعزيز القدرات الاستخباراتية على المستوى الوطني والإقليمي وعلى مستوى المنظّمات الدولية.

كذلك أقرّ المجلس الأوروبي في كانون الأول 2005 إستراتيجية الاتحاد الأوروبي ضدَّ الإرهاب بمختلف أنواعه وصوره ، التي تقوم على أربع ركائز أساسية هي: الوقاية من ظاهرة الإرهاب؛ حماية المواطنين والبنية التحتية والنقل عبر دعم هياكل الأمن؛ تعقّب الإرهابيين بمعنى السعي لمنع المجموعات الإرهابية أو الإرهابيين كأفراد من التواصل في ما بينهم وخاصة أن شبكة الانترنت تسهل هذا التواصل دون الحاجة إلى أعباء التنقل ومن التحرك بحرّية، ومن التخطيط لعمليات إرهابية، وذلك عبر تفكيك الشبكات التي توفّر لهم الدعم والتمويل؛ والردّ، بمعنى القدرة على إدارة آثار العمليات الإرهابية ممكنة الوقوع، وتخفيف وقعها من منظور يقوم على التعاون والتضامن.

واعتمد مجلس الاتحاد الأوروبي خطة عمل محدّدة لمكافحة التشدّد والتجنيد للإرهاب في العام 2005، تتصدّى بالتفصيل لمسألة الوقاية، مع توجيه اهتمام خاص لتطوير القدرات على مواجهة الظروف التي يمكن أن تسهّل انتشار التشدّد أو الراديكالية والتجنيد، وذلك من خلال التعاون بين الدول الأعضاء والمؤسسات الاتحادية، فضلاً عن الدول الأخرى والمنظّمات الدولية[2].

بالإضافة إلى ذلك، ثمة اعتراف متزايد بأهمية القيام بعمل وقائي واسع النطاق على أساس الحوار بين الثقافات والأديان، من أجل تعزيز المعرفة والتفاهم المتبادل، وبالتالي تضييق المجال الذي تنشط فيه الدعاية الأصولية وأعمال تجنيد الإرهابيين، وقد جعل الاتحاد الأوروبي من مكافحة الإرهاب، أحد العناصر الأساسية في حواره السياسي مع المجموعات الإقليمية والبلدان الأخرى.

ويضطلع الاتحاد الأوربي بدورٍ قيادي في هذا المجال بهدف إقامة شراكة أوروبية وغربية مع الإسلام المعتدل، سواء في البلدان الأصلية أم مع الجاليات الإسلامية المقيمة بدول الاتحاد، كذلك

[1] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، مرجع سابق، ص 31.

[2] إلياس أبو جودة، مرجع سابق، ص 9.

تتضمّن اتفاقات المشاركة والتعاون وغيرها من أدوات السياسة الخارجية بندًا خاصًا عن مكافحة الإرهاب.

وفي إطار السياسة الخارجية والأمنية المشتركة، أقيم حوار مع دول مجلس التعاون الخليجي في شأن موضوع تمويل الإرهاب، وعلى جبهة مكافحة تمويل الإرهاب، يتم تفعيل أنشطة الاتحاد الأوروبي في القطاعات والمحاور المختلفة، بالإضافة إلى تشجيع دعم تعميق التعاون مع الدول الأخرى.

وقد حدّد الاتحاد الأوروبي أيضًا سلسلة من الإجراءات المتعلقة بمراقبة الحدود وتبادل المعلومات والتعاون القضائي والبوليسي، وقد تم اعتماد العديد من الاتفاقيات التشريعية في إطار التعاون القضائي والعقوبات وتعاون أجهزة الشرطة. وفي هذا الصدد، يمكن ذكر القرارات المتعلقة بأطر العمل في شأن مذكرة التوقيف الأوروبية؛ وتلك المتعلقة بفرق التحقيق المشتركة؛ والاتفاقات الخاصة بمكافحة الإرهاب؛ والاتفاق حول إنشاء "أوروجوست" (وهو جهاز الاتحاد الأوروبي المختص بالتحقيقات والعقوبات التي تعني دولتين من الاتحاد أو أكثر وبأشكال خطرة من الإجرام)؛ وتلك المتعلّقة بإعادة تدوير الأموال أو غسلها والاعتراف بمصادرة أدوات الجرائم وعائداتها؛ والاتفاق حول الاعتراف المتبادل بقرارات المصادرة[1].

وفي هذا السياق، يجدر التذكير باتفاقية أيار 2000 الخاصة بالدعم المتبادل بين الدول الأعضاء في شأن العقوبات والجنايات والبروتوكولات الإضافية المعدّلة للاتفاقية التأسيسية للمكتب الأوروبي للشرطة "أوروبول".

وابتداءً من 1 أيار 2005 باشرت الوكالة الأوروبية للحدود الخارجية "فرونتكس" عملها وهو يشمل أيضًا تنسيق التعاون لوقف تدفقات الهجرة غير الشرعية، وبهدف تعزيز مكافحة الهجرة غير الشرعية، من المقرَّر في المستقبل استخدام الإحصاء البيولوجي في التحقّق من الهوية على الحدود وعلى أراضي دول الاتحاد الأوروبي.

وترمي هذه الإجراءات إلى الوقاية من خطر أن تصبح تدفقات المهاجرين غير الشرعيين قناة يعبرها الإرهابيون[2].

[1] إلياس أبو جودة، مرجع سابق، ص 9.

[2] Conseil de l'Union Européenne, Plan d'action pour lutter contre le terrorisme- Le Monde Diplomatique, 13 février 2006: www.consilium.europa.eu/media.(09/07/2018 à 23:47)

وبتاريخ 16 ماي 2005 تمكن مجلس أوروبا من اعتماد اتفاقية للوقاية من الإرهاب التي دخلت حيز التنفيذ في 01 جوان 2007، وقد شملت هذه الاتفاقية على إستراتيجية واضحة المعالم ارتكزت على سياسة الوقاية، وفي البداية آثرت الدول الأوروبية الانضمام الى هذه الاتفاقية ماعدا بلغاريا، إلا أنها انضمت فيما بعد، وقد حاولت الاتفاقية توضيح بعض النقاط التي كانت محل خلاف في السابق كتحديد الجرائم موضوع المتابعة وتعريف الإرهاب.

وتضمنت ديباجة الاتفاقية الرفض التام للإرهاب، وعدم قبول أي تبرير بشأنه حيث ورد في نصها مايلي:" إن الجرائم الإرهابية المشمولة بنص هذه الاتفاقية لا يمكن بأي حال من الأحوال قبول أي تبرير بشأنها سواء كان التبرير ذا طابع سياسي أو فلسفي أو إيديولوجي أو عنصري أو ديني، كما أكدت ديباجة الاتفاقية على أن جميع الإجراءات التي تتخذ للوقاية من الإرهاب، أو لزجر الجرائم الإرهابية يجب أن تكون متماشية مع مقتضيات دولة القانون والقيم الديمقراطية ولحقوق الإنسان وللحريات الأساسية، إضافة إلى احترام مقتضيات القانون الدولي، بما في ذلك القانون الدولي الإنساني عندما يكون موجبا للتطبيق أي فيما لا علاقة بحالات النزاعات المسلحة.

هذا وتضيف الديباجة أن الوقاية من الإرهاب وقمعه يجب أن لا تضر بالمبادئ المقررة المتعلقة بحرية التعبير وبحرية الاجتماع" .

وتلزم الاتفاقية الدول الأعضاء عند وضع تدابير الوقاية من الإرهاب بكل أشكاله وصوره حتمية مسايرة المبادئ والقيم الديمقراطية التي تسير وفقهم دولة القانون وأحكام حقوق الإنسان المنصوص عنها في المواثيق الدولية والقانون الدولي، حيث لا تكون هناك انتهاكات خطيرة في هذا المجال[1].

ولم تتضمن الاتفاقية الأوربية للوقاية من الإرهاب تعريفا للإرهاب، ولا النص على الإرهاب الالكتروني لكنها نصت في المادة الأولى منها على أن الفعل الإرهابي هو ذلك السلوك المنصوص عنه في الاتفاقيات الدولية التي أبرمت بشأن مكافحة الإرهاب المنصوص عنها في ملحق الاتفاقية واعتبرت أن الأعمال الإرهابية هي أعمال تهدف إلى ترويع السكان بصورة خطرة أو تستهدف إرغام حكومة أو منظمة دولية على القيام بعمل أو الامتناع عن القيام بعمل، أو أنها تستهدف زعزعة أو تدمير المنشآت الأساسية السياسية أو الدستورية، الاقتصادية أو الاجتماعية لدولة من الدول أو

[1] ساعد الهام حورية، مرجع سابق، ص 108.

لمنظمة من المنظمات[1]، لم تتمكن هذه الاتفاقية من حل إشكالية مفهوم الإرهاب لكنها اعتمدت معيار الهدف محاولة إزالة اللبس القائم حول تعريفه.

استحدثت أحكام المواد من 5 إلى 7 من هذه الاتفاقية أفعال إجرامية الغرض منها منع انتشار الإرهاب ميزت بين المساهمة الأصلية والمساهمة التبعية، حيث يعتبر فاعل أصلي في مفهوم هذه الاتفاقية كل شخص ارتكب إحدى الجرائم المتعلقة بالتحريض على الإرهاب[2] والتجنيد في صفوف الجماعات الإرهابية[3]، وجميع أشكال التمويل بالسلاح أو أي مواد أخرى من شأنها السماح بانتعاش التنظيم الإجرامي.

واشتملت الاتفاقية أيضا على أحكام جزائية في مجال المساهمة التبعية وحددتها بأعمال الاشتراك في إتيان أي فعل من الأفعال الإرهابية والمنصوص عليها في الاتفاقية، كما نصت الاتفاقية على التنظيم وإعطاء الأوامر بغرض القيام بإحدى الأفعال المنصوص عليها في الاتفاقية، وكذلك جرمت الاتفاقية تسهيل مهمة الجماعات الإرهابية مع العلم بالغرض الذي تسعى إليه هذه الجماعات.

لم تكتف الاتفاقية على تجريم هذه الأفعال الإرهابية ولكنها ألزمت الدول الأعضاء على النص على تجريم هذه الأفعال ضمن تشريعاتها الداخلية، وترتيب ما يلزم من جزاءات بخصوصها، وضرورة التكفل بضحايا الإرهاب[4] ، وكذا النص على مسؤولية الشخص المعنوي مدنيا وجزائيا وحتى إداريا في حالة تورطه في إحدى الأفعال المشار إليها سابقا.

لمنع انتشار الإرهاب ألزمت الاتفاقية على الدول الأعضاء على ضرورة تكوين سلطات مختصة بقمع الإرهاب، وإشراك المؤسسات الحكومية في الوقاية من الإرهاب محاربته وخصت بالذكر التربية والتعليم والثقافة والإعلام والاتصال للدور الذي تلعبه هذه المؤسسات في التحسيس والتوعية بمخاطر الإرهاب والنتائج الوخيمة التي تنجم عن النشاط المكثف للتنظيمات الإرهابية، وذلك في إطار الاحترام التام لحقوق وحريات الأفراد، كما تطلب من الدول الأعضاء تبني سياسة وقائية تعتمد على التعاون بين السلطات المخول لها صلاحية قمع الجرائم الإرهابية، وذلك من خلال تبادل المعلومات فيما بينها

[1] من خلال هذا التعريف نلاحظ أن هذه الاتفاقية تشمل حتى الإرهاب الالكتروني فهو أيضا كغيره من أنواع الإرهاب الأخرى من نشر الفزع والخوف، وزعزعة وتدمير المنشآت...الخ ، وبالتالي يمكن القول أن هذه الاتفاقية جاءت عامة للوقاية من جميع أنواع وصور وأشكال الجريمة الإرهابية .

[2] المادة الخامسة من الاتفاقية الأوربية للوقاية من الإرهاب لسنة 2005.

[3] المادة السادسة من ذات الاتفاقية.

[4] المادة 13 من الاتفاقية الأوربية للوقاية من الإرهاب 2005.

وتكثيف الإجراءات الأمنية للحفاظ على حياة الأشخاص وحماية المؤسسات العامة والخاصة من الاعتداءات الإرهابية كما تنص الاتفاقية في ذات السياق على أن التسيير الناجح للازمات والتحكم فيها يكون بواسطة تكوين المختصين والتخطيط والتنسيق بين الجهات المخول لها ذلك[1] .

### ثالثا: إنشاء الاتحاد الأوربي لهيئات متخصصة في المجال القضائي والأمني.

في سبيل مكافحة الإرهاب بكل أنواعه استحدثت أوروبا هيئات لتجسيد التعاون الأمني والقضائي وهذا سعيا إلى توحيد الجهود وأهمية التعاون في هذا المجال، وهذا نظرا لخطورة الإرهاب على الأمن والسياسة والاقتصاد في أوروبا والعالم بأسره، لا سيما بعد ظهور الإرهاب الالكتروني الذي يعتبر أكثر أنواع الإرهاب شراسة، ومن اجل ذلك كان على الدول الأوربية التكتل والالتزام بأحكام ومبادئ نابعة من مقومات المجتمع الأوروبي من أجل إيجاد الحلول اللازمة لذلك، وفي هذا المجال قامت الدول الأوربية بتأسيس جهاز قضائي موحد كان أداة فعالة في معالجة القضايا الإرهابية، وتوحيد الجهود بين الدول الأوربية في مجال تنفيذ الإجراءات الجزائية خاصة بالنسبة للمساعدات القضائية كالقبض على المتهمين وتنفيذ الإنابات القضائية، وتسهيل عمليات الاتصال بين الأجهزة القضائية للدول الأوربية[2].

عملت الدول الأوربية جاهدة لمحاربة الجرائم الإرهابية التي شهدتها، حيث أدركت أنه من خلال الخسائر البشرية والمادية أن القضاء التقليدي لن يكون جديرا بمكافحة هذه الجريمة الخطيرة، فقامت بإنشاء هياكل قضائية مختصة بقضايا الإرهاب ومنها الإرهاب الالكتروني.

#### 01- تأسيس قضاء أوربي.

في سنة 2002 أنشأت الدول الأوربية قضاء أوربي أطلق عليه "Eurojust"، وأوكلت له مهمة مواجهة الجرائم الخطيرة بما فيها الإجرام المنظم والإرهاب، وبما أن جريمة الإرهاب الالكتروني شكل مستحدث من جرائم الإرهاب فان هذا القضاء مختص، كما يقدم هذا القضاء الدعم للسلطات القضائية في مجال العدالة الجزائية، وتتكون هذه الهيئة من 20 قاضي يكون لكل دولة عضو في الاتحاد تمثيل واحد، ومكنت هذه الهيئة الدول الأعضاء من تبادل المعلومات القضائية والتنسيق فيما بين السلطات

[1] المادة الثالثة من نفس الاتفاقية.

[2] ساعد الهام حورية، مرجع سابق، ص 112.

المختصة بإجراء التحقيقات والتحريات، بالإضافة إلى المشاركة في الندوات الدولية وحماية المعلومات من التسرب وتعمل هذه الهيئة بصفة وكيل الجمهورية أو قاضي[1].

### 02- إنشاء شبكة القضاء الأوروبي.

لتسهيل التعاون القضائي بين الدول الأوربية في مجال مكافحة الإرهاب والإجرام الخطير تم إنشاء شبكة القضاء الأوربي (R-J-E)، Réseau judiciaire Europeen، وذلك في 29 جوان 1998.

تعتبر هذه الهيئة وسيلة للدعم غير مباشر للمختصين في مجال جمع المعلومات الخاصة بالاتصالات والاستعلام حول الشبكات الإجرامية، وأداة دعم مباشرة للمساعدة القضائية الجزائية.

كما تمكن القضاء الأوربي من إبرام معاهدة تعاون وتنسيق مع المنظمة الدولية للشرطة الجنائية بتاريخ 09 جوان 2004، بغية تحسين إطار التعاون بينهما في مجال تبادل المعلومات والوصول إلى إنشاء شبكة أمن تختص بهذا المجال، نصت المعاهدة على ضرورة التنسيق الثنائي بين الفرق في مسائل التحقيق ووضع وثيقة تحرر فيها أهم التهديدات التي يمكن أن يشكلها الإجرام المنظم وجرائم الإرهاب جميعها مهما كان شكلها أو صورتها[2].

### 03- تعيين قضاة للاتصال أو التنسيق لتسهيل مجال التعاون القضائي.

تعمل الدول الأوربية عل تعيين قضاة لها في دول أخرى أطلق عليهم قضاة الاتصال أو التنسيق ويسمح هذا النظام بالاتصال بين القضاة في دول أخرى، ويكفل سرعة البت في طلبات المساعدة القضائية، وهو النموذج الذي طبقته فرنسا حيث قامت بتعيين عدة قضاة في دول أوروبا كإيطاليا واسبانيا يعملون كهمزة وصل بين هذه الدول الأوربية وفرنسا حيث يتولون تسهيل الإجراءات في مجال المتابعة الجزائية وتتم العملية باتصال قاضي في وزارة العدل للدولة المضيفة وتنحصر وظيفتهم في تقديم المساعدة من أجل صياغة طلبات المساعدة القضائية، والمشاركة في المفاوضات من أجل إبرام المعاهدات في هذا الإطار وتبادل المعلومات بشأن التشريعات والقضايا الهامة، وكذلك عقد دورات تدريبية[3].

---

[1] أمير فرج يوسف، الجريمة المنظمة عبر الوطنية، دار المطبوعات الجامعية ، الإسكندرية، 2008، ص 406.

[2] ساعد الهام حورية، مرجع سابق، ص 114.

[3] نفس المرجع ، ص 114.

### 04 – اتفاقية التعاون الأوروبي في مجال تنفيذ أوامر الاعتقال.

بعد أحداث 11 سبتمبر 2001 قامت الدول الأوربية باتخاذ آلية جديدة في مجال التعاون القضائي تخص تنفيذ أوامر الاعتقال، وفي هذا الشأن تم إبرام اتفاقية بين أعضاء الاتحاد الأوروبي أكد من خلالها الاتحاد أن الوصول إلى إبرام مثل هذا الاتفاق يعتبر نقطة تحول هامة في العلاقات بين الدول الأعضاء خاصة فيما يتعلق بطلبات التسليم التي أصبحت تتم بسهولة، وكانت ايطاليا الدولة الأخيرة التي طبقت هذا النظام في سنة 2005.

وبحلول سنة 2005 تم تسجيل 104 حالة تسليم ، وبعدما كانت عملية التسليم تستغرق على الأقل تسعة أشهر أصبحت تتم في 45 يوما فقط[1].

وتجدر الإشارة أن دول الاتحاد الأوروبي كانت سباقة بوضع أسس للتعاون الأمني بإنشاء آليات وأسس فعالة في الميدان الشرطي بالتنسيق مع الجهات الأمنية الأخرى، وقد اعتمدت الدول الأوروبية المتكتلة في منظمة الاتحاد الأوروبي على إبرام معاهدات فيما بينها تكون سندا لها في هذا الإطار.

ومن خلال الاتفاقيات التي أبرمها الاتحاد الأوروبي في مجال مكافحة الإرهاب سعت الدول الأعضاء إلى:

### 01– تأمين الحدود بحزام أمني مشدد.

وكان ذلك بموجب معاهدتي "شينغان" و" ماسترخت"، حيث تم السماح للمواطنين التنقل بسهولة وكذلك تعزيز أطر التعاون بين هذه الدول من أجل الحفاظ على الأمن والنظام العام واتخاذ تدابير جديدة لمواجهة التحديات الأمنية التي تواجه القارة الأوربية في مجال الجريمة المنظمة والجرائم الإرهابية، وتلخص هذه التدابير في حق مراقبة المشتبه فيهم عبر الحدود وملاحقة المجرمين.

وبموجب المادة 40 من الاتفاقية التنفيذية لمعاهدة "شينغان" تم السماح لأفراد الضبطية القضائية الحق في مراقبة المجرمين داخل إقليم دولة أخرى طرف في المعاهدة وفقا للشروط المنصوص عليها في الاتفاقية، وتختلف باختلاف الحالات، ففي الحالات العادية لا يسمح لأفراد الضبط القضائي الاستمرار بالمراقبة في دولة أخرى إلا بعد الحصول على إذن مسبق من الدولة المعنية، إلا أنه يمكن السماح بذلك في الأوضاع الاستعجالية، كما تسمح أيضا بنود الاتفاقية قيام رجال الأمن بإجراءات المعاينة والتفتيش ، وأخذ الصور الشمسية للمشتبه فيهم، وسماع الشهود وعدم المساس بحرية الأفراد.

[1] ساعد الهام حورية، مرجع سابق، ص 114.

كما تضمنت هذه الاتفاقيتين على حق متابعة المجرمين عبر الحدود وإقرار نظام "شينغان" لتسجيل وتبادل المعلومات الذي يعتبر قاعدة لتكنولوجيا المعلومات المتعلقة بالأشخاص المطلوب البحث عنهم ويربط المركز الرئيسي لهذه القاعدة بستراسبورغ بنظم المعلومات للدول الأعضاء، وفي كل الحالات يجب احترام الحريات الأساسية للأشخاص ومبدأ سيادة الدول.

### 02- توثيق الإجراءات الجمركية في حركة التنقل على مستوى القارة الأوروبية.

ويتم ذلك بواسطة آلية لتجسيد التعاون الشرطي[1] بين أعضاء القارة الأوروبية تعلقت بمراقبة حركة تنقل الأشخاص والأموال والبضائع عبر الحدود ووضع إجراءات يعتمد عليها في مجال الهجرة كما تم وضع الخطوط العريضة للإستراتيجية التي ستتبع اتجاه دول العالم الثالث وتوثيق التعاون الأمني والقضائي والجمركي بين الدول الأعضاء، بما يكفل مواجهة الإرهاب وعناصر الجريمة المنظمة النشيطة على مستوى القارة الأوروبية.

### 03- إنشاء جهاز شرطي أوروبي.

لطالما راود أوروبا حلم إنشاء جهاز شرطي أوروبي، حيث دعا المستشار الألماني "هيملوت كول" إلى إنشاء "انتربول أوروبي" بقصد مكافحة الجريمة المنظمة وجرائم المخدرات والجرائم الإرهابية وقد تم تكريس الفكرة في معاهدة الاتحاد الأوربي سنة 1992 من خلال ملحق المعاهدة حول التصريح المتعلق بالتعاون الشرطي .

ولقد استطاعت دول الاتحاد الأوروبي بفضل الجهود المبذولة في هذا الشأن من إنشاء جهاز الأوروبول أو الأيروبول سنة 1995، والذي تم تفعيله كوحدة للتعاون الأمني على مستوى القارة الأوروبية.

---

[1] نصت عليها اتفاقية ماسترخت سنة 1992 التي دخلت حيز التنفيذ سنة 1993، وتم الاتفاق عليها من قبل المجلس الأوروبي في مدينة ماسترخت الهولندية في ديسمبر 1991، ودخلت هذه المعاهدة، التي تم توقيعها في 7 فبراير 1992 في ماسترخت، حيز التنفيذ في الأول من نوفمبر 1993، ويرجع تأخر تطبيقها إلى تأخر قبول الدانماركيين للمعاهدة وشروطها وبسبب قضية دستورية ضدها أقيمت في ألمانيا، وقد أدخلت معاهدة الاتحاد الأوروبي عدة تغييرات على قوانين المجموعة الأوروبية وعلى قوانين المجموعة الأوروبية الذرية، التي كانتا تشكل نواة الاتحاد الأوروبي. شكلت أيضا المعاهدة أساس الدستور الأوروبي، الذي تم الاتفاق عليه لاحقا في عام 2004.

وكانت مهام الأوروبول تحليل المعلومات وتبادلها مع الدول الأعضاء، ولقد أثبت هذا الجهاز دوره القيم والفعال في مكافحة الجرائم الإرهابية من خلال التحقيق في 21 قضية إرهابية على مستوى الدول الأوروبية[1].

والأوروبول يعتمد في أداء مهامه على كفاءة وجدارة رجال الشرطة وعلى مساعدة الوحدة الوطنية فبموجب إنشاء جهاز الانتربول تعين كل دولة وحدة وطنية مكلفة بتنفيذ مهام جهاز الأوروبول كأداة اتصال بين جهاز الأوروبول والمصالح الوطنية المختصة.

العلاقة التي تربط الأوروبول والوحدة الوطنية القوانين الوطنية والدستورية للدولة، كما تمنح للوحدة الوطنية جميع الإمكانيات التي تمكنها من مباشرة مهامها.

وتقوم كل وحدة وطنية بتعيين ضابط واحد على الأقل يقوم بالاتصال مع جهاز الأوروبول فمهمة هؤلاء الضباط هي تمثيل مصالح الوحدات الوطنية أمام الجهاز، وكذلك المساهمة في تبادل المعلومات بين الوحدات الوطنية للأوروبول[2].

كما اعتمدت الدول الأوربية زيادة على ذلك ومن اجل لتنسيق فيما بينها على تعيين منسق أوروبي يعمل على توضيح الدور الذي يجب أن تعتمده أوروبا في مكافحة جميع جرائم الإرهاب مهما كان نوعها أو صورتها، مع ضرورة اتخاذ إستراتيجية للتعاون بين الدول الأعضاء، ودور المنسق فضلا عن ذلك الحث على سبل التعاون بين أعضاء المجموعة الدولية والعمل وفق نداءات متكررة بحتمية التنسيق، وتكثيف الجهود بين هذه الدول.

### 04- تأسيس مركز الموقف الموحد الأوربي.

يقصد بمركز الموقف الموحد تجمع الخبراء لتحليل التقديرات الاستخباراتية الذي يرفع تقريره إلى منسق الشؤون الخارجية والسياسة الأمنية في الاتحاد الأوروبي.

عمل الاتحاد الأوروبي على تأسيس خلية في بلجيكا تقوم باستقبال خبراء ومستشارين للإجابة على أسئلة الدول الأوربية في مجال التصدي لما يسمى ب"الدعاية الجهادية" وهذا بتاريخ 05 جانفي 2015 في الفترة التي تزايدت فيها عمليات التجنيد ضمن صفوف التنظيمات الإرهابية المستحدثة

[1] مختار حسين شبيلي، التعاون الدولي لمواجهة الجريمة المنظمة، جامعة نايف للعلوم الأمنية، الرياض، 2013، ص 248.

[2] ساعد الهام حورية، مرجع سابق، ص 117.

كمنظمة الدولة الإسلامية وذلك بواسطة استغلال الإرهابيين لشبكة الانترنت وتفشي جريمة الإرهاب الالكتروني في العالم بأسره لا في أوروبا فحسب.

ففي السنوات الأخيرة تمكنت التنظيمات الإرهابية من تجنيد حوالي ثلاثة آلاف أوروبي من دول الاتحاد الأوروبي بواسطة مواقع عبر شبكت الانترنت، مما أدى إلى تخوف أوروبا من قيامهم بعمليات إرهابية في أوروبا اثر عودتهم إليها، أو حتى وهم في أماكنهم .

من أجل ذلك تستعين الدول الأوربية بخبراء في الميدان لفهم أسباب وعوامل الانسياق في صفوف الجماعات الإرهابية الجديدة من أجل إيجاد الحلول المناسبة لمنع ذلك ولوقاية أوروبا من خطر وجودهم[1].

كما توصلت أوربا في هذا الإطار وفي سبيل مكافحة الإرهاب الالكتروني إلى إبرام اتفاقية سنة 2005 تلتزم بموجبها شركات الهاتف والانترنت الاحتفاظ بسجلات الاتصالات والرسائل النصية والبريد الالكتروني لأكثر من سنتين، والأخذ بجواز السفر البيومتري، مع اعتماد مشروع نيكسوس الذي يعتبر من أهم المشاريع التي اعتمدا الاتحاد الأوروبي في مكافحة الإرهاب الالكتروني[2] .

أما في أجندة الاتحاد الأوروبي للسنوات ما بين 2015 إلى غاية 2020 فثمة مجموعة أهداف تسعى إلى إعادة تصويب الأمن الداخلي وسط التركيز على سلسلة معطيات، منها مواصلة تطوير فاعلية نظام المعلومات "شينغان"، وتعزيز الإطار القضائي الجنائي، وتعزيز التعاون بين الأوروبول وباقي الأجهزة الأوروبية المخولة تقويم التهديدات، إضافة إلى تعزيز التبادل الاستخباراتي على المستويين الأوروبي والدولي فيما يتعلق بالأسلحة المحظورة.

كما أن المفوضية ستواصل العمل مع البرلمان الأوروبي والمجلس بهدف تبني قواعد مشتركة عن ملفات المسافرين، علما أن هذا النظام سيحسن القدرة على تفادي الجريمة المنظمة والإرهاب في عالم يتحرك فيه الأفراد بلا ضوابط وخاصة بعد تفشي الإرهاب الالكتروني واستغلال الإرهابيين لشبكة الانترنت أسوأ استغلال.

---

[1] ساعد الهام حورية، مرجع سابق، ص 118.

[2] ملف السلامة العامة والإرهاب، إصدارات الانتربول – التقرير السنوي لسنة 2009، متوافرة في الموقع: https://www.interpol.int

كما تم وضع صندوق للأمن الداخلي في أوروبا للفترة الممتدة بين 2014 إلى 2020 بميزانية قدرها 3.8 مليار أورو[1] .

## الفرع الثاني: جهود الحلف الأطلسي في مكافحة الإرهاب الالكتروني.

حصلت تطورات مهمة في هيكلية الحلف ووظائفه الجديدة بعد انتهاء الحرب الباردة فعلى مستوى المؤسسات السياسية للحلف، أنشئ مجلس تعاون شمال الأطلسي في العام 1991 الذي طوّر في العام 1997 إلى مجلس الشراكة الأوروبي– الأطلسي، لتكون مهمته تنظيم الأعباء والمسؤوليات بين أوروبا ومنطقة الأطلسي وتوزيعها، ولضبط احتمالات الصراعات والنزاعات داخلها، واحتوائها عبر تطوير آلية التعاون في جميع المجالات، سواء كانت أمنية أو سياسية أو عسكرية أو اقتصادية.

ومن المؤسسات السياسية التي تم إدخالها إلى الهيكلية السياسية للناتو أيضًا، برنامج الشراكة من أجل السلام، والمجلس المشترك الدائم للناتو وروسيا، وميثاق الناتو – أوكرانيا وتكشف هيكلية الحلف الجديدة ووظائفه أن الناتو أخذ يولي تنفيذ استراتيجيته في التوسع نحو الشرق اهتمامًا متزايدًا، من خلال التعاون مع مؤسسات عسكرية وسياسية خارج إطاره بعضها أوروبي مثل اتحاد غرب أوروبا وبعضها دولي مثل الأمم المتحدة.

وقد جرى التشديد على المفهوم الاستراتيجي الجديد لدور حلف شمال الأطلسي في أثناء قمة الحلف في واشنطن، التي عقدت في العام 1999 لمناسبة مرور خمسين عامًا على تأسيسه، وتم توسيع مهمات الناتو من حيث مصادر التهديد إلى درجة تتيح للحلف، نظريًا على الأقل، القدرة على التدخل خارج مسرح عملياته التقليدية وتحت عدة مسوغات، مثل مكافحة الإرهاب، ومنع انتشار أسلحة الدمار الشامل، وحماية حقوق الأقليات.

وبعد أحداث 11سبتمبر، أصبحت أفغانستان الدولة الأولى التي تشهد خروجًا لحلف الأطلسي على دوره ومهماته التي تمدّدت منذ تشكّله بعد نهاية الحرب العالمية الثانية، وفي سياق مهمات حلف شمال الأطلسي الجديدة، يحتوي الإعلان حول الإرهاب، الصادر في 2 أفريل 2004، سلسلة من الإجراءات والتدابير العملية الرامية إلى تحسين أعمال تبادل المعلومات بين أجهزة الاستخبارات

[1] كيف تكافح أوروبا الإرهاب... وماذا تتضمّن "أجندة" 2015؟، مقالة منشورة في موقع النهار: https://newspaper.annahar.com تاريخ الاطلاع 2018/07/11 على الساعة 15:33.

وبمناسبة انعقاد قمة حلف شمال الأطلسي في "ريغا" في كانون الأول 2006، أعاد "ناتو" تأكيد التزامه مكافحة الإرهاب بموجب القانون الدولي ومبادئ الأمم المتحدة.

كما بدأ العمل على إعداد حزمة من الإجراءات بعنوان "الدفاع ضد الإرهاب"[1]، لتطوير تكنولوجيات متقدّمة ترمي إلى مواجهة تهديد الإرهاب، مثل حماية القوات الحليفة من المتفجرات المرتجلة ومعدات إطلاق الصواريخ المحمولة لحماية الموانئ وغيرها من التدابير. وقد شجّعت دول الناتو على تطوير قدراتها في مكافحة الإرهاب، وخصوصًا تكثيف نشر المعلومات الاستخباراتية في إطار الحلف، ولاسيما تلك التي تعني مسارح العمليات.

وعن موقف الحلف الأطلسي من هجمات الإرهاب الالكتروني فقد جاء اهتمامه في شكل خطوات عملية تمثلت في نص الدليل السياسي الشامل لحلف الناتو الذي تبناه رؤساء دول وحكومات الحلف في نوفمبر من سنة 2006 على تعزيز القدرة على حماية أنظمة المعلومات ذات الأهمية الكبيرة بالنسبة للحلف ضد الهجمات على الانترنت .

كما أن الهجوم على "استونيا" أثار الجدل حول قدرة الحلف على التصدي لتلك الهجمات وإمكانية تطبيق المادة الخامسة من اتفاقية الحلف التي تقر بأن أي اعتداء على أحد أعضاء الحلف يمثل اعتداء على باقي دوله[2].

على الرغم من أن حلف الناتو اعتبر الهجوم الالكتروني لا يكون شبيها بعمل عسكري إلا إذا تم تحديد مسؤولية مرتكبيه ، فقد تبنى الحلف سياسة دفاعية في الفضاء الالكتروني فيما عرف ب:" a new policy on cyber defence"، وهذا إلى جانب أمن الطاقة في قمة بوخارست التي عقدت في

[1] إلياس أبو جودة، مرجع سابق، ص 10.

[2] تنص المادة 05 من اتفاقية حلف الشمال الأطلسي في 1949/04/04 بقولها:" يتفق الأطراف على أن أي هجوم أو عدوان مسلح ضد طرف منهم، أو عدة أطراف في أوروبا أو أمريكا الشمالية يعتبر عدوانا عليهم جميعا، وبناءا عليه فأنهم متفقون على أنه في حالة وقوع مثل هذا العدوان المسلح، فان على كل طرف منهم، تنفيذا لما جاء في المادة 51 من ميثاق الأمم المتحدة، عن حق الدفاع الذاتي عن أنفسهم، بشكل فردي أو جماعي، تقديم المساندة والعون للطرف أو الأطراف التي تتعرض للهجوم باتخاذ الإجراءات الذاتية بالتعاون مع الأطراف الأخرى دون تأخير بما في ذلك استخدام قوة السلاح التي يرى أنها لازمة لإعادة الأمن إلى منطقة شمال الأطلسي وتأكيده.

ويتم إبلاغ مجلس الأمن دون تأخير بكل هجوم وعدوان مسلح، وكل الإجراءات المضادة المتخذة اتجاهه ويتم وقف الإجراءات بمجرد اتخاذ مجلس الأمن للخطوات الضرورية لإعادة استقرار السلام والأمن الدوليين".

2008/04/04، وهي القمة التي شهدت مشاركة روسيا لأول مرة منذ تأسيس الحلف في إطار التعاون بين روسيا وحلف الناتو.

وقد وصف رئيس وحدة الدفاع الالكتروني التابع لحلف الناتو الإرهاب الالكتروني بأنه يفرض خطورة على الأمن القومي لا تقل عن خطورة هجمات الأسلحة الصاروخية وخاصة وأن هجمات الفضاء الالكتروني التي تستهدف البنية التحتية لا يمكن عمليا إيقافها، ومن ثم فان الدول بحاجة إلى تقوية نظمها المعلوماتية، لاسيما مع ما بات يمثله الإرهاب الالكتروني من مشكلة عالمية مستقبلية وأنشأ الحلف لهذا الغرض وحدة عمل في قمة بوخارست في أفريل 2008، خاصة بدراسة احتمال تعرض أعضائه لهجمات مماثلة لما تعرضت له استونيا.

تم تشكيل قيادة دفاع وفرق خاصة عبر الفضاء الالكتروني للتصدي لأي محاولة لشن هجمات الكترونية وبذلك بهدف التنسيق فيما بين دول الحلف في حال تعرض أحدها لهجمات الفضاء الالكتروني التعاون الأمني في حماية بنياتها الأساسية، هذا ويسعى الحلف إلى إنشاء مركز امتياز في الدفاع الالكتروني في "تالين" عاصمة استونيا أفتتح رسميا في سنة 2009[1] .

في ماي سنة 2008 وقعت سبعة دول من أعضاء حلف الناتو على وثيقة تقضي بإنشاء دفاع الكتروني مشترك CCO، مركز للخبرة والتدريب COE، في عاصمة استونيا ويهدف مركز الخبرة إلى البحث والتدريب والتطوير المشترك حول حرب الفضاء الالكتروني بالتعاون مع ألمانيا وايطاليا ولا تيفيا وليتونيا وسلوفاكيا واسبانيا واستونيا.

ويأتي اتفاق الدفاع المشترك بشان الهجمات الالكترونية بعد عام من تعرض استونيا إلى هجمات الكترونية كبيرة، كما دعا الحلف وزراء دفاعه إلى تطوير سياسات دفاعية خاصة بشان الهجمات الالكترونية في أكتوبر سنة 2007 .

وقد عرض اقتراح على دول الحلف لتشكيل مديرية أمن موحدة للحلف للتعامل مع الإرهاب والتحديات الأمنية التي يرون أن مصدرها الصين وإيران، ويمتد التعاون الأمني إلى الإرهابيين المطلوبين عبر ضفتي الأطلسي، والى وضع استراتيجيات مشتركة لمكافحة الإرهاب، وقد أطلق على البرنامج اسم "خادم في السماء"، وتم تأكيد أنه لا يمكن للحف الأطلسي والاتحاد الأوروبي ولا لأي دولة التعامل مع التهديدات الأمنية الجديدة بصورة منفردة فيما سيستغرق تطوير مؤسسات أمنية جديدة

[1] Nick Heath,Nato- Cyber terrorism as dangerous as missile attack: http//software.silicon.com/security/0.39024655.39170300.00.htm .

وقتا طويلا، وتم تبني تلك الدعوة عمليا في أوائل سنة 2008 بإنشاء سلطة إدارة الدفاع الالكتروني التي يكون من مهامها إدارة عملية الدفاع في مواجهة تلك الهجمات من خلال الاتصالات ونظم المعلومات التابعة للحلف العمل على دعم حلفاء الحلف في مواجهة تلك التهديدات التي تشكلها تلك الهجمات[1].

يسعى حلف الناتو إلى تبادل المعلومات على مستوى دوله، ومن أجل وجود آلية للإنذار المبكر حول أي نشاط مريب، والكشف عن أي هجوم معلوماتي محتمل، وبالفعل بدأت بعض الدول الأعضاء في الحلف إلى اتخاذ إجراءات لحماية نفسها من تهديدات عصر الانترنت بإنشاء فرق وطنية لطوارئ الكمبيوتر، وجاءت هذه الجهود بالتعاون مع الاتحاد الأوروبي في سبيل الحد من تأثير هجمات الإرهاب الالكتروني في المدى القريب إلى الدرجة التي إذا تم اكتشاف هجوم مثلا على موقع "تشيكي" على الانترنت بواسطة مستخدم من شبكة فرنسية، فانه يمكن لفرق طوارئ الكمبيوتر التشيكية أن تطلب من نظيرتها الفرنسية قطع قنوات الاتصال المستخدمة في الهجمات، وهذا ما دفع حلف الناتو لتشكيل فرق خاصة مكلفة بالتصدي لأي محاولة لشن هجمات الكترونية عبر الانترنت، وقد جاء هذا بعد حادثة استونيا في سنة 2007، التي تلقت دعم من الولايات المتحدة الأمريكية وألمانيا ورومانيا وايطاليا واسبانيا، ومن أجل التعامل مع عواقب الهجمات الالكترونية شكل الحلف فرقا جاهزة للتدخل في غضون أربع وعشرون ساعة في الدول المستهدفة كتلك التي سبق إنشاؤها من طرف الحلف للرد على هجمات كيميائية أو بيولوجية أو إشعاعية محتملة.

ودخل الفضاء الالكتروني ضمن إستراتيجية الحلف الدفاعية ووضع الأمن الالكتروني ضمن التهديدات الجديدة لدول الحلف، وقد تطور موقف الحلف من الهجمات الالكترونية وهذا لتزايد الإحساس بتصاعد الخطر على الدول الأعضاء أو على النطاق العالمي.

في مارس 2013 برز تغيير في موقف حلف الناتو من الهجمات الالكترونية واعتبر أن استخدام فيروس "ستاكس نت" على إيران سنة 2010 وما تلاها والمسؤول عنها إسرائيل والولايات المتحدة الأمريكية يعد عملا من أعمال القوة، وذلك وفقا لما أطلق عليه دليل تالين عاصمة استونيا للقانون الدولي للتطبيق على الحرب الالكترونية، وقد جاء ذلك بتكليف من منظمة حلف الشمال الأطلسي

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 387.

وبالتعاون مع مركز التميز للدفاع الالكتروني في استونيا وتم الإقرار بأن الأفعال التي تقتل أو تجرح الأشخاص أو تدمر أو تلحق الضرر بالكائنات هي أفعال تعبر عن استخدام القوة بشكل لا لبس فيه[1]

## الفرع الثالث: جهود المنظمات الإقليمية المتخصصة في مكافحة الإرهاب الالكتروني.

سيتم في هذا العنصر معالجة دور منظمتين إقليميتين متخصصتين في مجال مكافحة الإرهاب الالكتروني هما الإتحاد الدولي للاتصالات، والمنظمة العالمية للملكية الفكرية حيث أن هاتين المنظمتين نشأتا على المستوى الإقليمي إلا انه ما لبثت كل منظمة منهما إلا واكتسبت طابع العالمية نظرا للدور المهم والفعال الذي تقوم به كل منظمة في مجال تكنولوجيا المعلومات التي أصبحت مطمعا للجماعات الإرهابية تستغلها لتحقيق أهدافها الإرهابية بشكل أبشع وأشرس وبتكاليف اقل وبخطورة اقل بالنسبة للإرهابيين.

### أولا: الإتحاد الدولي للاتصالات.

نشأ الإتحاد الدولي للاتصالات بمقتضى اتفاقية باريس عام 1865 تحت اسم "إتحاد التلغراف الدولي" ثم عدل الاسم ليصبح "الإتحاد الدولي للاتصالات السلكية واللاسلكية".

في سنة 1947 انضم الإتحاد الدولي للاتصالات إلى هيئة الأمم المتحدة وصار إحدى الوكالات المتخصصة في عمل الاتصالات المنطوية تحت مظلة الأمم المتحدة فأصبح بمثابة ملتقى دولي رئيس لهذه الأنشطة ، يضم في عضويته 482 عضوا من الشركات العلمية والصناعية العاملة بالقطاعين العام والخاص[2]

ومن المهام التي يضطلع هذا الإتحاد تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية.

[1] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 388.

[2] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، مرجع سابق، ص 25 .

كما يقوم الإتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجمع المعلومات ونشرها[1]، وهذا من أجل بناء قدرات الدول الأعضاء وخاصة الدول النامية منها لتنسيق الاستراتيجيات الوطنية وحماية البني التحتية للشبكات ضد المخاطر من خلال التوعية والتقييم الذاتي وبناء القدرات، وتوسيع نطاق المراقبة والإنذار وقدرات الاستجابة للحوادث للدول والجهات المعنية .

هذا ويعمل الإتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على وضع المعايير المتعلقة بالأمن المعلوماتي، إذ يقوم الإتحاد، بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات، بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات.

تجدر الإشارة إلى أنه تم تعاون الإتحاد الدولي مع مجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي .

وفي مساعي شاملة حول التعاون الإقليمي والدولي، تم في المؤتمر الإقليمي حول الأمن الإلكتروني بالتعاون مع الإتحاد الدولي للاتصال في قطر في شباط من سنة 2008 دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تُعَد بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا المعلومات والاتصال[2]

من جهة ثانية، طالبت القمة العالمية لمجتمع المعلومات في تونس في نوفمبر 2005 بأن ينسق الإتحاد الدولي للاتصالات آلية لبناء الثقة والأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات عبر إطلاق برنامج الأمن الإلكتروني العالمي وهو إطار أعدَّه الإتحاد الدولي للاتصالات بهدف اقتراح إستراتيجيات للتوصل إلى حلول لتعزيز الثقة والأمن في مجتمع المعلومات.

وتم لهذا الغرض تعيين فريق خبراء لإسداء المشورة إلى الأمين العام للإتحاد، بشأن المسائل المعقدة التي تكتنف موضوع الأمن السيبراني.

---

[1] خليل حسين، التنظيم الدولي– النظرية العامة والمنظمات العالمية، دار المنهل اللبناني، بيروت، 2010، ص 455.

[2] الإعلان الختامي للمؤتمر الإقليمي حول الأمن المعلوماتي في قطر، متوافر على الرابط :
http://www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf تاريخ الاطلاع 2018/07/12 على الساعة 00:07.

فريق الخبراء رفيع المستوى ويتألف من متخصصين مرموقين عالميًّا في مجال الأمن السيبراني ومستمدين من خلفية واسعة النطاق تمثل صانعي السياسات، الحكومات، الأوساط الأكاديمية، القطاع الخاص.

وسيقوم الفريق بصياغة المقترحات التي ستُقدَّم إلى الأمين العام للإتحاد بشأن الاستراتيجيات طويلة الأجل لتعزيز الأمن السيبراني في خمسة مجالات هي كالآتي[1] :

- في المجال القانوني ، يتم إسداء المشورة بشأن كيفية التعامل مع الأنشطة الإجرامية التي تُرتكب عبر شبكات تكنولوجيا المعلومات والاتصالات من خلال وضع تشريعات بطريقة متوافقة دوليًا.
- وفي مجال "التدابير التقنية والإجرائية" فيتم التركيز على التدابير الرئيسة الرامية إلى معالجة مواطن الضعف في منتجات البرمجيات، بما في ذلك خطط الاعتماد والبروتوكولات والمعايير.

وتضع "الهياكل التنظيمية" إطار العمل وإستراتيجيات الاستجابة، فيما يتعلق بمنع الهجمات السيبرانية وتتبُّعها والردِّ عليها وإدارة الأزمات المتعلقة بها. بما في ذلك حماية أنظمة البنية التحتية الحرجة للمعلومات.

ويركز مجال "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات من أجل زيادة الوعي ونقل الخبرة المتخصصة، تعزيز الأمن المعلوماتي في إطار برنامج السياسات العامة الوطنية.

ويهدف مجال "التعاون الدولي" إلى وضع إستراتيجية للتعاون والحوار والتنسيق على الصعيد الدولي في مجال التصدي للأخطار الإلكترونية[2].

مما تقدم يتضح أن انخراط الاتحاد الدولي للاتصالات السلكية واللاسلكية في التفاصيل التقنية غير السياسية لمساعدة الدول والمنظمات والجهات المرتبطة بهذا الاتحاد في تهيئة وتطوير بينة المعلومات واستخداماتها المختلفة وتعزيز قدراتها في مجال أمن المعلومات لمواجهة الأخطار التي

[1] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، مرجع سابق، ص 26.

[2] التقرير السنوي للاتحاد الدولي للاتصالات السلكية واللاسلكية لسنة 2007، متوافرة في الرابط: https://www.mpttn.gov.dz/sites/.../Decret%20pres%20n°07-377.pdf، تاريخ الاطلاع: 2018/07/16 على الساعة: 00:26 .

تخلفها محاولات إساءة استغلال هذه التقنيات من قبل بعض الجهات الإرهابية، فالإرهاب الالكتروني أصبح أخطر آفة تهدد العالم بأسره .

## ثانيا : المنظمة العالمية للملكية الفكرية.

المنظمة العالمية للملكية الفكرية، منظمة دولية تابعة للأمم المتحدة تعنى بالتشريع وتوفير المعلومة وتنسيق التعاون الدولي في مجال الملكية الفكرية، وتهدف المنظمة إلى إرساء نظام فعال وقادر على حماية حقوق الملكية الفكرية (حقوق المؤلف– وبراءات الاختراع– والتصاميم الصناعية والعلامات التجارية ) من أجل تحفيز الإبداع والابتكار عبر العالم.

تأسست المنظمة العالمية للملكية الفكرية بمقتضى اتفاقية دولية وُقعَت في استوكهلم يوم 14 يوليو 1967 ودخلت حيز التنفيذ عام 1970 وعدّلت عام 1979.

وقد حلت المنظمة مكان المكاتب الدولية المتحدة لحماية الملكية الفكرية التي أسست عام 1893 وانضمت إلى أسرة منظمات الأمم المتحدة عام 1974 لتصبح بذلك وكالة أممية متخصصة، يبلغ عدد أعضاء المنظمة حاليا 188 بلدا.

واختارت المنظمة تاريخ 26 أفريل من كل سنة يوماً عالميا للملكية الفكرية، وهو اليوم الذي دخلت فيه اتفاقية الاتفاقية الدولية التي وقعت في استوكهلم حيز التنفيذ عام 1970.

وتشير الملكية الفكرية إلى إبداعات العقل من اختراعات ومصنفات أدبية وفنية وتصاميم وشعارات وأسماء وصور مستخدمة في التجارة[1].

كما أن الملكية الفكرية محمية قانونا بحقوق منها مثلا براءات الاختراع، وحقوق المؤلف والعلامات التجارية التي تمكّن الأشخاص من كسب الاعتراف، أو فائدة مالية من ابتكارهم أو اختراعهم.

ويرمي نظام الملكية الفكرية، من خلال إرساء توازن سليم بين مصالح المبتكرين ومصالح الجمهور العام، إلى إتاحة بيئة تساعد على ازدهار الإبداع والابتكار .

[1] المنظمة العالمية للملكية الفكرية، مقالة منشورة على موقع الجزيرة :http://www.aljazeera.net تاريخ الاطلاع 2018/07/12 على الساعة 01:47.

تؤكد المنظمة العالمية للملكية الفكرية أن حماية الملكية الفكرية والابتكار هما أمران متلازمان حيث لا سبيل إلى تحفيز الناس على الإبداع والابتكار دون حماية حقوقهم الفكرية، ولا يمكن الدفع بالشركات إلى الاستثمار في البحث والتطوير دون حماية ابتكاراتها من أن تُنتَهك من الآخرين.

وترى المنظمة أن الطريق نحو الإبداع والابتكار وتطوير الحلول الجديدة يمر حتما عبر إرساء منظومة قانونية عالمية تضمن حماية حقوق الملكية الفكرية من أي انتهاك، بما يعود بالمنفعة على الجميع، فمن جهة ينتفع ذوو الحقوق بثمار منجزاتهم، ومن جهة أخرى تنتفع المجتمعات من إبداعاتهم وابتكاراتهم.

وتعمل المنظمة على توحيد القوانين الوطنية في مجال حماية الملكية الفكرية والتنسيق بين البلدان الأعضاء في هذا المجال.

كما تتوفر المنظمة على مركز للتحكيم والوساطة يُعهَد إليه بمهمة تسوية المنازعات الدولية المتعلقة بالملكية الفكرية بالرجوع إلى هيئة محايدة من خبراء قانونيين دوليين متخصصين في هذا المجال وبالتالي تمكين المتنازعين من تجنب اللجوء إلى المحاكم وتعقيدات مسار التقاضي أمامها.

تسعى هذه المنظمة إلى تحقيق أهداف إستراتيجية اعتمدتها الدول الأعضاء في ديسمبر 2008 وهي[1]:

- ضمان تطور متوازن للإطار التشريعي والمعايير الدولية بشأن الملكية الفكرية.
- تقديم خدمات عالمية وبجودة عالية في مجال الملكية الفكرية.
- تسهيل الانتفاع بالملكية الفكرية في سبيل التنمية.
- تنسيق البنية التحتية العالمية للملكية الفكرية وتطويرها.
- جعل المنظمة مرجعا عالميا ومصدرا للمعلومات والدراسات في ما يخص الملكية الفكرية.
- التعاون الدولي على إذكاء الاحترام للملكية الفكرية.
- تناول مسائل الملكية الفكرية في علاقتها بقضايا السياسات العامة العالمية.

[1] طارق عزت رخا ، المنظمات الدولية المعاصرة ، دار النهضة العربية ، القاهرة ، 2006 ، ص 214.

– وضع آلية تواصل متجاوب بين المنظمة والدول الأعضاء وجميع أصحاب المصالح.

– إرساء بنية دعم إداري ومالي فعالة لتمكين المنظمة من تنفيذ برامجها.

تتألف البنية الهيكلية للمنظمة أساسا من سبعة قطاعات، يرأس كل منها مسؤول برتبة نائب مدير عام أو مساعد مدير عام تحت القيادة العامة للمدير العام، وتتألف القطاعات من أقسام ويرأسها مديرون، وتتولى مسؤولية الاضطلاع بجميع الأنشطة اللازمة لتنفيذ البرامج وتحقيق الأهداف التي توافقت عليها الدول الأعضاء.

ويختص كل قطاع من هذه القطاعات السبعة بمجال اشتغال محدد، وهي كالتالي: قطاع البراءات والتكنولوجيا، وقطاع العلامات والتصاميم، وقطاع الثقافة والصناعات الإبداعية وقطاع التنمية، وقطاع البنية التحتية العالمية، وقطاع القضايا العالمية، وقطاع الإدارة والتسيير.

كما تتوفر المنظمة على أقسام أخرى تتبع مباشرة للمدير العام، وهي: قسم الموارد البشرية، وقسم الاستشارات القانونية، وقسم البلدان المتقدمة والبلدان في طور الانتقال، وقسم الرقابة الداخلية، وقسم الدراسات الاقتصادية والإحصائيات، ومكتب الأخلاقيات.

وتتوفر المنظمة على خمسة مكاتب خارجية توجد في المدن التالية: طوكيو وبكين وسنغافورة وريو دي جانيرو وموسكو[1].

وبالرجوع إلى اتفاقية إنشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها "المصنفات الأدبية والفنية والعلمية والاختراعات" ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عددا من الخبراء بهدف حماية برامج الحاسب الآلي وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب ساد الاتجاه لدى أغلب الدول إلى خضوع برامج الحاسوب لقوانين حماية حق المؤلف[2] .

وقد جاءت منظمة التجارة العالمية عام 1994 لتؤيد هذا التوجه أي حماية حق المؤلف وعدم السماح بالتلاعب في مؤلفاته من خلال الحاسب الآلي أو بث أفكار إرهابية من خلال هذه المؤلفـــات

[1] طارق عزت رخا ، مرجع سابق، ص 214.

[2] نفس المرجع، ص 214.

مما يزيد من انتشار الأفكار الإرهابية ويكثر عدد المؤيدين والمناصرين للتنظيمات الإرهابية، وتستكمل طريقه من خلال إبرام اتفاقية التربس المتعلقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما تفرضه من التزامات على الدول الأعضاء لفرض إجراءات تنفيذية وعقوبات جنائية لمواجهة أي اعتداء على حق المؤلف وخاصة القرصنة[1].

وعموما وفي إطار الجهود الأوربية في مكافحة جريمة الإرهاب الالكتروني تمتلك أوربا حاليا شبكة خاصة تسمى "الوكالة الأوربية لأمن المعلوماتية"ENISA" "The European and Information Security Agency"، ومقرها أثينا باليونان، وهي مكلفة بمراقبة القرصنة الالكترونية داخل المجال الأمني الأوروبي، وكانت المملكة المتحدة قد اقترحت قيام منظمة دولية للأمن تحت اسم"world security organization" "WSO"، تعنى بمكافحة هجمات الفضاء الالكتروني وتوفير الأمن للمستخدمين والحكومات، وذلك في سياق الجهود الدولية المبذولة في مواجهة الأخطار التي تأتي من مجالات الجو والبحر والفضاء.

وتم عقد اجتماع كان محل اهتمام رجال الأعمال والقطاع الخاص، وأجهزة الاستخبارات والشركات العاملة في تكنولوجيا المعلومات والأكاديميين السياسيين، وذلك بهدف إطلاق مبادرة عالية أقوى من الانتربول[2] .

## المبحث الثاني: الدور العربي في مكافحة الإرهاب الالكتروني.

عانت الدول العربية والإسلامية من جرائم الإرهاب، بل ولقد عرفت جميع صورها ومؤخرا بدأت الدول العربية من الإرهاب الالكتروني مما ألحق بها خسائر بشرية ومادية فادحة مما أدى إلى إشاعة الخوف والفزع وسط المجتمع المدني، فأثر ذلك سلبا على السير العادي للحياة، الأمر الذي دعا الدول العربية إلى تكثيف الجهود فيما بينها من اجل مكافحة هذه الظاهرة البشعة والخطيرة وهذا عن طريق منظماتها والهيئات التابعة لها والتي تأتي على رأسهم جامعة الدول العربية والتي كان لها الدور الأكبر في وضح الخطط والاستراتيجيات لمكافحة جميع صور الإرهاب التي من ضمنها جريمة الإرهاب الالكتروني، فيعود الفضل لها في وضع الآليات التشريعية والعملية جمعت بين مجموعة الدول العربية

[1] سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، مرجع سابق، ص 27.

[2] عادل صادق، (استخدام الإرهاب الالكتروني في الصراع الدولي)، مرجع سابق، ص 377.

والإسلامية فكانت الاتفاقيات التي أبرمتها مسايرة للاتفاقيات الأممية والدولية والإجراءات العملياتية التي تمت في صياغتها على مستوى المنظمة الدولية للشرطة الجنائية.

فبسبب تفاقم الظاهرة الإرهابية في العصر الحاضر، وأمام ثورة المعلومات التي ساهمت في سرعة الحركة والاتصال وابتكار أساليب جديدة في التخطيط للعمليات الإرهابية وتنفيذها ومن ذلك أصبحت الوقاية من الإرهاب ومحاربته مهمة غير يسيرة تتطلب تظافر جهود جميع الدول العربية للقضاء على هذه الظاهرة من خلال تعاون دولي فعال تسخر له جميع الإمكانيات اللازمة على جميع المستويات القانونية والقضائية والأمنية والاقتصادية والاجتماعية والتربوية والإعلامية وغيرها.

وتمثل جامعة الدول العربية النموذج الكامل في مجال التعاون الإقليمي لمكافحة الإرهاب بمختلف أشكاله ومظاهره وخاصة الإرهاب الالكتروني والوقاية منه، سواء من حيث الإطار القانوني لهذا التعاون العربي والمتمثل في الاستراتيجيات والاتفاقيات العربية والقوانين النموذجية، أو من حيث المؤسسات والأجهزة التي يتم من خلالها هذا التعاون، وفي مقدمتها مجلس وزراء الداخلية العرب وأجهزته، ومجلس وزراء العدل العرب، وفريق الخبراء العرب المعني بمكافحة الإرهاب على اعتبارها نقطة اتصال مع لجان مجلس الأمن المعنية بمكافحة الإرهاب.

تأسست جامعة الدول العربية كمنظمة إقليمية عقب الحرب العالمية الثانية، كرد فعل ضد رغبة الحلفاء في تقسيم العالم إلى مناطق نفوذ في مؤتمرات طهران، في ظل هذه الظروف وبعد توقيع بروتوكول لسكندرية سنة 1944 نشأت جامعة الدول العربية[1] التي أخذت على عاتقها الحفاظ على كيان ووحدة الشعب العربي المسلم، وعلى حق كل الشعوب العربية في تقرير مصيرها، واتخذت القاهرة مقرا لها.

جامعة الدول العربية اهتمت منذ نشأتها بمجال السلم والأمن في العالم العربي والدفاع عن حقوق الشعوب المظلومة، وحماية المقومات العربية، وقد اعتبرت هذه المنظمة الإقليمية الإرهاب الذي اجتاح معظم الدول العربية والإسلامية بكل صوره وأنواعه خطر كبير على المقومات العربية والدعائم التي تحاول الجامعة المحافظة عليها، وكذلك اعتبرت الإرهاب عائقا أمام تقدم ورقي الشعوب العربية والإسلامية.

[1] ساعد الهام حورية، مرجع سابق، ص 119.

إن المتتبع لجهود جامعة الدول العربية في مكافحة الإرهاب تأخرت نوعا ما حتى سنة 1993 عندما ناقش مجلس وزراء الإعلام العرب قضية الإرهاب وقرر وضع آليات وخطة عمل لمواجهته في دورته السادسة والعشرون التي عقدت في القاهرة.

وفي يناير سنة 1997 اعتمد مجلس وزراء الداخلية العرب في دورة انعقاده الرابع عشر إستراتيجية عربية لمكافحة الإرهاب تهدف إلى توفير أمن المواطن العربي وضمان سلامته وحريته وحقوقه، وفي أفريل سنة 1998 ، وفي دورة انعقاد خاص اعتمد مجلسا وزراء الداخلية العرب ووزراء العدل العرب الاتفاقية العربية لمكافحة الإرهاب[1]، وكذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والموقعة في القاهرة في 2010/12/21 .

ومما سبق سوف نتعرض إلى أهم جهود جامعة الدول العربية في مكافحة الإرهاب الالكتروني من خلال المطلبين، حيث خصص المطلب الأول إلى المجالس التابعة لجامعة الدول العربية ومن خلال هذا المطلب نتعرض إلى جهود هذه المجالس في مجال مكافحة الإرهاب الالكتروني، وأما المطلب الثاني فقد خصص إلى نتائج جهود جامعة الدول العربية في مكافحة الإرهاب الالكتروني.

## المطلب الأول: المجالس التابعة لجامعة الدول العربية.

يقوم التعاون العربي في مجال مكافحة جرائم الإرهاب في إطار جامعة الدول العربية على ثلاث وجهات رئيسية وهي: وزراء الداخلية العرب– وزراء الإعلام العرب– وزراء العدل العرب، وأما الوجهة الرابعة فهي حلقة الاتصال بين المجالس الثلاثة التابعة لجامعة الدول العربية وهي فريق الخبراء العرب المعني بمكافحة الإرهاب.

### الفرع الأول: دور مجلس وزراء الداخلية العرب في مكافحة الإرهاب الالكتروني.

يعتبر مجلس وزراء الداخلية العرب هيئة فعالة على مستوى جامعة الدول العربية ويعود إليه الفضل في دراسة مختلف العراقيل التي تعوق مسار الدول العربية في العديد من الميادين من بينها القضايا الأمنية التي أهمها الإرهاب عموما والإرهاب الالكتروني خاصة .

[1] محمد فتحي عيد، واقع الإرهاب في الوطن العربي، أكاديمية نايف للعلوم الأمنية، الرياض، 1999، ص 178.

ويعمل المجلس بالتنسيق مع هيئات الجامعة كالمكتب الدائم لشؤون المخدرات، المنظمة العربية للدفاع الاجتماعي ضد الجريمة، وهيئة مؤتمرات قادة الشرطة والأمن العرب التابعة لمجلس وزراء الداخلية العرب التي اتخذت على عاتقها دراسة موضوع الجريمة بمختلف أشكالها، وفي مجال الإرهاب أخذ المجلس على عاتقه ضرورة إيجاد الآليات الردعية والوقائية للقضاء عليه مهما كانت صورته وشكله[1].

في بادئ الأمر لم يعن مجلس وزراء الداخلية العرب بمحاربة الإرهاب الالكتروني، بل عمد إلى السعي من اجل تطويق الظاهرة الإرهابية في صورتها التقليدية، واتخاذ إجراءات عديدة متنوعة تجسدت في عقد المؤتمرات والاجتماعات وإبرام الاتفاقيات ووضع الاستراتيجيات والخطط المرحلية والنموذجية والقوانين الاسترشادية وقواعد المعلومات المتعلقة بالجرائم الإرهابية، كما حرص المجلس على تعزيز التعاون مع المنظمات والهيئات العربية والدولية المعنية بمكافحة الإرهاب.

وتتجسد جهود مجلس وزراء الداخلية العرب من خلال مايلي:

### أولا: عقد المؤتمرات والاجتماعات .

دعا مجلس وزراء الداخلية العرب الدول الأعضاء إلى عقد مؤتمر سنوي المسؤولين عن مكافحة الإرهاب سنة 1998 من اجل الاتفاق على خطة عمل لبعث مجال التعاون الأمني عن طريق تبادل التجارب والخبرات بين الدول العربية، حيث يكون هذا المؤتمر فرصة لدراسة مختلف الظواهر السلبية في المجتمعات العربية من مختلف جوانبها، وكانت هناك دعوة موجهة للدول الأعضاء لعقد اجتماعات دورية على مستوى الأمانة العامة للمجلس في هذا المجال تم عقد اجتماع سنوي للجنة المختصة بالجرائم المستحدثة، حيث يوجد في الوقت الحالي على مستوى الأمانة العامة لمجلس وزراء الداخلية لجنة خاصة بدراسة الظواهر الإجرامية المستحدثة منها الإرهاب الالكتروني وغيره من صور الإرهاب المستحدثة[2].

[1] حسنين المحمدي البوادي، مرجع سابق، ص 163.

[2] ساعد الهام حورية، مرجع سابق، ص 126.

وقبل إقرار عقد هذه المؤتمرات كانت الأمانة العامة قد خصصت الاجتماع الثالث للجنة الجرائم الإرهابية المستجدة سنة 1995، كما خصصت الاجتماع السادس لهذه اللجنة عام 1998 لجرائم العنف في صورها الحديثة والسبل الكفيلة بمواجهتها.

وقبل ذلك كان الاجتماع الأول لهذه اللجنة عام 1987، وقد تناول مكافحة الجرائم المنظمة قبل أن يحل موضوع الإرهاب محلها في الاجتماعات اللاحقة.

### ثانيا: إعداد مدونات والاستراتيجيات والخطط المرحلية.

وضع مجلس وزراء الداخلية العرب مدونة قواعد سلوك للدول الأعضاء من أجل مكافحة الإرهاب سنة 1996، تتعهد من خلالها الدول الأعضاء بعدم القيام أو الشروع أو الاشتراك في أية عملية إرهابية والحيلولة دون اتخاذ أراضيها مسرحا للتخطيط أو تنفيذ تلك الأعمال، كما يحظر على أية دولة عضو بموجب هذه المدونة استقبال أو إيواء أو تدريب أو تسليح أو تمويل عناصر الإرهاب والتخريب، بالإضافة إلى تبادل المعلومات بين الدول الأعضاء في مجال التحري والقبض على الهاربين أو المحكوم عليهم في جرائم إرهابية وتتعهد من خلالها الدول الأعضاء بتضييق الخناق على الجماعات الإرهابية، وتعمل على عدم جعل أراضيها مسرحا للعمليات الإرهابي، ويحظر على الدول الأعضاء بموجب هذه المدونة استقبال أو إيواء أو تدريب أو تسليح أو تمويل عناصر الإرهاب والتخريب[1].

في ذات الشأن أجمعت الدول الأعضاء ضمن هذه المدونة على تقديم المساعدات المتبادلة بينها في مجال إجراءات التحري والقبض على الأشخاص الهاربين المتهمين والمحكوم عليهم في الجرائم الإرهابية وعلى حماية الحدود وسد منافذ مرور الإرهابيين إليها ومنع مرور الأسلحة والذخائر والمتفجرات لأغراض غير مشروعة.

كما أعدت الأمانة العامة للمجلس عدة خطط نموذجية لمحاربة بعض صور الإرهاب منها الإرهاب الالكتروني، ففي سنة 2001 تم إقرار مشروع لمكافحة جرائم خطف الطائرات وتحرير الرهائن ومداهمة عصابات الإجرام المنظم.

[1] ساعد الهام حورية، مرجع سابق، ص 126.

في سنة 2002 بادر المجلس بوضع خطتين نموذجيتين، تضمنت الأولى القواعد القانونية للجريمة الإرهابية، والثانية كيفية التصدي الميداني لهذه الجريمة، وفي نفس السنة تم اتخاذ تدابير لحماية وسائل النقل الجوي والبحري والمنشآت التابعة لهما من مختلف الاعتداءات الإرهابية، وذلك بوضع خطة عمل لسنة 2003[1].

ويمكن أن نوجز أهم النقاط التي دعت إليها تلك المدونة بما يلي[2]:

- ضرورة مكافحة جرائم الإرهاب وفقا لأحكام الشريعة الإسلامية والمواثيق العربية والدولية.
- وجوب اتخاذ تدابير لمكافحة الإرهاب على الأصعدة الوطنية والعربية والدولية في إطار التعاون العربي والتعاون العربي الدولي.
- تؤكد المدونة على ضرورة التمييز بين الإرهاب والنضال المشروع للشعوب من أجل تقرير المصير والتحرر الوطني من جميع أشكال الاحتلال والاستعمار والتمييز العنصري.
- وجوب اتخاذ تدابير فعالة وفقا للقانون الدولي وميثاق جامعة الدول العربية ومقررات مجلس وزراء الداخلية العرب، لمكافحة الإرهاب.
- كما أجمعت الدول على أهمية وضرورة تقديم المساعدة المتبادلة في مجالات إجراءات التحري والقبض على الأشخاص الهاربين المتهمين، أو المحكوم عليهم بجرائم إرهابية.

## ثالثا: الاهتمام بالجانب التوعية الأمنية والتحسيس بخطورة الإرهاب.

أولى مجلس وزراء الداخلية العرب أهمية كبيرة للإطار التحسيسي والتوعوي كإجراءات وقائية ضد الإرهاب، مع توضيح لبعض المفاهيم التي كانت عائق أمام وضع تشريعات وإجراءات كفيلة بمكافحة الظاهرة والحد من خطورتها، وحاولت الوقوف عند مفهوم الإرهاب الإسلاموي الذي اتخذه الإرهابيون ذريعة للدعاية الجهادية وعاملا لتجنيد الشباب في صفوف هذه التنظيمات وتمويه المجتمع الدولي الذي اتهم الإسلام بأنه السبب الأساسي في انتشار ظاهرة الإرهاب.

[1] ساعد الهام حورية، مرجع سابق، ص 126،127.

[2] عمار تيسير بجبوج، مرجع سابق، ص 456 .

في نفس الإطار حاول المجلس تصحيح تلك المفاهيم التي كان يروج بها الإرهابيين ابتداءا من سنة 1996، حيث أعد خطة إعلامية عربية نموذجية للتوعية الأمنية والوقاية من الجريمة سنة 1998[1].

كما توجد خطة مماثلة لتوعية المواطن من خطر الإرهاب سنة 1999، وأنتج في سنة 2000 أفلام للتوعية من مخاطر الإرهاب، وحث المواطن على ضرورة التعاون مع الأجهزة الأمنية وبالإضافة إلى هذه الإجراءات قام بإصدار صحيفة يوضح من خلالها موقفه اتجاه هذه الظاهرة[2].

دعت الدورة 32 لمجلس وزراء الداخلية العرب التي انعقدت في الجزائر في 11 مارس 2015 بقصر الأمم بنادي الصنوبر[3] الدول المشاركة إلى ضرورة إشراك رجال الدين والتربية والإعلام في عملية مكافحة الإرهاب مع وجوب استحداث أجهزة وهيئات جديدة تتلاءم والتحديات الأمنية الراهنة لضمان نجاعة التخطيط الأمني.

وأبرزت الندوة أن الحل الأمني وحده غير كافي في القضاء على الجريمة التي بلغت ذروتها في السنوات الأخيرة لذلك ركزت على أهمية العنصر البشري في القضاء على مختلف الظواهر الإجرامية الخطيرة، وفي سياق أشغال الندوة وضرورة عمل الدول الأعضاء على الحد من انتشار وقدرة التنظيمات الإرهابية على التجنيد، ولا يمكن لهذه المبادئ أن تتحقق إلا بإتباع سياسة وقائية نابعة من إيمان الدول الأعضاء بضرورة القضاء على الإرهاب[4].

[1] ساعد الهام حورية، مرجع سابق، ص 127.

[2] نفس المرجع، ص 127.

[3] وقد حضر هذه الدورة أصحاب السمو ومعالي وزراء الداخلية للدول العربية ووفود أمنية رفيعة المستوى إضافة إلى ممثلين عن مجلس التعاون لدول الخليج العربي، اتحاد المغرب العربي، منظمة التعاون الإسلامي، رابطة العالم الإسلامي المنظمة الدولية للشرطة الجنائية، المنظمة الدولية للحماية المدنية والدفاع المدني، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، المنظمة العربية للسياحة، جامعة نايف للعلوم الأمنية والاتحاد الرياضي العربي للشرطة.

[4] تغطية أعمال الندوة 32 لمجلس وزراء الداخلية العرب، مجلة الشرطة ، العدد 126، مارس 2015، ص 20.

## رابعا: في مجال تجميع تشريعات مكافحة الإرهاب والاتفاقيات المبرمة في هذا الشأن.

من أجل تنفيذ الخطط الإستراتيجية العربية لمكافحة الإرهاب، كلفت الأمانة العامة للمكتب العربي للشرطة الجنائية التابع لها مايلي:

- تجميع تشريعات مكافحة الإرهاب المعمول بها في الدول الأعضاء وتعميمها على وزارات الداخلية في الدول العربية للاستفادة منها.
- تجميع الاتفاقيات الثنائية ومتعددة الأطراف المعقودة في مجال مكافحة الإرهاب لتعميمها على سائر الدول الأعضاء.

وقد قام المكتب خلال السنوات الماضية، بتجميع كثير من تشريعات مكافحة الإرهاب النافذة في الدول العربية، والاتفاقيات المبرمة بهذا المجال سواء أكانت مخصصة حصرا بالإرهاب، أم كانت اتفاقية أمنية عامة تتعرض لمكافحة الإرهاب في نصوصه.

وقد تم تعميم هذه التشريعات والاتفاقيات على الدول العربية للاستفادة منها[1].

## خامسا: في مجال القوانين الاسترشادية والخطط النموذجية.

حرصا من مجلس وزراء الداخلية العرب على توفير أطر قانونية استرشادية تستهدي بها الدول العربية في سن أو تعديل تشريعات مكافحة الإرهاب أقر مجلس وزراء الداخلية العرب قانونين نموذجيين تم تعميمهما على الدول الأعضاء للاستفادة منهما وهما:

- القانون العربي النموذجي لمكافحة الإرهاب.
- القانون العربي النموذجي الخاص بالأسلحة والذخائر والمتفجرات.

وفي نطاق تنفيذها للخطط المرحلية للإستراتيجية العربية لمكافحة الإرهاب، أعدت الأمانة العامة مجموعة من الخطط النموذجية لمواجهة هذه الظاهرة بجوانبها المختلفة.

وقد تم تعميم هذه الخطط على الدول الأعضاء للاستفادة منها، وهي الخطط هي[1]:

[1] عمار تيسير بجبوج، مرجع سابق، ص 457.

- خطتان نموذجيتان لمواجهة أعمال الإرهاب سنة 2000، ركزت إحداهما على الجوانب القانونية، في حين ركزت الثانية على الجوانب العملية الميدانية.
- خطة نموذجية لمواجهة خطف الطائرات وتحرير الرهائن 2001.
- خطة نموذجية لمداهمة عصابات الإجرام المنظم سنة 2001.
- خطة نموذجية لمواجهة الأعمال الإرهابية في وسائل النقل سنة 2002.
- خطة أمنية عربية لمواجهة أعمال الإرهاب على متن البواخر والسفن.

**سادسا: في مجال إجراءات ملاحقة الإرهابيين.**

يقوم المكتب العربي للشرطة الجنائية بملاحقة الإرهابيين من خلال القيام بالإجراءات التالية[2]:

- تفعيل التعاون بين الدول العربية في مجال إجراءات البحث والتحري والقبض على الأشخاص الهاربين من مرتكبي الجرائم الإرهابية.
- التنسيق بين الدول العربية في مجال تبادل الخبرات والمعلومات بشأن قضايا الإرهاب.
- تلقي وتعميم طلبات البحث وكف البحث عن الأشخاص الهاربين من متهمين أو محكوم عليهم في جرائم الإرهاب.
- تطوير قاعدة المعلومات المنشأة في المكتب حول ظاهرة الإرهاب بكافة صورها وأشكالها وتزويد الأجهزة الأمنية العربية بالمعلومات المتوفرة، وبكل المستجدات في هذا المجال وهذا حتى يمكنها مكافحة الإرهاب المتطور والحديث (الإرهاب الالكتروني).
- تنقيح القائمة السوداء لمدبري ومنفذي الأعمال الإرهابية بصورة دورية وتعميمها على الدول الأعضاء.

**سابعا: في مجال التوعية الإعلامية بمخاطر الإرهاب.**

[1] محمد بن علي كومان، تقرير حول دور مجلس وزراء الداخلية العرب في مكافحة الإرهاب، ص 8 متوافرة على الرابط: www.aim-coucil.org/SiteCollectionDocuments/2.pdf، تاريخ الزيارة 2015/07/17 على الساعة 01:26 .

[2] عمار تيسير بجبوج، مرجع سابق، ص 458.

دائما في نطاق الأمانة العامة لمجلس وزراء الداخلية العرب، وفي إطار تنفيذ الخطة الإعلامية للتوعية الأمنية ضد الجريمة، والمنبثقة عن الإستراتيجية الإعلامية العربية للتوعية الأمنية والوقاية من الجريمة، وضع الخطط الإعلامية التوعوية التالية وتعميمها على الدول الأعضاء للاستفادة منها، وأهم هذه الخطط هي[1]:

- في سنة 1992 تم وضع خطة توعية لتأكيد المفاهيم الأساسية للدين الإسلامي وتصحيح المفاهيم الخاطئة التي يروجها دعاة العنف والتطرف.
- في سنة 1998 تم وضع خطة إعلامية نموذجية للتوعية الأمنية والوقاية من الجريمة.
- في سنة 1999 تم وضع خطة إعلامية عربية نموذجية شاملة لتوعية المواطن ضد أخطار الإرهاب وتحصينه بالقيم الروحية والأخلاقية والتربوية.
- في سنة 2000 تم وضع خطة إعلامية نموذجية شاملة لتوعية المواطن العربي ضد أخطار الإرهاب.

من مهام المكتب العربي للإعلام الأمني التابع للأمانة العامة أيضا إنتاج الأفلام الإعلامية التي تحذر من مخاطر الإرهاب بمختلف أشكاله وصوره وخاصة أمام التطور التكنولوجي وظهور الإرهاب الالكتروني، كما تحث هذه الأفلام المواطنين على التعاون مع الأجهزة الأمنية في مكافحته[2].

وتجدر الإشارة أن مجلس وزراء الداخلية العرب يحرص على التعاون مع الهيئات الدولية المتخصصة المعنية بمنع الجريمة ومكافحة الإرهاب، فالأمانة العامة ترتبط بمذكرة تفاهم مع المنظمة الدولية للشرطة الجنائية، حيث تحدد هذه المذكرة أوجه التعاون بشأن قضايا الإجرام، ومن بينها وأهمها الإرهاب وخاصة الإرهاب الالكتروني، كما تشارك في اجتماعات لجنة مكافحة الإرهاب التابعة لمجلس الأمن والمنشأة بالقرار رقم 1373 السابق الذكر[3].

وفي الأخير توجت أعمال وجهود مجلس وزراء الداخلية العرب بوضع تصور أولي لمشروع اتفاقية عربية لمكافحة الإرهاب سنة 1997، بحيث شكلت الأمانة العامة لمجلس وزراء الداخلية العرب

[1] عمار تيسير بجبوج، مرجع سابق، ص 458.
[2] محمد بن علي كومان، مرجع سابق، ص 10.
[3] عمار تيسير بجبوج، مرجع سابق، ص 459.

فريق عمل متكون من ممثلين عن الدول الأعضاء للقيام بهذا العمل عقدت من اجل ذلك اجتماعين تم من خلالهما صياغة مشروع الاتفاقية في صورتها النهائية عرض على المجلس وزراء العدل في نوفمبر سنة 1997، وعلى مجلس وزراء الداخلية في جانفي 1998 .

وفي اجتماع مشترك بين المجلسين تم إقرار هذه الاتفاقية في شكلها النهائي في 22 أفريل 1998، وقد تم إبرام هذه الاتفاقية تحت شعار "التضامن العربي من أجل مواجهة الإرهاب" .

كما كان لانعقاد مؤتمر تونس في الفترة بين 30 –31 جانفي سنة 2007 فرصة لمجلس وزراء الداخلية العرب لوضع تصور جديد لمحاربة جميع أشكال العنف التي تتعرض إليها المجتمعات العربية، ومنه تم إقرار لبنة عمل جديدة قوية للعمل الأمني المشترك من خلال تدخلات العديد من المؤتمرين[1].

وقد عقدتا بمشاركة الأمانة العامة لمجلس وزراء الداخلية العرب وخبراء من الدول العربية والأمم المتحدة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والمنظمات الإقليمية والدولية المعنية وصدر عن كل منهما مجموعة من التوصيات الاتفاقية العربية حول جرائم الحاسوب والموقعة من مجلسي وزراء الداخلية العدل العرب 21 ديسمبر 2010 والتي تتضمن مواد حول مكافحة استخدام الانترنت لأغراض إرهابية[2].

## الفرع الثاني: مجلس وزراء الإعلام العرب.

قبل أن نتعرف على دور مجلس وزراء العرب وجب أن نوضح المقصود بالإعلام العربي وجهازه وعلاقته بالإرهاب .

### أولا: تعريف الإعلام العربي وجهازه .

[1] ساعد الهام حورية، مرجع سابق، ص 128.

[2] عبد الله حامد الكيلاني، جهود مكافحة الإرهاب النووي على الصعيد العربي، مداخلة في قمة جامعة الدول العربية الرياض، في الفترة بين 3–5 جوان 2013 ، ص 10.

يمكن تعريف الإعلام العربي بأنه:" الوظيفة الإعلامية التي تمارسها جامعة الدول العربية باسم ونيابة عن، وبالاشتراك مع، الأقطار العربية وتحت إشرافها لصالح الوطن العربي في مجموعة".

أنشئ جهاز الإعلام العربي في جامعة الدول العربية في أفريل 1946، ومر جهاز الإعلام العربي بالجامعة بعدة تطورات تناولت دمج بعض الوحدات الإدارية حتى استقر شكل التنظيم سنة 1981 .

وتتكون الإدارة العامة للإعلام العربي في الجامعة من ثلاث إدارات فرعية:

1. إدارة التخطيط الإعلامي والتنسيق.
2. إدارة الإنتاج الإعلامي.
3. إدارة شؤون المكاتب.

بالإضافة إلى مكتب الإدارة العامة للإعلام[1].

## ثانيا: وظائف الإدارة العامة للإعلام.

تعتبر الوظيفة الإعلامية للجامعة إحدى الوظائف الأساسية للإدارة العليا بحكم المادة الخامسة من النظام الداخلي للأمانة العامة.

وتتبع الإدارة العامة أسلوبا تنظيميا تخدم وسائل الاتصال ووحدات تنظيمية تخدم الجماهير المستهدفة، إلى جانب الوحدات الميدانية المتمثلة في مكاتب الإعلام العربي في الخارج، والتي تتولى مسؤولية تنفيذ الوظيفة الإعلامية مباشرة.

وحددت وظائف الإدارة العامة في الإعلام ب[2]:

- تنسيق العمل الإعلامي في الجامعة وتوجيهه.

[1] مصطفى يوسف كافي، وآخرون، الإعلام والإرهاب الالكتروني، الطبعة الأولى، دار الإعصار العلمي،2015، ص 41.

[2] مصطفى يوسف كافي، وآخرون، مرجع سابق، ص 42.

- إعداد البحوث عن القضايا العربية، واتجاهات الرأي العام "العالمي" في مناطق مختلفة ومعالجة تقارير البحوث والمعلومات.
- إعداد المواد الإعلامية المختلفة، وضمان وصولها إلى غايتها وذلك من خلال:

1. تفهم التيارات الفكرية والحضارية والسياسية التي تسيطر على الرأي العام الخارجي واستنباط أفضل الطرق للتأثير فيه، وبالتالي التعرف على أساليب الدعاية المعادية من استعمارية وصهيونية وما تضمه من برامج، والتخطيط لمواجهته.
2. تجميع المواد الإخبارية والإعلامية عن الدول الأعضاء والقضايا العربية وإبلاغها للمكاتب وأجهزة الدعوى العربية في الخارج، التي بدورها تقوم بصياغتها وإبلاغها للرأي العام العالمي بوسائل الاتصال العامة المختلفة، وبواسطة ما تعقده من صلات بقيادات الرأي العام العالمي
3. وضع مشروعات إعلامية طويلة المدى والحرص على تنفيذها.

غير أن إعادة تحديد وظائف الإدارة العامة للإعلام سنة 1981، حيث جاءت أكثر دقة وشمولا مما كانت عليه في اللائحة التنظيمية سابقة الذكر، إذ ربطت الوظائف الإعلامية للإدارة العامة للإعلام بوظائف أجهزة الإعلام القطرية وبالوظائف الإعلامية للمنظمات العربية المتخصصة، تجسيدا ودفعا للإعلام العربي المشترك[1].

## ثالثا: علاقة الإعلام بالإرهاب الالكتروني.

منذ ظهور الإرهاب الالكتروني كصورة مستحدثة للإرهاب، لم يعد هذا الأخير يتمثل في استخدام القوة والعنف فقط، بل إنه ينشر الخوف والفزع في المجتمع كما يؤثر على أمن الدول واستقرارها ويمس اقتصادها وكل مصالح الدولة الحيوية دون الحاجة إلى استخدام السلاح والعنف، بل امن الوسيلة الأساسية المستخدمة في هذه الصورة المستخدمة هي شبكة الانترنت.

ويعتبر الإرهاب الالكتروني من أخطر المشاكل التي تواجه العالم في الوقت الحاضر خاصة في الدول النامية التي من ضمنها الدول العربية وهذا لضعف تحكمها في شبكات الانترنت، وتتعاظم هذه

[1] مصطفى يوسف كافي، وآخرون، مرجع سابق، ص 43.

المشكلة المعاصرة كونها مشكلة عالمية لتشغل رجال السياسة والاقتصاد والصحافة والباحثين والعامة على المستوى العالمي[1].

وحتى يتمكن الإرهابي تحقيق أهدافه الإرهابية في جميع صور الجرائم الإرهابية فإنه يعتمد بالدرجة الأولى على تجاوب أجهزة الإعلام معه، وليس بالضروري أن يكون التجاوب بالتعاطف، بل المهم أن تنقل هذه الأجهزة الرسالة إلى أوسع قطاع من الرأي العام العالمي.

فيعتمد الإرهابي في هذه الحالة على موهبة رجل الإعلام في إبراز المثير من الأخبار ولذلك فهو يعمد إلى القيام بالمثير من العمليات التي تفرض نفسها في الصفحات الأولى من الصحف وأغلفة المجلات وفي مطلع النشرات المذاعة والمتلفزة، وبناءا على ما تقدم فهناك من الفقه من يرى بأن كل من الإعلام والإعلامي أفضل صديقين للرجل الإرهابي[2] .

اعتبر الفقه الدولي هذا الاستنتاج صحيحا وذلك للدور الخطير الذي تلعبه وسائل الإعلام في تغطيتها للقضايا الدولية وكشفها للرأي العام العالمي من خلال عرضها لأخبار العمليات الإرهابية التي تقع، كما أن أهمية أي عمل إرهابي تقاس بمدى ما يحصل عليه من تغطية إعلامية، ومن أجل الحصول على هذه التغطية يلجأ الإرهابيون إلى اختيار مسارح لعملياتهم تتوافر كل عناصر الإثارة الضرورية .

فإستراتيجية الإرهاب وخاصة الإرهاب الالكتروني هي سيكولوجية "نفسية" أكثر منها عسكرية وكذلك فإنه من خلال العمل الإرهابي تستطيع منظمة صغيرة أن تحصل على حجم إعلامي كبير جدا.

غير أن إغفال أو تجاهل العمليات الإرهابية يسئ إلى أمانة نقل الأخبار وبالتالي إلى المهمة الأساسية للإعلام، أما إبرازها فيدفع بالإعلام إلى الوقوع في فخ الإرهاب، من هنا عمدت أجهزة الإعلام مؤخرا إلى استغلال الإرهابي بنسبة ما يستغلها هو، فأصبحت هذه الأجهزة تكتفي بنشر أخبار العمليات الإرهابية دون أن تتحدث عن القضية التي من أجلها يقوم الإرهابي بعملياته، بذلك يستطيع

[1] مصطفى يوسف كافي، وآخرون، مرجع سابق، ص 175،176 .

[2] Laqueur WALTER, Age of terrorism-Boston, Little, brown and CO-USA, 1987, p65.

الإرهابي أن يستقطب الاهتمام، ولكنه يعجز عن توصيل رسالته إلى الرأي العام، ومما تقدم يتبين أن استخدام وسائل الإعلام والدعاية عنصر أساسي وجوهري في النظم السياسية الإرهابية[1].

يتفق خبراء وباحثوا الإعلام في الوطن العربي على قصور أداء الإعلام العربي على كافة الأصعدة، فالخريطة الإعلامية العربية في الوقت الحاضر تعكس كل التناقضات الاجتماعية والصراعات السياسية والإيديولوجية، فالسمة البارزة للإعلام العربي الراهن هو تبعيته المطلقة الكاملة للأنظمة العربية السائدة، وإن الاستثناءات في هذا المجال في حالات محدودة جدا، وضعيفة جدا وهشة جدا، ومعظمها مخترقة من الداخل، بمعنى أن الأنظمة هي التي أوجدتها أو تساعدها، وبالتالي توجهها وترسم مساراتها وسياساتها الأمر الذي جعل الفرصة سانحة أمام الجماعات والتنظيمات الإرهابية لنشر أفكارها عبر المواقع الالكترونية واختراق المواقع الإعلامية وحجبها دون أدنى مقاومة من هذه الأخيرة[2].

لتفادي كل هذه الأسباب والظروف أعلن مجلس وزراء الإعلام العرب مؤخرا عن التوجه إلى العالم من خلال محطة تليفزيونية عربية مشتركة، وهذا كنوع من الجهود المشتركة لتقوية الإعلام العربي ونشر الوعي، ومحاولة الحد من انتشار الجريمة ومنها جريمة الإرهاب الالكتروني، حيث يساعد هذا الإعلام العربي على محاربة الأفكار الإرهابية والتحذير من تفشي هذه الظاهرة الخطيرة في المجتمع.

ومن أجل ذلك يمثل مجلس وزراء الإعلام العرب نقطة البداية في العمل العربي المشترك لمكافحة جرائم الإرهاب، وتمثل ذلك خلال اجتماع المجلس في دورته السادسة والعشرين التي عقدت في القاهرة في شهر يوليو سنة 1993، حيث ناقش المجلس قضية الإرهاب ولأول مرة على المستوى الوزاري العربي، وقرر وضع آليات لمواجهة التطرف وتوعية الرأي العام العربي لمخاطره ونتائجه ونوقشت خطة لمواجهة الإرهاب تدعو إلى توعية الرأي العام داخل الوطن العربي وخارجه بمخاطر الإرهاب التي تهدف إلى عزل المجتمعات العربية عن العالم من خلال تغطيتها إعلاميا على أوسع نطاق ممكن، وتبصير الرأي العام العربي من خلال مواد إعلامية مسموعة ومقروءة ومرئية بمسؤوليته

[1] مصطفى يوسف كافي، وآخرون، مرجع سابق، ص 177.

[2] نفس المرجع، ص 46.

نحو حماية الأجيال الناشئة من السقوط في براثن الإرهاب، وتلبية حاجة الشباب في كل الميادين والارتقاء بوعيهم الثقافي.

كما تم التأكيد في هذه الدورة من ضرورة وضع خطة للتنوير الديني لتقديم الدين في صورته الصحيحة السمحة بعيدا عن روح التعصب، وتكثيف البرامج الإعلامية التي تبرز خطورة الإرهاب على المكونات الرئيسة للاقتصاد العربي، والتزام وسائل الإعلام بالموضوعية حتى لا تقع فريسة للشائعات والأقاويل، وإدراج ظاهرة الإرهاب ضمن نشاطات مكتب الجامعة العربية في الخارج من خلال الملتقيات والمحاضرات[1].

وانصب اهتمام مجلس وزراء الإعلام العرب في المواجهة الإعلامية للإرهاب على مقاومة الفكر المتطرف والحيلولة دون تمكينه من التأثير في الرأي العام وتحديدا لدى شريحة الشباب، لضمان عدم تدفق أي دماء جديدة في شريان الإرهاب بحيث يسهل محاصرته والحد منه، ومن ثم تطهير المجتمعات العربية منه.

وقد عقد المجلس سنة 2000 اجتماعا مشتركا مع مجلس وزراء الداخلية العرب تم من خلاله الاتفاق على التعاون في مجال مكافحة الإرهاب وتوظيف الإعلام العربي للتوعية بخطورة الإرهاب.

كما صدرت عن مجلس وزراء الإعلام العرب في دورة انعقاده الحادية الأربعين في 19 يونيو 2008 توصيات في سياق تأكيد دور الإعلام العربي في التصدي لظاهرة الإرهاب حيث جاء فيه[2]:" أن مجلس وزراء الإعلام العرب بعد الاطلاع على مذكرة الأمانة العامة، وبعد النظر في توصية اللجنة الدائمة للإعلام العربي يقرر:

1. الموافقة على توصية اللجنة العليا للتنسيق بين القنوات الفضائية العربية في اجتماعها الثالث عشر الذي انعقد في تونس في المدة من 12 إلى 13 /2008/6 وذلك في بندها السابع الذي يطالب من اتحاد إذاعات الدول العربية دعوة اللجنة عقب إعادة هيكلتها إلى التركيز في

[1] محمد فتحي عيد، مرجع سابق، ص 178.

[2] البند السابع من القرار ق/296- دع/40-2007/6/20 في دورة انعقاده العادي الواحد والأربعون في 19 يونيو 2008 ، متوافر على الرابط: www.arableagueonline.org/las/picture gallery/awards19june08.pdf .

إسهاماتها في التصدي الإعلامي لظاهرة الإرهاب والتطرف على المحاور الخمسة التي اعتمدها مجلس وزراء الإعلام العرب في قراره ق/296-د ع/40-2007/6/20.

2. الطلب مجددا من مؤسسات وأجهزة الإعلام العربية الحرص على التدقيق فيما تعرضه من أفلام وبرامج حرصا على عدم ظهور مواد يكون من شأنها تشويه الصورة العربية.
3. الطلب من مؤسسات وأجهزة الإعلام العربية الاسترشاد في إنتاجها البرامجي، في مجال التصدي لظاهرة الإرهاب، بما يصدر عن اللجنة الدائمة للإعلام العربي وفريق الخبراء الدائم المعني بالتصدي لظاهرة الإرهاب، من توصيات وأفكار.

وفيما يتعلق بالخطوات العملية التي قام بها مجلس وزراء الإعلام العرب في التصدي لظاهرة الإرهاب، فقد وافق المجلس في ختام دورته الثالثة والأربعين التي عقدت في القاهرة بتاريخ 23 يونيو 2010 على تكليف مركز أبحاث متخصص لإعداد مسودة مشروع إستراتيجية عربية إعلامية مشتركة لمواجهة ظاهرة الإرهاب، ولتعمل على تصحيح صورة العرب والمسلمين أمام الرأي العام الدولي، على أن ترسل تلك المسودة للدول العربية لدراستها خلال الأربعة أشهر لإبداء ملاحظاتها ومرئياتها حولها لصياغتها من قبل المركز في صورتها النهائية لعرضها على الاجتماع الذي يليه للمجلس[1] .

وتجدر الإشارة انه وبوعي من مجلس وزراء إعلام العرب بدور الإعلام في مجابهة هذه الآفة الخطيرة، فقد تضمنت قرارات القمم العربية التأكيد على تعزيز دور الإعلام السمعي والبصري والرقمي في مكافحة الإرهاب، ومنع الإعلام الذي يشيع روح الكراهية والتفرقة والطائفية والتكفير ويشجع على الغلو والتطرف المؤدي للإرهاب.

هذا ويشكل تبادل الخبرات والمعلومات والدعم الفني اللازم في كافة المجالات المرتبطة بمكافحة الإرهاب لبنة أساسية في جهود جامعة الدول العربية في هذا المجال، حيث تم تنظيم عدد من ورش العمل والدورات التدريبية العربية خاصة في مجالات مراقبة حركة البضائع والأشخاص وتأمينها من

[1] عمار تيسير بجبوج، مرجع سابق، ص 460،461.

الهجمات الإرهابية، ومكافحة حيازة الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، وأهم الجهود والمتعلقة بدراستنا مكافحة استخدام الانترنت من طرف الإرهابيين ولأغراض إرهابية[1].

وحول الإعلام وأجندة التنمية المستدامة، وافق مجلس وزراء الإعلام العرب على خارطة الطريق الإعلامية لتنفيذ أجندة التنمية المستدامة 2030 واعتبارها أحد برامج الخطة الجديدة للتحرك الإعلامي العربي في الخارج على أن يتم الصرف منها لتنفيذ خارطة الطريق الإعلامية.

وطلب المجلس من وزارات الإعلام أو الجهات المعنية بالإعلام في الدول الأعضاء التعاون والتنسيق مع الأمانة الفنية لمجلس وزراء الإعلام العرب لتنفيذ خارطة الطريق الإعلامية العربية.

كما حث المجلس اتحاد إذاعات الدول العربية على الالتزام بتعهداته للاستفادة من الأكاديمية المتطورة للتدريب الإعلامي في مجال التدريب على التنمية المستدامة إسهامًا منه في نشر الوعي بمتطلبات هذا المشروع الحيوي ووضعها في خدمة جامعة الدول العربية ومجلس وزراء الإعلام العرب.

وفيما يتعلق بالمحور الفكري للدورة العادية الـ48 لمجلس وزراء الإعلام العرب، اختار المجلس موضوع "التوعية المجتمعية ضد الفكر المتطرف والإرهاب "[2] ليكون محورًا فكريًا للدورة، وطلب من الأمانة العامة لجامعة الدول العربية تعميم المحور الفكري على الدول الأعضاء والمنظمات والاتحادات الممارسة لمهام إعلامية التي تعمل بصفة مراقب في مجلس وزراء الإعلام العرب لتسليط الضوء على مضمونه وتنظيم فعاليات تناقش ما ورد به.

وحول المنظمات والاتحادات والمجالس والهيئات العربية الممارسة لمهام إعلامية، طلب مجلس وزراء الإعلام العرب مجددًا من المنظمات والاتحادات الممارسة لمهام إعلامية التي لم تواف الأمانة

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، الرباط، في الفترة من 14-16 أكتوبر 2014 متوافرة على الرابط: https://repository.nauss.edu.sa/ ، تاريخ الاطلاع 2018/07/17 على الساعة 01:20 .

[2] إجراءات قانونية للتعامل مع القنوات المسيئة- وزراء الإعلام العرب يضعون إستراتيجية مكافحة الإرهاب 2030 مقالة منشورة في الموقع عاجل الالكترونية: https://www.ajel.sa/local/1910531، تاريخ الاطلاع 2018/07/18 على الساعة 01:35.

العامة للجامعة العربية بالبيانات والمستندات الرسمية المطلوبة لتقنين وتنظيم العلاقة بينها وبين هذه المنظمات سرعة موافاتها بالمطلوب في موعد أقصاه شهرين من تاريخه.

### الفرع الثالث: مجلس وزراء العدل العرب.

كان لمجلس وزراء العدل العرب الدور الكبير في تفعيل الجهود العربية المبذولة في مجال مكافحة الإرهاب بكل أشكاله وصوره، وقد أصدر المكتب التنفيذي للمجلس المنعقد في بيروت في ختام أعمال دورته الرابعة والعشرون في نوفمبر 2008 توصيات أكدت على مايلي[1]:

1. أهمية تعزيز التعاون العربي والدولي لمكافحة الإرهاب وتفعيل آليات هذا التعاون وتفعيل الآلية التنفيذية للاتفاقية العربية لمكافحة الإرهاب.
2. دعت التوصيات الدول العربية التي لم تصدق على هذه الاتفاقية إلى الإسراع بإتمام إجراءات التصديق عليها.
3. التأكيد على أهمية التعاون العربي الثنائي والجماعي لتفعيل أحكام الاتفاقية، مع التركيز على تعزيز التعاون العربي والدولي في مجال مكافحة الإرهاب.
4. تعميم مشروع الاتفاقية العربية غسل الأموال وتمويل الإرهاب على الدول العربية لإبداء ملاحظاتها قبل عرضها على الاجتماع المقبل للمكتب التنفيذي.

كما أشرفت الأمانة الفنية للمجلس، بالتعاون مع مكتب الأمم المتحدة المعني بالمخدرات والجريمة من خلال مكتبه الإقليمي بالقاهرة، على عقد ندوة إقليمية عربية حول مكافحة الإرهاب في مقر الأمانة العامة لجامعة الدول العربية في الفترة من 16 إلى 17 فيفري 2005، حيث شارك فيها الأمين العام المساعد للأمم المتحدة، المدير التنفيذي للجنة مكافحة الإرهاب المشكلة بموجب قرار مجلس الأمن رقم 1373 لسنة 2001، وصدر عن الندوة مجموعة من التوصيات كمايلي[2]:

---

[1] موقع مجلس وزراء العدل العرب متوافر على الرابط:

http//www.arablegalnet.org/ArabMinisters/ArabMinDecList.aspx?ID=24.

[2] عمار تيسير بجبوج، مرجع سابق، ص 461.

- أكدت على التوصيات الصادرة عن مؤتمر الرياض الدولي لمكافحة الإرهاب الذي عقد خلال الفترة من 5 إلى 8 فيفري 2005.
- أوصت بالعمل على استكمال إعداد مشروع اتفاقية الأمم المتحدة الشاملة لمكافحة الإرهاب توصلا إلى وضع تعريف دولي للإرهاب يكون أساسا للتمييز بين الإرهاب وحق الشعوب في مقاومة الاحتلال، مع الأخذ في الاعتبار أن قتل الأبرياء المدنيين لا تقره الشرائع السماوية ولا المواثيق الدولية.
- كما دعت الندوة إلى إنشاء مركز إقليمي تدريبي لمكافحة الإرهاب والجريمة المنظمة تحت مظلة مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والذي مقره فيينا وقد حددت التوصيات مهام هذا المركز بما يلي[1]:

1. تأسيس إطار العمل القانوني المطلوب استجابة لما تتطلبه الصكوك الدولية.
2. تدعيم التعاون الإقليمي ودون الإقليمي في المسائل الجنائية، والتشارك في المعلومات الاستخباراتية وتبادلها، والاستفادة من أساليب التحريات المتقدمة.
3. تشجيع التعاون في مجال منع الجريمة والعدالة الجنائية، وتسهيل التفاعل بين مختلف البلدان بهدف الاستفادة من الممارسات الناجحة في هذا المجال.
4. تنظيم حلقات تدريب تخصصية للقضاء والمدعين العامين وموظفي الجمارك والمصارف وتدريب رجال إنفاذ القانون على كيفية تعقب ومتابعة واكتشاف الصلة بين التنظيمات الإرهابية وعصابات الجريمة المنظمة عبر الوطنية والمتجرين بالمخدرات وغاسلي الأموال.

- كما أكدت الندوة على اعتبار الأمم المتحدة حجر الزاوية فيما يتعلق بتوحيد جهود التعاون الدولي لمكافحة الإرهاب.
- العمل على اتخاذ التدابير اللازمة لمنع الإرهابيين من حيازة أسلحة الدمار الشامل ومكوناتها.

[1] الرسالة الموجهة إلى رئيس مجلس الأمن(S/2005/309) من المراقب الدائم لجامعة الدول العربية لدى الأمم المتحدة المؤرخة في 10 ماي 2005، والتي تتضمن توصيات الندوة الإقليمية حول مكافحة الإرهاب المعقودة يومي 16-17 فيفري 2005 متوافرة على الرابط: http//daccess-ods.un.org/TMP/712647.html .

- تشجيع الدول الأعضاء على تفعيل وتعزيز التعاون الدولي والإقليمي ودون الإقليمي والثنائي في مجال مكافحة الإرهاب، خاصة في مجال تسليم المجرمين وطلبات المساعدة القضائية مع الأخذ بعين الاعتبار العلاقة الوثيقة بين الإرهاب والأشكال الأخرى للجريمة المنظمة، مثل غسل الأموال والاتجار غير المشروع بالأسلحة والمتفجرات، والاتجار بالمخدرات والاتجار بالأشخاص، وذلك استجابة لما تضمنته الصكوك الدولية والإقليمية المشار إليها.

وعرضت نتائج المؤتمر والندوة ضمن تقرير الأمين العام على مجلس الجامعة على مستوى القمة في دورته السابعة عشرة التي عقدت بالجزائر في مارس 2005، فأكد القادة العرب في بيانهم الختامي على أهمية ما توصل إليه المؤتمر والندوة من نتائج.

وقامت الأمانة الفنية بإرسال تقرير وتوصيات الندوة الى الوفد الدائم لجامعة الدول العربية لدى الأمم المتحدة، فقام هذا الأخير بإيداعها كوثيقة من وثائق مجلس الأمن تحت رقم 309 لسنة 2005

وفي اجتماع المكتب التنفيذي لمجلس وزراء العدل العرب الرابع والأربعين الذي عقد في القاهرة بتاريخ 24 ماي 2010 اعتمد المكتب مشروع الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب بناءا على قرار مجلس وزراء الداخلية العرب رقم 579–د27 بتاريخ مارس 2010.

كما حث الدول العربية المصدقة على الاتفاقية العربية لمكافحة الإرهاب والتي لم تصدق على تعديل الفقرة الثالثة من المادة الأولى منها، والذي أقره مجلسا وزراء العدل والداخلية العرب الة التصديق على التعديل وإيداع وثائق التصديق لدى الأمانة العامة[1].

كما أدان وزراء العدل العرب كافة الاعتداءات الإرهابية التي تتعرض لها الدول العربية وجميع أشكال الإرهاب ومظاهره أيا كان مصدره.

وطالب الوزراء بالعمل على تعزيز تدابير الوقاية من الإرهاب ومعالجة أسبابه واقتلاع جذوره وتجفيف منابعه الفكرية والمالية ووضع برامج تهدف إلى تعزيز ثقافة التسامح والتعددية ومحاربة التطرف.

وأكد الوزراء، في ختام أعمال الدورة الثانية والثلاثين لمجلس وزراء العدل العرب التي عقدت بمقر الجامعة العربية بالعاصمة المصرية القاهرة برئاسة العراق، على أن جميع التدابير المستخدمة في

[1] عمار تيسير بجبوج، مرجع سابق، ص 462،463.

مكافحة الإرهاب يجب أن تتفق مع المبادئ المعترف بها في القانون الدولي بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني.

وحث مجلس وزراء العدل العرب الدول العربية على التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والانترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها، ووضع آلية وطنية للتعامل مع المواقع الإلكترونية ذات الصلة بالتنظيمات الإرهابية.

كما دعا المجلس الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في 21 ديسمبر 2010 في القاهرة إلى تعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الإلكتروني[1].

ودعا المجلس إلى تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة لمواجهة خطر استخدام الإرهابيين لأسلحة الدمار الشامل أو مكوناتها، ودعم أمن المطارات والموانئ والحدود.

وفيما يتعلق بشبكة التعاون القضائي العربي بمجال مكافحة الإرهاب والجريمة المنظمة قرر مجلس وزراء العدل العرب عقد اجتماع للجنة الفنية لخبراء وزارات العدل في الدول العربية لإعداد مشروع النظام الداخلي لهذه الشبكة في ضوء ما يرد من ملاحظات الدول العربية، تمهيدا لعرض نتائج أعمالها على الدورة القادمة للمجلس وتكليف الأمانة الفنية للمجلس للتنسيق مع الأمانة العامة لمجلس وزراء الداخلية العرب بشأن إنشاء شبكة التعاون القضائي العربي في مجال مكافحة الإرهاب.

وكان مجلس وزراء العدل عقد دورته الثانية والثلاثين بمقر الجامعة العربية برئاسة وزير العدل العراقي خلفا لنظيره الأردني، وحضور الأمين العام المساعد للشؤون القانونية لدى الجامعة العربية ومشاركة وزراء العدل العرب أو من يمثلهم.

[1] مجلس وزراء العدل العرب يطالب بالحيلولة دون استغلال الإرهابيين تكنولوجيا المعلومات، مقالة منشورة في موقع القدس العربي: http://www.alquds.co.uk/?p=635412 تاريخ الاطلاع 2018/07/19 على الساعة 02:11.

وأكد وزير العدل العراقي في كلمة له خلال افتتاح أعمال الجلسة ضرورة تضافر الجهود العربية والدولية لمكافحة ظاهرة الإرهاب بكافة أشكالها وصورها التي استفحلت في العديد من بلدان المنطقة، مشيرا إلى الحرب التي تخوضها بلاده الآن ضد الإرهاب في الموصل وذلك بالتعاون مع الشركاء الدوليين والعرب.

ومن جانبه، أكد وزير العدل السعودي الرئيس الفخري للمجلس أن المنطقة العربية تمر حاليا بمرحلة تحتاج لتوحيد الرؤى، وذلك لمواجهة ما يحيط بها من تحديات تتطلب التكاتف للتصدي لها وأعرب عن أمله في أن يسهم الاجتماع بما يناقشه من موضوعات هامة في التوصل لنتائج فاعلة نحو تعزيز التعاون العربي والدولي في مكافحة الإرهاب.

ويأتي انعقاد المجلس بدعوة من الأمين العام لجامعة الدول العربية وبناء على ما نصت عليه المادة الثامنة من النظام الأساسي لمجلس وزراء العدل العرب، نظرا لما تشهده المنطقة من متغيرات وتحديات[1].

وفي الجلسة الافتتاحية لأعمال المكتب التنفيذي لمجلس وزراء العدل العرب في دورته التاسعة والخمسين والتي تناولت عدة بنود أهمها الاتفاقية العربية لمكافحة الإرهاب، وقد شدد الحضور علي دعوة الدول العربية غير المصدقة علي الاتفاقية علي التصديق عليها، وإيداع وثائق التصديق لدي الأمانة العامة لجامعة الدول العربية .

كما تناولت الجلسة تكثيف الجهود لتعزيز التعاون العربي في مجالات تبادل المعلومات و إثراء قواعد البيانات بين الدول العربية، أيضا الإجراءات المتخذة في شان غسل الأموال وتمويل الإرهاب ومتابعة التحقيقات في ذلك الأمر لوضع آلية عربية لضبط الأموال الممولة للإرهاب، وآلية أخري لمنع استغلال العناصر الإرهابية لتكنولوجيا المعلومات في بث أفكارهم الهدامة وخدمة أغراضهم الدنيئة .

وتضمنت الجلسة موضوع تنظيم ورش عمل لتنمية موارد بشرية عربية في مجال غسل الأموال وتمويل الإرهاب، كما أدان جميع الحضور الأعمال الإرهابية الأخيرة في كافة دول العالم سيما الدول العربية مؤكدين أن كافة التدابير المستخدمة لمكافحة الإرهاب متفقة مع القانون الدولي الإنساني .

[1] مجلس وزراء العدل العرب يطالب بالحيلولة دون استغلال الإرهابيين تكنولوجيا المعلومات، مرجع سابق.

وصرح مساعد وزير العدل لشؤون الإعلام أن موضوع مكافحة الإرهاب قد تصدر مشاريع القرارات التي تم طرحها اليوم علي مائدة المكتب التنفيذي لمجلس وزراء العدل العرب، ومن هذه المشاريع مشروع قرار بشأن شبكة التعاون القضائي العربي في مجال مكافحة الإرهاب و الجريمة المنظمة، والنظر في مشروع النظام الداخلي لشبكة التعاون القضائي في مكافحة الإرهاب وتعميم هذا المشروع [1].

كذلك تناول الاجتماع في هذا الشأن تعميم مشروع القانون العربي الاسترشادي الخاص بمساعدة ضحايا الأعمال الإرهابية علي وزارت العدل و الداخلية و الجهات المعنية بمكافحة الإرهاب في كافة الدول العربية، وتشكيل لجنة من كافة هذه الجهات لمراجعة مشروع القانون.

والجدير بالذكر أن المكتب التنفيذي للمجلس ينعقد كل ستة أشهر بدعوة من رئيسه بمقر الأمانة العامة للجامعة، أو في أي دولة عضو بالمجلس بناء على دعوة منها وموافقة المجلس .

ويتشكل المكتب من ستة أعضاء ثلاثة أعضاء من مجلس الجامعة على مستوى القمة (الرئاسة السابقة، والرئاسة الحالية، والرئاسة اللاحقة)، ثلاثة أعضاء بالتناوب وفقا للترتيب الهجائي للدول الأعضاء، و في حال الجمع بين العضوية في المكتب التنفيذي وفقا للترويكا والعضوية حسب الترتيب الهجائي ينتقل الدور للدولة التي تلي في الترتيب الهجائي، وأن للمجلس أن ينتخب دولة أو دولتين لضمهما كأعضاء بالمكتب التنفيذي لمدة عامين في حالة الضرورة [2].

ودائما في إطار جهود مجلس وزراء العدل العرب في مكافحة الإرهاب بمختلف أشكاله وصوره ومنها الإرهاب الالكتروني دعا المكتب التنفيذي لمجلس وزراء العدل العرب، الدول العربية التي لم تصادق على الاتفاقية العربية لمكافحة الإرهاب إلى إتمام إجراءات التصديق عليها.

---

[1] مجلس وزراء العدل العرب": مكافحة الإرهاب يتصدر أهم المشاريع..العمل على منع استغلال العناصر الإرهابية لتكنولوجيا المعلومات..ومحاربة غسل الأموال على أجندة الأولويات"، الدورة 59 بتاريخ 22 نوفمبر 2016 ، منشورة في موقع انفراد: http://www.innfrad.com/News/14/456518 تاريخ الاطلاع 2018/07/19 على الساعة 02:54.

[2] مجلس وزراء العدل العرب": مكافحة الإرهاب يتصدر أهم المشاريع..العمل على منع استغلال العناصر الإرهابية لتكنولوجيا المعلومات..ومحاربة غسل الأموال على أجندة الأولويات"، مرجع سابق.

وقرر "المكتب" في ختام أعمال دورته الستين بمقر الأمانة العامة للجامعة العربية برئاسة وزير العدل السعودي تكثيف التعاون العربي في مجال تبادل المعلومات المتعلقة بمكافحة الإرهاب وتفعيل أحكام المادة الرابعة من الاتفاقية العربية لمكافحة الإرهاب بشأن تبادل المعلومات والتحريات وتبادل الخبرات[1].

[1] تنص المادة الرابعة من الاتفاقية العربية لمكافحة الإرهاب على أنه:"تتعاون الدول المتعاقدة لمنع ومكافحة الجرائم الإرهابية، طبقا للقوانين والإجراءات الداخلية لكل دولة، من خلال الآتي:

أولا- تبادل المعلومات:

1. تتعهد الدول المتعاقدة بتعزيز تبادل المعلومات فيما بينها حول:

أ- أنشطة وجرائم الجماعات الإرهابية وقياداتها وعناصرها وأماكن تمركزها وتدريبها ووسائل ومصادر تمويلها وتسليحها وأنواع الأسلحة والذخائر والمتفجرات التي تستخدمها، وغيرها من وسائل الاعتداء والقتل والدمار.

ب- وسائل الاتصال والدعاية التي تستخدمها الجماعات الإرهابية وأسلوب عملها، وتنقلات قياداتها وعناصرها ووثائق السفر التي تستعملها.

2. تتعهد كل من الدول المتعاقدة، بإخطار أية دولة متعاقدة أخرى، على وجه السرعة، بالمعلومات المتوفرة لديها عن أية جريمة إرهابية تقع في إقليمها تستهدف المساس بمصالح تلك الدولة أو بمواطنيها، على أن تبين في ذلك الإخطار ما أحاط بالجريمة من ظروف والجناة فيها وضحاياها والخسائر الناجمة عنها والأدوات والأساليب المستخدمة في ارتكابها، وذلك بالقدر الذي لا يتعارض مع متطلبات البحث والتحقيق.
3. تتعهد الدول المتعاقدة، بالتعاون فيما بينها لتبادل المعلومات لمكافحة الجرائم الإرهابية، وان تبادر بإخطار الدولة أو الدول الأخرى المتعاقدة بكل ما يتوافر لديها من معلومات أو بيانات من شأنها أن تحول دون وقوع جرائم إرهابية على إقليمها أو ضد مواطنيها أو المقيمين فيها أو ضد مصالحها.
4. تتعهد كل من الدول المتعاقدة، بتزويد أية دولة متعاقدة أخرى. بما يتوافر لديها من معلومات أو بيانات من شأنها:

أ- أن تساعد في القبض على متهم أو متهمين بارتكاب جريمة إرهابية ضد مصالح تلك الدولة، أو الشروع أو الاشتراك فيها سواء بالمساعدة أو الاتفاق أو التحريض.

ب- أن تؤدى إلى ضبط أية أسلحة أو ذخائر أو متفجرات أو أدوات أو أموال استخدمت أو أعدت للاستخدام في جريمة إرهابية.

5. تتعهد الدول المتعاقدة، بالمحافظة على سرية المعلومات المتبادلة فيما بينها، وعدم تزويد أية دولة غير متعاقدة أو جهة أخرى بها، دون أخذ الموافقة المسبقة للدولة مصدر المعلومات.

ثانيا- التحريات:

تتعهد الدول المتعاقدة بتعزيز التعاون فيما بينها، وتقديم المساعدة في مجال إجراءات التحري والقبض على الهاربين من المتهمين أو المحكوم عليهم بجرائم إرهابية وفقا لقوانين وأنظمة كل دولة.

ثالثا- تبادل الخبرات:

ورحب "وزراء العدل العرب" باقتراح مجلس وزراء الداخلية العرب بالتوقيع على كل من "الاتفاقية العربية لتنظيم نقل وزراعة الأعضاء والأنسجة البشرية ومنع ومكافحة الاتجار فيها"، و"الاتفاقية العربية لمنع ومكافحة الاستنساخ البشرى"، و"البروتوكول العربي لمكافحة جرائم الاتجار بالبشر وخاصة النساء والأطفال"، و"البروتوكول العربي لمنع ومكافحة القرصنة البحرية والسطو المسلح" خلال الاجتماع المشترك لمجلسي وزراء العدل والداخلية العرب لتفعيل الاتفاقيات العربية ذات الصلة بمكافحة الإرهاب.

وبشأن الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، دعا "المكتب" التي لم تصادق على الاتفاقية إلى إتمام إجراءات التصديق[1].

وأكد رفضه كل أشكال الابتزاز من قبل الجماعات الإرهابية بالتهديد أو قتل الرهائن أو طلب فدية لتمويل جرائمها الإرهابية، داعيا الدول إلى الامتناع عن تقديم أي شكل من أشكال الدعم الصريح أو الضمني إلى الكيانات أو الأشخاص الضالعين في الأعمال الإرهابية وربط كل أشكال الابتزاز من قبل الجماعات الإرهابية من تهديد أو قتل الرهائن أو طلب فدية

وقرر تكثيف التعاون العربي الثنائي والجماعي بين الجهات القضائية في الدول العربية بمجال التحقيقات والمتابعات والإجراءات القضائية المتعلقة بغسل الأموال وتمويل الإرهاب.

ودعا إلى وضع تدابير وآليات وطنية لضمان فعالية تتبع وحجز ومصادرة الأموال المغسولة أو الموجهة لتمويل الإرهاب بالسرعة اللازمة، وفيما يتعلق بتعزيز التعاون العربي والدولي في مجال مكافحة الإرهاب، طالب "تنفيذي مجلس وزراء العدل العرب" بضرورة اتخاذ تدابير على المستوى

1. = تتعاون الدول المتعاقدة، على إجراء وتبادل الدراسات والبحوث لمكافحة الجرائم الإرهابية، كما تتبادل ما لديها من خبرات في مجال المكافحة.
2. تتعاون الدول المتعاقدة، في حدود إمكانياتها على توفير المساعدات الفنية المتاحة لإعداد برامج أو عقد دورات تدريبية مشتركة، أو خاصة بدولة أو مجموعة من الدول المتعاقدة عند الحاجة، للعاملين في مجال مكافحة الإرهاب، لتنمية قدراتهم العلمية والعملية ورفع مستوى أدائهم".

[1] تنفيذي وزراء العدل العرب" يدعو للمصادقة على اتفاقية مكافحة الإرهاب"، الدورة الستين لمجلس وزراء العدل العرب القاهرة في 2017/05/17 منشور في موقع اليوم السابع: https://www.youm7.com/story/2017/5/1789 تاريخ الاطلاع 2018/07/19 على الساعة 03:53 .

الوطني من أجل منع تنقل المقاتلين الإرهابيين الأجانب من أراضى الدول الأعضاء وإليها للانضمام إلى التنظيمات الإرهابية ووضع النظم القانونية والإجراءات الإدارية المناسبة لمعاقبة هؤلاء المقاتلين والحد من الخطر الذي يمثلونه لدولهم الأصلية، والدول التي يعبرونها والدول التي يسافرون إليها .

ودعا الدول العربية إلى سن وتطوير تشريعاتها الجنائية وملاءمتها مع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لكي تتناول بالتجريم الصور المستحدثة من الجرائم الالكترونية لمنع الإرهابيين من استخدام الانترنت، وتعزيز التعاون والتنسيق مع المنظمات الدولية والإقليمية المعنية بمواجهة كافة أشكال جرائم الإرهاب الالكترونية[1].

وأكد إدانة الاعتداءات الإرهابية التي تعرضت لها دول عربية وجميع أشكال الإرهاب ومظاهره وأيا كان مصدره والعمل على تعزيز تدابير الوقاية من الإرهاب ومعالجة أسبابه واقتلاع جذوره وتجفيف منابعه الفكرية والمالية ووضع برامج تهدف إلى نشر ثقافة التسامح الديني ومحاربة التطرف.

وشدد المكتب التنفيذي لمجلس وزراء العدل العرب على أنه لا مجال لربط الإرهاب بأي دين أو جنسية أو حضارة والتسامح والتفاهم بين الثقافات والشعوب والأديان، وأكد على أن جميع التدابير المستخدمة في مكافحة الإرهاب يجب أن تتفق مع قواعد القانون الدولي بما في ذلك القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، داعيا الدول الأعضاء إلى توعية السلطات الوطنية المسؤولة عن مكافحة الإرهاب بأهمية هذه الالتزامات.

ودعا الدول العربية إلى الامتناع عن تقديم أي شكل من أشكال الدعم الصريح أو الضمني إلى الكيانات أو الأشخاص الضالعين في الأعمال الإرهابية والتصدي لتلك الأعمال الإرهابية، وأكد على مواصلة التعاون القائم بين جامعة الدول العربية وأجهزة المنظمات الدولية والإقليمية المعنية بمكافحة الإرهاب.

ودعا "المكتب" إلى تعظيم الاستفادة من إمكانيات مركز الأمم المتحدة لمكافحة الإرهاب المنشأ في نيويورك بمبادرة من خادم الحرمين الشريفين، ومركز الملك عبد الله بن عبد العزيز العالمي للحوار بين إتباع الديانات والثقافات في فيينا والمركز الدولي للتميز لمكافحة التطرف في أبو ظبي والمركز الإفريقي للبحوث والدراسات في مجال مكافحة الإرهاب بالجزائر، ومركز النهرين للدراسات الإستراتيجية في العراق، ومنتدى النهضة للتواصل الحضاري بالسودان ومركز محمد بن نايف للمناصحة والرعاية

[1] تنفيذي وزراء العدل العرب" يدعو للمصادقة على اتفاقية مكافحة الإرهاب"، مرجع سابق.

بالمملكة العربية السعودية وكل من مركز محمد السادس للعلماء الأفارقة ومعهد محمد السادس لتكوين الأئمة والمرشدين والمرشدات بالمملكة المغربية ومركز الدوحة الدولي لحوار الأديان بقطر.

وفيما يتعلق بمشروع إنشاء شبكة التعاون القضائي العربي في مجال مكافحة الإرهاب والجريمة المنظمة، قرر المكتب التنفيذي لمجلس وزراء العدل العرب، رفع مشروع النظام الداخلي لهذه الشبكة إلى مجلس وزراء العدل العرب في دورته القادمة لاعتماده[1].

كما اعتمد مجلسا وزراء العدل والداخلية العرب القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها في سنتي 2003 و2004 ونصت المادة (21) منه على " كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن .. " [2].

## الفرع الرابع: فريق الخبراء العرب المعني بمكافحة الإرهاب.

عقب أحداث 11 سبتمبر سنة 2001 شكل الأمين العام لجامعة الدول العربية في إطار الأمانة العامة فريقا من كبار المسؤولين والخبراء في الأجهزة المعنية بمكافحة الإرهاب في الدول العربية لدراسة قرار مجلس الأمن رقم 1373 لسنة 2001، ومتابعة تنفيذه وبحث الصعوبات التي تتعرض لها الدول العربية في ذلك.

بموجب القرار رقم 6504 بتاريخ 3 مارس 2005 تم اعتماد الفريق من قبل مجلس الجامعة على المستوى الوزاري كآلية عربية لمكافحة الإرهاب تحت اسم "فريق الخبراء العرب المعني بمكافحة الإرهاب".

وصادق مجلس الجامعة على المستوى الوزاري في دورته 132 بالقرار رقم 7101 بتاريخ 09 سبتمبر 2009 على النظام الداخلي لفريق الخبراء العرب المعني بمكافحة الإرهاب والذي تضمن نشأة الفريق كجهاز دائم مختص بمسائل مكافحة الإرهاب في نطاق جامعة الدول العربية تحت إشراف

[1] تنفيذي وزراء العدل العرب" يدعو للمصادقة على اتفاقية مكافحة الإرهاب"، مرجع سابق.

[2] عبد الله حامد الكيلاني، مرجع سابق، ص 10.

مجلس الجامعة على المستوى الوزاري، ويعقد فريق الخبراء العرب المعني بمكافحة الإرهاب اجتماعين سنويا قبل كل دورة عادية لمجلس الجامعة.

وتتجلى أهداف فريق الخبراء العرب المعني بمكافحة الإرهاب فيما يلي[1]:

- وضع أسس التعاون وسبل تفعيله بين الدول العربية في مجال مكافحة الإرهاب.
- تنسيق الجهود والبرامج والأنشطة التي تقوم بها المجالس الوزارية والمنظمات العربية المتخصصة المعنية بمكافحة الإرهاب، وخاصة مجالس العدل والداخلية والإعلام والشؤون الاجتماعية العرب.
- متابعة الإجراءات والتدابير المتعلقة بتصديق الدول الأعضاء في الاتفاقية العربية لمكافحة الإرهاب وعلى الصكوك الدولية الخاصة بالإرهاب، وتنفيذها وملاءمة تشريعاتها الوطنية مع أحكامها.
- متابعة تنفيذ القرارات والاستراتيجيات العربية والدولية المتعلقة بمكافحة الإرهاب.
- تنسيق المواقف العربية تجاه قضايا مكافحة الإرهاب إقليميا ودوليا بغرض إعداد تصور لموقف موحد بشأنها في المحافل الدولية.
- دراسة الاتفاقيات العربية ذات الصلة وغيرها من المجالات المتصلة بمكافحة الإرهاب في إطار جامعة الدول العربية، واقتراح التوصيات المناسبة لتفعيلها.
- التعاون مع المنظمات الدولية والإقليمية وهيئاتها ولجانها المختصة بالشؤون المتعلقة بمكافحة الإرهاب.
- اقتراح عقد دورات تدريبية وندوات وورش عمل متخصصة بمشاركة خبراء من الأمم المتحدة والمنظمات الإقليمية المعنية.
- إعداد خطط وبرامج للمساعدة والدعم الفني للدول العربية من الجهات العربية والدولية في مجال دعم القدرات والتدريب للعاملين في مجال مكافحة الإرهاب.
- تعزيز آليات وتدابير لمساعدة ضحايا الإرهاب.

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 10.

هذا ويتولى مهام الأمانة الفنية لفريق الخبراء العرب المعني بمكافحة الإرهاب قسم شؤون مكافحة الإرهاب تحت إشراف قطاع الشؤون القانونية بالأمانة العامة لجامعة الدول العربية[1].

## المطلب الثاني: نتائج جهود جامعة الدول العربية في مجال مكافحة الإرهاب الالكتروني.

أثمرت الجهود التي بذلتها جامعة الدول العربية من خلال المجالس التابعة لها في مجال مكافحة الإرهاب بمختلف أشكاله وصوره وخاصة جريمة الإرهاب الالكتروني التي أصبحت تهدد عالما بأسره وهذا نظرا للتطور العلمي والتكنولوجي بنتائج عكست رغبة الدول العربية في الوقوف في وجه الإرهاب ، وأهم هذه النتائج التي أثمرت من جهود جامعة الدول العربية في هذا الشأن تمثلت في إبرام جملة من الاتفاقيات العربية ، بالإضافة إلى إقرار الإستراتيجية العربية المتعلقة بمكافحة الإرهاب، وهو الأمر الذي سوف نوضحه من خلال فرعين اثنين.

### الفرع الأول : الاتفاقيات العربية في مجال مكافحة الإرهاب الالكتروني.

من أجل الوقاية من الجرائم الإرهابية ومكافحتها مهما كان نوعها أو صورتها ومنها جريمة الإرهاب الالكتروني أبرمت جامعة الدول العربية بواسطة مجلسيها، مجلس وزراء الداخلية العرب ومجلس وزراء العدل العديد من الاتفاقيات في هذا الشأن، وسوف نتعرض لأهم هذه الاتفاقيات بشيء من التفصيل:

#### أولا: الاتفاقية العربية لمكافحة الإرهاب.

توجت جهود جامعة الدول العربية في مجال مكافحة الإرهاب على الصعيد العربي بإبرام الاتفاقية العربية لمكافحة الإرهاب في اجتماع مشترك لمجلسي وزراء العدل والداخلية العرب بالقاهرة في 22 أفريل 1998 ، ودخلت حيز النفاذ بتاريخ 7 ماي 1999،وصادقت عليها حوالي 18 دولة عربية، ولقد لقيت هذه الاتفاقية اهتمام وترحيب كبيرين في كافة المحافل الدولية، واعتبرت نموذجا يحتذى به في التعاون الإقليمي في مجال مكافحة الإرهاب خاصة وأنها كانت سباقة في تعريفها للإرهاب بشكل

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 10.

واضح ودقيق، وتؤكد على ضرورة التمييز بين الإرهاب والحق المشروع للشعوب في مقاومة الاحتلال والعدوان دون المساس بالوحدة الترابية للدول .

وقد قامت لجنة وزارية مشتركة بتكليف من مجلسي وزراء العدل والداخلية العرب بوضع آلية لتنفيذ الاتفاقية العربية لمكافحة الإرهاب، تتضمن الإجراءات والنماذج التنفيذية للاتفاقية وعددها 52 نموذجا في مجال التعاون الأمني والقضائي[1]، وكلف المكتب العربي للشرطة الجنائية بمتابعة تنفيذ الدول العربية للاتفاقية، وإعداد تقرير سنوي بهذا الشأن يعرض على المجلسين في الدورة العادية لكل منهما، وقد تم تكليف المكتب أيضا بمتابعة الإجراءات والنماذج التنفيذية مع الدول الأعضاء وتقييمها بعد مضي خمس سنوات على دخولها حيز العمل .

وفي إطار تفعيل أحكام الاتفاقية قرر مجلس الجامعة على مستوى القمة في قراره رقم 231 بتاريخ 28 مارس 2002 النظر في إمكانية إدراج أفعال التحريض والإشادة بالأعمال الإرهابية، وطبع ونشر وتوزيع المنشورات ذات الصلة بالإرهاب، وجمع الأموال تحت ستار جمعيات خيرية لصالح الإرهاب، واكتساب واستعمال ممتلكات لأغراض إرهابية، وضمن الجرائم المنصوص عليها في الاتفاقية العربية لمكافحة الإرهاب، وتنفيذا لهذا القرار تم تشكيل لجنة فنية مشتركة من مجلسي وزراء العدل والداخلية العرب قامت بصياغة مشروع تعديل للاتفاقية وفق ما تضمنه قرار القمة، وتم اعتماد مشروع التعديل بقرار من مجلس وزراء العدل العرب رقم 492-د.ع-19 بتاريخ 08 أكتوبر 2003 وقرار مجلس وزراء الداخلية العرب رقم 418-د.ع-21 بتاريخ 5 جانفي 2004 ودعت الأمانة العامة للجامعة العربية الدول الأعضاء إلى اتخاذ الإجراءات الدستورية للمصادقة على هذا التعديل

أما على المستوى الدولي فقد تم إيداع الاتفاقية لدى منظمة الأمم المتحدة وإدراجها في وثائق الجمعية العامة رقم (A/54/301) و(A/55/179 ) و(A/56/160 ) الصادرة بتاريخ 23 سبتمبر 1999، 26 جويلية 2000، 3 جويلية 2001 كأحد الصكوك القانونية الدولية المتصلة بمنع الإرهاب الدولي وقمعه، كما أودعت قائمة الدول المصادقة على الاتفاقية لدى الأمم المتحدة، وتم تعميمها

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 5.

كوثيقة من وثائق الجمعية العامة في إطار البند 151 من جدول الأعمال المعنون" التدابير الرامية إلى القضاء على الإرهاب الدولي"[1].

## 01- تحديد مفهوم الإرهاب والاعتراف بحق الشعوب في تقرير مصيرها.

تضمنت نصوص الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 مفهوم الإرهاب والجريمة الإرهابية وذلك في الباب الأول وبالتحديد في نص المادة الأولى، مستندة في ذلك على أحكام ومبادئ الاتفاقيات الدولية التي أبرمت بشأن التصدي لمختلف أشكال الإرهاب -ومنها الإرهاب الالكتروني محل دراستنا- فقد نصت الفقرة "ب" من المادة الأولى على تعريف الإرهاب بقولها:" كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه 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 أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر"، بينما حددت الفقرة "ج" الجريمة الإرهابية بأنها:" أي جريمة أو الشروع فيها ترتكب تنفيذا لغرض إرهابي في أي دولة من الدول المتعاقدة سواء على رعاياها أو ممتلكاتها أو مصالحها يعاقب عليها قانونها الداخلي"[2] .

حاولت الاتفاقية من خلال مادتها الثانية حصر الأفعال الخارجة عن نطاق الإرهاب واعترفت ضمنها بحق الشعوب في تقرير مصيرها، وأن كفاحها ضد الاحتلال الأجنبي والعدوان معترف به دوليا فلا يمكن التذرع بالإرهاب لمنع هذه الشعوب من السعي من أجل تحقيق حريتها واستقلالها، وحددت الاتفاقية العربية لمكافحة الإرهاب الأفعال التي لا تندرج ضمن الجرائم السياسية، وهي الاعتداء على ملوك ورؤساء الدول المتعاقدة والحكام وزوجاتهم أو أصولهم أو فروعهم والتعدي على أولياء العهد، أو نواب رؤساء الدول، أو رؤساء الحكومات أو الوزراء في أي من الدول المتعاقدة ، بالإضافة إلى التعدي على الأشخاص المتمتعين بالحماية بما فيهم السفراء والدبلوماسيين في الدول المتعاقدة أو المعتمدون لديها وكذلك القتل العمدي والسرقة المصحوبة بإكراه ضد الأفراد أو السلطات أو وسائل النقل والمواصلات، أعمال التخريب والإتلاف للممتلكات العامة والممتلكات المخصصة لخدمة عامة

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 5.
[2] ساعد الهام حورية، مرجع سابق، ص 129.

حتى ولو كانت مملوكة لدولة أخرى من الدول المتعاقدة وجرائم تصنيع أو تهريب أو حيازة الأسلحة أو الذخائر أو المتفجرات أو غيرها من المواد والوسائل التي تستخدم لارتكاب الجرائم الإرهابية[1] .

## 02- تعزيز التعاون العربي في المجالين الأمني والقضائي.

سعت الدول العربية الموقعة على الاتفاقية العربية لمكافحة الإرهاب في إطار التعاون فيما بينها ووضعت تدابير لمنع وقوع الجريمة الإرهابية، كما حددت بوضوح التزامات الدول المتعاقدة في هذين المجالين ، كما تعهدت بعدم تمويل أو تنظيم أو ارتكاب أي عمل إرهابي أو الاشتراك فيه بأي صورة كانت، وعليه فإن أسس التعاون العربي الأمني وفقا لهذه الاتفاقية على محورين أساسيين:

### تدابير منع ومكافحة الجرائم الإرهابية.

حيث تتعهد الدول المتعاقدة بعدم تنظيم أو تمويل أو ارتكاب الأعمال الإرهابية أو الاشتراك فيها بأي صورة من الصور، والتزاما منها بمنع ومكافحة الجرائم الإرهابية مهما كان نوعها أو صورتها وهذا طبقا للقوانين والإجراءات الداخلية لكل منها فإنها تعمل على[1]:

---

[1] تنص المادة الثانية من الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 بما يلي:" أ- لا تعد جريمة، حالات الكفاح بمختلف الوسائل، بما في ذلك الكفاح المسلح ضد الاحتلال الأجنبي والعدوان من أجل التحرر وتقرير المصير وفقا لمبادئ القانون الدولي، ولا يعتبر من هذه الحالات كل عمل يمس بالوحدة الترابية لأي من الدول العربية.

ب- لا تعد أي من الجرائم الإرهابية المشار إليها في المادة السابقة من الجرائم السياسية.

وفي تطبيق أحكام هذه الاتفاقية، لا تعد من الجرائم السياسية - ولو كانت بدافع سياسي - الجرائم الآتية :

1- التعدي على ملوك ورؤساء الدول المتعاقدة والحكام وزوجاتهم أو أصولهم أو فروعهم.

2- التعدي على أولياء العهد، أو نواب رؤساء الدول، أو رؤساء الحكومات، أو الوزراء في أي من الدول المتعاقدة.

3- التعدي على الأشخاص المتمتعين بحماية دولية، بمن فيهم السفراء والدبلوماسيون في الدول المتعاقدة أو المعتمدون لديها.

4- القتل العمد والسرقة المصحوبة بإكراه ضد الأفراد أو السلطات أو وسائل النقل والمواصلات.

5- أعمال التخريب والإتلاف للممتلكات العامة والممتلكات المخصصة لخدمة عامة حتى ولو كانت مملوكة لدولة أخرى من الدول المتعاقدة.

6-جرائم تصنيع أو تهريب أو حيازة الأسلحة أو الذخائر أو المتفجرات، أو غيرها من المواد التي تعد لارتكاب جرائم إرهابية.

**أ- تدابير المنع.**

- الحيلولة دون اتخاذ أراضيها مسرحا لتخطيط أو تنظيم أو تنفيذ الجرائم الإرهابية أو الشروع أو الاشتراك فيها بأية صورة من الصور، بما في ذلك العمل على منع تسلل العناصر الإرهابية إليها أو إقامتها على أراضيها فرادى أو جماعات أو استقبالها أو إيوائها أو تدريبها أو تسليحها أو تمويلها أو تقديم أية تسهيلات لها.
- التعاون والتنسيق بين الدول المتعاقدة، وخاصة المتجاورة منها والتي تعاني من الجرائم الإرهابية بصورة متشابهة أو مشتركة، كما هو الحال بين الجزائر تونس.
- تطوير وتعزيز الأنظمة المتصلة بالكشف عن نقل واستيراد وتصدير وتخزين واستخدام الأسلحة والذخائر والمتفجرات وغيرها من وسائل الاعتداء والقتل والدمار وإجراءات مراقبتها عبر الجمارك والحدود لمنع انتقالها من دولة متعاقدة إلى أخرى أو إلى غيرها من الدول إلا لأغراض مشروعة على نحو ثابت.
- تطوير وتعزيز الأنظمة المتصلة بإجراءات المراقبة وتأمين الحدود والمنافذ البرية والبحرية والجوية لمنع حالات التسلل منها.
- تعزيز نظم تأمين وحماية الشخصيات والمنشآت الحيوية ووسائل النقل العام.
- تعزيز الحماية والأمن والسلامة للشخصيات وللبعثات الدبلوماسية والقنصلية والمنظمات الإقليمية والدولية المعتمدة لدى الدولة المتعاقدة وفقا للاتفاقيات الدولية التي تحكم هذا الموضوع.
- تعزيز أنشطة الإعلام الأمني وتنسيقها مع الأنشطة الإعلامية في كل دولة وفقا لسياستها الإعلامية، وذلك لكشف أهداف الجماعات والتنظيمات الإرهابية وإحباط مخططاتها، وبيان مدى خطورتها على الأمن والاستقرار.
- تقوم كل دولة من الدول المتعاقدة بإنشاء قاعة بيانات لجمع وتحليل المعلومات الخاصة بالعناصر والجماعات والحركات والتنظيمات الإرهابية ومتابعة مستجدات ظاهرة الإرهاب والتجارب الناجحة في مواجهتها، وتحديث هذه المعلومات وتزويد الأجهزة المختصة في الدول المتعاقدة بها، وذلك في حدود ما تسمح به القوانين والإجراءات الداخلية لكل دولة.

[1] المادة الثالثة من الاتفاقية العربية لمكافحة الإرهاب لسنة 1998.

وهدف الاتفاقية العربية لمكافحة الإرهاب من هذا النص حتى تتماشى آليات المكافحة مع التطور الذي عرفته الجريمة الإرهابية وظهور جريمة الإرهاب الالكتروني التي تعتمد على استغلال الجماعات الإرهابية لشبكة الانترنت.

### ب- تدابير المكافحة.

وتكون تدابير مكافحة الجرائم الإرهابية حسب الاتفاقية العربية لمكافحة الإرهاب كمايلي[1]:

- القبض على مرتكبي الجرائم الإرهابية ومحاكمتهم وفقا للقانون الوطني، أو تسليمهم وفقا لأحكام هذه الاتفاقية، أو الاتفاقيات الثنائية بين الدولتين الطالبة والمطلوب منها التسليم.
- تأمين حماية فعالة للعاملين في ميدان العدالة الجنائية.
- تأمين حماية فعالة لمصادر المعلومات عن الجرائم الإرهابية والشهود فيها.
- توفير ما يلزم من مساعدات لضحايا الإرهاب.
- إقامة تعاون فعال بين الأجهزة المعنية وبين المواطنين لمواجهة الإرهاب، بما في ذلك إيجاد ضمانات وحوافز مناسبة للتشجيع على الإبلاغ عن الأعمال الإرهابية وتقديم المعلومات التي تساعد في الكشف عنها والتعاون في القبض على مرتكبيها.

## التعاون الأمني العربي لمنع ومكافحة الجرائم الإرهابية.

وفقا لنص المادة الرابعة من الاتفاقية العربية لمكافحة الإرهاب تتعاون الدول المتعاقدة لمنع ومكافحة الجريمة الإرهابية، طبقا للقوانين والإجراءات الداخلية لكل دولة، من خلال الآتي:

### أ- تبادل المعلومات.

تعاهدت الدول المتعاقدة بتعزيز تبادل المعلومات فيما بينها حول أنشطة وجرائم الجماعات الإرهابية وقيادتها وعناصرها وأماكن تمركزها وتدريبها ووسائل ومصادر تمويلها وتسليحها، ووسائل الاتصال التي تستخدمها الجماعات الإرهابية.

[1] عمار تيسير بجبوج، مرجع سابق، ص 465.

زيادة على ذلك يجب أن تخطر دولة متعاقدة أي دولة متعاقدة أخرى –على وجه السرعة– بما لديها من معلومات عن أية جريمة إرهابية ارتكبت في إقليمها بهدف المساس بمصالح تلك الدولة، أو بمواطنيها، أو بما قد يتوافر لديها من معلومات أو بيانات من شأنها أن تحول دون وقوع مثل هذه الجرائم.

كما تعهدت الدول الأعضاء في الاتفاقية العربية لمكافحة الإرهاب بالمحافظة على سرية المعلومات المتبادلة فيما بينها، وعدم تزويد أية دولة غير متعاقدة أو أية جهة أخرى بها، دون أخذ الموافقة المسبقة للدولة مصدر المعلومات[1] .

**ب– التحريات.**

تعاهدت الدول الأطراف في الاتفاقية العربية لمكافحة الإرهاب بتقديم المساعدة في مجال التحري والقبض على الهاربين من المتهمين أو المحكوم عليه بجرائم إرهابية[2].

**الخبرات.**

تعهدت الدول المتعاقدة التعاون على إجراء تبادل الدراسات والبحوث لمكافحة الجرائم الإرهابية والتعاون من أجل توفير المساعدات الفنية المتاحة بإعداد برامج أو عقد دورات تدريبية مشتركة يكون الهدف منها تنمية القدرات العلمية والعملية ورفع مستوى أداء العاملين في مجال مكافحة الإرهاب[3].

**حماية الشهود والخبراء.**

نظرا إلى أهمية الشاهد والخبير في مجال مكافحة جرائم الإرهاب بكل أشكالها ومظاهرها تضمن الاتفاقية العربية لمكافحة الإرهاب على إجراءات الحماية للشهود والخبراء فكل من الشهود والخبراء دور فعال في مجال التحريات وجمع المعلومات وتحديد هوية الإرهابيين من جهة، ومن جهة ثانية شعور الشهود والخبراء بأنهم محميين أمنيا وقضائيا يجعلهم يشاركون بشكل جدي وفعال إلى جانب رجال

[1] جبار علي صالح، الجهود العربية لمكافحة الإرهاب، مجلة دراسات دولية، مركز الدراسات الإستراتيجية والدولية بغداد العدد السادس والأربعون، 2010، ص 117.

[2] المادة الرابعة من الاتفاقية العربية لمكافحة الإرهاب.

[3] الفقرة الثانية /1و2 من المادة الرابعة من الاتفاقية العربية لمكافحة الإرهاب.

الأمن والقضاء في عملية محاربة الإرهاب بواسطة المعلومات التي يقدمونها حول الشبكات الإرهابية وعن الأفعال والخطط المستقبلية للاعتداءات الإرهابية.

وترجع أهمية هذا الإجراء لتفادي الاعتداء عليهم من قبل التنظيمات الإرهابية ومن أجل ذلك خصتهم الاتفاقية بحصانة وحماية ، فقد يكون حضور الشاهد أو الخبير أمرا ضروريا وخاصة في جريمة الإرهاب الالكتروني تتطلب الخبرة في أمور الانترنت والشبكات ومن أجل ذلك قد يتطلب الأمر أن ينتقل الخبير أو الشاهد إلى الدولة المتعاقدة والطالبة لهذا الإجراء– الشهادة أو الخبرة– ففي هذه الحالة يتعين على الدولة الطالبة التأشير على ذلك في طلبها ويتعين عليها أن ترفق الطلب أو التكليف بالحضور على بيان تقريبي لمبلغ التعويض ونفقات السفر والإقامة، وعلى تعهدها بدفعها وتقوم الدولة المطلوب إليها طلب حضور الشاهد أو الخبير تبليغ المعني، وإحاطة الدولة الطالبة بالجواب[1] .

فلا يجوز إجبار الشاهد أو الخبير على الامتثال للتكليف بالحضور حتى في حالة ما إذا تضمن التكليف بالحضور بيانا لجزاء التخلف، بينما في حالة امتثاله طواعية في إقليم الدولة فيتم تكليفه بالحضور طبقا لأحكام التشريع الداخلي لتلك الدولة، كما لا يجوز إخضاع الشاهد أو الخبير لإجراءات المحاكمة أو الحبس أو تقييد حريته في إقليم الدولة الطالبة عن أفعال وأحكام سابقة على مغادرته لإقليم الدولة المطلوب إليها، وذلك أيا كانت جنسيته طالما كان حضوره في إقليم تلك الدولة بناء على تكليف بالحضور، فهو يتمتع بحصانة وحماية يستمدها من التكليف بالحضور الذي يتضمن بيان لسبب تكليفه ونوع الجريمة المطلوب من أجلها للإدلاء بشهادته أو خبرته في ميدان معين، بينما تنقضي هذه الحصانة والحماية أذا بقي هذا الأخير في إقليم الدولة الطالبة بحضوره لمدة ثلاثون يوما متعاقبة بعد انتهاء مهمته وكان بإمكانه مغادرتها أو عاد إليها مرة ثانية بعد مغادرتها[2].

كما تتعهد الدولة الطالبة بأن تكفل للشاهد الحماية من أية علانية تؤدي إلى تعريضهم أو تعريض أسرهم أو أملاكهم إلى الخطر الناتج عن الإدلاء بشهادتهم أو خبرتهم وفي حالة وجود شاهد أو خبير محبوس في الدولة المطلوب منها تكليفه بالحضور فيتم نقله مؤقتا إلى المكان الذي ستعقد فيه الجلسة المطلوب سماع شهادته أو الإدلاء بخبرته وفقا للشروط وفي المواعيد التي تحددها الدولة المطلوب

[1] ساعد الهام حورية، مرجع سابق، ص 133.

[2] الفقرة الثالثة من المادة 36 من الاتفاقية العربية لمكافحة الإرهاب.

منها ذلك، ويمكن رفض النقل لعدة أسباب قد تتعلق بالشاهد أو الخبير عند عدم قبوله ذلك، أو يكون وجوده ضروري من أجل إجراءات جنائية في الدولة المطلوب منها النقل، كما قد يكون سبب الرفض أنه يسبب إطالة لمدة الحبس أو هناك اعتبارات أخرى تحول دون نقله، وفي حالة نقله يبقى الشاهد أو الخبير محبوسا في الدولة الطالبة إلى غاية إعادته للدولة المطلوب منها ماعدا في حالة ما إذا طلبت الدولة المطلوب منها النقل من الدولة الطالبة إطلاق سراحه[1] .

## التعاون القضائي العربي في مجال مكافحة الجرائم الإرهابية.

من خلال الاتفاقية العربية لمكافحة الإرهاب يتضح أن التعاون القضائي العربي يرتكز على خمسة محاور أساسية:

### أ- تسليم المجرمين.

تلتزم الدول العربية بمقتضى المادة الخامسة من هذه الاتفاقية بتسليم المتهمين أو المحكوم عليهم في جرائم الإرهاب، وذلك طبقا للقواعد والشروط المنصوص عليها في هذه الاتفاقية، وقد استثنت المادة السادسة منها بعض الحالات من التسليم، فيما بينت المادتان السابعة والثامنة بعض الأحكام والإجراءات الخاصة به.

[1] تنص المادة 38 من الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 على أنه:"

1. إذا كان الشاهد أو الخبير المطلوب مثوله أمام الدولة الطالبة محبوسًا في الدولة المطلوب إليها،فيجرى نقله مؤقتًا إلى المكان الذي ستعقد فيه الجلسة المطلوب سماع شهادته أو خبرته فيها، ذلك بالشروط وفى المواعيد التي تحددها الدولة المطلوب إليها، ويجوز رفض النقل:
أ- إذا رفض الشاهد أو الخبير المحبوس.
ب- إذا كان وجوده ضروريًا من أجل إجراءات جنائية تتخذ في إقليم الدولة المطلوب منها.
ج- إذا كان نقله من شأنه إطالة أمد حبسه.
د- إذا كانت هناك اعتبارات تحول دون نقله.
2. يظل الشاهد أو الخبير المنقول محبوسًا في إقليم الدولة الطالبة إلى حين إعادته إلى الدولة المطلوب إليها، ما لم تطلب الدولة الأخيرة إطلاق سراحه.

**ب- الإنابات القضائية.**

ألزمت الاتفاقية كل دولة متعاقدة أن تقدم للدول الأخرى المساعدة الممكنة واللازمة للتحقيقات أو لإجراءات المتعلقة بالجرائم الإرهابية، واستحدثت حكما في مجال التعاون القضائي مؤداه أنه إذا انعقد الاختصاص القضائي لإحدى الدول المتعاقدة بمحاكمة متهم عن جريمة إرهابية، فيجوز لهذه الدولة أن تطلب إلى الدول التي يوجد المتهم في إقليمها محاكمته عن هذه الجريمة، شريطة موافقة هذه الدولة وهذا من خلال نص المادة 14 من الاتفاقية العربية لمكافحة الإرهاب[1].

ويترتب على قبول طلب المحاكمة وفق إجراءات الملاحقة والتحقيق والمحاكمة في الدولة الطالبة باستثناء ما تستلزم سبل التعاون بين الدولتين، مع العلم أن الإجراءات المتخذة تتم وفقا لقانون الدولة التي يتم فيها الإجراء، ولا يجوز للدولة الطالبة أن تحاكم أو تعيد محاكمة المتهم إلا إذا امتنعت الدولة المطلوب منها المحاكمة من إجرائها، ويجب أن تقوم الدولة المطلوب منها المحاكمة بإخبار الدولة الطالبة عن القرار الذي اتخذته بشأن طلب المحاكمة، كذلك إخبارها عن سير التحقيقات ونتيجة المحاكمة[2]، وللدولة المطلوب منها المحاكمة اتخاذ ما تراه مناسبا من تدابير بحق المتهم وحسب قوانينها، سواء كان ذلك قبل وصول طلب المحاكمة أو بعده .

أن نقل الاختصاص لا يرتب مساسا بحق المتضرر من العمليات الإرهابية فله المطالبة بالتعويض عن الأضرار سواء أمام قضاء الدولة الطالبة أو أمام دولة المحاكمة[3] .

**الأشياء والعائدات المتحصلة عن الجريمة والناتجة عن ضبطها.**

تلتزم الدولة التي قررت تسليم الشخص المطلوب تسليمه بضبط وتسليم الأشياء والعائدات المتحصلة من الجريمة الإرهابية، أو المستعملة فيها أو المتعلقة بها للدولة الطالبة سواء وجدت في حيازة الشخص المطلوب تسليمه أو لدى الغير، سواء سلمت الشخص أو لم تسلمه لهروبه أو وفاته أو

[1] جبار علي صالح، مرجع سابق، ص 119

[2] المادة 16 من الاتفاقية العربية لمكافحة الإرهاب.

[3] المادتين 17 و18 من الاتفاقية العربية لمكافحة الإرهاب .

لأي سبب آخر، وذلك بعد التحقق من أن تلك الأشياء متعلقة بالجريمة الإرهابية، وذلك مع عدم الإخلال بحقوق الغير حسن النية[1] .

### تبادل الأدلة.

ألزمت الاتفاقية العربية لمكافحة الإرهاب الدول المتعاقدة، أن تقوم بفحص الآثار والأدلة الناتجة عن الجرائم الإرهابية الواقعة على إقليمها، ولها طلب المساعدة في فحص الأدلة من أي دولة عضو في الاتفاقية، وللدولة التي وقعت الجريمة على أراضيها الحق بتزويد الدولة التي وقعت الجريمة ضد مصالحها بالنتيجة[2].

## 02- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أبرمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقاهرة في 21 ديسمبر 2010 وصادقت عليها الدول العربية الأعضاء في جامعة الدول العربية من بينها الجزائر وذلك بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014[3].

تتوج الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الجهود العربية في التصدي للجرائم المعلوماتية التي من ضمنها جريمة الإرهاب الالكتروني، وقد أكدت هذه الاتفاقية في مقدمتها على أنها جاءت رغبة من هذه الدول لتعزيز التعاون فيما بينها قصد مكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، ولتبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي من هذه الجرائم الخطيرة التي تأتي في مقدمتها جريمة الإرهاب الالكتروني، وأخذا بالمبادئ الدينية والأخلاقية السامية، لا سيما أحكام الشريعة الإسلامية، وأيضا بالتراث الإنساني للأمة العربية التي تنبذ جرائم الإرهاب مهما كان شكلها أو مظاهرها، مع مراعاة النظام العام لكل دولة[4].

---

[1] عمار تيسير بجبوج، مرجع سابق، ص 467.

[2] جبار علي صالح، مرجع سابق، ص 120.

[3] مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة 1435 هـ الموافق لـ 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21، جريدة رسمية للجمهورية الجزائرية العدد 57، الصادرة بتاريخ 4 ذو الحجة 1435 هـ الموافق لـ 28 سبتمبر 2014 م، ص 4.

[4] يزيد بوحليط، مرجع سابق، ص 99.

وحددت المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 الهدف منها من خلال مادتها الأولى بقولها:" تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها ".

اشتملت الاتفاقية على خمسة فصول، بمجموع اثنان وأربعون مادة ، شملت التعريف بالمصطلحات، والنص على متعددة منها وأهمها وأخطرها جريمة الإرهاب الالكتروني.

تطبق أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الجرائم المعلوماتية وذلك بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية[1] :

1. إذا ارتكبت هذه الجريمة المعلوماتية في أكثر من دولة، فكما هو الحال في جريمة الإرهاب الالكتروني يمكن أن يمتد تنفيذها في أكثر من دولة، ويكون الفاعلين في دولة أخرى تماما وهذا لان هذه الجريمة تتم بواسطة كمبيوتر وشبكة انترنت
2. ارتكبت الجريمة المعلوماتية في دولة أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أخرى، أي أن تكون هذه الجريمة عابرة للدول وهو أمر متوافر في الجرائم المعلوماتية كثرا وخاصة جريمة الإرهاب الالكتروني.
3. ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطتها في أكثر من دولة، كما هو الحال بالنسبة للتنظيمات الإرهابية كتنظيم داعش مثلا والذي ينشط في معظم الدول العربية، سعيا منها لتأسيس دولة إسلامية تجمع الدول العربية حسب فكرها المتطرف.
4. إذا ارتكبت الجريمة المعلوماتية في دولة واحدة، إلا أن آثارها كانت شديدة في دولة أو مجموعة من الدول الأخرى[2].

بالنسبة للإرهاب الالكتروني فإن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تعرف جريمة الإرهاب الالكتروني ، لكنها اكتفت بذكر الأفعال المميزة له وهذا من خلا ل نص المادة 15

[1] المادة الثالثة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

[2] المادة الثالثة من ذات الاتفاقية

من نفس الاتفاقية والتي جاءت تحت عنوان " الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات"، وحسب هذه المادة فإن الأعمال التي تميز جريمة الإرهاب الالكتروني هي كالتالي:

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

وتسعى الدول العربية المتعاقدة من خلال هذه الاتفاقية التعاون على مكافحة الجرائم المعلوماتية التي تهدد أمنها واستقرارها، والتي من بينها – وتهم موضوع دراستنا المتواضعة– جريمة الإرهاب الالكتروني، لكن دون أن يمس هذا التعاون بالسيادة الوطنية لأية دولة بحيث تلتزم كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى[1].

ودائما في إطار صون سيادة الدول العربية المتعاقدة في هذه الاتفاقية، فإنه ليس في هذه الأخيرة ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي[2] .

أخذت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات نفس موقف اتفاقية بودابست لسنة 2001 فيما يتعلق بالشروع والمساهمة الجنائية في الجرائم المعلوماتية، حيث نصت المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي جاءت بعنوان" الشروع والاشتراك في ارتكاب الجرائم " على أنه:

1. الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.
2. الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية

[1] المادة الرابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في فقرتها الأولى.

[2] الفقرة الثانية من المادة الرابعة من نفس الاتفاقية.

3. يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا"

من خلال هذه المادة نجد أن هذه الاتفاقية اعتدت بالاشتراك في جميع الجرائم الالكترونية ومنها جريمة الإرهاب الالكتروني وهو الموقف ذاته في اتفاقية بودابست[1]، أما الشروع فقد أرجعت حرية الأخذ به للدولة الطرف الأخذ به كليا أو جزئيا، وفقا لما يتماشى وقوانينها الداخلية – وسبق توضيح الشروع والمساهمة الجنائية في جريمة الإرهاب الالكتروني–.

وعن التعاون الإقليمي العربي في مكافحة جريمة الإرهاب الالكتروني والوقاية منها على اعتبارها تدخل ضمن الجرائم المعلوماتية فقد خصصت لها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الفصل الرابع والذي جاء بعنوان " التعاون القانوني والقضائي" .

**الاختصاص.**

وفقا للمادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فإنه وفي إطار الاختصاص في جريمة الإرهاب الالكتروني تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها وذلك إذا ارتكبت هذه الجريمة كليا أو جزئيا أو تحققت :

1. في إقليم الدولة الطرف.
2. على متن سفينة تحمل علم الدولة الطرف
3. على متن طائرة مسجلة تحت قوانينها الدولة الطرف.

[1] المادة 11 من اتفاقية بودابست لسنة 2001 والتي تنص: " **الشروع والاشتراك**

1. يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم تبعا لقانونه الداخلي، كل اشتراك إذا تم عمدا بغرض إحدى الجرائم المشار إليها في المواد 2–10 من الاتفاقية الحالية بنية ارتكاب تلك الجريمة.
2. يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم وفقا لقانونه الداخلي– كل شروع عمدي لارتكاب إحدى الجرائم المشار إليها في المواد 3–5،7،8،9(فقرة 1–أ جـ) من الاتفاقية الحالية.
3. يمكن لكل طرف أن يحتفظ بالحق في عدم تطبيق كل أو بعض الفقرة 2 من المادة الحالية".

4. من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها، أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.
5. إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

دائما في إطار الاختصاص تلتزم الدولة الطرف بتبني الإجراءات الضرورية فيما يتعلق بالجرائم التي يجوز فيها التسليم، وجريمة الإرهاب الالكتروني من ضمنها وهذا في الحالات التي يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف، ولا يقوم بتسليمه إلى طرف آخر بناءا على جنسيته بعد طلب التسليم[1].

وفي حالة تنازع الاختصاص بين أكثر من دولة طرف، فتقدم الطلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها، ثم الدولة التي وقعت الجريمة في إقليمها، ثم الدولة التي يكون الشخص المطلوب من رعاياها، وإذا اتحدت جميع الظروف فتقدم الدولة الأسبق في طلب التسليم[2] .

**تسليم المجرمين.**

كغيرها من الاتفاقيات الدولية والإقليمية تضمنت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تسليم المجرمين، حيث يمكن تبادل المجرمين بين الدول الأطراف في هذه الاتفاقية في جريمة الإرهاب الالكتروني، وهذا بشرط أن يكون قانون الدولة المعنية ينص بسلب الحرية على هذه الجريمة لفترة لا تقل عن سنة واحدة أو بعقوبة أشد وهذا وفقا لما نصت عليه المادة 31 من نفس الاتفاقية في فقرتها الأولى –أ .

أما إذا انطبقت عقوبة أدنى ومختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق (الفقرة الأولى –ب).

وإذا قامت أي دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم، ففي هذه الحالة وحسب هذه الاتفاقية يمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بجريمة الإرهاب الالكتروني –

[1] الفقرة الثانية من المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] الفقرة الثالثة من نفس المادة من ذات الاتفاقية.

على اعتبارها موضوع دراستنا فضلا على أنها تدخل ضمن الجرائم المنصوص عليها في الفقرة الأولى من المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[1].

أما بالنسبة للدول التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة الأولى من المادة 31 من نفس الاتفاقية والتي يدخل ضمنها جريمة الإرهاب الالكتروني قابلة لتسليم المجرمين بين تلك الدول وهذا حسب الفقرة الرابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

ويخضع تسليم المجرمين في جريمة الإرهاب الالكتروني للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب، أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها تسليم المجرمين، وهذا وفقا للفقرة 5 من المادة 31 من الاتفاقية لمذكورة.

وأما عن حالات الامتناع عن التسليم التي تضمنتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] وهي نفس الحالات التي نصت عليها اتفاقية بودابست من خلال المادة 24 منها والتي سبق شرحها في عنصر التعاون الدولي لمكافحة جريمة الإرهاب الالكتروني.

وبالنسبة لإجراءات التسليم وفقا للاتفاقية العربية لمكافحة تقنية المعلومات، فتلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين، أو التوقيف الإجرائي في ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

وتقوم الأمانة العامة لمجلس وزراء الداخلية العرب، والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائما[3].

[1] الفقرة الثالثة من المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] الفقرة 6 من المادة 31 السالفة الذكر.

[3] الفقرة 7-أ و ب من المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

**المساعدة القضائية المتبادلة.**

في إطار التعاون القضائي العربي لمكافحة جريمة الإرهاب الالكتروني يتعين على جميع الدول المتعاقدة تبادل المساعدة فيما بينها لأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجريمة الإرهاب الالكتروني، وتلتزم كل دولة طرف بتبني الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثون الى المادة الثانية والأربعون من هذه الاتفاقية، وهذا وفقا لما نصت عليه الفقرتين الأولى والثانية من المادة 32 من هذه الاتفاقية.

وعن إجراءات طلب المساعدة على المستوى الإقليمي العربي، يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني، على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير)، وتأكيد الإرسال حسب ما تطلب الدولة الطرف ، ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة عن الاتصالات[1] .

وتخضع المساعدة الثنائية تخضع للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة– باستثناء ما يرد فيه نص في هذه الاتفاقية– أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون (الفقرة الرابعة من المادة 32).

ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني والتي من ضمنها جريمة الإرهاب الالكتروني بناء على كون الطلب يخص جريمة تعتبر من الجرائم المالية[2].

[1] الفقرة الثالثة من المادة 32 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] الفقرة الرابعة من المادة 32 من نفس الاتفاقية.

**- تبادل المعلومات العرضية.**

حسب الاتفاقية العربية لمكافحة تقنية المعلومات فإنه يجوز للدولة الطرف ودائما ضمن حدود قانونها الداخلي وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسل إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية، أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف[1].

ويجوز للدولة قبل أن تعكي المعلومات للدولة الأخرى على نحو ما تم شرحه سابقا أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة المستقبلة للمعلومات أن تلتزم بهذا الطلب وجب عليها إبلاغ الدولة الطرف المزودة بذلك، والتي بدورها تقرر مدى إمكانية التزويد بالمعلومات مشروطة بالسرية، ويجب أن تبقى المعلومات بين الطرفين[2] .

في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطالبة والمطلوب منها، فتطبق الإجراءات التالية[3]:

- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.
- على السلطات المركزية أن تتصل ببعضها مباشرة.
- على كل دولة طرف أن تتصل وقت التوقيع وإيداع أدوات التصديق أو القبول أو الموافقة بالأمانة العامة لمجلس وزراء الداخلية العرب، والأمانة الفنية لمجلس وزراء العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة.
- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف ، وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائما .

[1] المادة 33 فقرة أولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] المادة 33 فقرة 2 من ذات الاتفاقية

[3] المادة 34 من نفس الاتفاقية الفقرات من 2-9 "الإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة".

- يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة.
- يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها.
- قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذا سيتم تلبية الطلب جزئيا أو يكون خاضعا للشروط التي قد تراها ضرورية.
- تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة بنتيجة تنفيذ الطلب، وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة للمساعدة بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو لأسباب التي تؤخره بشكل كبير.
- يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج ضمن التعاون القضائي ما عدا القدر الكافي لتنفيذ الطلب، وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.
- وفي الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.
- يجوز عمل الاتصالات وتقديم الطلبات بواسطة الانتربول[1].

[1] المادة 34 من نفس الاتفاقية الفقرات من 2-9 "الإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة".

- في حالة تقديم الطلب وفقا للإجراءات السابقة وكانت السلطة المطلوب منها غير مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك.
- إن الاتصالات والطلبات التي تتم والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.
- يجوز لكل دولة طرف وقت التوقيع أو التصديق أو القبول أو الإقرار أو الانضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب، والأمانة الفنية لمجلس وزراء العدل العرب لأن الطلبات يجب توجيهها إلى السلطة المركزية لغاية الفعالية.

ولا يمكن تطبيق كل هذه الإجراءات السابقة في حالة وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة طالبة المساعدة والمطلوب منها[1] .

ويجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب في حالة عدم وجود معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع الساري بين الدول الأطراف الطالبة للمساعدة والمطلوب منها بشرط[2]:

- الحفاظ على عنصر السرية للدولة الطرف الطالبة للمساعدة، ولا يتم الالتزام بالطلب في غياب هذا العنصر.
- عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب.
- إذا لم تستطع الدولة الطالبة الالتزام بالشرط السابق يجب عليها إعلام الدولة الطرف الأخرى والتي ستقرر بعدها مدى إمكانية توفير المعلومات، وإذا قبلت الدولة الطرف الطلب بهذا الشرط فهو ملزم لها.
- أي دولة طرف توفر المعلومات أو المواد بحسب الشرط السابق لتوفير المعلومات يجوز لها أن تطلب من الدولة الطرف الأخرى أن تبرر استخدام المعلومات أو المواد.

[1] المادة 34 فقرة أولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] المادة 36 من نفس الاتفاقية " السرية وحدود الاستخدام".

كما يجوز لأي دولة طرف في هذه الاتفاقية ودائما في إطار المساعدة المتبادلة أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة أو الواقعة ضمن أراضي الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها حسبما تنص هذه الاتفاقية، وتلتزم أيضا الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة.

وتتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة معرضة للفقد أو التعديل[1].

ويجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة أخرى طرف أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة بغض النظر عن الموقع الجغرافي للمعلومات، كما يجوز لها أن تستقبل معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة ن وهذا وفقا لما جاء في المادة 40 من هذه الاتفاقية(الوصول إلى معلومات تقنية المعلومات عبر الحدود ) .

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات الى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية[2] .

هذا وتكفل كل دولة طرف وفقا للمبادئ الأساسية لنظامها القانوني وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات التي من ضمنها جريمة الإرهاب الالكتروني –محل الدراسة– أو لجمع الأدلة بشكلها الالكتروني في جريمة معينة، ويجب أن تشمل مثل هذه المساعدة تسهيل أو تنفيذ[3] :

[1] المادتين 37 "الحفظ العاجل للمعلومات المخزنة في أنظمة المعلومات" و39" التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومة المخزنة" من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[2] المادة 42 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[3] المادة 43 من نفس الاتفاقية.

- توفير المشورة الفنية.
- حفظ المعلومات استنادا للمادتين 37 و38 من هذه الاتفاقية.
- جمع الأدلة وإعطاء المعلومات القانونية وتحديد مكان المشبوهين.
- يجب أن يكون لدى ذلك الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة.
- إذا لم يكن الجهاز المذكور المعين من قبل أي دولة طرف جزءا من سلطات تلك الدولة الطرف المسؤولة عن المساعدة الثنائية الدولية فيجب على ذلك الجهاز ضمان القدرة على التنسيق مع تلك السلطات بصورة عاجلة.
- على كل دولة طرف ضمان توفر العنصر البشري الكفء من أجل تسهيل عمل الجهاز المتخصص.

وفي الأخير يمكن القول أن هذه الاتفاقية محاولة جد محمودة من جامعة الدول العربية لمكافحة جريمة الإرهاب الالكتروني، لما تتمتع به الاتفاقية من مواكبة للاتفاقيات الدولية وتطوير أساليب وأسس التعاون العربي لمكافحة مثل هذه الجريمة المستحدثة.

## الفرع الثاني: الاستراتيجيات والقوانين العربية لمكافحة جريمة الإرهاب الالكتروني.

لمكافحة الجرائم الإرهابية بكل أشكالها ومظاهرها اعتمدت جامعة الدول العربية من خلال مجالسها، وقد انتهجت الجامعة العربية في سبيل ذلك العديد من الاستراتيجيات والقوانين التي أنتجت ثمارها في مكافحة الإرهاب الالكتروني والوقاية منه.

### أولا : الاستراتيجيات العربية لمكافحة الإرهاب الالكتروني.

وسوف نتعرض في هذا العنصر إلى أهم الاستراتيجيات العربية لمكافحة جرائم الإرهابية والوقاية منها كما يلي:

## 01- الإستراتيجية العربية لمكافحة الإرهاب 1997.

اعتمد مجلس وزراء الداخلية العرب في دورة انعقاده الرابع عشر في يناير 1997 إستراتيجية عربية لمكافحة الإرهاب، والتي تعتبر بمثابة القاعدة الصلبة التي تستند إليها الدول العربية فيما بينها في مكافحة هذه الجرائم.

وتهدف هذه الإستراتيجية إلى الدفاع عن الصورة الحقيقية للعروبة والإسلام، والحفاظ على أمن واستقرار الوطن العربي ودعم أسس الشرعية وسيادة القانون والنظام، وتوفير أمن الفرد العربي وضمان سلامة شخصيته وحريته وحقوقه وممتلكاته، وحماية أمن المؤسسات والهيئات والمرافق العامة فيه وتنمية وتطوير التعاون بين الدول العربية في مجال مكافحة الإرهاب، وتعزيز التعاون مع دول العالم في هذا المجال.

وركزت هذه الإستراتيجية على التدابير الوقائية، التي تمنع وقوع الجريمة ودراسة الأسباب التي تؤدي إلى وقوعها ووضع الحلول الجذرية لها، والعمل على تعزيز التعاون بين الدول العربية في المجالات القانونية والقضائية بغية تبسيط إجراءات تسليم المجرمين الإرهابيين، وتحقيق تعاون فعال في هذا الشأن.

وتحث الإستراتيجية العربية الدول الأعضاء على المشاركة في المؤتمرات الدولية الإقليمية الخاصة بمكافحة الإرهاب وإيصال وجهة النظر العربية للوقوف، في وجه المحاولات الرامية لتشويه صور الإسلام والمسلمين[1] .

ويعتمد تنفيذ هذه الإستراتيجية على خطط مرحلية مدتها ثلاث سنوات (قرت الأولى عام 1998) يساهم فيها كل من الأمانة العامة لمجلس وزراء الداخلية العرب(الجهاز الإداري والفني للمجلس) وجامعة نايف العربية للعلوم الأمنية(الجهاز العلمي والأكاديمي للمجلس) وتتضمن دعوة كل دولة عربية إلى اعتماد الآليات التالية:

[1] عمار تيسير بجبوج، مرجع سابق، ص 468.

- تشكيل لجنة وطنية لمكافحة الإرهاب مكونة من ممثلي الأجهزة المختصة، تتولى التوجيه والإشراف والتنسيق بين مختلف الأجهزة التي تشارك في أنشطة مكافحة الإرهاب.
- إنشاء وحدة متخصصة لجمع المعلومات عن الأعمال الإرهابية، وتحليلها وتبادلها مع الأجهزة الأمنية المعنية الأخرى.
- إنشاء وحدة خاصة لمكافحة الإرهاب ذات كفاءة عالية، وتجهيز مناسب للتعامل مع الأعمال الإرهابية.

وتم تنفيذ الإستراتيجية العربية لمكافحة الإرهاب وفق مرحلية سادسة (2013-2015) أقرها مجلس وزراء الداخلية العرب، وتهدف إلى الاستمرار في متابعة تنفيذ بنود الإستراتيجية لتحقيق مواجهة فعالة للإرهاب بكافة أشكاله وصوره (ومنها جريمة الإرهاب الالكتروني) وتجفيف منع تمويله، مع اتخاذ كل ما يلزم لمنع تسرب تصنيع الأسلحة الكيميائية والبيولوجية للإرهابيين، وحث الدول العربية على أن تكون مستعدة بشكل كامل لمواجهة أي تهديدات تمثلها الجماعات الإرهابية وتستخدم فيها الأسلحة البيولوجية والكيميائية[1] .

هذا وتولي الخطة السادسة أهمية كبيرة لشبكة الانترنت، حيث أن المكتب العربي للإعلام الأمني الذي مقره القاهرة يقوم بمتابعة المواقع الالكترونية التي تحث على نشر الأفكار المتطرفة، أو التي تعمل على تجنيد إرهابيين جدد بالإضافة إلى المواقع الالكترونية التي تحتوي على إرشادات حول صنع المتفجرات والأسلحة، ويقوم المكتب بموافاة الدول العربية بأسماء هذه المواقع لمراقبتها ورصدها والعمل على إغلاقها.

وفيما يتعلق بمواقع التواصل الاجتماعي، فتقابلها جهود مكثفة لمنع استغلالها من قبل الإرهابيين والمتطرفين، حيث حثت الخطة المرحلية السادسة الدول على وضع ضوابط وشروط لاستعمال تلك المواقع ضمن تدابير وقائية تعزز سياسة تجفيف منابع الإرهاب.

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 03.

وترسيخا لأحد أهم أهداف "الإستراتيجية العربية لمكافحة الإرهاب" في مجال التعاون العربي اعتمد مجلسا وزارة العدل والداخلية العرب في اجتماعهما المشترك سنة 1998 "الاتفاقية العربية لمكافحة الإرهاب"[1].

## 02- الإستراتيجية العربية للأمن الفكري 2013.

يتضمن الأمن الفكري كمفهوم معايير مختلفة ومنها الأمن الفكري والسياسي والاجتماعي والأمن الفري الاقتصادي، وكلها عمليات دقيقة تحدث خلال عمليات التفاعل المتوقعة بين الثقافة والمجتمع.

ووعيا من جامعة الدول العربية بأن الأمن الفكري بات اليوم مجالا لا غنى في العمل الرامي إلى مواجهة الإرهاب، إذ أن المواجهة الفكرية للإرهاب هي الوحيدة التي من شأنها تجفيف منابعه وتصحيح الأفكار المغلوطة وإعادة المغرر بهم إلى جادة الصواب، أصدر مجلس وزراء الداخلية العرب قرارا برقم 613، د 2011/28 بشأن "مشروع الإستراتيجية العربية للأمن الفكري" ينص على الطلب إلى الأمانة العامة تشكيل لجنة مفتوحة العضوية من الدول الأعضاء لدراسة مشروع الإستراتيجية العربية للأمن الفكري، وعرض على الموضوع على دورة مقبلة للمجلس.

وقد تضمنت توصيات الاجتماع الحادي عشر لفريق الخبراء العرب المعني بمكافحة الإرهاب (القاهرة 5-6 سبتمبر 2011) التي اعتمدها مجلس الجامعة على المستوى الوزاري بالقرار رقم 7394 بتاريخ 13 سبتمبر 2011 "إشراك رئيس فريق الخبراء العرب والأمانة الفنية للفريق كطرف أساسي في اجتماعات اللجنة مفتوحة العضوية المنشأة بموجب قرار مجلس وزراء الداخلية العرب رقم 613 د2011/28 بشأن مشروع الإستراتيجية العربية للأمن الفكري، وعرض الموضوع على الاجتماع المقبل للفريق"

ومن جهته أكد مجلس الجامعة على المستوى الوزاري بالقرار رقم 7468 د.ع 137 -10 مارس 2012 على دعم جهود مجلس وزراء الداخلية العرب بشأن إعداد مشروع الإستراتيجية العربية للأمن الفكري ودعوة الدول العربية إلى عرض مرئياتها على اللجنة مفتوحة العضوية المشكلة في هذا الشأن

[1] نفس المرجع، ص 03.

وقد انعقد اجتماع اللجنة المعنية بدراسة مشروع الإستراتيجية العربية للأمن الفكري في مقر مجلس وزراء الداخلية بتونس، خلال يومي 4-5 جويلية 2012 الذي اعتمده مجلس وزراء الداخلية العرب في دورته الثلاثون المنعقدة بالمملكة العربية السعودية في مارس 2013.

وتتجلى أهم مضامين الإستراتيجية فيما يلي[1]:

- إنشاء إدارات أو وحدات متخصصة في كل دولة تمثل المرجعية العلمية والإدارية تتولى وضع الاستراتيجيات والتشريعات الوطنية، ورسم خطط وبرامج الأمن الفكري بالتنسيق مع المؤسسات الحكومية والأهلية، وبناء قواعد البيانات والمعلومات ووضع المعايير والإشراف على تنفيذ الأنشطة والفعاليات ذات الصلة، وتقويمها حسب إمكانيات الدول وتقديراتها.
- تعزيز التعاون العربي- العربي والتعاون العربي- الدولي في مجال الأمن الفكري.
- تشجيع البحث العلمي لتشخيص الواقع واستكشاف الأساليب الحديثة والمستجدات العلمية التي تسهم في تعزيز الأمن الفكري.
- وضع خطط مرحلية لتنفيذ الإستراتيجية تتضمن مجموعة من البرامج تقوم بتنفيذها الأمانة العامة لمجلس وزراء الداخلية العرب وجامعة نايف العربية للعلوم الأمنية.
- إنشاء مكتب عربي للأمن الفكري بالرياض تابع للأمانة العامة لمجلس وزراء الداخلية العرب إنشاء هذا المكتب في دورته 31 المنعقدة بالمملكة المغربية في مارس 2014.

## ثانيا: قوانين الجامعة العربية في مجال مكافحة الإرهاب الالكتروني.

اعتمدت جامعة الدول العربية جملة من القوانين لمكافحة الجرائم الإرهابية بكل مظاهرها وصورها وهذا محاولة من الجامعة للحد من هذه الظاهرة الإجرامية التي أصبحت في تطور مستمر إلى أن وصلت إلى جريمة الإرهاب الالكتروني.

### 01- القانون العربي النموذجي لمكافحة الإرهاب 2002.

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 03.

ينشأ القانون النموذجي نمط مقترح على المشرعين في الحكومات الوطنية للنظر في اعتماده كجزء من تشريعاتهم الداخلية، فهو نمط لقانون المراد منه أن تشرعه الحكومات كتشريع داخلي، ويكون من الناحية الفعلية مثل أي مشروع قانون آخر يقره البرلمان، ومن ثم لا توجد به قوائم "موقعين" كالتي توجد في حالة المعاهدات[1] .

وقد تم إقرار القانون العربي النموذجي لمكافحة الإرهاب سنة 2002 من قبل مجلس وزراء الداخلية العرب كخطوة لدعم جهود جامعة الدول العربية في سن قوانينها الوطنية وبناء قدراتها في هذا المجال، وكترسيخ لأحد الأهداف المسطرة من قبل الإستراتيجية العربية لمكافحة الإرهاب لسنة 1997.[2]

ويعتبر القانون العربي النموذجي لمكافحة الإرهاب بمثابة مرجع لتنفيذ الالتزامات المنبثقة عن معايير حددتها الاتفاقية العربية لمكافحة الإرهاب، ومن شأنه تعزيز القدرة التشريعية للدول العربية لمكافحة هذه الآفة.

ويتميز القانون العربي النموذجي لمكافحة الإرهاب بأنه قابل للتوسيع وشامل يضم كل الإجراءات القانونية للوقاية من الأعمال الإرهابية ومكافحتها، وهو يتضمن 25 مادة موزعة على ثلاثة فصول.

تضمن الفصل الأول التعريفات، ويتكون من مادتين تعرفان الإرهاب والجريمة الإرهابية مع تعداد عدد من الجرائم التي لا تعد سياسية ولو كانت بدافع سياسي من قبيل التعدي على الملوك ورؤساء الدول، أو التعدي على الأشخاص المتمتعين بحماية دولية، أو القتل العمد والسرقة المصحوبة بالإكراه ضد الأفراد أو السلطات أو وسائل النقل والمواصلات[3] .

أما الفصل الثاني والذي يشتمل المواد من 3 إلى المادة 20 فهو يعنى بالعقوبات، وهي تتراوح بين الإعدام والسجن المؤبد والسجن المحدد على حسب الحالات التي يعددها القانون علما أن المادة 20 تنص على مايلي:" يعفى من العقوبات المقررة للجرائم الإرهابية المنصوص عليها في هذا القانون

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 03.

[2] إستراتيجية جامعة الدول العربية في مكافحة الإرهاب متوافرة على الرابط: https://repository.nauss.edu.sa

[3] القانون العربي النموذجي لمكافحة الإرهاب لسنة 2002.

كل من بادر من الجناة بإبلاغ السلطات الإدارية أو القضائية قبل البدء في تنفيذ الجريمة، ويجوز للمحكمة الإعفاء من العقوبة إذا حصل الإبلاغ بعد إتمام الجريمة، وقبل البدء في التحقيق ومكن الجاني السلطات من القبض على مرتكبي الجريمة الآخرين، أو على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة"

أما الفصل الثالث والأخير يشتمل على المواد المتبقية أي من المادة 21 إلى المادة 25 فيحمل عنوان "أحكام مختلفة" مرتبطة بالأساس بالحماية الأمنية اللازمة للمخبر أو الشاهد أو الخبير في الجرائم الإرهابية، وبالمساعدات اللازم ضمانها تشريعيا لضحايا الإرهاب.

ويدعو الفصل الأخير من القانون العربي النموذجي لمكافحة الإرهاب إلى إصدار تشريعات خاصة بتوفير الحماية للعاملين في ميدان العدالة الاجتماعية.

بعد سنة 2002 تعزز الإطار العربي تحت مظلة جامعة الدول العربية بقوانين استرشادية نموذجية أخرى ذات الصلة بالإرهاب، وهي:

- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها والذي يعتمده مجلس وزراء العدل العرب سنة 2003 ومجلس وزراء الداخلية العرب سنة 2004.
- القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية والذي اعتمده مجلس وزراء العدل بتاريخ 29 نوفمبر 2006.
- القانون العربي الاسترشادي لمكافحة غسيل الأموال وتمويل الإرهاب والذي اعتمد بموجب قرار مجلس وزراء العدل العرب رقم 1000/د 29 بتاريخ 26 نوفمبر 2013 بصنعاء- اليمن، وقد جاء كخطوة إضافية للإطار التشريعي الذي استهلته الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب في هذا الشأن[1].

## 02- القانون العربي الاسترشادي لمكافحة غسل الأموال وتمويل الإرهاب 2013.

دائما في إطار الجهود المبذولة للحد من ظاهرة غسل الأموال وتمويل الإرهاب، وتماشيا مع المواثيق والمعايير الدولية تم اعتماد القانون العربي الاسترشادي لمكافحة غسل الأموال وتمويل

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 03.

الإرهاب وذلك بموجب قرار مجلس وزراء العدل العرب رقم 1000/د 29 بتاريخ 26 نوفمبر 2013 في صنعاء– اليمن.

ويرجع اعتماد هذا القانون الذي يشتمل على سبع وعشرون مادة على ضوء ما ورد في المنهجية المستحدثة بالمعايير الدولية في مجال غسل الأموال وتمويل الإرهاب، حيث جاء هذا القانون متفقا مع التوصيات الصادرة عن لجنة العمل المالي الدولي والمذكرات التفسيرية لها، ومع ما تضمنته الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب .

وعن تفاصيل القانون تعرضت المادة الثانية منه على تعريف أهم المصطلحات التي يرتكز عليها هذا القانون وهو مصطلح "غسل الأموال" حيث آثر المشرع أن يستخدم تعبير غسل الأموال بدلا عن غسيل الأموال باعتبار أن الغسل في اللغة هو إزالة الأوساخ عن شيء، في حين أن الغسيل هو كناية عن الشيء المغسول نفسه، وبذلك يكون الغسل أدق في الإفصاح عن المعنى المرجو من هذا القانون[1].

ويلاحظ على هذا القانون ان المشرع توسع في مجال غسل الأموال فنص على صور متعددة للسلوك الإجرامي حرصا على تغطية كافة جوانب السلوك الإجرامي.

وحرصا من المشرع على توضيح أهمية التعاون الدولي في مكافحة مثل هذه الجرائم وخاصة الإرهاب، عنيت المواد 22، 23، 24 من القانون على إيلاء أهمية خاصة للتعاون القضائي الدولي فأتاح للجهات القضائية تبادل يد العون بخصوص المساعدات والإنابات القضائية وفي تسليم المتهمين والمحكوم عليهم والأشياء في ضوء أحكام الاتفاقية الثنائية أو متعددة الأطراف، ووفقا لمبدأ المعاملة بالمثل[2].

ورغبة في تحقيق المزيد من التعاون الدولي أجازت المادة 25 من القانون للجهات القضائية أن تأمر بتنفيذ الأحكام الجنائية النهائية الصادرة من الجهات القضائية في الدول الأخرى بمصادرة الأموال في جرائم غسل الأموال وجرائم تمويل الإرهاب، وذلك في إطار القواعد والإجراءات المنصوص عليها في الاتفاقيات الثنائية أو متعددة الأطراف والتي تكون الدولة المطلوب فيها الإجراء طرفا فيها.

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 04.
[2] القانون العربي الاسترشادي لمكافحة غسل الأموال وتمويل الإرهاب.

كما أجازت المادة ومن أجل تحقيق نفس الغرض إبرام اتفاقيات ثنائية أو متعددة الأطراف تنظم التصرف في حصيلة الأموال المحكوم نهائيا بمصادرتها في تلك الجرائم وقواعد توزيع هذه الحصيلة بين الدول الأطراف.

أما المادة 26 من نفس القانون فقد نصت على الإجراءات التفصيلية من أجل تنفيذ أحكام هذا القانون وذلك بأن تصدر السلطة المختصة في كل دولة اللائحة والقرارات التنفيذية للمشروع خلال المدة التي تقررها[1] .

## 03- القانون الإماراتي العربي الاسترشادي لمكافحة تقنية المعلومات.

بعد أن أصبحت جرائم الانترنت مشكلة عالمية تؤثر على كل دول العالم، وخاصة أن الجرائم المعلوماتية ومنها جريمة الإرهاب الالكتروني لا تخضع للسيطرة القوية، وخاصة أن عدد ضحايا هذا النوع من الجرائم في تزايد مستمر فقد بلغ على الصعيد العالمي 431.21 مليون، السبب الذي دفع معظم دول العالم ومنها الدول العربية إلى تبني مجموعة من القوانين الصارمة للتصدي لهذا النوع من الجرائم، وأيضا تبني برامج وخطط لمكافحتها.

ونظرا لأن أجهزة الكمبيوتر والانترنت تلعب دورا أساسيا ومهما في تسهيل ارتكاب الجرائم التقليدية كجريمة الإرهاب، وقد أكدت دراسة لشركة خليجية للحاسبات الآلية G.BM في سنة 2013 أن خبراء تكنولوجيا المعلومات في دول مجلس التعاون يؤكدون أن منطقة الخليج تشكل هدفا رئيسيا للجرائم الالكترونية، كما ورد في تقرير "Norton Symantec " لسنة 2013 أن كلا من المملكة العربية السعودية ودولة الإمارات العربية المتحدة من دول مجلس التعاون الخليجي، ضمن الأربع وعشرين دولة الأولى في العالم التي تزيد فيها التهديدات المقلقة بتسرب البيانات .

وبما أن تطور تكنولوجيات الاتصالات والمعلومات يجري على مستوى دولي خارجا عن نطاق سيطرة هذه الدول، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الانترنت يشكل تحديا كبيرا للحكومات وبالتالي إن جرائم الانترنت تمثل تحديا كبيرا للحكومات، وبالتالي فان جرائم الانترنت تمثل تحديا كبيرا للأجهزة القانونية في كل من البلدان المتقدمة والنامية على السواء.

[1] ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، مرجع سابق، ص 04.

وضمن جهود مجلس وزراء العدل العرب لجامعة الدول العربية في مكافحة الجرائم الالكترونية ومنها الإرهاب الالكتروني، قرر هذا المجلس اعتماد "قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها 2004"[1].

ويتكون قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها من 27 مادة ، تضمنت المادة الأولى التعريف للمصطلحات المهمة والتي تساعد على توضيح مفهوم الجريمة أكثر.

وعن جريمة الإرهاب الالكتروني فقد خصصت له المادة 21 منه بقولها: " كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن...."[2].

تضمن أيضا هذا القانون كغيره من القوانين النص على المساهمة الجنائية على الجرائم المنصوص عليها في الفصل الأول ومن بينها جريمة الإرهاب الإلكتروني.

أما المشرع فقد نصت عليه المادة 24 من هذا القانون ، وقد قررت للشروع في جريمة الإرهاب الالكتروني بنفس العقوبة المقررة للجريمة[3].

وقد اعتمد هذا القانون من طرف مجلس وزراء العدل العرب في دورته التاسعة عشرة بموجب القرار رقم 495-د 19 في 8 أكتوبر 2003، أما مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بموجب القرار رقم 417-د 2004/21.

---

[1] ليلى حسين، فعالية القوانين الوطنية والدولية في مكافحة الجرائم الالكترونية، بحث في العلوم القانونية، قسم القانون في الأكاديمية العربية في الدانمارك، منشورة في موقع المنهل: https://platform.almanhal.com، تاريخ الاطلاع 2018/07/26 على الساعة 00:49.

[2] قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2004 والذي اعتمده مجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم 417 سنة 2004 .

[3] تنص المادة 24 من القانون الإماراتي العربي الاسترشادي لمكافحة تقنية المعلومات بقولها: " يعاقب على الشروع في الجرائم المنصوص عليها في المواد ( 3-15 ) بنصف العقوبة المقررة لها ويعاقب على الشروع في الجرائم المنصوص عليها في المواد (16-22 ) بذات العقوبة المقررة لها".

ولم ينص هذا القانون على التعاون الأمني والقضائي بين الدول العربية كغيره من القوانين الباقية إلا أن لهذا القانون الفضل في تعريف المصطلحات وأيضا تعداد الجرائم الالكترونية وخاصة منها جريمة الإرهاب الالكتروني.

## الفصل الثاني: الآليات الدولية العالمية في مكافحة الإرهاب الالكتروني.

إن اهتمام المنظمات الدولية العالمية بظاهرة الإرهاب الالكتروني ظهر بصورة جلية بعد أحداث الحادي عشر من سبتمبر من سنة 2001، على عكس اهتمامها بظاهرة الإرهاب التقليدي، الذي ظهر بظهور موجة العنف في الكثير من دول العالم حيث ظهرت الكثير من التنظيمات الإرهابية التي تعمل بأساليب وحشية ضاربة بذلك الأنظمة السياسية لمختلف الدول، الأمر الذي أدى إلى انتشار الخوف والفزع في الكثير من دول العالم جراء الاعتداءات الإرهابية المختلفة .

هذه الأوضاع التي آل إليها العالم أدت بكل من الأمم المتحدة ومنظمة الشرطة الجنائية الدولية بأجهزتهما المختلفة التدخل بموجب إجراءات صارمة لمكافحة مختلف جرائم الإرهاب.

وبما أن جريمة الإرهاب الالكتروني ما هي إلا صورة جد متطورة ومستحدثة للإرهاب التقليدي فإن اهتمام هذه المنظمات الدولية العالمية بها تغير بتغير وسائل ارتكاب هذه الجريمة المستحدثة، جراء ذلك اتخذت وسائل مكافحة الإرهاب الالكتروني مسار آخر يسعى ليتناسب مع تطور وسائل ارتكاب هذه الجريمة.

إلى جانب جهود المنظمات السابقة في مكافحة الإرهاب الالكتروني كرست الاتفاقيات الدولية مبدأ التعاون القضائي بين الدول المختلفة في مكافحة هذه الجريمة العابرة للحدود، حيث تطورت وسائل الاتصال التي سهلت عملية التواصل بين مختلف التنظيمات الإرهابية، ويتضمن هذا التعاون التنسيق بين مختلف الجهات القضائية في إطار تنفيذ الأحكام الجزائية وتسليم المجرمين وتنفيذ الإنابات القضائية، بالإضافة إلى مباشرة التحريات حول التنظيمات الإرهابية كما يشمل إجراءات المحاكمة، وعليه فإن التعاون القضائي في مكافحة جريمة الإرهاب الالكتروني يستغل التطور العلمي في تطوير أساليب عمله وتسهيل مهام الأجهزة المختصة في هذا المجال.

ومما سبق ومن أجل توضيح كل النقاط التي سبق الحديث عنها ارتأينا تقسيم هذا الفصل إلى مبحثين كالتالي:

المبحث الأول: دور المنظمات الدولية العالمية في مكافحة جريمة الإرهاب الالكتروني.

المبحث الثاني: التعاون القضائي الدولي في مجال مكافحة جريمة الإرهاب الالكتروني.

## المبحث الأول: دور المنظمات الدولية العالمية في مكافحة جريمة الإرهاب الالكتروني.

لعبت منظمة الأمم المتحدة دورا مهما وفعالا في مكافحة الإرهاب ، فقد قامت بأول دراسة عن الإرهاب الدولي سنة 1972 بهدف الوصول إلى اتفاق عالمي حول تحديد موحد يكون ساريا في جميع دول العالم، لكن ذلك لم يتحقق وباءت هذه المحاولة بالفشل، إلا أن منظمة الأمم المتحدة واصلت سعيها في مكافحة الإرهاب من خلال اللجان التي شكلتها والقرارات الصادرة عنها في مجال التنديد بمختلف أشكال الإرهاب ، فلهذه المنظمة كبير الفضل في إبرام العديد من الاتفاقيات التي اعتبرت مكسب تشريعي مهم لجميع الدول الأعضاء في تعديل تشريعاتها الداخلية.

بالمقابل وفي نفس السياق نجد لمنظمة الشرطة العالمية دور مهم لا يمكن تجاهله في إيجاد الوسائل الكفيلة لمكافحة الإرهاب مهما تطورت صوره وتعددت أشكاله، ويتضح ذلك جليا من خلال جهودها المبذولة بواسطة إصدارها لقرارات وتوصيات، وإنشاء لجان خاصة بمكافحة هذه الجريمة الخطيرة والتي تتطور مع التطور العلمي والتكنولوجي، هذا الأمر جعل من منظمة الشرطة العالمية من المنظمات الهامة والمتخصصة في محاربة جرائم الإرهاب ومنها جريمة الإرهاب الالكتروني، فقد سعت بكل ما تملكه من إمكانيات في الحد من جريمة الإرهاب الالكتروني .

ولإبراز الدور المهم في مكافحة جريمة الإرهاب الالكتروني لكل من منظمة الأمم والمتحدة ومنظمة الشرطة الجنائية الدولية قسمنا هذا الفصل إلى مطلبين كمايلي:

المطلب الأول: دور الأمم المتحدة في مكافحة الإرهاب الالكتروني.

المطلب الثاني: دور منظمة الشرطة الجنائية الدولية مكافحة الإرهاب الالكتروني.

## المطلب الأول: دور الأمم المتحدة في مكافحة الإرهاب الالكتروني.

تأسست هيئة الأمم المتحدة بموجب البند الرابع من بيان موسكو الصادر بتاريخ 1943/10/30 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 1943/12/01، وفي الفترة ما بين 08/21 إلى غاية 10/07 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 1945/04/25 وخلال هذا المؤتمر تم الاتفاق على ميثاق يتكون من 111 مادة تتمحور حول مبدأ المساواة بين جميع الشعوب، والحفاظ على السلم والأمن الدوليين[1]، حيث كان لكل من الجمعية العامة ومجلس الأمن الدور الهام والأكبر في مكافحة جرائم الإرهاب.

وقد عملت هذه المنظمة وفقا لإجراءات واكبت من خلالها جل الأحداث الدولية والتي صاحبها تطور في الأفعال الإجرامية للمنظمات الإرهابية، ويظهر هذا بوضوح من خلال القرارات التي تم إصدارها في هذا المجال، وخاصة بعد أحداث 11 سبتمبر 2001 وظهور جريمة الإرهاب الالكتروني كصورة مستحدثة وجد متطورة للإرهاب.

وسوف يتم تفصيل هذا العنصر من خلال فرعين، نتناول في الأول دور كل من الجمعية العامة ومجلس الأمن في مكافحة الإرهاب الالكتروني

### الفرع الأول: دور الجمعية العامة في مكافحة الإرهاب الالكتروني .

كان تدخل الأمم المتحدة في مكافحة الإرهاب بكل صوره وأشكاله ضروريا وهذا بسبب تصاعد الهجمات الإرهابية وتطورها حتى مست الكثير من بقاع الأرض إن لم نقل جميعها وهذا في الوقت الذي كانت فيه العديد من الدول تفتقر للآليات الوطنية والتشريعية والإجرائية لمكافحة الإرهاب مهما تطورت صورته، فعدم وجود تعريف محدد وموحد بين جميع دول العالم دفع بمنظمة الأمم المتحدة

[1] ساعد الهام حورية، مرجع سابق، ص 10.

لعقد مؤتمرات ولقاءات سعت أن تكون ايجابية ومجدية في مجال تحديد مفهوم للإرهاب، وإيجاد الأساليب التي من شانها الحد من زحف وخطورة التنظيمات الإرهابية، فأشرفت على العديد من المؤتمرات التي تعتبر بمثابة آلية من آليات التصدي لظاهرة الإرهاب بمختلف أشكاله، كما استندت الجمعية العامة للأمم المتحدة على أسلوب إصدار القرارات للتعبير عن رفضها الشديد للإرهاب ولزحف التنظيمات المتطورة للإرهاب، فكانت قراراتها في بادئ الأمر مجرد توصيات لا تحمل في طياتها أي معنى للإلزامية بل مجرد محاولة للتعبير عن رفض الجمعية العامة للإرهاب، إلا أن الدول اعتمدتها فيما بعد في سياساتها الجنائية المعادية للإرهاب.

في العقود الأخيرة من القرن العشرين، مضت الدول الأعضاء قدمًا في عملها في مجال مكافحة الإرهاب، عن طريق الجمعية العامة للأمم المتحدة على كل من المسارين القانوني والتنفيذي، وقد توصّلت هذه الأخيرة، نتيجة جهودها، إلى اعتماد العديد من الاتفاقيات والبروتوكولات الدولية التي تتناول الإرهاب. وتوِّج عملها باعتماد إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، في 8 أيلول 2006، وقد شدّدت الدول الأعضاء على أهمية الصكوك الدولية القائمة لمكافحة الإرهاب.

ويمكن أن نلخص جهود الجمعية العامة فيما يلي:

**أولا: عقد لقاءات ومؤتمرات لدراسة ظاهرة الإرهاب.**

قبل أحداث الحادي عشر من سبتمبر 2001 عقدت العديد من المؤتمرات تحت إشراف الجمعية العامة للأمم المتحدة، كندوة بروكسل، التي أشرفت عليها الجمعية العامة البلجيكية للحقوقيين الديمقراطيين عام 1973 بالتعاون مع مركز القانون الدولي، حيث ناقشت هذه الندوة مسألة الإرهاب ورغم محاولة إيجاد تعريف موحد وشامل ودقيق للإرهاب إلا أنها لم توفق في ذلك، فانبثق عن هذه الندوة بعض النصوص القانونية التي تجرم بعض الأفعال الإرهابية، أما مؤتمر جنيف سنة 1975 والذي كان حول " ظاهرة العنف ذو الأهمية عبر القومية والعالمية المقارنة"، حيث حاول المؤتمرون من خلاله وضع تعريف للظاهرة الإرهابية، إلا أن هذه المحاولة باءت هي الأخرى بالفشل، ويرجع السبب في ذلك إلى خلو التشريعات الداخلية من النصوص التي يمكن بواسطتها تجريم السلوك الإجرامي الذي يمكن اعتباره من قبيل العمل الإرهابي[1].

[1] إمام حسانين عط الله ، مرجع سابق، ص 189، 190.

وفي سنة 1990 وبالضبط في مؤتمر هافانا بكوبا طرحت من جديد مسألة الإرهاب بشكل واضح من خلال جدول أعماله والذي نتج عنه صدور القرار رقم 32 المتعلق "بالأنشطة الإجرامية والإرهابية"، وتدابير مكافحة الإرهاب الدولي، فنص على ضرورة استحداث تدابير على الصعيدين الدولي والإقليمي والثنائي من شانها مواجهة العنف الإرهابي أساسها التعاون بين أجهزة إنفاذ القانون وسلطات النيابة العامة والقضاء مع ضرورة التعاون والتكامل بين مختلف الأجهزة المسؤولة عن إنفاذ القانون والعدالة الجنائية وإيلاء الاهتمام لأجهزة حقوق الإنسان[1] .

في مؤتمر القاهرة والذي انعقد سنة 1995 تم ربط الإرهاب بالجريمة المنظمة بناءا على اقتراح مصري، في حين طرح مؤتمر فيينا الذي انعقد في الفترة من 10 إلى 17 أفريل 2000 للنقاش موضوع " الجريمة والعدالة ومواجهة تحديات القرن الحادي والعشرون"، وقد شاركت فيه العديد من الدول بالإضافة إلى منظمات حكومية وغير حكومية، فالمؤتمر كان فرصة للاتفاق حول خطة عمل لمكافحة الجريمة المنظمة بما فيها الجريمة الإرهابية، وهذه الخطة بنيت على ضرورة إيجاد أساليب لمواجهة تحديات الجريمة خاصة المستحدثة منها كالإرهاب الالكتروني، وقد أكد المؤتمر على تعزيز أطر التعاون بين الدول بين الدول مع استحداث نظام عدالة أساسه حماية الضحايا والحد من زحف الإجرام العابر للأوطان، فهذه المؤتمرات لم يكن لها الشأن الكبير في تعريف الإرهاب ولا في تحديد الوسائل التي بواسطتها يمكن مكافحته، لكن نظرة الأمم المتحدة للإرهاب كان لها وجها واتجاها آخر بعد أحداث سبتمبر 2001، فزاد اهتمامها بالإرهاب المستحدث، وأشرفت على عقد لقاءات ومؤتمرات أخرى على المستوى الدولي، وقد طرحت من خلالها العديد من المواضيع منها قضية منع تمويل وتدعيم الإرهاب[2] .

وبعد هذه النبذة حول أهم مؤتمرات الجمعية العامة قبل أحداث 11 سبتمبر 2001 سوف نتعرض إلى أهم هذه المؤتمرات بعد أحداث 11 سبتمبر لأنها ما يهم موضوع دراستنا، من اجل التعرف على دور الجمعية العامة في مكافحة الإرهاب الالكتروني كمايلي:

### 01- مؤتمر الجزائر الدولي.

انعقد هذا المؤتمر في الجزائر العاصمة في الفترة من 27 إلى 29 أكتوبر 2002، وكان حول الإرهاب، وتم هذا الملتقى الدولي بحضور أكثر من 200 مشارك منهم بعض منظمات حقوق

[1] ساعد الهام حورية، مرجع سابق، ص 12.

[2] Thierry Meyssan,11septembre2001, L'effroyable imposture, Ed Carnot, Paris ,p 89.

الإنسان، وقد برمجت في هذا المؤتمر أكثر من 40 مداخلة في الورشات العامة، خصص لمناقشة موضوع الإرهاب أربع ورشات، الورشة الأولى خصصت لدراسة الإرهاب الإسلاموي وأعمال العنف بينما الورشة الثانية فكانت لدراسة تطور أسلوب الاغتيالات الفردية والجماعية والوسائل التي لجأت إليها التنظيمات الإرهابية في تنفيذ عملياتها الإجرامية تحت غطاء الدين، أما الورشة الثالثة فقد ركزت اهتمامها على مجال التعاون الدولي في مجال محاربة الإرهاب وجميع الجرائم العابرة للأوطان، وأما الورشة الرابعة فقد اهتمت بموضوع العلاقة بين الإرهاب والإعلام وحقوق الإنسان، وهذا لعدة اعتبارات تمحورت أساسا حول اعتماد الإرهاب على وسائل الإعلام للدعاية والتأثير على الرأي العام، ودور الإعلام في التحسيس بخطورة الإرهاب[1].

هذا وقد دعا مؤتمر الجزائر أيضا الدول المشاركة إلى تحضير مشروع اتفاقية دولية تجمع بين الدول الأعضاء، تكون هذه الاتفاقية مكسب تشريعي لكافة الدول في مجال الوقاية ومكافحة الإرهاب وقد جاءت هذه الفكرة اثر مداخلة للسيد ممثل خلية مكافحة الإرهاب على مستوى مركز الأمم المتحدة للوقاية من الإجرام العابر للحدود السيد "**ألكس سميث**"، وقد تضمنت عرض دور الأمم المتحدة في تجسيد مبدأ الوقاية من الإرهاب، بحيث تعمل هذه المنظمة الدولية جاهدة على إيجاد أسس لتنمية التعاون الدولي وتمكين الدول الأعضاء من مواجهة الخطر الجديد المهدد لكافة دول العالم، والمتمثل في الإرهاب بمختلف أشكاله، وان سياسة التعاون الدولي لا يمكن أن تتجسد ميدانيا إلا في إطار اتفاقية تجمع كافة الدول، على غرار تلك الاتفاقية الخاصة بالجريمة العابرة للأوطان، كما أضاف أيضا ممثل الأمم المتحدة أن منظمة الأمم المتحدة باعتبارها منظمة دولية مهمتها الحفاظ على السلم والأمن الدوليين فلها الحق في إنشاء قواعد قانونية دولية يلتزم بها أعضاء المجتمع الدولي، مؤكدا أن هذه المنظمة ستقدم الدعم من أجل تأسيس مراكز أو مؤسسات خاصة في الدول التي تحتاج لهذا الدعم في مجال مكافحة الإرهاب[2].

### 02- مؤتمر أذربيجان لمواجهة تحديات الإجرام الخطير.

انعقد مؤتمر دولي حول تعزيز إطار التعاون بين الدول في مجال مكافحة الإرهاب بمختلف أشكاله وذلك في عاصمة أذربيجان في الفترة مابين 18 و19 مارس 2013، تحت إشراف المنظمة

[1] ساعد الهام حورية، مرجع سابق، ص 14.

[2] نفس المرجع، ص 14.

الإسلامية للتربية والعلوم والثقافة إيسيسكو، بالتعاون مع مكتب المخدرات والجريمة للأمم المتحدة، بغية تأسيس تبادل واستقراء الآراء بشان مواجهة تحديات الإرهاب والمساعدة على الفهم الجيد للظاهرة وتقديم أفكار لمواجهة جميع الأنماط والتصورات الخاطئة التي من شأنها إشاعة جو من العداء وانعدام الثقة بين الدول[1].

كما حث المشاركون على ضرورة تقديم الدعم واقتراح مشاريع تمكن مكتب الأمم المتحدة المعني بمكافحة المخدرات والجريمة في مواجهة مختلف المستجدات التي تنشا من جراء تطور جرائم الإرهاب ووسائل ارتكابه في زمن التطور التكنولوجي والتغير في السياسات الدولية في مختلف الجوانب، كما تم من خلال هذا المؤتمر مناقشة مواضيع تتعلق بالتنمية الاجتماعية وأساليب إعادة الإدماج الاجتماعي ومنع النزاعات ودعم ضحايا الإرهاب.

هذا وقد تعرض المؤتمرون أيضا إلى بعض المواضيع الخاصة بحوار الثقافات والتحالف بين الحضارات ودورهما في مواجهة الإرهاب وخاصة الالكتروني، كحظر التحريض على تلك الأفعال ومكافحة استغلال تلك الصراعات في تنمية الإرهاب، أيضا ضرورة تقديم المساعدات الفنية في إعداد التشريعات وتدريب القضاة والمدعين العامين والمحققين من أجل تمكينهم من مواكبة تطور الجريمة الإرهابية في المجال القضائي[2].

## 03- مؤتمر واشنطن الدولي ودور مؤسسات المجتمع المدني في الوقاية ومحاربة الإرهاب.

انعقد هذا المؤتمر في واشنطن بالولايات المتحدة الأمريكية بعد الأحداث التي عرفتها جريدة "شارل إيبدو" الفرنسية في أواخر سنة 2014 ، والاعتداءات الأخيرة على الرعايا المصريين من قبل تنظيم الدولة الإسلامية يومي 18 و19 فيفري 2015، وقد حضر هذا المؤتمر حوالي 75 دولة ومنظمة دولية وإقليمية من أجل دراسة ظاهرة انتشار التنظيمات الإرهابية الجديدة، والبحث عن الوسائل التي من شأنها محاربة التطرف وتجنيد الإرهابيين.

[1] نفس المرجع، ص 14، 15 .

[2] وثيقة المؤتمر الدولي حول تعزيز التعاون في مجال مكافحة الإرهاب المنعقد بباكو عاصمة أذربيجان 2013 متوافرة في الموقع: http://www.albawabhnews.com، تم الاطلاع بتاريخ 2018/05/03 على الساعة 17:43 .

وقد جاءت هذه المبادرة بعد عدة لقاءات عقدتها الولايات المتحدة الأمريكية مع بعض الجمعيات والشخصيات الإسلامية وغير الإسلامية، وكان ذلك في واشنطن ولوس أنجلس ومينا بوليس، حيث ساعدت هذه اللقاءات على بناء أطر جديدة في معالجة التطرف والإرهاب ومنع انتشار ثقافة العنف في العالم بواسطة إدماج المسؤولين عن الإطار الاجتماعي من معلمين ورجال دين والأمن في بعث سياسة وقائية أساسها التكفل بالفئات الضعيفة من المجتمعات السريعة التأثير والتجنيد في صفوف الجماعات الإرهابية بسهولة .

وفي هذا الإطار وجه المؤتمر دعوة إلى كافة الدول وجميع القطاعات المختصة إلى استخدام وسائل التكنولوجيا للمشاركة بآرائهم واقتراحاتهم من اجل التوصل إلى وضع إجراءات، وقواعد تكفل منع انتشار ظاهرة التطرف والعنف

ويعتبر هذا المؤتمر من المؤتمرات التي كان لها الفضل الكبير والكثير من الفعالية في مجال مكافحة الإرهاب بمختلف أشكاله وخاصة المستحدثة نظرا لما أسفر عنه من توصيات تمحورت أهمها حول عدم كفاية الرد الأمني لوضع حد لانتشار التنظيمات الإرهابية، كما أن الرد الأمني قد يسبب ضحايا وخسائر مادية تكون الدولة في غنى عنها، فدعت الأمم المتحدة إلى العمل وفق الأساليب الوقائية القائمة على مبدأ الحكم الراشد والبحث عن المبررات والأسباب التي تسببت في تطور الإرهاب حتى وصل إلى تطور مذهل، وبالتالي إمكانية إيجاد الوسائل التي بواسطتها يمكن الحد من انتشار هذا النوع من الإرهاب[1] .

## ثانيا: التدابير المتخذة من طرف الجمعية العامة لمكافحة الإرهاب الالكتروني.

اعتمدت الجمعية العامة للأمم المتحدة إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب في 8 أيلول 2006، بهدف تحسين الجهود الوطنية والإقليمية والدولية في هذا المجال، وللمرة الأولى تتفق الدول الأعضاء جميعها على نهج استراتيجي موحّد لمكافحة الإرهاب بمختلف أشكاله وصوره واتخاذ خطوات عملية فرديًا وجماعيًا لمنعه ومكافحته.

وتضمّنت هذه الإستراتيجية العالمية خطة عمل تناولت مجموعة كبيرة من التدابير الرامية إلى معالجة الظروف المساعدة على انتشار الإرهاب، ومنعه ومكافحته، وبناء قدرات الدول على التصدّي له، وتعزيز دور الأمم المتحدة في هذا الصدد، وضمان احترام حقوق الإنسان، والتمسّك بسيادة القانون

[1] ساعد الهام حورية، مرجع سابق، ص 16.

في مكافحة الإرهاب، كما تدعو الإستراتيجية الدول الأعضاء إلى العمل مع منظومة الأمم المتحدة لتنفيذ أحكام خطة العمل الواردة في الإستراتيجية، كما تدعو في الوقت ذاته كيانات الأمم المتحدة إلى مساعدة الدول الأعضاء في جهودها، وتتخذ إدارات الأمم المتحدة وبرامجها وصناديقها ووكالاتها إجراءات في عدد من المجالات، تماشيًا مع الإستراتيجية بصفتها الفردية، ومن خلال الجهود المشتركة المبذولة في إطار فرقة العمل المعنيّة بتنفيذ مكافحة الإرهاب[1]، وتقوم فرقة العمل حاليًا بتنمية التعاون مع عدد من المنظّمات الإقليمية ودون الإقليمية، من بينها: منظّمة المؤتمر الإسلامي (OIC) المنظّمة الإسلامية للتربية والعلم والثقافة (ISESCO)، الإتحاد الأوروبي (EU) المجلس الأوروبي (COE)، ومنظّمة الأمن والتعاون في أوروبا (OSCE)[2].

ومن أهم التدابير التي اتخذتها الجمعية العامة في مجال مكافحة الإرهاب مهما كانت أشكاله أو صوره ، وعلى ذلك فان هذه التدابير تشتمل على الإرهاب الالكتروني باعتباره احدث صورة للإرهاب كمايلي:

### أ- التدابير الرامية إلى معالجة الظروف المؤدية إلى انتشار الإرهاب

تساهم الأمم المتحدة في معالجة الظروف المؤدية إلى انتشار الإرهاب، من خلال الخطوات الآتية:

---

[1] تشمل فرقة العمل المعنية بتنفيذ مكافحة الإرهاب ممثلين من: المديرية التنفيذية لمكافحة الإرهاب (CTED)، إدارة عمليات حفظ السلام (DPKO)، إدارة الشؤون السياسية (DPA)، إدارة شؤون الإعلام (DPI)، إدارة السلامة والأمن =(DSS)، خبراء اللجنة المنشأة بموجب القرار 1540 التابعة للوكالة الدولية للطاقة الذرية (IAEA)، منظّمة الطيران المدني الدولي (ICAO)، المنظّمة البحرية الدولية (IMO)، صندوق النقد الدولي (IMF)، فريق الرصد التابع للجنة المنشأة بموجب القرار 1267 والتابعة لمفوضية حقوق الإنسان (OHCHR)، مكتب شؤون نزع السلاح (ODA) مكتب الشؤون القانونية (OLA)، منظّمة حظر الأسلحة الكيميائية (OPCW)، المقرّر الخاص المعني بتعزيز حقوق الإنسان وحمايتها في سياق مكافحة الإرهاب، التابع لبرنامج الأمم المتحدة الإنمائي (UNDP)، منظّمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) (UNESCO)، معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة (UNICRI) مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، منظّمة الجمارك العالمية (WCO)، البنك الدولي منظّمة الصحة العالمية (WHO)، وتتجاوز فرقة العمل، في عملها التخطيطي والتنسيقي، منظومة الأمم المتحدة الأوسع نطاقًا لتشمل كيانات أخرى، من قبيل المنظّمة الدولية للشرطة الجنائية (الانتربول) (Interpol).

[2] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، الأمم المتحدة، الدورة الثانية والستون، نيويورك، 7 تموز 2008، A/62/898 ص.1-2.

– تعزيز قدرات المنظّمة الدوليّة واستخدامها على أفضل وجه، في مجالات عدة وأبرزها منع نشوب الصراعات، والتفاوض، والوساطة، والتوفيق، والتسوية القضائية، وسيادة القانون وحفظ السلام، وبناء السلام، من أجل المساهمة في الحيلولة بنجاح دون نشوب الصراعات طويلة الأمد، التي تستعصي على الحل، ومكافحتها بالوسائل السلمية.

وإن معالجة هذه الصراعات بالوسائل السلمية، سيساهم في تعزيز مكافحة الإرهاب على الصعيد العالمي، وفي هذا السياق، "لقد ساعد الممثلون الخاصون للأمين العام ومبعوثوه بتقديمهم دعمًا على سبيل الوساطة، وبمساندتهم إدارة الشؤون السياسية، على تيسير التوصّل إلى اتفاقات سلام في 13 صراعًا في مختلف أنحاء العالم منذ العام 2001، وسيعمل مكتب دعم بناء السلام ووحدة دعم الوساطة واللذان أنشأتهما الإدارة مؤخرًا، على زيادة تحسين قدرة الأمم المتحدة في مجال صنع السلام وبنائه".

– مواصلة وضع ترتيبات، في ظل مبادرات الأمم المتحدة وبرامجها، لتعزيز الحوار والتسامح والتفاهم بين الحضارات والثقافات والشعوب والأديان، وتعزيز الاحترام المتبادل للأديان والقيم والمعتقدات الدينية والثقافات ومنع التشهير بها.

– ترويج ثقافة السلام والعدالة والتنمية البشرية، والتسامح العرقي والوطني والديني، واحترام جميع الأديان أو القيم الدينية أو المعتقدات أو الثقافات، عن طريق القيام، عند الاقتضاء، بوضع برامج للتثقيف والتوعية العامة وتشجيعها، تشمل جميع قطاعات المجتمع. "وتشجّع حاليًا منظّمة الأمم المتحدة للتربية والعلم والثقافة الحوار بين الحضارات والثقافات والشعوب، بما يشمل الحوار بين الأديان والعقائد، وتعمل إدارة شؤون الإعلام مع الدول الأعضاء، ووسائط الإعلام، والمؤسسات التعليمية والمنظّمات غير الحكومية، والمجتمع المدني، على تشجيع الحوار والاحترام والتسامح والتنوّع الثقافي. وتنظّم الإدارة سلسلة من الحلقات الدراسية التي تحمل عنوان "التخلّص من عدم التسامح"، ترمي إلى دراسة المظاهر المختلفة لعدم التسامح، فضلاً عن اكتساب سبل تشجيع الاحترام والتفاهم في ما بين الشعوب. وقد أكّدت الحلقات الخمس التي عُقدت حتى الآن على: التصدي لمعاداة السامية وكره الإسلام، ودور وسائل الإعلام في تأجيج شعلة التسامح، ومنع الإبادة الجماعية"[1].

[1] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، الأمم المتحدة، الدورة الثانية والستون، نيويورك، 7 تموز 2008، A/62/898 ص1،2.

– التصميم على تحقيق الأهداف والغايات الإنمائية في المؤتمرات الرئيسة التي تعقدها الأمم المتحدة من بينها الأهداف الإنمائية للألفية، على نحو كامل، بهدف القضاء على الفقر، وتعزيز النمو الاقتصادي المتواصل، وتحقيق التنمية المستدامة والرفاه العالمي للجميع.

– السعي إلى تحقيق خطط التنمية وتعزيزها والدمج الاجتماعي على جميع الأصعدة، انطلاقًا من إدراك أنّ إحراز نجاح في هذا المجال، ولاسيّما في ما يتعلّق ببطالة الشباب، أمر يمكن أن يحدّ من التهميش، وما يستتبعه من شعور بالغبن يغذّي التطرّف والتجنيد لصالح الإرهاب.

– رفع مستوى التعاون والمساعدة اللذين تقدّمهما منظّمة الأمم المتحدة في مجالات سيادة القانون وحقوق الإنسان والحكم الرشيد، دعمًا للتنمية الاقتصادية والاجتماعية والبيئية المتواصلة.

**ب– تدابير منع الإرهاب ومكافحته ولاسيّما عن طريق حرمان الإرهابيين الوصول إلى الوسائل التي تمكّنهم من شنّ اعتداءاتهم، وبلوغ أهدافهم وتحقيق الأثر المتوخى من أعمالهم الإرهابية[1]:**

– "الامتناع عن تنظيم أنشطة إرهابية أو التحريض عليها أو تيسيرها أو المشاركة فيها أو تمويلها أو التشجيع عليها أو التهاون إزاءها، واتخاذ تدابير عملية مناسبة تكفل عدم استخدام أراضي الدول في إقامة منشآت أو معسكرات تدريب إرهابية، أو لتدبير أعمال إرهابية أو تنظيمها، ترتكب ضدّ دول أخرى أو ضدّ مواطنيها.

– كفالة القبض على مرتكبي الأعمال الإرهابية ومحاكمتهم أو تسليمهم، وفق أحكام ذات صلة بالقانون الوطني والدولي، ولاسيما قانون حقوق الإنسان، وقانون اللاجئين والقانون الإنساني الدولي وتكثيف التعاون، وفق ما يقتضيه الحال، في تبادل المعلومات الدقيقة المتعلّقة بمنع الإرهاب ومكافحته في الوقت المناسب.

– تعزيز التنسيق والتعاون بين الدول في مكافحة الجرائم التي قد تكون على صلة بالإرهاب، من بينها الاتجار بالمخدرات بجميع جوانبه، والاتجار غير المشروع بالأسلحة، ولاسيّما الأسلحة الصغيرة وتلك

[1] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، مرجع سبق ذكره، ص7، 13.

الخفيفة، بما فيها منظومات الدفاع الجوي المحمولة، وغسل الأموال، وتهريب المواد النووية والكيميائية والبيولوجية والإشعاعية وغيرها من المواد التي يمكن أن تكون فتاكة.

– تشجيع المنظّمات الإقليمية ودون الإقليمية المعنية، على إنشاء آليات أو مراكز لمكافحة الإرهاب أو تعزيز الموجود منها. وتوفير التعاون والمساعدة، من قبل مكتب الأمم المتحدة المعني بمكافحة المخدرات والجريمة والمنظّمة الدولية للشرطة الجنائية. وتشجيع الدول على تطبيق المعايير الدولية الشاملة التي تجسّدها التوصيات المتعلقة بغسل الأموال، والتوصيات الخاصة المتعلقة بتمويل الإرهاب.

– تكثيف التعاون الإقليمي والدولي، بهدف تحسين مراقبة الحدود والضوابط الجمركية لمنع تحرّك الإرهابيين وكشفهم، ومنع الاتجار غير المشروع بالأسلحة الصغيرة والأسلحة الخفيفة، والذخائر والمتفجرات التقليدية، والأسلحة والمواد النووية أو الكيميائية أو البيولوجية أو الإشعاعية وكشفها.

– تشجيع لجنة مكافحة الإرهاب على مواصلة العمل مع الدول، بهدف تيسير اعتماد تشريعات واتخاذ تدابير إدارية لتنفيذ الالتزامات المتصلة بسفر الإرهابيين، مستفيدة من الممارسات التي طوّرتها المنظّمات الدولية التقنية، كمنظّمة الطيران المدني الدولي، ومنظّمة الجمارك العالمية والمنظّمة الدولية للشرطة الجنائية"[1].

وفي هذا الإطار، "لقد أعدّت واعتمدت أيضًا لجنة مكافحة الإرهاب ستة عشر صكًا قانونيًا عالميًا تحت إشراف الأمم المتحدة والمنظّمات الحكومية الدولية المتصلة بها، وأغلبية هذه الصكوك سارية وتوفّر إطارًا قانونيًا لاتخاذ إجراءات متعدّدة الأطراف ضدّ الإرهاب ولتجريم أعمال إرهابية محدّدة، ولجنة مكافحة الإرهاب ومديريتها التنفيذية لمكافحة الإرهاب مسؤولتان عن رصد قراري مجلس الأمن 1373 (2001) و 1624 (2005) وتنفيذهما وتيسير تقديم المساعدة التقنية إلى البلدان التي تطلبها.

وبموجب نظام الجزاءات المفروضة على القاعدة وطالبان، قامت حتى الآن فرقة الرصد، التي تساعد مجلس الأمن في التشجيع على تنفيذ نظام الجزاءات، بإعداد ستة تقارير تحليلية، تتضمن تقويمًا للطابع المتميّز للتهديد الذي تمثله القاعدة وطالبان وأفضل التدابير للتصدي له. وقد زارت الفرقة 72 دولة من الدول الأعضاء لمناقشة كيفية تحسين نظام الجزاءات، وهناك اتفاق بينها و24 هيئة

[1] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، مرجع سابق، ص7، 13.

دولية وإقليمية على التعاون. وأنشأت أيضًا أربع مجموعات إقليمية من وكالات الاستخبارات والأمن من مختلف البلدان لتقديم مزيد من المشورة والمقترحات كي ينظر فيها مجلس الأمن. وقام العنصر العسكري وعنصر الشرطة في عمليات الأمم المتحدة لحفظ السلام بتهيئة بيئة أكثر أمانًا في 16 منطقة من مناطق الصراع في مختلف أنحاء العالم في السنوات الخمس الماضية. وقد ساعد ذلك على الحدّ من الفرص المتاحة للإرهابيين لتجنيد عناصر للقيام بعملياتهم في تلك المناطق.

وقام معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة بجمع بيانات من بلدان منطقة أوروبا وآسيا الخمسة والعشرين بشأن الاستراتيجيات الوطنية لمكافحة الاتجار غير المشروع بالمواد الكيميائية أو البيولوجية أو الإشعاعية أو النووية. وتعنى منظّمة الصحة العالمية بالتأهب على صعيد الصحة العمومية والاستجابة لجميع طوارئ الصحة العمومية التي تبعث على القلق الدولي، أيًا كان مصدرها أو منشؤها، في إطار اللوائح الصحية الدولية (2005) وتنفّذ الوكالة الدولية للطاقة الذرية خطتها الثانية المكرسة للأمن النووي (NSP)[1].

وكانت الخطة الأولى تغطي السنوات 2002- 2005، بينما تغطي الثانية السنوات 2006-2009، وهي موجهة إلى زيادة تحسين الأمن وتعزيزه عالميًا في ما يتعلّق بالمواد النووية وغيرها من المواد الإشعاعية من حيث استخدامها وتخزينها ونقلها وذلك بدعم الدول في جهودها الرامية إلى تعزيز جهودها الوطنية لتحقيق الأمن النووي، وبدأ مكتب شؤون نزع السلاح (ODA) المرحلة الأولى من إقامة قاعدة بيانات شاملة وواحدة بشأن الحوادث البيولوجية وفق التكليف الصادر من الإستراتيجية.

وسيتعهد المكتب أيضًا قائمة خبراء ومختبرات من أجل آلية التحقيق التابعة للأمين العام والمعنية بالاستخدام المزعوم للأسلحة البيولوجية، وفي أوائل العام 2007 أرسل مكتب شؤون نزع السلاح طلبًا إلى جميع الدول الأعضاء لكي تقدّم له قائمة مستكملة بالخبراء وبالمختبرات المؤهلين ويجري حاليًا تقديم مقترحات لإجراء استعراض كامل للمبادئ التوجيهية التقنية وللإجراءات المتعلّقة بهذا التحقيق.

وتضع منظّمة الطيران المدني الدولي معاهدات ومعايير دولية وممارسات موصى بها فضلاً عن مادة إرشادية لحماية الطائرات والمطارات ومرافق الملاحة الجوية الأخرى، وقد أجرت مراجعات أمنية في 156 دولة من الدول الأعضاء حتى 31 آذار 2007، ونسّقت المساعدة المقدّمة لعلاج أوجه

[1] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، مرجع سابق، ص7، 13.

القصور التي ظهرت في أثناء المراجعات، وهي تتناول أيضًا أمن وثائق السفر وتركيب نظم وإجراءات الموافقات على دخول الحدود، وساعدت المنظّمة الدولية للشرطة الجنائية (الانتربول) مجلس الأمن التابع للأمم المتحدة في تنفيذ نظام الجزاءات المفروضة على القاعدة وطالبان وذلك بتعميم معلومات على سلطات إنفاذ القانون على نطاق العالم[1].

### ج- التدابير الرامية إلى بناء قدرات الدول على منع الإرهاب ومكافحته.

إن بناء القدرات في جميع الدول عنصر أساس في الجهود العالمية لمكافحة الإرهاب ومن التدابير الواجب اتخاذها لتنمية قدرة الدول على منع الإرهاب:

- تشجيع المساعدة التقنية والمالية وتقديمها، من قبل مكتب الأمم المتحدة المعني بالمخدرات والجريمة، والوكالة الدولية للطاقة الذرية، ومنظّمة حظر الأسلحة الكيميائية، والمنظّمة البحرية الدولية ومنظّمة الجمارك العالمية، ومنظّمة الطيران المدني الدولي، لبناء قدرات الدول، ولاسيّما في مجالات أمن الموانئ والأمن البحري وأمن الطيران المدني.

- التشجيع على تبادل المعلومات في شأن التعاون بين الدول الأعضاء، وهيئات الأمم المتحدة المعنية بمكافحة الإرهاب، والوكالات المتخصصة المعنية، والمنظّمات الدولية والإقليمية ودون الإقليمية المعنية، والجهات المانحة، بهدف تنمية قدرات الدول على تنفيذ قرارات الأمم المتحدة ذات الصلة بالموضوع، والاتفاقيات والبروتوكولات الدولية المتصلة بمنع الإرهاب وقمعه.

- تشجيع صندوق النقد الدولي والبنك الدولي ومكتب الأمم المتحدة المعني بالمخدرات والجريمة والمنظّمة الدولية للشرطة الجنائية، على تعزيز التعاون مع الدول لمساعدتها على أن تمتثل تمامًا للمعايير والالتزامات الدولية المتصلة بمكافحة غسل الأموال وتمويل الإرهاب[2].

وفي سياق تنفيذ هذه التدابير، حدّدت المديرية التنفيذية لمكافحة الإرهاب احتياجات أكثر من 90 دولة من الدول الأعضاء من حيث المساعدة التقنية، وأعطتها أولوية، وأحالت تلك الاحتياجات إلى المانحين المحتملين. ويضطلع برنامج الأمم المتحدة الإنمائي، بوجوده الميداني في 166 بلدًا، بأنشطة عديدة، بناء على طلب الحكومات، للنهوض بالحكم وسيادة القانون، مما يتضمن برامج لدعم تشريعات

[1] نفس المرجع، ص7، 13.

[2] "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب"، 8 أيلول 2008، مرجع سابق.

لمكافحة غسل الأموال وتنفيذها وتعزيز نظم العدالة، وتقدم إدارة عمليات حفظ السلام التدريب لضباط ومسؤولي الشرطة وإنفاذ القانون الوطني بشأن الأمور الإجرامية ومن بينها الاختطاف، وجمع المعلومات، وأخذ الرهائن والحماية الشخصية، والتحقيق في الاغتيالات، وعمليات القتل، وتفجيرات القنابل. وقدّم معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة الدعم لدول أعضاء عديدة تشارك في الأعمال التحضيرية الأمنية لمختلف الأحداث، وقدّم المعهد أيضًا تدريبًا لمخططي الأمن من 17 بلدًا في أميركا اللاتينية، بينما شجّع في أوروبا على استحداث مجال بحوث متكاملة بشأن أمن الأحداث الكبرى. وتضمّنت أنشطة الوكالة الدولية للطاقة الذرية مساعدة الدول على تحديد احتياجاتها العامة من حيث الأمن النووي، تدريب مسؤولي الجمارك ومسؤولي الحدود الآخرين، وتركيب معدّات للكشف عند معابر الحدود، وتنفيذ التعهدات الحالية والمستقبلية المتعلّقة بالصكوك من قبيل اتفاقية الحماية المادية للمواد النووية التي جرى تعديلها مؤخرًا، واتفاقية قمع أعمال الإرهاب النووي، وقرار مجلس الأمن 1540 (2004).

وتساهم منظّمة حظر الأسلحة الكيميائية في الجهود العالمية لمكافحة الإرهاب بالتشجيع على الانضمام العالمي إلى اتفاقية الأسلحة الكيميائية. وهي تواصل جهودها في إطار ولايتها، لمساعدة الدول على بناء قدرتها على منع الإرهابيين من الحصول على المواد الكيميائية، ومن خلال البرنامج العالمي للأمن البحري، اضطلعت المنظّمة البحرية الدولية بـ41 بعثة استشارية قطرية، وعقدت ما مجموعه 27 حلقة دراسية وطنية و55 حلقة دراسية إقليمية فضلاً عن حلقات عمل أو دورات، ودرّبت زهاء 4400 شخص على وسائل كفالة الأمن البحري. وقدّم صندوق النقد الدولي مساعدة تقنية لـ 158 بلدًا، من خلال حلقات عمل تدريبية وطنية وإقليمية ومساعدة مكيّفة خصوصًا لبناء القدرة من قبيل صياغة التشريعات وتعزيز قدرات القطاع المالي على مكافحة غسل الأموال ومكافحة تمويل الإرهاب[1].

وتبدأ المنظّمة الدولية للشرطة الجنائية وتنسق، برامج تدريبية عديدة تشمل مجالات مختلفة ذات أولوية من مجالات الجريمة، وترمي إلى تحسين قدرة الدول على مكافحة الإرهاب[2].

[1] "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب"، 8 أيلول 2008، مرجع سابق.

[2] تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، مرجع سابق، ص 13، 20.

## د- التدابير الرامية إلى ضمان احترام حقوق الإنسان وسيادة القانون في سياق مكافحة الإرهاب

إن تعزيز حقوق الإنسان للجميع وحمايتها، وسيادة القانون، أمر أساس بالنسبة إلى جميع عناصر إستراتيجية الأمم المتحدة، ومن الضروري اتخاذ التدابير الآتية:

- يتعيّن على الدول أن تكفل في أي تدابير تتخذها لمكافحة الإرهاب، الوفاء بالالتزامات المنوطة بها بموجب القانون الدولي، ولاسيما قانون حقوق الإنسان، وقانون اللاجئين والقانون الإنساني الدولي فضلاً عن النظر في قبول اختصاص هيئات رصد حقوق الإنسان الدولية والإقليمية المعنية.

- المساعدة في إنشاء نظام العدالة الجنائية وتعهده من قبل مكتب الأمم المتحدة المعني بالمخدرات والجريمة، يتسم بالفعالية ويقوم على سيادة القانون، ويكون بوسعه أن يكفل تقديم أي شخص يشارك في تمويل الأعمال الإرهابية أو التخطيط لها أو تدبيرها أو ارتكابها أو دعمها، إلى العدالة.

- دعم مجلس حقوق الإنسان في عمله المتعلق بمسألة تعزيز حقوق الإنسان للجميع وحمايتها في سياق مكافحة الإرهاب[1].

وضمن هذه المجالات، تقوم مفوضية الأمم المتحدة لحقوق الإنسان بالدعوة إلى تعزيز جميع حقوق الإنسان وحمايتها، وتنفيذ تدابير فعالة لمكافحة الإرهاب، وذلك كهدفين متكاملين يعزّز كل منهما الآخر. وتقدّم المفوضية المساعدة والمشورة إلى الدول الأعضاء بناء على طلبها، في شأن حماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، بما يتضمّن وضع تشريعات وسياسات لمكافحة الإرهاب وصون حقوق الإنسان.

وقد ركّزت المفوضية اهتمامها على تعميق فهم الالتزامات الدولية المتعلّقة بحقوق الإنسان في سياق مكافحة الإرهاب، عن طريق إجراء بحوث وتحاليل مركزة، والتشجيع على تعزيز حماية حقوق الإنسان من خلال القيادة وأنشطة الدعوة، وتقديم المساعدة التقنية والتدريب واستحداث أدوات لمساعدة العاملين في هذا المجال.

ويعمل المقرّر الخاص المعني بتعزيز حقوق الإنسان وحمايتها في سياق مكافحة الإرهاب، في إطار مجلس حقوق الإنسان الجديد، على تحديد أفضل الممارسات المتعلّقة بتدابير مكافحة الإرهاب

[1] إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية، مرجع سابق ص 20، 23.

التي تحترم حقوق الإنسان والحريات الأساسية وتبادلها وتشجّعها ويبحث المقرّر الخاص أيضًا الادعاءات بحدوث انتهاكات لحقوق الإنسان في سياق مكافحة الإرهاب. ويقوم بزيارات لبلدان ويتراسل مع أكثر من 30 بلدًا في شأن قوانينها وممارساتها.

وقدّم معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة تدريبًا للمدّعين العامين وغيرهم من مسؤولي التحقيق المختصين من 19 بلدًا في أميركا اللاتينية في شأن حماية الشهود، مع تركيز محدّد على الأشخاص الذين يشاركون أو الذين شاركوا في جماعات إرهابية أو جماعات جريمة منظّمة فضلاً عن التركيز على ضحايا الإرهاب. وترمي أنشطة التدريب إلى تحسين مهارات بلوغ الحد الأمثل في استخدام المعلومات التي يقدّمها الشهود وفق حق الدفاع، وإلى ترويج النهج الملائم إزاء ضحايا الإرهاب[1].

## الفرع الثاني: دور مجلس الأمن في مكافحة الإرهاب الالكتروني.

يعتبر مجلس الأمن الجهاز الرئيسي في هيئة الأمم المتحدة في مجال حفظ السلم والأمن الدوليين، وهو يتمتع بهذا الاختصاص طبقا لأحكام ميثاق الأمم المتحدة، فهو الجهاز الفعال الذي يملك حق إلزام الدول بقراراته في ميدان هذا التخصص المسند إليه، ويتشكل هذا المجلس من 15 عضو، خمسة منهم دائمون والعشرة الباقون مؤقتون ينتخبون لمدة سنتين[2]، ولمجلس الأمن قرارات صارمة في مجال مكافحة الإرهاب وخاصة بعد أحداث 11 سبتمبر 2001 وظهور ما يعرف بالإرهاب الالكتروني، حيث التزمت بها الدول ضمن سياستها اتجاه محاربة الإرهاب الالكتروني والوقاية منه، فهذه القرارات أصبحت شاملة لجميع أعمال الإرهاب دون استثناء، وهذا لأن هيئة الأمم المتحدة أدركت أن الإرهاب لا يتعلق بقضية معينة ولا بدولة واحدة أو دين معين، فجرائم الإرهاب وخاصة الإرهاب الالكتروني منتشر وموجود في كل رقعة من العالم[3].

يلتزم مجلس الأمن بالحفاظ على السلم والأمن الدوليين طبقا للاختصاص الممنوح له حسب أحكام ميثاق الأمم المتحدة، وهو بذلك يعتبر الجهاز الرئيسي في هيئة الأمم المتحدة فهو الجهاز

[1] إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية، مرجع سابق ص 20، 23.

[2] سهيل حسين الفتلاوي، الإرهاب الدولي وشرعية المقاومة، دار الثقافة، عمان– الأردن، 2009، ص 140.

[3] نفس المرجع، ص 140.

الفعال الذي يملك حق إلزام الدول بقراراته في مجال تخصصه ويتشكل مجلس الأمن من 15 عضو، خمسة منهم دائمون و العشرة الباقون مؤقتون ينتخبون لمدة سنتين حيث تنص المادة 23 من ميثاق الأمم المتحدة على :" 1. يتألف مجلس الأمن من خمسة عشر عضواً من الأمم المتحدة، وتكون جمهورية الصين وفرنسا، واتحاد الجمهوريات الاشتراكية السوفيتية، والمملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، والولايات المتحدة الأمريكية أعضاء دائمين فيه وتنتخب الجمعية العامة عشرة أعضاء آخرين من الأمم المتحدة ليكونوا أعضاء غير دائمين في المجلس، ويراعى في ذلك بوجه خاص وقبل كل شيء مساهمة أعضاء الأمم المتحدة في حفظ السلم والأمن الدولي وفي مقاصد الهيئة الأخرى، كما يراعى أيضاً التوزيع الجغرافي العادل.

2. ينتخب أعضاء مجلس الأمن غير الدائمين لمدة سنتين، على أنه في أول انتخاب للأعضاء غير الدائمين بعد زيادة عدد أعضاء مجلس الأمن من أحد عشر عضواً إلى خمسة عشر عضواً، يختار اثنان من الأعضاء الأربعة الإضافيين لمدة سنة واحدة والعضو الذي انتهت مدته لا يجوز إعادة انتخابه على الفور.

3. يكون لكل عضو في مجلس الأمن مندوب واحد"[1].

وفي مجال مكافحة الإرهاب أصدر مجلس الأمن العديد من القرارات الصارمة، وخاصة بعد أحداث 11 سبتمبر 2001 بالولايات المتحدة الأمريكية، وقد التزمت بها الدول ضمن سياستها ضد جرائم الإرهاب والوقاية منه[2].

وما يلاحظ على قرارات مجلس الأمن المتعلقة بالإرهاب فقد تميزت بالجزئية قبل سنة 1999[3]، لكن بعد ذلك عرفت بأنها قرارات شاملة لجميع الجرائم الإرهابية دون استثناء، ومهما كانت الوسيلة لمتبعة في ارتكابه، وفي ذلك إدراكا من هيئة الأمم المتحدة أن الإرهاب لا يتعلق بقضية معينة ولا بدولة واحدة ولا بدين معين، لكنه منتشر وموجود في كل رقعة من العالم وبصور مختلفة ومتنوعة.

[1] ميثاق الأمم المتحدة، متوافر في الموقع :http://www.un.org .

[2] سهيل حسين الفتلاوي، مرجع سابق، ص140

[3] ساعد الهام حورية، مرجع سابق، ص 20.

وتجدر الإشارة إلى أنه بعد الحرب الباردة دخل العالم بأسره في سياق تحديات لا تقل أهمية عن التحديات التي كانت أثناء الحرب الباردة من حيث الخطورة، وقد تميزت الفترة اللاحقة على الحرب الباردة بالأحادية القطبية بعد انهيار الكتلة الشرقية الذي صاحبه تغيير في الأنظمة السياسية والاقتصادية للكثير من الدول، وانتشرت الرأسمالية وبدأت تظهر بوادر الديمقراطية التي أدت إلى ميلاد الكثير من الحركات السياسية، التي اعتمدت على نداءات متعددة من اجل التغيير في أنظمة الحكم في الكثير من الدول الأمر الذي أدى إلى تصاعد الوتيرة الأصولية على امتداد العالم، والحركات الأصولية هي تلك التنظيمات الدينية السياسية التي تنادي بضرورة تواجد نموذج ديني مثالي في النصوص الدينية، وان هذا النموذج صالح التطبيق في الوقت الراهن، بحيث قامت هذه الحركة التي تزايد نموها في السنوات الأخيرة ، بالوقوف ضد الهيمنة الأمريكية بعد انهيار الاتحاد السوفيتي سابقا وقد رفضت هذه الحركات أمركة العالم، والتخفيف من شدة ضعف بعض الدول اقتصاديا محاولة إيجاد إيديولوجية محلية بديلة مستمدة من افتراضات عقائدية قومية، قد تكون منبثقة من المسيحية الإسلامية، اليهودية، وغيرها من الديانات والتي تعمل في سبيل إيجاد نظام سياسي اقتصادي مثالي منبعه الدين، كما ظهر اقتصاد المعرفة والذي يقصد به التطور الهائل في ميدان تكنولوجيا المعلومات الذي أدى إلى ظهور نمط جديد من الاقتصاد تمثل في توظيف المعلومات وتحويلها إلى تكنولوجيا قابلة للنقل والتطوير، منها الانترنت وتكنولوجيا الاتصال والهاتف المحمول وغيرها وبسببه ظهر نمط جديد للإرهاب وهو الإرهاب الالكتروني[1]، الأمر الذي سهل الاتصال بين التنظيمات الإرهابية والإجرامية وبفضلها تطور أسلوب العمل الإرهابي، حيث وجد الإرهابيون البيئة المناسبة للنمو وتزايدت مخاطره، فكان لابد لمجلس الأمن التدخل بآليات التصدي لهذه الجريمة الخطيرة.

وسوف نتعرض لدور مجلس الأمن في مكافحة الإرهاب الالكتروني وذلك من خلال استعراض قراراته قبل ظهور الإرهاب الالكتروني حيث كانت قراراته جزئية، وبعد ظهوره وذلك بالاعتماد على الرؤية الشاملة والموحدة، وبعدها سوف نتعرض إلى مدى قوة وإلزامية قرارات مجلس الأمن في مجال مكافحة الإرهاب .

## أولا: قرارات مجلس الأمن في التعامل مع الإرهاب قبل ظهور الإرهاب الالكتروني

[1] ساعد الهام حورية، مرجع سابق ، ص 21.

تطورت الجريمة الإرهابية في السنوات الأخيرة كثيرا وتعددت صورها وتشعبت أنماط السلوك الإجرامي في ارتكابها، وبذلك أصبحت هذه الجريمة مشكلة أمنية عويصة تهدد السلم والأمن الدوليين في العالم، وهذا لاتساع رقعته ليشمل تقريبا كل منطقة من العالم فلم تسلم من شروره أي دولة مهما كانت درجة تطورها، وخاصة الدول العربية.

مجلس الأمن كان يتعامل مع جريمة الإرهاب قبل الاعتداءات التي أصابته بالجزئية وبمنظور حالة بحالة محاولا اتخاذ قرارات خاصة بكل قضية وإيجاد الحلول المناسبة طبقا لنوعية الاعتداء وآثاره، ويتضح ذلك من القرارات الصادرة عنه قبل سنة 1999.

## 01- حماية الطيران المدني.

أصدر مجلس الأمن قرارا بشان الطيران المدني في 20 جويلية 1972، أعرب فيه عن قلقه العميق اتجاه التهديدات التي يتعرض إليها مستعملي الطيران المدني، وكذلك الطاقم العامل بالطائرات وذلك بسبب عمليات اختطاف الطائرات والتدخل غير المشروع في الملاحة الجوية، وقد تضمن القرار مايلي:" يساور أعضاء المجلس عميق القلق إزاء تهديد حياة الركاب والملاحين، نتيجة اختطاف الطائرات المدنية، أو غير ذلك من أعمال التدخل غير المشروع في الملاحة الجوية المدنية، وان أعضاء المجلس يرفضون ويرون ضرورة إنهاء الأعمال الموجهة ضد سلامة الطيران المدني والتي ترتكب في مختلف أنحاء العالم مع إلزام الدول اتخاذ التدابير اللازمة في هذا الشأن من أجل منعها ومن أجل متابعة مقترفي هذه الأفعال".

كما دعا المجلس في ختام قراره جميع الدول إلى توسيع وتقوية الجهود والتدابير الدولية القانونية في هذا المجال وفقا لالتزامات ميثاق الأمم المتحدة وذلك لضمان الحد الأعلى الممكن لسلامة الطيران المدني والثقة به.

بعد ذلك أصدر مجلس الأمن قراره الثاني رقم 286 الصادر بتاريخ 09 سبتمبر 1980 ضد أعمال العنف التي كانت تقع على الطيران المدني، حيث جاء هذا القرار بعد تصاعد عمليات اختطاف الطائرات في تلك الفترة، حيث أدان المجلس مثل هذه الاعتداءات دون استثناء، ووجه نداء إلى كافة

الدول من أجل اتخاذ جميع التدابير اللازمة لمنع مثل هذه الأعمال التي تزرع الرعب والخوف في نفوس المدنيين[1].

وبعد ذلك جاءت قضية لوكربي حيث طلب من ليبيا تسليم مواطنيها المتهمين من طرف الولايات المتحدة الأمريكية بجريمة تفجير الطائرة "بانام الأمريكية" فوق بلدة لوكربي باسكتلندا سنة 1988 وذلك بموجب قرار رقم 731 الصادر من مجلس الأمن بتاريخ 21 جانفي 1992، وقد رفضت ليبيا هذا القرار استنادا إلى القاعدة العرفية في القانون الدولي القائمة على مبدأ عدم تسليم الدولة لرعاياها على اثر ذلك اصدر مجلس الأمن قرار آخر بهذا الشأن في 31 مارس 1992، تحت رقم 748 وفحوى هذا القرار فرض جزاءات دبلوماسية واقتصادية على ليبيا، بالإضافة إلى الحظر الجوي بادعاء تورط ليبيا في جرائم الإرهاب الدولي، وامتناعها عن تسليم المتهمين في هذه القضية من رعاياها، إلا انه بعد ذلك تم تعليق هذه الجزاءات بعد موافقة ليبيا محاكمة المتهمين في هولندا أمام محكمة اسكتلندية في حين كان حرياً بمجلس الأمن احترام الميثاق الذي يقضي بضرورة إحالة النزاع إلى محكمة العدل الدولية لما فيه من مسائل قانونية وفقا لأحكام المادة 3/36 من الميثاق، وفي جلسة علنية عقدتها المحكمة في 14 أفريل 1992 أصدرت المحكمة قرارها بأغلبية (11) صوتا ضد (5) أصوات برفض الطلبين المتعلقين بشأن التدابير المؤقتة التي طلبتها ليبيا وذلك بسبب جوهري يتصل بقرار مجلس الأمن رقم 92/748، وبينت المحكمة أن ظروف وملابسات القضية ليست على النحو الذي يستدعي المحكمة أن تمارس سلطاتها لتقرير التدابير المؤقتة لحماية الحقوق التي تدعيها ليبيا كما أن مثل هذا الإجراء يتناقض فيما يبدو للولايات المتحدة من حقوق بموجب قرار مجلس الأمن[2].

لقد صاغت المحكمة موقفها من قرار مجلس الأمن رقم 92/748 في أثناء نظر القضية، وبعد إغلاق المرافعات الشفوية بثلاثة أيام بحذر شديد حيث أوضحت بأنها لا تستطيع في هذه المرحلة أن تحدد الأثر القانوني لقرار المجلس، (بما يعني إنها ستفعل ذلك فيما بعد)، وذكرت بأن ليبيا والولايات المتحدة ملتزمتان بقبول قرارات مجلس الأمن وفقا للمادة (25) من الميثاق، أن هذا الالتزام يسري القرار رقم 92/748 وانه وفقا للمادة (103) من الميثاق إذ تسمو الالتزامات المقررة فيهما وفقا للميثاق على أي التزام دولي آخر بما في ذلك اتفاقية مونتريال لأمن الطيران المدني لعام (1971)، وقد أثار قرار المحكمة برفض التدابير المؤقتة التي طلبتها ليبيا بحجة احتماله أن ينتقص من الحقوق التي تبدو للوهلة الأولى إن الولايات المتحدة تتمتع بها بموجب قرار مجلس الأمن رقم 92/748 ردود أفعال

[1] ساعد الهام حورية، مرجع سابق ، ص 22،23 .

[2] مقالة حول قضية لوكربي منشورة في الموقع الالكتروني: المرجع الالكتروني للمعلوماتية http://almerja.net تاريخ الاطلاع 2018/05/21، على الساعة 01:06 .

واسعة النطاق، اختلف فيها الفقهاء وشراح القانون الدولي ما بين مؤيد له ومعارض أو ناقد لموقف غالبية قضاة المحكمة فيما انتهوا إليه من رأي.

هذا فضلا عن انتقادات من قضاة المحكمة نفسها من خلال آرائهم المخالفة للقرار بل قد حرص معظم القضاة على إيضاح مواقفهم من جوانب القضية حتى المؤيدون لقرار المحكمة، إذ أن الاتجاه العام للقضاة يرى أن تدخل مجلس الأمن في القضية بقراره بموجب الفصل السابع، وهي معروضة على المحكمة أدى إلى إحراج المحكمة مما جعلها تقرر أن ظروف القضية لا تتطلب ممارسة سلطتها وفقا للمادة (41) من النظام الأساسي بفرض إجراءات تحفظية[1] .

وعن الآراء القضائية حول قرار مجلس الأمن رقم 92/748 فقد ذهب معظم القضاة في تأييد المحكمة من تبرير رفضها طلب ليبيا بشأن التدابير المؤقتة لحماية حقوقها. استنادا على قرار مجلس الأمن رقم 92/748، وذلك لأن ليبيا والولايات المتحدة ملتزمتان بالقرار وفقا لأحكام المادتين (25) و(103) من الميثاق[2]، تتطلب الأولى قبول وتنفيذ قرارات مجلس والثانية التي تجعل الأولوية في التنفيذ للالتزامات الدولية المترتبة على الميثاق في حالة تعارضها مع غيرها من الالتزامات الدولية بما في ذلك اتفاقية مونتريال 1971 الواجبة التطبيق على هذا النزاع.

إلا أن هناك بعض القضاة قد انتقد بشدة قرار المحكمة في هذه الناحية حيث ذهب القاضي "بجاوي" في انتقاده في تفسير المحكمة بقوله "ينبغي التفرقة بين ممارسة المحكمة لسلطاتها بصورة فعالة للتأشير بالتدابير المؤقتة والتي تعد مبررة وفقا لوقائع القضية، وبين الآثار المترتبة على إبطال هذه التدابير بموجب قرار مجلس الأمن رقم 92/748 [3]، وبذلك فان هذا القاضي يرى: "أنه ينبغي على المحكمة التمسك بحقها الأصيل في التأشير بالتدابير المؤقتة بدعوى الأطراف بعدم تفاقم النزاع وامتداده، هذا ويضيف هذا القاضي في رأيه المخالف لقرار المحكمة: "أن التدابير المؤقتة تستلزم توافر عدة شروط لكن المحكمة لم تجهد نفسها بالبحث عما إذا كانت تلك الشروط موجودة في الطلب الليبي أم لا، بل إن المحكمة قد اكتفت بأمرها الصادر بالاستناد على واقعة خارجية وهي القرار رقم 748

[1] مقالة حول قضية لوكربي، مرجع سابق .

[2] تنص المادة 25 من الميثاق على أنه:" يتعهد أعضاء "الأمم المتحدة" بقبول قرارات مجلس الأمن وتنفيذها وفق هذا الميثاق".

أما المادة 103 من الميثاق تنص:" إذا تعارضت الالتزامات التي يرتبط بها أعضاء "الأمم المتحدة" وفقاً لأحكام هذا الميثاق مع أي التزام دولي آخر يرتبطون به فالعبرة بالتزاماتهم المترتبة على هذا الميثاق."

[3] مقالة حول قضية لوكربي، مرجع سابق.

لكي تبرر عدم التأشير بهذه الإجراءات"، كما يرى انه كان ينبغي على المحكمة أن تتجاهل هذا القرار ولا تعول عليه، خاصة وانه قد صدر بعد إغلاق باب المرافعات[1].

أما القاضي "أودا" رئيس المحكمة بالإنابة والمؤيد لقرار المحكمة قد ذكر في رأيه الفردي الملحق بأمر المحكمة "أن قرار المحكمة ما كان ينبغي أن يستند كاملا إلى قرار مجلس الأمن رقم 748 باعتباره الأرضية الوحيدة في هذا الشأن ذلك لما قد ينجم من تناقض بين المحكمة والمجلس، أما القاضي شهاب الدين فقد أعلن في رأيه الانفرادي "أن القرار 748 لم يترك للمحكمة أي خيار تصل إليه بشأن الطلب الليبي إذا اتخذت أي قرار سوف يصطدم مباشرة مع قرار مجلس الأمن، ويضيف القاضي شهاب الدين "أن الأرضية القانونية للأمر ليست ناتجة من التصادم بين اختصاص مجلس الأمن واختصاص المحكمة، لكن من التصادم بين التزامات ليبيا بمقتضى قرار مجلس الأمن والتزاماتها المخولة لها بمقتضى اتفاقية مونتريـال، التي أوضح الميثاق بأن قرارات مجلس الأمن تسمو عليها، أما القاضي "ني" المؤيد لقرار المحكمة عبر في رأيه عن القرار 748 بقوله "إن نظر المجلس للقضية لا يمنع المحكمة من نظرتها أيضا، وان المجلس هو الجهاز السياسي الأكثر اهتماما بإزالة الإرهاب الدولي وحفظ السلم والأمن الدوليين، فإن المحكمة بوضعها الجهاز القضائي الرئيسي للأمم المتحدة هي الأكثر اهتماما بالإجراءات القانونية مثل مسائل التسليم والإجراءات المتصلة بتعقب المجرمين وتقدير التعويض، بالتالي يوافقه في رأيه مع القاضي بجاوي في اعتراضهما على نهج المجلس السياسي في تسوية المنازعات القانونية التي تباشرها المحكمة أصلا.

وأخيرا ذهب القاضي بجاوي في تأييده للملاحظات التي قدمتها ليبيا للمحكمة بشأن القرار 748 بقوله: "إن مشكلة القرار 748 الصادر عن المجلس لا تنحصر فقط في كونه قد تضمن توقيع جزاءات سياسية على ليبيا، وإنما في كونه قد تعرض لمسألة قانونية وهي تسليم المتهمين التي تخرج بحكم الميثاق عن اختصاص المجلس، وهذا فضلا عن أن القرار سيخلق نوعا من التداخل والتناقض بين جوهر النزاع القانوني الخاضع أصلا لاتفاقية مونتريـال وبين قرار المجلس القاضي بضرورة تسليم المتهمين إلى كل من الولايات المتحدة وبريطانيا، بما أن قرار المجلس القاضي بضرورة التسليم وهذا سيفضي في نهاية المطاف إلى إفراغ دعوى ليبيا أمام المحكمة من كل مضمون بحيث أصبحت مسألة تسليم المتهمين كلا لحلين متناقضين أحدهما قانوني والآخر سياسي الأمر الذي سيخلق تصادماً بين المحكمة والمجلس خاصة إذا أخذنا في الحسبان ان المحكمة ليست جهة استئناف لقرارات المجلس بحيث تملك تعديل أو إلغاء تلك القرارات كما إن المجلس لا يملك أن يحل مكانة المحكمة في ممارسة اختصاصاتها القضائية والقانونية التي عهد بها الميثاق إليها، ومن ابرز الآراء القضائية في هذه

[1] نفس المرجع.

القضية التي أثارت مسألة الرقابة القضائية بالنسبة لقرارات مجلس الأمن بموجب الفصل السابع بشكل واضح في الرأي المنفصل للقاضي شهاب الدين حيث ذكر: "أن المسالة المثارة الآن والمتمثلة في اعتراض Libya's challenge على شرعية القرار 92/748[1] فيما إذا كان قرار مجلس الأمن قد يتجاوز الحقوق القانونية للدولoverride the legal rights of states إذا كان الحال كذلك، هل هناك أي قيود على سلطات مجلس الأمن التقديرية؟ وما هي تلك القيود، وما هي الهيأة فيما عدا مجلس الأمن التي تملك الاختصاص في الإفصاح عن ماهية تلك الحدود؟.

في ذات المسألة آثار القاضي "ويرمانتري" في رأيه المنفصل بتساؤله "هل مجلس الأمن في تأدية وظائفه المتنوعة حر من أي قيود أم هناك حدود من المبادئ والقواعد القانونية والتي يؤدي من خلالها هذه المسؤوليات؟ وأجاب بان المادة 2/24 من الميثاق تقدم لنا مثل هذه الحدود بالإضافة لذلك لجأ لدراسة الأعمال التحضيرية للميثاق التي أظهرت بجلاء بعض هذه القيود على سلطات المجلس من اقتراحات المندوب البلجيكي والفرنسي اللذين طالبا بوضع القيود الكفيلة بضمان أن يكون عمل المجلس وفقا لمبادئ وأغراض الأمم المتحدة الواردة في الميثاق، وهذا ما ذهب إليه القاضي "ويرمانتري" بقوله: "إن السلطات التي يمارسها مجلس الأمن بشأن حفظ السلم والأمن الدوليين ليست مطلقة، بل مقيدة باحترام ميثاق الأمم المتحدة وقواعد القانون الدولي، هذا فضلا عن إن مسؤولية حفظ السلم والأمن الدوليين، وان تحمل المجلس بشأنها المسؤولية الأولى إلا انه لا يتحملها وحده بشكل مطلق بل تسعى أيضاً الأجهزة الأخرى للأمم المتحدة لتحقيق هذا الهدف الأسمى.

ويلاحظ ما إذا كان قد أتيح من قبل للمحكمة أن تحدد موقفها في مسألة الرقابة القضائية في قضية ناميبيا، عندما ذكرت بقولها :"لا يجوز لها أن تقوم بسلطة الرقابة القضائية أو الاستئناف على القرارات الصادرة بواسطة أجهزة الأمم المتحدة المعنية" إلا إن هذا التوجه السابق من المحكمة لا يشكل أي عقبة في سبيل وجود نوع من الرقابة على مشروعية قرارات المجلس والجمعية العامة بشأن مدى انسجامهما مع أحكام الميثاق وقواعد القانون الدولي، كما ذكر القاضي "ويرمانتري": "ليس هناك ما يمنع المحكمة أن تضع القرار الصادر من مجلس الأمن للرقابة وفقا لاختصاصها الوظيفي الذي يتطلب منها أن تبت في أي مسائل محددة تعرض أمامها وفقا للقانون الدولي"[2].

ويبدو أن التدابير المؤقتة في هذه القضية تظهر مدى محاولة المحكمة في تحقيق نوع من التوازن بين وظائفها القضائية مع سلطات المجلس السياسية، كما أشار إلى ذلك القاضي "بجاوي" بضرورة وجود درجة من التوازن إذا كانت المحكمة ليست مكلفة بدور الرقابة بصيغة الاستئناف في

[1] مقالة حول قضية لوكربي، مرجع سابق.

[2] مقالة حول قضية لوكربي، مرجع سابق .

قرارات المجلس، كما إن هذا الأخير ليس من مهامه أن يحل محل المحكمة في ممارسة وظائفها القضائية، كما بين القاضي "Laches" بقوله :"إن وظيفة المحكمة تطبيق القانون الدولي كقانون عالمي ليعمل به في إطار الأمم المتحدة أم خارجها، وينبغي احترامه كجزء من ذلك القانون مثل القرار الملزم لمجلس الأمن"، وهكذا إذا كان بعض القضاة في آرائهم الفردية أو المنفصلة لم يرفضوا إمكانية قيام المحكمة بفحص شرعية القرار 748 لكن ذلك لم يحدث لتعرض المحكمة لضغوط كما حدث في القضايا السابقة، وذلك بافتراض مشروعية قرارات الأمم المتحدة، فيما عدا القاضي "القشيري" الذي أعلن صراحة بان القرار 748 كان قد تجاوز نطاق اختصاص المجلس في هذه المرحلة من الإجراءات على الرغم من أن المحكمة غالبا ما تؤكد افتراض شرعية قرارات الأمم المتحدة بوصفها قد صدرت صحيحة وفقا لأحكام الميثاق، إذ لا يتوقع من المحكمة في المستقبل القريب أن تنعقد لتقرير قانونية أو شرعية أو لتعلن بوضوح عدم مشروعية قرارات الأمم المتحدة، خاصة إذا كان القرار صادر من مجلس الأمن في إطار مسؤولياته المتعلقة بحفظ السلم والأمن الدوليين، لذا يلاحظ أن المحكمة تحاول دائما تجنب التشكيك مباشرة في قرارات المجلس، وهذا ما يلاحظ من تعليقات قضاة المحكمة في آرائهم الفردية والمنفصلة والمشتركة في انتقاداتهم لقرارات المجلس ويلمحون إلى لفت الأنظار لمسألة الرقابة القضائية على هذه القرارات، بل يهددون بإصدار قرار يحكم بإبطالها، سواء لعدم مشروعيتها أو لتجاوزها نطاق الاختصاص المحدد في الميثاق، لكن الحقيقة غير ذلك إذ إن معظمهم يظهرون عجزهم وعدم قدرتهم على الإفصاح عن سلطة الرقابة القضائية[1] .

في خلاصة هذه القضية لا بد من الرجوع إلى الإشارة المهمة في الإعلان المشترك للقضاة حيث أظهروا دعما لقرار المحكمة بالاعتماد على القرار 748 دون اعتبار فيما إذا كان متجاوزا لنطاق سلطات المجلس، من خلال هذه الآراء القضائية السابقة التي تفيد في تأكيد الاستنتاج إذا كان مجلس الأمن يباشر سلطاته بموجب الفصل السابع من الميثاق خاصة تلك المتعلقة بحفظ السلم والأمن الدوليين[2].

## 02-رفض وإدانة إرهاب الدول.

طالما رفض مجلس الأمن تورط الدول في الجرائم الإرهابية، وعارض بشدة مساندتها ودعمها ويظهر ذلك جليا في العديد من القضايا الدولية، ومن هذه القضايا القضية الليبية [3]-قضية لوكربي

[1] مقالة حول قضية لوكربي، مرجع سابق.

[2] نفس المرجع .

[3] فبعد توجيه الاتهام إلى ليبيا صدرت الوثيقة رقم 23309 بعد انضمام فرنسا، وقد أكدت هذه الوثيقة بالإضافة إلى مطالب أخرى التزام ليبيا بصورة ملموسة بالتخلي عن جميع أشكال الإرهاب، وعن مساعدة الجماعات الإرهابية ، ولما

التي سبق وان تعرضنا لشرحها- حيث تصدى مجلس الأمن لهذا النزاع وأصدر عدة قرارات متلاحقة تؤكد على ليبيا وجوب تنفيذ طلبات الولايات المتحدة الأمريكية وبريطانيا وفرنسا[1] .

كما أكد مجلس الأمن على رفضه الشديد لتورط الدول في الأعمال الإرهابية من خلال قراره رقم 883 لسنة 1993 مستندا إلى أحكام الفصل السابع من ميثاق الأمم المتحدة[2].

في نفس الاتجاه صدر قرار آخر رقم 1044 لسنة 1996 في قضية محاولة اغتيال الرئيس المصري السابق "حسني مبارك" في العاصمة الأثيوبية "أديس أبابا" حيث حث هذا القرار على قمع الإرهاب الدولي، بما فيها تلك التي تتورط فيها الدول، وهذا الأمر عنصر جوهري وأساسي للحفاظ على السلم والأمن الدوليين[3] .

هذا وقد نص المجلس على جزاءات مخالفة قرار 1044، لتشمل هذه الجزاءات تخفيض البعثات الدبلوماسية إلى السودان بسبب رفض هذه الأخيرة تسليم المتورطين في هذه القضية، كما فرض الحظر الجوي عليها طبقا للقرار 1070 الصادر في نفس السنة.

إلا أنه تم تعليق تطبيق هذه العقوبات بعد الأحداث التي وقعت في الولايات المتحدة الأمريكية في 11 سبتمبر 2001[4] .

لم يتوان مجلس الأمن أيضا في التدخل إثر الهجمات التي أصابت كال من سفارتي الولايات المتحدة الأمريكية في "دار السلام" و "نيروبي"، ففي 7 أغسطس 1998، قام أعضاء في تنظيم القاعدة بتفجير السفارتين الأمريكيتين في نيروبي، كينيا وفي دار السلام، تنزانيا. ووقع الهجومان خلال دقائق قليلة تفصل بينهما، وكان أولهما في دار السلام، حيث قُتل 11 شخصا وأصيب 85 آخرين

---

رفضت ليبيا هذه المطالب والتي من أهمها تسليم رعاياها لما فيها من مساس بالسيادة الوطنية الليبية، حينها رفضت الولايات المتحدة الأمريكية رد ليبيا بالرفض وواصلت تصعيد الموقف وإعداد مسرح دولي لفرض العقوبات على ليبيا وقد لجأت الولايات المتحدة الأمريكية إلى استغلال مجلس الأمن باعتباره أداة دولية مؤثرة ذات قوة ملزمة لاستصدار قرارات تناسب المواقف والمصالح الأمريكية. لمزيد من التفاصيل راجع ماجد الحموي، قضية لوكربي بين السياسة =والقانون- العلاقة بين محكمة العدل الدولية ومجلس الأمن، مجلة جامعة دمشق، المجلد السابع عشر، العدد الثاني سوريا، 2001، ص 35.

[1] نفس المرجع، ص 37.

[2] قرار مجلس الأمن رقم 883 المؤرخ في 11 نوفمبر 1993 المتعلق بقضية لوكربي الليبية .

[3] قرار مجلس الأمن رقم 1044، الصادر في الجلسة رقم 3627 المنعقدة في 21 جانفي 1996 .

[4] ساعد الهام حورية، مرجع سابق، ص 24.

بجروح، وأدى انفجار نيروبي إلى مقتل 213 شخصا، من بينهم 12 أمريكيا، وإصابة عدد يقدر بنحو 4000 شخص من بينهم السفيرة "باتريشيا بوشنيل".

وتسبب الانفجار في إلحاق أضرار بالغة بمباني السفارتين، كما دمر الانفجار مكاتب ومصالح تجارية قريبة منهما[1].

قامت الولايات المتحدة الأمريكية بالرد على هذه الهجمات التي لحقت بسفارتيها وذلك بضرب مصنع أدوية الشفاء الكائن بالخرطوم، والذي تم تشييده في الفترة من 1992 إلى غاية 1996 وبدأ العمل في سنة 1997، وعلى الرغم من أنه كان يستورد الأدوية من الولايات المتحدة الأمريكية وألمانيا، السويد وايطاليا، الهند وسويسرا وتايلاند إلا أنها شنت هجوما عليه بصواريخ "كروز"، حيث قضت على شخص وأصابت 11 شخصا إلا أن الخسائر شملت عدد كبير من سكان السودان، حيث تم قطع التمويل بالدواء، الأمر الذي ألحق بهم أضرارا كبيرة، إلا أن أمريكا تذرعت بالعديد من الأسباب أهمها الانتقام للاعتداءات التي وقعت على سفارتيها، وأما السبب الآخر هو استخدام المصنع لغاز الأعصاب المتمثل في vx، والسبب الثالث وهو الأهم أن هذا المصنع تربطه بالقاعدة المتورط الأول في تلك الاعتداءات[2].

وقد أيد مجلس الأمن تصرف الولايات المتحدة الأمريكية واعتبرها في حالة دفاع شرعي على نفسها.

### ثانيا: الاعتماد على الرؤية الشاملة والموحدة.

تغير موقف مجلس الأمن في تعامله مع القضايا الإرهابية منذ سنة 1999 فوضع إستراتيجية شملت أربع محاور أساسية تمثلت في:

1. رفض الأعمال الإرهابية.
2. فرض آليات ملزمة للدول بهدف القضاء على الظاهرة.
3. بناء قرارات حكومية في إطار مكافحة الإرهاب
4. فرض عقوبات على الدول الممولة والمساندة للإرهاب.

[1] أعمال الإرهاب، مقالة منشورة في موقع : المكافآت من أجل العدالة،www. rewardsforjustice.net وتم الاطلاع يوم 2018/05/23 على الساعة 00:55 .

[2] ساعد الهام حورية، مرجع سابق، ص 24.

ومن أجل أن ينفذ مجلس الأمن هذه الإستراتيجية كان لزاما عليه إصدار العديد من القرارات اعترف من خلالها بحق الدول في الدفاع عن نفسها سواء كان هذا الدفاع فرديا أو جماعيا ضد الاعتداءات الإرهابية، وسد جميع مصادر التمويل أمام التنظيمات الإرهابية، من أجل إضعاف قدراتها ومنع استمرارية النشاط الإجرامي، هذا بالإضافة إلى أن مجلس الأمن أنشأ لجنة خاصة لمكافحة الإرهاب بغرض تجسيد المبادئ السابقة وهذا على غرار تلك التي أنشأتها الجمعية العامة[1]

## 01- قرار شامل بإدانة جميع الأعمال الإرهابية.

في سنة 2001 أصدر مجلس الأمن قرارا تحت رقم 1269 أدان بموجبه جميع أشكال التهديد للسلم والأمن الدوليين، بشكل عام وشامل لجميع أشكال الإرهاب، وتميز هذا القرار عن القرارات التي بقته في أنه وسع من استخدام الفصل السابع من ميثاق الأمم المتحدة بحيث ينقل مكافحة الإرهاب خارج حدود الدولة إلى النطاق الدولي، كما تضمن هذا القرار أيضا تفعيل في الآليات القانونية التي تم وضعها من قبل الأمم المتحدة، حيث طلبت من الدول تطبيق هذه التدابير، وبموجب أحكام هذا القرار أنشأ مجلس الأمن لجنة قانونية ضمت جميع الأعضاء وانحصرت مهامها في التصدي للتنظيمات الإرهابية، وفي نفس السياق عين الأمين العام للأمم المتحدة بناء على طلب المجلس فرقة للدعم التحليلي تقوم بتحليل المعطيات مساعدة منها لهذه اللجنة في أداء مهامها[2].

## 02- قرارات مجلس الأمن حول الحق بحق الدول في الدفاع الشرعي الفردي والجماعي.

في 12 سبتمبر من سنة 2001 أصدر مجلس الأمن قراره رقم 1368، الذي تلاه قرار آخر رقم 1373 في 28 من سبتمبر من نفس السنة، رفض من خلالهما المجلس وأدان بشدة جميع أعمال الإرهاب الدولي، وخاصة الهجمات التي تعرضت لها كل من واشنطن ونيويورك، حيث اعتبرها المجلس تهديدا للسلم والأمن الدوليين، ومن خلال القرارين اعترف مجلس الأمن للدول بحقها في الدفاع الشرعي الفردي والجماعي وهذا طبقا لنص المادة 51 من ميثاق الأمم المتحدة التي تبيح حق الدولة في الدفاع عن نفسها[3]، وقد أعرب المجلس قلقه الكبير إزاء تزايد الأعمال الإرهابية، والتهديدات التي

[1] ساعد الهام حورية، مرجع سابق، ص 24،25 .

[2] أسمهان بوضياف، دور الدول والمنظمات العالمية والإقليمية في مكافحة الإرهاب الدولي والعلاقات الدولية، مذكرة ماجستير في القانون، جامعة بن عكنون- الجزائر، 2009، ص 101.

[3] تنص المادة 51 من ميثاق الأمم المتحدة على أنه:" ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء (الأمم المتحدة) وذلك إلى أن

تشكلها هذه الأعمال على الأمن والسلم الدوليين، وقد طلب من خلال هذين القرارين من جميع دول العالم العمل من أجل محاربة الإرهاب وملاحقة الجناة ومحاكمتهم والتوقف عن تقديم المساعدات للتنظيمات الإرهابية وإيوائها.

وأما عن موقف مجلس الأمن الدولي فبدوره أكد في أكثر من مناسبة على رفض خروج الدفاع الشرعي عما رسمته المادة (51) من الميثاق من ضوابط، كما يتضح ذلك في القرار 486 لعام 1981 الذي أدان فيه إسرائيل نتيجة الضربة الوقائية التي قامت بها ضد مفاعل تموز العراقي على اعتباره موقع مشكوك فيه لتطوير أسلحة الدمار الشامل كما عارض مجلس الأمن الغزو الأمريكي على العراق تحت مسمى الحرب الوقائية والتي قامت بها الولايات المتحدة الأمريكية استنادا إلى مبدأ الدفاع الشرعي الوقائي، وهذا ما يظهر لنا مدى التناقض في مواقف الإدارة الأمريكية من مبدأ الدفاع الشرعي الوقائي حسب مصالحها، ففي الوقت الذي ناشدت فيه "واشنطن"،"نيودلهي" في 05أفريل2003 بعدم اعتماد مبدأ الضربة الاستباقية ضد "إسلام أباد" نجدها بالمقابل هي من تكرس أول تطبيق عملي لهذا المبدأ.

ونلاحظ انه بعد أحداث 11سبتمبر2001 أصبحت كل المواقف المعارضة والرافضة لما يعرف بالدفاع الشرعي الوقائي( الحرب الوقائية) بدأت تتقهقر وتنصهر، وأصبح القانون الدولي في الوقت الراهن يسمح للدول بالقيام بضربة استباقية- إما منفردة أو بصورة جماعية- (تحت لواء مجلس الأمن) كحالة من حالات الدفاع الشرعي عن النفس، فأصبح الدفاع الشرعي للدول بذلك لا يستند في أساسه القانوني لوجود عدوان مسلح، وإنما أيضا إلى وجود خطر ناشئ عن فعل يحتمل معه وقوع اعتداء على إحدى المصالح المحمية بحكم القانون الدولي بل لم يقتصر الأمر عند هذا الحد بل وصل إلى وجود محاولات لتقنين الدفاع الشرعي الوقائي الذي تحول من مبدأ نبذه وعارضه الجميع إلى مبدأ مقبول بل ومستحب على مستوى الممارسات ، وحتى القانون الدولي[1].

لتنفيذ هذه الإستراتيجية طلب مجلس الأمن من الدول تكثيف مجال التعاون بينهم وهو ما انعكس بالخصوص في القرار 1269 -السالف الذكر- الصادر في 12 أكتوبر 1999 معلنا بذلك استعداده

---

يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس- بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق- من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه".

[1] صابرة شعنبي، حق الدفاع الشرعي في القانون الدولي الجنائي، مذكرة ماجستير في القانون العام، جامعة عباس لغرور- خنشلة- قطب تبسة، 2012/2011، ص 111.

لاتخاذ جميع التدابير التي يراها مناسبة من اجل مكافحة وقمع الإرهاب والرد على الاعتداءات الإرهابية التي وقعت على الولايات المتحدة الأمريكية تحت مسؤولية الأمم المتحدة.

إن مجلس الأمن يسعى من خلال هذه القرارات إلى تأييد الجهود الرامية إلى تحقيق الاشتراك العالمي في الاتفاقيات الدولية القائمة لمناهضة الإرهاب وتنفيذها عالميا، ووضع صكوك دولية جيدة للتصدي لخطر الإرهاب، وإذ يؤكد من جديد أن قمع أعمال الإرهاب الدولي بما فيها الأعمال التي تكون الدول مساهمة فيها، وللإسهام الأساسي في صون السلم والأمن الدوليين فان مجلس الأمن من خلال قراراته[1]:

1. يدين إدانة قاطعة جميع أعمال الإرهاب، وأساليب ممارستها بوصفها أعمال إجرامية لا يمكن تبريرها، بغض النظر عن دوافعها، وذلك بجميع أشكالها ومظاهرها، وأينما وقعت أيا كان مرتكبوها ولا سيما الأعمال التي تهدد السلم والأمن الدوليين.

2. يجب على الدول أن تنفذ تنفيذا كاملا للاتفاقيات الدولية المناهضة للإرهاب والتي هي طرف فيها، ويشجع المجلس جميع الدول على النظر على سبيل الأولوية في الانضمام إلى الاتفاقيات التي ليست أطراف فيها، ويشجع أيضا على التعجيل باعتماد الاتفاقيات المعلقة.

3. يؤكد على دور الأمم المتحدة الحيوي في تعزيز التعاون الدولي في مكافحة الإرهاب ويشدد على أهمية زيادة التنسيق فيما بين الدول والمنظمات الدولية والإقليمية.

4. يهيب بجميع الدول أن تقوم في جملة أمور باتخاذ خطوات ملائمة في إطار هذا القانون والتيقظ من اجل:

- التعاون فيما بينها لا سيما من خلال اتفاقات وترتيبات ثنائية ومتعددة الأطراف لمنع وقمع أعمال الإرهاب وحماية مواطنيها وغيرهم من الأشخاص من الهجمات الإرهابية وتقديم مرتكبي تلك الأعمال للعدالة.

- القيام عن طريق إعمال جميع الوسائل القانونية، بمنع وقمع أي عمل إرهابي أو الإعداد له أو تمويله في أقاليمها.

[1] عمار تيسير بجبوج، مرجع سابق، ص 429،430.

- حرمان من يخططون لأعمال إرهابية أو يمولونها أو يرتكبونها من الملاذات الآمنة وذلك بكفالة اعتقالهم ومحاكمتهم أو تسليمهم.
- اتخاذ تدابير مناسبة وفقا للأحكام ذات الصلة من القانون الوطني والدولي، بما في ذلك المعايير الدولية لحقوق الإنسان، قبل منح حق اللجوء للشخص الذي يطلبه، للتأكيد من أن طالب اللجوء لم يشترك في أعمال إرهابية.
- تبادل المعلومات وفقا للقانون الدولي والوطني والتعاون في المسائل الإدارية والقضائية لمنع ارتكاب أعمال إرهابية

## 03- قرار منع تمويل الإرهاب[1].

بارتفاع معدل النشاط الإجرامي وبروز تنظيمات إرهابية جديدة ذات إمكانيات مادية لا بأس بها ازداد قلق المجتمع الدولي لما في ذلك من تهديد للسلم والأمن الدوليين، فكان منع تمويل الإرهاب ضمن مبادئ إستراتيجية مجلس الأمن التي أرادها شاملة ومانعة للأفعال الإرهابية،ومن أجل ذلك أصدر القرار رقم 1373 في 28 سبتمبر 2001، تم من خلاله تفعيل آليات مكافحة تمويل الإرهاب حيث دعا مجلس الأمن من خلال قراره الدول منع التمويل مهما كانت طبيعته، والامتناع عن تقديم المساعدات للتنظيمات الإرهابية من إيواء وتوفير الأمن لهم، ووضع على عاتق الدول التزامات تتمحور حول وجوب اتخاذ التدابير المناسبة لوضع حد للانتشار الكبير والواسع للتنظيمات الإرهابية وتشديد الخناق عليها ووقف جميع الإمدادات والمساعدات ضمن تشريعاتها الوطنية، وهذا بهدف تطبيق نص القرار[2].

يعتبر القرار 1373 الصادر عن مجلس الأمن في سنة 2001 أهم القرارات التي صدرت في تلك الفترة، حيث بموجب هذا القرار أنشئت لجنة مكافحة الإرهاب في أكتوبر من نفس السنة، مهمتها متابعة تنفيذ هذا القرار وتعزيز التعاون بين الدول في سياق مكافحة الإرهاب وتعد هذه اللجنة من أهم أجهزته الفرعية الفعالة، وهذه اللجنة ملزمة برفع تقارير تبين فيها ما اتخذته من خطوات في مجال المهام المنوطة بها لمجلس الأمن، وتتشكل لجنة مكافحة الإرهاب من ممثلين عن الدول الأعضاء في المجلس، وفي مارس من سنة 2004 تم تقديم اقتراح التمس فيه تغيير تشكيلة اللجنة، وبموجب القرار رقم 1535 ألحقت بها هيئة سميت" المديرية التنفيذية لمكافحة الإرهاب"، وهذا من اجل تسيير العمل

[1] قرار مجلس الأمن رقم 1373 الصادر بتاريخ 28 سبتمبر 2001 .

[2] ساعد الهام حورية، مرجع سابق، ص 26.

اليومي للجنة وجمع البيانات والمعلومات المتعلقة بجهود الدول في مجال مكافحة الإرهاب تنفيذا للقرار 1373 .

تقوم اللجنة بزيارات ميدانية للدول بموافقتها، من اجل رصد التقدم المحقق في مجال مكافحة الإرهاب خاصة في إطار التدابير المتخذة لسد منافذ التمويل، وتقييم طبيعة المساعدات التقنية التي تحتاجها الدول في إطار التدابير المتخذة لد منافذ التمويل، كما تعمل هذه اللجنة على تقديم المساعدات التقنية والمالية من أجل تمكين الدول من تنفيذ مخطط مكافحة الإرهاب، وتعتمد على التقارير المقدمة من قبل الدول التي تعتبر وسيلة اتصال بين اللجنة والدول الأعضاء، زيادة على ذلك تعقد اللجنة اجتماعات خاصة بغية بناء علاقات وطيدة مع المنظمات الدولية، والإقليمية ذات الصلة[1].

القرار 1373 يستند إلى الفصل السابع من ميثاق الأمم المتحدة الذي يجيز لمجلس الأمن اتخاذ التدابير اللازمة لحماية الأمن والسلم الدوليين والمنصوص عليهما في أحكام المواد من 39الى 42 من ميثاق الأمم المتحدة[2].

## 04- قرار منع انتشار الأسلحة البيولوجية والكيماوية والنووية.

أصدر مجلس الأمن قرار بهذا الشأن تحت رقم 1540 سنة 2004، وأعرب المجلس من خلال هذا القرار عن قلقه وقلق المجتمع الدولي كافة من إمكانية حيازة التنظيمات الإرهابية لهذا النوع من الأسلحة الفتاكة، كما أكد المجلس من خلال نفس القرار على ضرورة تقوية أسس التعاون الدولي والإقليمي وتكثيف الجهود الدولية من اجل منع انتشار مثل هذه الأسلحة عند التنظيمات الإرهابية ودعا الدول إلى وضع إجراءات أمنية مشددة لردع ومنع كل أشكال التهريب بما فيها تهريب الأسلحة مع الالتزام بن تشريعات وطنية في هذا المجال كما دعا المجلس من خلال هذا القرار إلى إنشاء لجنة تتألف من أعضاء المجلس لمراقبة بنود هذا القرار، ومطالبة الدول رفع تقاريرها إلى هذه اللجنة[3].

إن قرارات مجلس الأمن جاءت في مجملها بعد سنة 2001 رافضة لجميع أنواع الإرهاب وأشكاله ومختلف الأعمال الإجرامية التي ترتكب ضد المدنيين بقصد القتل أو إلحاق إصابات خطيرة أو بث الرعب في نفوس أشخاص معينين أو لتخويف جماعة من السكان أو إرغام حكومة أو منظمة دولية على القيام بعمل، أو الامتناع عن القيام بعمل، الأمر الذي يشكل جرائم في نطاق الاتفاقيات

[1] ساعد الهام حورية، مرجع سابق، ص 26،27.

[2] عمار تيسير بجبوج، مرجع سابق، ص 431.

[3] ساعد الهام حورية، مرجع سابق، ص 27.

والبروتوكولات الدولية ذات الصلة بمكافحة جميع أنواع الإرهاب، وهذا دون قبول أي مبرر ذو طابع سياسي، فلسفي، عقائدي، عنصري، عرقي أو ديني أو أي مبرر من هذا القبيل[1] .

اعتبر مجلس الأمن من خلال قراره 1566 أن الإرهاب بجميع أنواعه وأشكاله من اخطر التهديدات التي تواجه العالم في القرن 21، ومن خلاله أكد على أهمية المنهج الشامل والفعال الذي ينطوي على المساهمة الايجابية والتعاون الذي يجب أن يكون بين جميع أعضاء المجتمع الدولي[2].

## 05- قرار مجلس الأمن لمكافحة الإرهاب باستخدام الانترنت

ومازالت قرارات مجلس الأمن متعددة وكثيرة ويصعب حصرها إلا أنها جميعها أجمعت على ضرورة مكافحة جميع أشكال الإرهاب التي من ضمنها الإرهاب الالكتروني –محل دراستنا– ومن هذه القرارات –بالإضافة لما سبق– القرار الذي صدر في 12ديسمبر 2016 أكد مجلس الأمن من خلاله التزامه بسيادة جميع الدول وسلامة أراضيها واستقلالها السياسي وفقا لميثاق الأمم المتحدة، وأن الإرهاب بجميع أشكاله ومظاهره يمثل أحد أشد الأخطار التي تهدد السلام والأمن، أهاب مجلس الأمن بالدول أن تتبادل حيثما اقتضى الأمر المعلومات عن المقاتلين الأجانب وغيرهم من الإرهابيين والمنظمات الإرهابية بما يشمل المعلومات البيومترية والبيوجغرافية عبر قنوات إنفاذ القانون الثنائية ولإقليمية والعالمية.

جاء ذلك في القرار2322 الذي تبناه مجلس الأمن بالإجماع في جلسة إحاطة رفيعة المستوى بشأن التعاون القضائي الدولي في مجال مكافحة الإرهاب وأخطار الأعمال الإرهابية التي تهدد السلام والأمن الدوليين. وقد شارك في الجلسة التي ترأسها وزير العدل الاسباني "رافائيل كاتالا"، و"جان بول لابورد"، المدير التنفيذي للمديرية التنفيذية للجنة مكافحة الإرهاب، وزراء العدل أو أعضاء من النيابة العامة.

وشدد القرار على أهمية أن يأتي هذا التعاون على نحو يمتثل للقانون الدولي والقوانين والسياسات الوطنية والتعاون في المسائل الإدارية والشرطية والقضائية لمنع ارتكاب الأعمال الإرهابية ومكافحة التهديد الذي يشكله الإرهابيون الأجانب بما في ذلك العائدون[3].

[1] القرار رقم 1566 لسنة 2004 .

[2] ساعد الهام حورية، مرجع سابق، ص 28 .

[3] ساعد الهام حورية، مرجع سابق، ص 28.

كما أهاب القرار بالدول النظر في إمكانية السماح عن طريق القوانين والآليات المناسبة بنقل الإجراءات الجنائية حسب الاقتضاء في القضايا المتصلة بالإرهاب.

وأكد المجلس أن مثل هذا التعاون من شأنه منع الإرهابيين من الاستفادة من الجريمة المنظمة العابرة للحدود الوطنية وعلى إخضاع الإرهابيين ومن يعملون معهم من مرتكبي الجريمة المنظمة للتحقيق وعلى بناء القدرات اللازمة لملاحقتهم قضائيا.

كما أهاب القرار بجميع الدول أن تكفل وفقا للقانون الدولي إلا يسيء مرتكبو الأعمال الإرهابية أو منظموها أو ميسروها وضعهم كلاجئين وعدم الاعتراف بوجود بواعث سياسية كأسباب لرفض طلبات تسليم الأشخاص المدعى أنهم إرهابيون.

وحث قرار مجلس الأمن الدول الأعضاء على النظر في التصديق على الاتفاقيات الدولية ذات الصلة الموضوعة لدعم التعاون الدولي في المسائل الجنائية مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000 والبروتوكولات الملحقة بها والانضمام إلى تلك الاتفاقيات وتنفيذها.

كما حث أيضا الدول على أن تقيم حسبما تقتضي الحاجة وبمساعدة من مكتب الأمم المتحدة المعني بالمخدرات والجريمة وبالتعاون الوثيق مع اليونسكو الانتربول، تعاونا قضائيا موسعا في مجال إنفاذ القانون في جهود منع ومكافحة جميع أشكال الاتجار بالملكية الفكرية وما يتصل بها من جرائم مما يعود بالفائدة على الإرهابيين أو الجماعات الإرهابية، وان تتخذ تدابير وطنية على المستويين التشريعي والتنفيذي حيثما اقتضى الأمر.

شجع القرار الدول الأعضاء على اتخاذ إجراءات تعاونية لمنع الإرهابيين من التجنيد والتصدي لما يروجون على الانترنت وفي وسائل التواصل الاجتماعي من دعاية متطرفة عنيفة وتحريض على العنف، وذلك في ظل احترام حقوق الإنسان والحريات الأساسية وبما يتفق مع التزاماتها بموجب القانون الدولي، مشددا على أهمية التعاون مع المجتمع المدني والقطاع الخاص في هذا المسعى.

وأشار جون بول لابورد، المدير التنفيذي للجنة مكافحة الإرهاب في كلمته أمام المجلس، إلى أن الإرهاب هو تهديد دولي ويجب أن يتم إيجاد رد مناسب له، وأكد على عدم التسامح مع الإفلات من العقاب وملاحقة الإرهابيين حتى يمثلوا أمام العدالة ويتم إعادة الكرامة للضحايا.

وأضاف قائلا "إن الالتزام الدولي أمر ضروري لأننا لا زلنا نواجه تهديدا معقدا غير مركزي وأيضا ديناميكيا متحركا ومتنوعا على المستوى الجغرافي. سياستنا ومناهجنا ينبغي أن تتجاوز الحدود المتعارف عليها بالنسبة للأمن وأن تكون هناك رؤية شاملة تقوم على التعاون الدولي المعزز، وذلك

ليس فقط بين الدول الأعضاء ولكن أيضا بالتعاون مع المنظمات المتخصصة وكذلك المنظمات الإقليمية"[1].

## ثالثا: مدى قوة وإلزامية قرارات مجلس الأمن في مجال مكافحة الإرهاب.

سبق وأن قلنا أن الإرهاب الالكتروني ما هو إلا نوع مستحدث وشكل جديد لجريمة الإرهاب التقليدية ومن أجل ذلك فان موقف مجلس الأمن منه هو نفسه موقفه من جميع الأعمال الإرهابية التي تشكل تهديدا للسلم والأمن الدوليين.

اعتبر مجلس الأمن الإرهاب تهديد لسلامة وامن البشرية في جميع القرارات التي أصدرها بمكافحة الإرهاب باعتباره صاحب الاختصاص في هذا المجال، وتعتبر القرارات الوسيلة التي تستطيع بواسطتها المنظمات الدولية الإفصاح عن إرادتها الخاصة في حل نزاع معين أو تسوية وضعية معينة فتدخل مجلس الأمن في قضايا الإرهاب يعد من ضمن وظائفه ومهامه السامية في حماية الدول البشرية جمعاء من انتشار هذه الظاهرة الخطيرة، ولمجلس الأمن باعتباره أهم جهاز من أجهزة الأمم المتحدة فعالية كبيرة في مجال محاربة الإرهاب من خلال القرارات التي أصدرها، والتي أدان من خلالها الإرهاب بمختلف أشكاله، وفرض في بعض الأحيان جزاءات على الدول التي تقدم الدعم والإيواء للتنظيمات الإرهابية ، إلا أن التساؤل الذي وجب أن يطرح في هذه الحالة مدى إلزامية هذه القرارات للدول أم أنها مجرد توصيات؟؟؟؟.

### 01- قرارات مجلس الأمن مجرد توصيات .

يرى البعض أن قرارات مجلس الأمن في مجال مكافحة الإرهاب مجرد توصيات مثلها مثل تلك التوصيات الصادرة عن الجمعية العامة، واستند هذا الرأي إلى أحكام ميثاق الأمم المتحدة، فلا يوجد ما يمنح هذه القرارات القوة الإلزامية، وهذا لأن أحكام الفصل السادس من ميثاق الأمم المتحدة تمنح لمجلس الأمن حق التدخل لحل النزاعات الدولية بالطرق السلمية وفي حالة تعذر ذلك يحق له اللجوء إلى ما ورد من تدابير في القسم السابع الذي يعطي الحق إلى مجلس الأمن في اتخاذ الحل العسكري في حالة العدوان، وفي حالة الرجوع إلى أحكام المادة 36 من الميثاق نجدها تنص على أنه:" – لمجلس الأمن في أية مرحلة من مراحل نزاع من النوع المشار إليه في المادة 33 أو موقف شبيه به أن يوصي بما يراه ملائماً من الإجراءات وطرق التسوية.

[1] قرار مجلس الأمن رقم 2322 لسنة 2016 متوافر في الموقع: https://news.un.org وتم الاطلاع في 2018/05/27 على الساعة 02:40.

– على مجلس الأمن أن يراعي ما اتخذه المتنازعون من إجراءات سابقة لحل النزاع القائم بينهم.

–على مجلس الأمن وهو يقدم توصياته وفقا لهذه المادة أن يراعي أيضاً أن المنازعات القانونية يجب على أطراف النزاع – بصفة عامة – أن يعرضوها على محكمة العدل الدولية وفقاً لأحكام النظام الأساسي لهذه المحكمة."[1]

أما المادة 38 وما يليها فهي تنص على أن المجلس الأممي يمكنه التدخل لحل النزاعات بالطرق السلمية وان يوصي الأطراف المتنازعة بضرورة العمل وفق أحكام وديباجة الأمم المتحدة، كما أن المجلس في حالة ما إذا طبق الفصل السادس من الميثاق فانه يلتزم بالالتزام المبرم بين أطراف النزاع والتي يمكنها عرض ما تراه مناسب من تدابير في هذا المجال، وحسب ما يراه أصحاب هذا الرأي فان قضايا الإرهاب لا تعتبر من النزاعات المسلحة أو شكل من أشكال العدوان الذي يتطلب من المجلس إصدار قرارات ملزمة بشأنها ومنه تعتبر هذه القرارات مجرد توصيات وليست لها أي قوة إلزامية[2] .

## 02– قرارات مجلس الأمن إلزامية.

يرى أصحاب هذا الرأي أن القرار الدولي يستمد قوته الإلزامية طبقا لمصدره القانوني حيث اعتمد مجلس الأمن في قراراته التي خص بها مكافحة الإرهاب على أحكام ميثاق الأمم المتحدة، وأهم القرارات الصادرة عن مجلس الأمن طرحت إشكالية الشرعية الدولية كان بعد الأحداث التي شهدتها الولايات المتحدة الأمريكية في 2001/09/11 وهما القرارين 1368 و1373 حيث استند المجلس في إصدارها على أحكام الفصل السابع من ميثاق الأمم المتحدة خاصة أحكام المادة 51 السالفة الذكر[3] بالإضافة إلى نص القرار 1373 الذي يتضمن مقاطعة جميع الدول التي لا تلتزم ببنوده وفرض عقوبات اقتصادية وحتى عسكرية وخاصة بالنسبة للدول التي تأوي الإرهابيين وتساعد على انتشار التنظيمات الإرهابية والفكر الإرهابي، كما شمل على الآليات التنفيذية التي تطبق أحكام هذا القرار كإنشاء لجنة مكافحة الإرهاب وهذا لضمان التزام جميع الدول بأحكامه، وهذا لا يتنافى وأحكام ميثاق الأمم المتحدة الذي يستمد منه المجلس القوة الإلزامية، بالإضافة إلى أن المجلس اعتبر أن الأعمال الإرهابية بمختلف أنواعها سواء التقليدية أو المستحدثة تشكل تهديدا للسلم والأمن الدوليين، مما يسمح

[1] ميثاق الأمم المتحدة :www.un.org .

[2] ساعد الهام حورية، مرجع سابق، ص 29.

[3] التي تنص على حق الدفاع الشرعي الفردي والجماعي.

للمجلس من استخدام أحكام الفصل الرابع من الميثاق وكذلك الفصل السادس من أجل أداء المهام المنوطة به والمتمثلة في استتباب الأمن في العالم[1].

## الفرع الثاني: دور منظمة الشرطة الجنائية الدولية مكافحة الإرهاب الالكتروني.

إن أية دولة لا تستطيع بمفردها القضاء على الجريمة أو الحد منها، لاسيما إذا كانت عابرة للحدود، وترتكب باستخدام الانترنت من قبل أفراد أو جماعات منظمة في إقليم دولة معينة ثم تنتقل إلى دولة أخرى، مما يقلل من فرص تعقبها وإلقاء القبض على مرتكبيها ومعاقبتهم، فقد ساهمت التطورات التكنولوجيا الحديثة التي شهدها العالم ف العصر الحديث وبالتحديد بعد النصف الثاني من القرن العشرين، في تطور الأساليب الإجرامية المستخدمة في ارتكاب الجرائم وظهور أنواع جديدة من الجرائم مثل الإرهاب الالكتروني.

فالتصدي لأشكال الجريمة في عصرنا الحديث من المهمات الصعبة والخطيرة، وبذلك تطرح المشكلة على الصعيد الجنائي الدولي، لتبني إجراءات أكثر فعالية في هذه السياسة لأنها تستلزم تنسيقاً قوياً للوسائل القانونية والمادية، من أجل الكشف عن الجرائم، وإلقاء القبض على المجرمين، ومعاقبتهم ومنع خطرهم على الفرد والمجتمع.

جميع هذه الأمور المتقدمة تتطلب إيجاد واستحداث أساليب حديثة لمكافحة الجريمة والحد منها على الصعيدين الداخلي (الوطني) والدولي، وهذا الأمر لا يتم إلا من خلال خلق أو إنشاء جهاز أو منظمة دولية تأخذ على عاتقها مكافحة الجريمة والمجرمين من خلال تعقبهم تمهيداً لإلقاء القبض عليهم وتسليمهم إلى الجهات المختصة، وتعمل هذه المنظمة وفقا لقواعد وأصول قانونية توافق عليها جميع الدول التي تنظم إلى الاتفاقية المنشأة لها، ويتم استخدام التكنولوجيا الحديثة في إدارة هذه المنظمة من اجل تحقيق الأهداف المرجوة من إنشائها، وبالنظر لخلو المكتبة القانونية من دراسة تعني بتوضيح ماهية هذا الجهاز أو المنظمة، وكيفية تكوينها وما هي الآليات المتبعة في العمل، وما هي الأهداف المراد تحققها.

[1] ساعد الهام حورية، مرجع سابق، ص 30 .

ومن ذلك بات الأمر ضروريا لإنشاء منظمة الشرطة الجنائية الدولية والتي أصبحت تلعب دور مهم في دعم وتفعيل التعاون المتبادل على أوسع نطاق ممكن بين سلطات الشرطة الجنائية بين دول العالم، وقد أصبحت قناة اتصال مهمة بين أجهزة مكافحة جرائم الإرهاب بمختلف أنواعها.

ومن أجل ذلك قسمنا هذا العنصر إلى فرعين سوف نتعرض في العنصر الأول إلى ماهية المنظمة الدولية للشرطة الجنائية وأما الفرع الثاني فقد خصص إلى دورها في مكافحة الإرهاب الالكتروني.

## أولا: ماهية المنظمة الدولية للشرطة الجنائية "الانتربول".

ترجع البدايات الأولى للتعاون الدولي الشرطي إلى عام 1904 عندما أبرمت الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض والتي نصت في مادتها الأولى على انه:" تتعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة"، وبعد ذلك اخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية[1]، وهو ما سوف نوضحه بشيء من التفصيل.

### 01- نشأة المنظمة الدولية للشرطة الجنائية.

إن بداية التعاون الأمني في المجال الشرطي ترجع إلى سنة 1904 ، وذلك بمناسبة الاتفاقية الدولية الخاصة بمكافحة الاتجار بالرقيق و المبرمة في 18 ماي 1904 [2]، وقد تم إنشاء جهاز لتبادل المعلومات بين دول أمريكا الجنوبية سنة 1905 ، خاصة المعلومات المتعلقة باستخدام النساء والفتيات لغرض الدعارة في الخارج ، بهدف القضاء على هذه الجريمة في أقاليمها[3].

---

[1] محمد منصور الصاوي، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية (سنة النشر غير مذكورة)، ص 648.

[2] نصت المادة الأولى من الاتفاقية الدولية الخاصة بمكافحة الاتجار بالرقيق على " تتعهد كل الحكومات المتعاقدة على أن تنشئ أو تعين سلطة تركز لديها المعلومات الخاصة باستخدام النساء و الفتيات لغرض الدعارة في الخارج ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة الممثلة لها في كل الدول المتعاقدة ".

[3] محمد منصور الصاوي، مرجع سابق، ص 648.

معظم المتخصصين يرجعون تاريخ إنشاء هذه المنظمة إلى سنة 1923 ، عندما تم إنشاء اللجنة الدولية للشرطة الجنائية ، و كان هدف هذه اللجنة هو التنسيق بين أجهزة الأمن الوطنية للدول الأوروبية في مجال مكافحة الجريمة ، و لاسيما الجريمة المنظمة عبر الوطنية . و عند نشوب الحرب العالمية الثانية 1939-1945 توقف نشاط هذه اللجنة تماما بسبب الصراع المسلح الذي نشب بين الدول الأوروبية[1] .

وبعد الحرب العالمة الثانية دعا المفتش العام للشرطة البلجيكية السيد " لوفاج" إلى عقد مؤتمر دولي في بلجيكا من 6 إلى 9 جوان 1946 ، و حضر هذا المؤتمر 17 دولة وكان هدفه هو إحياء التعاون من جديد بين الدول ، خاصة في مجال مكافحة الجريمة والقضاء عليها و قد توصل هذا المؤتمر إلى إحياء الجنة الدولية للشرطة الجنائية ، وتم نقل مقرها إلى باريس ،كما أحدثت تعديلات هامة في نظام اللجنة و استحدث منصب الأمين العام و عهد به إلى "لوفاج " وأنشأت لجنة تنفيذية وتم في هذا المؤتمر لأول مرة استخدام مصطلح "المنظمة الدولية للشرطة الجنائية "[2]، وقد قامت الجمعية العامة في الدورة الخامسة و العشرون التي انعقدت في مدينة فيينا ، ما بين 07 و13 جوان 1956 بوضع ميثاق المنظمة ، وهو بمثابة دستور لها ، و قد تم إرسال الدستور المنظم لهذه الهيئة إلى جميع الدول الأعضاء من خلال وزارات الخارجية ، و ذلك للتصديق عليها و إبداء الاعتراضات و التحفظات إذا رأت الدول ذلك في مدة أقصاها ستة أشهر[3]، و بذلك أصبح دستور المنظمة نافذا إبتداءا من تاريخ 13 جوان 1956 [4] .

وتم إبرام اتفاقية بين المنظمة الدولية للشرطة الجنائية و فرنسا تتضمن الموافقة على وضع المقر الرئيسي للمنظمة على الأراضي الفرنسية بتاريخ 2 نوفمبر 1972 ومقرها حاليا مدينة ليون الفرنسية وفي أكتوبر 1977 وصل عدد الدول الأعضاء في المنظمة إلى 126 دولة ، وفي سنة 1988 أصبح عدد الدول الأعضاء في المنظمة 177 دولة بانضمام دولة جزر القمر ، ثم ارتفع إلى 184 دولة في سنـة 2006 .

---

[1] منتصر سعيد حمودة ، المنظمة الدولية للشرطة الجنائية ، الانتربول ، دار الفكر الجامعي، الإسكندرية، 2008 ص 11.

2 أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 260 .

[3] المادة 45 من النظام الأساسي للمنظمة الدولية للشرطة الجنائية .

[4] محمد منصور الصاوي ، مرجع سابق، ص 649

وقد تم إنشاء هذه المنظمة من أجل :

– تأكيد وتنمية المساعدة المتبادلة في أوسع نطاق ممكن بين سلطات الشرطة الجنائية في حدود القوانين القائمة في البلاد المختلفة ، وبروح الإعلان العالمي لحقوق الإنسان .

– إقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعال في منع و مكافحة جرائم القانون العام ·

وقد كان للمنظمة في سبيل تحقيق ذلك قدر كبير من الحرية التي اتفقت عليها الدول، ولم يقيدها في ذلك سوى نص المادة 3 من ميثاقها الذي يمنع على المنظمة أن تنشط أو تتدخل في مسائل أو شؤون ذات طابع سياسي أو عسكري أو ديني أو عنصري .

**02– أعضاء المنظمة ولغاتها.**

في بداية تأسيسها كانت المنظمة الدولية للشرطة الجنائية (الانتربول) تتكون من عدد محدد من الدول، إما اليوم فقد أصبحت تضم في عضويتها معظم دول العالم، فبلغ عدد الدول الأعضاء في الجمعية العامة للمنظمة 186 دولة، وهو قابل للزيادة والتوسع, ويوجد في كل دولة عضو مكتب وطني مركزي للمنظمة يقوم بالاتصال بالمكتب الرئيس للمنظمة في مدينة (ليون) من خلال شبكة اتصالات حديثة، لطلب المعلومات، أو لتزويد الرئيس بالمعلومات المطلوبة حول جرائم أو مجرمين معينين وتعد جمهورية العراق إحدى الدول الأعضاء في المنظمة..

أما اللغات الرسمية التي يتم عن طريقها التواصل بين المكاتب الوطنية والمركز الرئيس فهي اللغات الأربع الآتية: الإنكليزية، الفرنسية، العربية، الاسبانية، فتصدر نشرات المنظمة وتعقد مؤتمراتها وتجري اتصالاتها، وفقا لهذه اللغات الأربع فقط, ويتم ترجمة المراسلات والنشرات إلى هذه اللغات ويرى بعض الباحثين انه كان من الأنسب اعتماد اللغات الرسمية المعتمدة في الأمم المتحدة, وعدم الاقتصار على اللغات الأربع, لاسيما وان هذه المنظمة دولية وتضم في عضويتها معظم دول العالم وهي جهاز يعمل تحت أشراف ومتابعة الأمم المتحدة وان لم يكن تابع لها تبعية مباشرة، وهي تعتمد

لغات أكثر سعة وانتشارا[1]، وعليه يقترح تعديل نص المادة (54) من النظام العام للمنظمة الدولية للشرطة الجنائية، وجعل اللغات السبع المتعمدة في الأمم المتحدة هي ذاتها اللغات الرسمية للانتربول.

## 03- أهداف الانتربول.

تعرضت المادة الثانية من ميثاق المنظمة الدولية للشرطة الجنائية "الانتربول" لبيان الهدف الأساس من إنشاء المنظمة بقولها:" إن هدف المنظمة هو[2]:

1. تأكيد وتشجيع المعونة المتبادلة في أوسع نطاق ممكن بين سلطات الشرطة الجنائية في حدود القوانين القائمة في البلاد المختلفة، والاهتداء بروح الإعلان العالمي لحقوق الإنسان.
2. إقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعال ومؤثر في منع ومكافحة جرائم القانون العام".

يتضح من هذه المادة إن المنظمة تعمل على تأكيد وتشجيع التعاون الدولي بين سلطات الشرطة في الدول الأعضاء، نتيجة لما الم بالجماعة الدولية من تطورات في المجالات كافة، وخاصة في مجال المواصلات والتي كان لها أثرها في سهولة انتقال المجرمين بين الدول، بعد ارتكابهم لجرائمهم في البلدان المختلفة، الأمر الذي يتطلب التعاون بين أجهزة الشرطة في الدول كافة، لمكافحة مثل هذه الأعمال وهذا التعاون يتم في إطار القوانين النافذة في كل دولة وذلك لمكافحة جرائم القانون العام وهي الجرائم المعروفة عالميا بانتهاكها للقانون الطبيعي في أي مجتمع, فتدخل الانتربول يعود لطبيعة الجريمة التي قد يسهم عنصر أجنبي كونها عابرة للحدود، فقد يقترف شخص ما جريمة على ارض دولة ثم يهرب إلى دولة أخرى، أو عندما تكون الجريمة مرتكبة في عدة دول على مراحل، وهذا التعاون يجب أن يكون في إطار الإعلان العالمي لحقوق الإنسان، وبعيدا عن الأمور السياسية والدينية والعنصرية ، ويمكننا تلخيص أهداف الانتربول بما يأتي [3]:

---

[1] ضياء عبد الله عبود الجابر، وآخرون، المنظمة الدولية للشرطة الجنائية، بحث مقدم إلى مركز آدم للدفاع عن الحقوق والحريات منشور في الموقع www.annabaa.org، تاريخ الاطلاع 2018/06/23، على الساعة 06:02.

[2] نفس المرجع.

[3] هذه الجرائم تشمل الجرائم الإرهابية والجريمة المنظمة والاتجار بالمخدرات والرقيق والأعضاء البشرية، وغسيل الأموال والاتجار بالأسلحة، وتخريب وتعطيل وسائل المواصلات والاتصالات، منشورة في الموقع: http://www.aljazirah.com ، تاريخ الاطلاع 2018/06/23 على الساعة 06:21.

- العمل على تأمين وتنمية التعاون الدولي بين كافة سلطات الشرطة الجنائية في الدول الأعضاء.
- إنشاء وتفعيل كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها.
- العمل على منع الجرائم الدولية، أو الحد منها عن طريق مكافحة الإجرام العابر للحدود، عن طريق تعقب المجرمين والجرائم المرتكبة، وتسهيل عمليات إلقاء القبض عليهم وتسليمهم إلى الجهات المختصة[1].
- إن الغاية الأساسية للانتربول، هي العمل على قيام عالم أكثر أمنا وسلاماً بعد إن انتشرت العمليات الإجرامية وامتدت إلى عدد كبير من الدول، هذا من جانب، ومن جانب آخر ضعف أو محدودية الجهود الأمنية المحلية في التحدي للإجرام ولاسيما المنظم منه، وهذه هي أهم الأسباب التي دعت إلى ظهور المنظمة[2].

## 04- اختصاصات الانتربول وصلاحياته.

للانتربول اختصاصات وصلاحيات تقوم بها بواسطة الأجهزة التي تتكون منها، فدور الانتربول يتمثل بتقديم العون لهيئات الشرطة في الدول الأعضاء فيها، ويتم هذا العمل بصورة مباشرة عبر المكتب المركزية الوطنية في جميع البلدان الأعضاء في المنظمة.

وتتمثل هذه الوظائف والاختصاصات من خلال وظائف واختصاصات الأجهزة المكونة لبناء وهيكلية المنظمة، والتي تتلخص بالاتي:

**01** - جمع البيانات والمعلومات المتعلقة بالجرائم والمجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة – المكتب الرئيس في ليون – من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، ويتم ذلك عبر وسائل الاتصال المختلفة، كالهاتف والفاكس والتلكس والانترنيت

[1] محمود شريف بسيوني، الوثائق الدولية المعنية بحقوق الإنسان، المجلد الثاني، دار الشروق، القاهرة، 2003، ص 135

[2] محمد سامي النيراوي، شرح الأحكام العامة لقانون العقوبات الليبي، الطبعة الثالثة، منشورات جامعة قار يونس بنغازي، ليبيا، 1995، ص 120-143

(البريد الالكتروني)[1] ، وشبكة اتصالات تتم بواسطة منظومة اتصالات حديثة جدا تدعى (منظومة اتصالات الانتربول العالمية (7 / 24 – ا)[2].

**02**- التعاون مع الدول في ضبط المجرمين الهاربين، من خلال إصدار النشرات الدولية بمختلف أنواعها (الحمراء، الصفراء، الزرقاء، الخضراء، البرتقالية)، إضافة إلى النشرة الخاصة للانتربول – مجلس الأمن [3]إضافة إلى النشرات الدولية المخصصة للمخدرات والنقد المزيف، ومكافحة الإرهاب – وهو ما يتعلق بموضوع الدراسة– وتهريب الأسلحة، وغسيل الأموال ، والإجرام المالي المرتكب بواسطة التكنولوجيا المتقدمة[4].

**03**- تنظيم المؤتمرات والندوات الدولية، بهدف تبادل الخبرات من اجل تحسين وتشجيع التعاون الدولي الجنائي.

**04**- تقديم الخدمات في مجال الأدلة الجنائية، كبصمات الأصابع، والحمض النووي (DNA)، وبيان ضحايا الكوارث من خلال الاحتفاظ بسجلات الجرائم الدولية[5].

## 05- الطبيعة القانونية للانتربول.

اختف الفقه حول الطبيعة القانونية للمنظمة الدولية للشرطة الجنائية الدولية، وانقسموا في هذا الشأن إلى قسمين أو اتجاهين كالتالي:

### الاتجاه الأول.

[1] ضياء عبد الله عبود الجابر، وآخرون، مرجع سابق.

[2] تعد منظومة (24/7ا) منظومة عالمية متقدمة ومرنة قابلة للتوسع ومأمونة ويتم تبادل الرسائل بين المنظمة الدولية للشرطة الجنائية والمكاتب المركزية الوطنية في أنحاء العالم وبين الوصول إلى قاعدة بيانات المنظمة، ويتم تبادل المعلومات بسهولة وسرعة كبيرة، وهذه المنظومة لها فوائد عديدة بنظر النشرة الإعلامية للانتربول رقم ( / Com fs/2008-03 /TE – 01.

[3] استحدثت هذه النشرة عام (2005) استجابة لقرار مجلس الأمن رقم (1617) الذي دعي الأمين العام للأمم المتحدة إلى العمل مع الانتربول لتيسير أفضل الأدوات لمساعدة لجنة مجلس الأمن المشكلة بالقرار (1267) على الاضطلاع بولايتها بتجميد الأموال ومنع السفر وحظر توريد الأسلحة للأشخاص والكيانات المرتبطة بتنظيم القاعدة وحركة طالبان ينظر النشرة الإعلامية الصادرة عن الانتربول رقم (Com/fs 2005 – 03 / G1 – 01).

[4] David Bain Bridge, Introduction to Computer Law, Forth Edition, Longman, England, 2000,p 197.

[5] حسين محمود عبد الدايم، البصمة الوراثية وحجيتها في الإثبات– دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي، الطبعة الأولى، دار الفكر العربي، الإسكندرية، 2008، ص 35.

يرى أن المنظمة الدولية للشرطة الجنائية ليست شخصا من أشخاص القانون الدولي العام، وإنما هي شخص من أشخاص القانون الخاص، وهي منظمة غير حكومية و يستند في هذا الشأن بما يلي:

- قرار المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة سنة 1949 الذي اعترف فيه للمنظمة الدولية للشرطة الجنائية بطابع المنظمة الغير حكومية ذات الطابع الاستشاري .
- اقتصار المنظمة على الجانب الجنائي فقط ، و عدم التدخل في الأمور السياسية التي تكون من اختصاصات الحكومات ، و كذلك عدم التدخل في الأمور ذات الطابع العسكري أو العرقي أو الديني .
- أن الاتفاق المنشئ تم بناءا على اتفاق سلطات الشرطة في كل دولة وليس الحكومات قد عرف المجلس الاقتصادي والاجتماعي المنظمات غير الحكومية بأنها "المنظمات التي لا تنشأ عن طريق اتفاق دولي بين الحكومات ولا تتمتع بالشخصية القانونية الدولية ، ويتم إنشاؤها من طرف الأفراد أو حتى هيئات عامة عدا الدول ، وذلك بمقتضى دستور يحدده منشؤها و يتفقون عليه"[1].

**الاتجاه الثاني.**

يرى أن المنظمة الدولية للشرطة الجنائية هي منظمة دولية، وبالتالي فهي شخص دولي أشخاص القانون الدولي العام ، ويرون أن المنظمة تتمتع بالشخصية القانونية الدولية من خلال العناصر التالية:

**أ – الكيان الدائم .**

إن إطلاق اسم منظمة على الانتربول يعبر عن انصراف إرادة منشئيها إلى دمغها بطابع الدوام شأنها في ذلك شأن أي منظمة دولية حكومية ، إضافة إلى وجود أجهزة معينة تقوم عليها هذه المنظمة والتي حددها دستور هذه الأخيرة و تدل على أن المنظمة دائمة النشاط[2].

**ب– وجود إرادة ذاتية مستقلة تتحقق من خلالها الشخصية القانونية الدولية للمنظمة.**

[1] محمد منصور الصاوي ، مرجع سابق، ص 655 .

[2] نفس المرجع، ص 655 .

يقصد به أن تكون للمنظمة إرادة مستقلة عن إرادة الدول الأعضاء ومتميزة عنها وبالتالي تمتعها بالشخصية القانونية الدولية التي هي مناط اكتساب الحقوق وتحمل الالتزامات، والشخصية القانونية الدولية للانتربول تظهر في قيام المنظمة بإبرام الاتفاقيات الدولية ، والتي نذكر منها:

- اتفاقية دولية أبرمت بين منظمة الانتربول كمنظمة دولية حكومية وبين منظمة الأمم المتحدة سنـة 1971 والتي تتعلق بالتعاون في المجال الجنائي .
- اتفاقية أبرمت بين منظمة الانتربول وبين الحكومة الفرنسية ، والتي صادق عليها البرلمان الفرنسي سنة 1962، وأصبح هذا الاتفاق نافذا سنة 1972، وهذا الاتفاق يعترف لمنظمة الانتربول بصفة منظمة دولية حكومية ، ومقرها داخل الأراضي الفرنسية .

كما أن للمنظمة الدولية للشرطة الجنائية شخصية قانونية دولية في الأعمال والسلطة التي تتمتع بها في اتجاه أعضائها، بحيث يكون للمنظمة حق التملك والتعاقد ، وكذلك تعيين ما يلزم من عمال وهذا من أجل تأدية مهامها على أحسن وجه ممكن .

### ج- الاتفاق المنشـئ .

يعد من أكثر العناصر دلالة على المنظمة الدولية الحكومية أي المعاهدة الدولية ، والمقصود به الاتفاقية التي تبرم بإرادة الدول الأعضاء وتحدد في نصوصها جملة الأهداف والمهام التي تقوم بها في علاقاتها مع الدول الأعضاء ، والتي تعتمد في إطار مؤتمر دولي يعقد لهذا الغرض .

فالاتفاق المنشئ لمنظمة الانتربول والذي تم وضعه في مؤتمر فيينا سنة 1956 يعد اتفاقية دولية و هذا راجع إلى أن الممثلين في مؤتمر فيينا الذين وضعوا الميثاق المنشئ للمنظمة الدولية للشرطة الجنائية قد فوضوا من قبل دولهم صراحة أو ضمنا في وضع هذا الميثاق ، وأن حكومات الدول الأعضاء في منظمة الانتربول أسهمت في تمويلها لمدة زمنية تقدر بأكثر من 45 سنة .

مما تقدم يمكن القول أن الانتربول عبارة عن جهاز أمني رقابي عالمي يتمتع بالشخصية المعنوية والذمة المالية والاستقلالية الإدارية وأهلية التقاضي، ويعد منظمة دولية لها ميثاقها الخاص بها- نظامها الأساسي – ولها أنظمتها العامة الخاصة بآلية العمل فيها، ولها أجهزتها التي تقوم عليها وتعمل من خلالها على تحقيق الأهداف المنشودة ، وبالتالي تتمتع هذه المنظمة بكافة الحصانات

والامتيازات التي تتمتع بها المنظمات الدولية ، كونها قد أنشأت بقرار صادر عن الجمعية العامة للأمم المتحدة[1] .

ومما سبق نجد أن الرأي الراجح هو من يرى أن المنظمة الدولية للشرطة الجنائية "الانتربول" كيان قانوني دولي يتمتع بالشخصية القانونية الدولية المستقلة عن الدول الأعضاء، وهذه الاستقلالية أكد عليها ميثاق المنظمة[2]، وبالتالي فهي لا تخضع لأية دولة أو منظمة دولية أخرى، بل تعمل بالتعاون مع تلك الدول والمنظمات الدولية، على تحقيق الأهداف التي نص عليها ميثاقها (المادة 2) ففي 30 / 4/ 2007 عقد الأمينان العامان للانتربول والأمم المتحدة لقاء لمناقشة سبل التعاون بين المنظمتين، بعد أن أدى هذا التعاون إلى استخدام النشرة الخاصة للانتربول – مجلس الأمن التابع للأمم المتحدة التي تستهدف المجموعات والأفراد المرتبطين بتنظيم القاعدة وحركة طالبان[3].

كما أن منظمة الانتربول تتعاون مع الأجهزة التي أنشأتها الأمم المتحدة كالمحكمة الجنائية الدولية ليوغسلافيا السابقة[4]، كما أن الانتربول لها ممثل خاص في الأمم المتحدة وكل هذه الأمور تدلل على أن الانتربول منظمة مستقلة غير خاضعة لأية جهة ومنها المنظمة الدولية الأمم المتحدة هذا من جانب ومن جانب آخر هناك وثائق دولية تؤكد إن المنظمة الدولية للشرطة الجنائية (الانتربول)، رغم كونها منظمة مستقلة، لكن استقلاليتها ليست تامة فهي تخضع لإشراف وتوجيه المنظمة الدولية الأمم المتحدة كونها قد أنشأت بقرار من الجمعية العامة للأمم المتحدة، وتعمل بالتعاون والتنسيق معها على تحقيق الأهداف التي نص عليها ميثاق المنظمة، وهو أمر لابد منه كون الأمم المتحدة المنظمة الأم ولا يمكن تحقيق ذلك إلا بالتعاون والتنسيق معها، كما أن الأمم المتحدة قامت في عام 1971 بالتدخل في إعادة ترتيب وتنظيم الانتربول بصفته منظمة تتعامل مع الحكومات في الدول الأعضاء[5].

---

[1] ضياء عبد الله عبود الجابر، وآخرون، مرجع سابق.

[2] نصوص المواد (3، 4، 21، 30) من النظام الأساسي للانتربول (الميثاق).

[3] ضياء عبد الله عبود الجابر، وآخرون، مرجع سابق.

[4] فقد أصدر الانتربول نشرة بحث حمراء عن مجرم دولي فر من سجن في البوسنة بتاريخ 25 / أيار / 1996 هو "رادوفان ستانكوفج"، وكان المكتب الوطني المركزي في "سراييفو" قد أرسل رسالة عاجلة إلى كافة البلدان الأعضاء في الانتربول، يعلمهم فيه عن فرار هذا المجرم، كما صدرت نشرة حمراء بحق الجنرال الصربي "زادرافكوتولمر"

[5] مؤتمرات الانتربول منشور على موقع المنظمة على شبكة الانترنت: http://www.interpol.int

فالانتربول يتكون من أجهزة تعمل من خلالها على تحقيق أهدافها وهذه الأجهزة تتمثل بالجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب الوطنية المركزي، المستشارون وتدار المنظمة بواسطة مكتب اللجنة التنفيذية ومقره في مدينة ليون الفرنسية وتعد المكاتب الوطنية بمثابة فروع للمنظمة في الدول الأعضاء وتدخل وظائف هذه المكاتب في نطاق عمل المنظمة، والدول الأعضاء في المنظمة هي دول ذات سيادة وجدت من الضروري التعاون فيما بينها من أجل تظافر الجهود الدولية والوطنية في مكافحة الجريمة والمجرمين فاختارت الانضمام إلى المنظمة، فالتعاون الدولي الجنائي (الشرطي) بين أعضاء المنظمة يحكمه مبدأ (السيادة الوطنية) للدول الأعضاء[1].

مما تقدم يمكننا القول أن "الانتربول" منظمة دولية لها ميثاقها الخاص بها (نظامها الأساسي) ولها أنظمتها العامة الخاصة بالية العمل فيها، ولها أجهزتها التي تتكون منها وتقوم عليها وتعمـل من خلالها على تحقيق أهدافها المنشودة، وبالتالي تتمتع هذه المنظمة بكافة الحصانات والامتيازات التي تتمتع بها المنظمات الدولية، كونها قد أنشأت بقرار صادر عن الجمعية العامة للأمم المتحدة، كما أن الانتربول ليست دولة فوق الدول الأعضاء وليست حكومة دولية جنائية عالمية وإنما هي جهاز دولي "منظمة" تعمل تحت إشراف الأمم المتحدة بما يحقق الأهداف المقررة في ميثاقها، فالمنظمة لا تتدخل في الشؤون الداخلية للدول الأعضاء، ويخطر عليها خطرا مطلقا التدخل في المسائل والشؤون ذات الطابع السياسي أو العسكري أو الديني أو العنصري[2].

## 06- تكوين المنظمة (أجهزتها)

المنظمة الدولية للشرطة الجنائية تتكون من عدد من الأجهزة، شأنها في ذلك شأن أي منظمة دولية أخرى، تعمل من خلالها على تحقيق أهدافها التي نص عليها نظامها الأساسي (الميثاق)، وقد إشارات إلى هذه الأجهزة المادة الخامسة من النظام الأساسي بقولها:" تتكون المنظمة الدولية للشرطة الجنائية – الانتربول من:

- الجمعية العامة
- اللجنة التنفيذية (الهيئة التنفيذية)

[1] عبد المنعم متولي، الوجيز في قانون المنظمات الدولية، دار النهضة العربية، القاهرة، 2008، ص 109.

[2] تنص المادة الثالثة من النظام الأساسي (الميثاق) للانتربول على ما يأتي :" يحظر على المنظمة حظرا تاما أن تساهم أو تتدخل في مسائل أو شؤون ذات طابع سياسي أو عسكري أو ديني أو عنصري".

- الأمانة العامة
- المكاتب المركزية الوطنية
- المستشارون".

فالجمعية العامة هي أعلى سلطة في المنظمة[1]، وتتكون من مندوبي الدول الأعضاء في المنظمة الذين تعينهم دولهم، وكل دولة عضو في المنظمة لها أن توفد مندوباً واحداً أو عدة مندوبين، ولكن يجب عند تعدد المندوبين أن يترأس الوفد شخصاً واحداً فقط، ويضم الوفد عدداً من الفنيين والخبراء في مجالات الشرطة ووظائفها، وعلاقة الدولة بالمنظمة وتقوم الجمعية العامة بالوظائف الآتية:

**1.** القيام بالمهام والأعباء التي ينص عليها النظام الأساسي (الميثاق)

2. تحديد المبادئ العامة ووضع الإجراءات الكفيلة بتحقيق أهداف المنظمة المنصوص عليها في المادة (2) من النظام الأساسي.

3. دراسة برنامج عمل السنة التالية (القادمة)، والذي يقدمه الأمين العام والموافقة عليه.

4. تحديد أحكام كل نظام يعد ضرورياً لعمل المنظمة.

5. انتخاب الأشخاص للوظائف التي نص عليها النظام الأساسي للمنظمة, كرئيس المنظمة ونوابه الثلاث.

6. اعتماد القرارات وتوجيه التوصيات إلى الأعضاء بشأن المسائل باختصاص المنظمة.

7. تحديد ورسم سياسة المنظمة المالية.

8. دراسة الاتفاقيات مع المنظمات الأخرى والدول والموافقة عليها.

وتعقد الجمعية العامة دورة عادية سنوياً[2]، ولها أن تعتمد دورات استثنائية بناء على طلب اللجنة التنفيذية, أو أغلبية الأعضاء[3]، وتختار الجمعية في نهاية كل دورة مكان انعقادها للسنة التالية، وقد

[1] نص المادة (6) من النظام الأساسي للمنظمة (الميثاق).

[2] عقدت الجمعية العامة دورتها السادسة والسبعين (76) في مدينة مراكش المغربية للفترة من 5 – 8 / تشرين الثاني / 2007، الوثيقة الصادرة عن الانتربول بالرقم (2007 / 46 No) بتاريخ (9/11 / 2007).

[3] نص المادة (10) من النظام الأساسي للمنظمة (الميثاق).

تطرأ ظروف تجعل انعقاد دورة الجمعية العامة في المكان المتفق عليه مستحيلا أو غير ملائم فللجمعية أن تختار مكاناً آخر لانعقادها السنة التالية[1].

ويعود حق التصويت في الجمعية العامة لمندوب واحد لكل بلد، بمعنى آخر إن كل بلد عضو يتمتع بصوت واحد فقط داخل الجمعية العامة، وان تعدد مندوبيه ضمن الوفد الواحد[2]، ويتم اتخاذ القرارات في الجمعية العامة بالأغلبية البسيطة، عدا القرارات التي ينص النظام الأساسي (الميثاق) على ضرورة اعتقادها بأغلبية الثلثين، كانتخاب رئيس المنظمة في الاقتراع الأول[3].

أما اللجنة التنفيذية "الهيئة التنفيذية" فتتألف، من رئيس المنظمة الدولية للشرطة الجنائية "الانتربول"، وثلاثة نواب للرئيس، وتسعة مندوبين فيكون مجموع أعضائها ثلاثة عشر عضوا (13) ويجب أن يكون الأعضاء من بلدان مختلفة، فيراعي التوزيع الجغرافي في اختيارهم[4] بحيث تمثل القارات الخمس فيها، ويتم انتخاب الرئيس ونوابه من بين المندوبين من قبل الجمعية العامة للمنظمة وبأغلبية الثلثين عندما يكون الاقتراع لمرحلة واحدة، أما إذا لم يسفر الاقتراع الأول عن أي اختيار فيكتفي في الاقتراع الثاني بالأغلبية البسيطة[5]، ومدة ولاية الرئيس أربع سنوات، إما النواب فمدة ولايتهم ثلاث سنوات، ولا يجوز إعادة انتخاب الرئيس ونوابه للمناصب نفسها مرة ثانية، بمعنى أن ولايتهم تكون لمرة واحدة غير قابلة للتجديد[6].

ويتصرف أعضاء اللجنة التنفيذية عند قيامهم بمهامهم الرسمية باعتبارهم ممثلين للمنظمة لا لبلدانهم، فهم يعدون موظفين دوليين لهذا الغرض، مما يعني تمتعهم بجميع الامتيازات والحصانات الدبلوماسية الدولية المقررة للموظفين الدوليين[7]، ورئيس المنظمة يقوم بالمهام المناطة به والمنصوص عليها في المادة (18) من النظام الأساسي للمنظمة (الميثاق) والتي تتمثل بالاتي:-

1- يرأس دورات الجمعية العامة واللجنة التنفيذية، ويدير مناقشاتها.

---

[1] نص المادة (12) من النظام الأساسي للمنظمة (الميثاق).

[2] نص المادة (13) من النظام الأساسي للمنظمة (الميثاق).

[3] نص المادتين (14 – 16) من النظام الأساسي للمنظمة (الميثاق) وينظر أيضا الموقع الآتي: على شبكة الانترنت http://www.Interpol.int/public/icpo/GeneralAssembly/defaultAr.asp تاريخ الاطلاع: 2018/06/23 على الساعة 17:17.

[4] نص المادة (15) من النظام الأساسي للمنظمة (الميثاق).

[5] نص المادة (16) من النظام الأساسي للمنظمة (الميثاق).

[6] نص المادة (17) من النظام الأساسي للمنظمة (الميثاق).

[7] إبراهيم أحمد خليفة، القانون الدولي الدبلوماسي والقنصلي، دار الجامعة الجديد، الإسكندرية، 2007، ص 185.

2- يتحقق من انسجام أعمال المنظمة مع قرارات الجمعية العامة واللجنة التنفيذية.

3- الاتصال المباشر قدر الإمكان مع الأمين العام للمنظمة.

أما المهام التي تقوم بها اللجنة التنفيذية والتي تجتمع مرة واحدة في السنة على الأقل بدعوة من رئيسها فقد أشارت لها المادة (22) من النظام الأساسي للمنظمة، ويمكن إيجازها بالاتي:-

1- الإشراف على تنفيذ قرارات الجمعية العامة

2- إعداد جدول الأعمال لدورات الجمعية العامة

3- عرض كل ما تعتبره مفيد وذا جدوى من برامج العمل والمشاريع على الجمعية العامة

4- تراقب إدارة الأمين العام

5- ممارسة كافة السلطات والصلاحيات التي توكل إليها من قبل الجمعية العامة.

ولضمان قيام اللجنة التنفيذية بأعمالها بشكل مستمر نص الميثاق في المادة (46/أ) على انه :" عند الانتخاب الأول يختار بالقرعة نائبي الرئيس المنتخبين، ينتهي تفويضه بعد سنة"

ونصت الفقرة (ب) من المادة ذاتها على ما يأتي : "عند الانتخاب الأول يختار بالقرعة عضوان من اللجنة التنفيذية ينتهي تفويضهما بعد سنة، وعضوان آخران منها، ينتهي تفويضهما بعد سنتين"

وفي حالة وفاة احد أعضاء اللجنة التنفيذية أو استقالته، تقوم الجمعية العامة بانتخاب خلفا له، لما تبقى من مدة تفويض العضو المتوفى أو المستقيل[1].

ويبقى أعضاء اللجنة التنفيذية في وظائفهم حتى إنهاء دورة الجمعية العامة التي تنعقد في السنة التي تنتهي فيها مدة تفويضهم.

وعن الأمانة العامة للانتربول فهي تتألف من الأمين العام ومجموعة من الموظفين الفنيين والإداريين، مكلفين للقيام بأعمال المنظمة[2]، كمهام الاتصالات والأرشفة والبصمات والمخابرات والمترجمين ومتخصصون في الكمبيوتر، فالأمين العام، يتم تعيينه من قبل الجمعية العامة، بناء على اقتراح اللجنة التنفيذية، ومدة ولايته خمس سنوات قابلة للتجديد لأكثر من مرة، ويمكن تفويضه ولا يجوز بقاؤه في منصبه إلى بعد سن الخامسة والستين لكن له أن يتم مدة تفويضه إذا بلغ الخامسة

[1] نص المادة (23) من النظام الأساسي للمنظمة (الميثاق).

[2] نص المادة (27) من النظام الأساسي للمنظمة (الميثاق).

والستين أثنائها[1]، ويختار الأمين العام من ذوي الكفاءة العالية والخبرة في مجال شؤون الشرطة، ويجوز للجنة التنفيذية أن تقترح على الجمعية العامة إنهاء تفويض الأمين العام، إذا اقتضت ذلك ظروف استثنائية[2] .

وتعمل الأمانة العامة على مدار 24 ساعة ويتم ذلك بواسطة موظفين يختارهم الأمين العام ويتولى الإشراف عليهم، ويقوم بمهام الإدارة المالية للأمانة، وينظم الأقسام الدائمة ويشرف عليها ويديرها وفقا لتوجهات اللجنة التنفيذية والجمعية العامة، ويقدم إليهما الاقتراحات والمشاريع المتعلقة بأعمال المنظمة، وتكون مسؤوليته المباشرة أمام اللجنة التنفيذية والجمعية العامة، وهو يمثل المنظمة في كل أعماله التي يقوم بها والمتعلقة بالأمانة العامة لا بلده الذي ينتمي إليه، فلا يحق للامين العام أو للموظفين أثناء قيامهم بوظائفهم أن يطلبوا أو يقبلوا تعليمات من أي حكومة أو سلطة من خارج المنظمة، وعليهم أن لا يقوموا بأي عمل يسيء إلى وظيفتهم، ويلتزم كل عضو في المنظمة باحترام الطابع الدولي المحض لمهمة الأمين العام والموظفين، وبعدم التأثير عليهم عند قيامهم بأعمالهم.

ونصت المادة (26) من النظام الأساسي (الميثاق) على مهام الأمانة العامة والتي تتلخص بالاتي:-

1- تطبيق قرارات الجمعية العامة واللجنة التنفيذية.

2- العمل كمركز دولي لمكافحة جرائم القانون الدولي.

3- العمل كمركز فني وإعلامي للمنظمة.

4- القيام بإدارة المنظمة العامة.

5- تامين الاتصال بالسلطات الوطنية والدولية على أن تعالج مسائل التحري والتحقيق الجنائي عن طريق المكاتب المركزية الوطنية.

وتحتفظ الأمانة العامة بنوعين من الملفات المعلوماتية:-

1. ملفات عامة: تتضمن كافة البيانات والمعلومات عن المجرمين والجرائم المختلفة إلي يرتكبونها، وتصل إلى الأمانة عن طريق المكاتب الوطنية، ويتم ترتيبها من قبل قسم الأبحاث والدراسات فيكون لكل مجرم ملف خاص به.

[1] نص الماد (28 / 1) من النظام الأساسي للمنظمة (الميثاق).

[2] نص المادة (28 / 3) من النظام الأساسي للمنظمة (الميثاق).

2. ملفات خاصة: تميز كل مجرم عن غيره فيصبح من السهل التعرف عليه، وتوجد في هذا الملف بصمات أصابعه، صورته أو صوره، ماضيه الجنائي[1].

وتحتاج المنظمة الدولية للشرطة الجنائية (الانتربول)، لبلوغ أهدافها التي نص عليها الميثاق في مادته الثانية إلى تعاون دائم ونشط من الأعضاء الذين يتوجب عليهم بذل كافة الجهود المنسجمة مع قوانين بلدانهم للمشاركة في نشاطات المنظمة، ولتامين هذا التعاون يعين كل بلد هيئة تعمل (كمكتب مركزي وطني)، ويؤمن هذا المكتب الاتصال بمختلف سلطات الدولة (تشريعية، تنفيذية، قضائية) وأجهزتها المختلفة، والهيئات التي تعمل في الدول الأعضاء كمكاتب مركزية وطنية، والأمانة العامة للمنظمة، ويتم هذا الاتصال عبر وسائل تقنية تقليدية وحديثة وسريعة كالتلفون، الفاكس، التلكس الانترنت، الدوائر التلفزيونية المغلقة والمفتوحة، التليفاكس، إضافة إلى منظومة اتصالات حديثة ومتطورة تربط المنظمة بالمكاتب المركزية الوطنية في الدول الأعضاء[2].

وتقوم الدول الأعضاء بتعيين الموظفين الذين يعملون في مكاتبها المركزية الوطنية وفقا لقوانينها الداخلية دون أي تدخل من المنظمة[3].

وإضافة للمكاتب الوطنية المركزية في جميع الدول الأعضاء، توجد مكاتب إقليمية للمنظمة تنسق عمل المكاتب الوطنية وتعمل كحلقة اتصال، وتوجد (ستة) مكاتب إقليمية للمنظمة موزعة على دول العالم المختلفة (السلفادور، تايلاند، زمبابوي، كوتوفوار، ساحل العاج، الأرجنتين، كينيا)، إضافة إلى مكتب الاتصال مع منظمة الأمم المتحدة ومقره في مدينة نيويورك[4]، وتقوم المكاتب المركزية الوطنية بالمهام الآتية[5]:-

1- تحقيق الاتصال بين أجهزة الشرطة بداخل الدولة ونظائرها في الدول الأخرى (العربية والأجنبية).

---

[1] جمال محمد مصطفى، التحقيق والإثبات في القانون الجنائي، مطبعة الزمان، بغداد، 2004، ص 154 ، 157.

[2] مقررات اجتماع مجموعة دمج جهود مكافحة الإرهاب في الشرق الأوسط في 10/ ديسمبر / 2007 منشور على الموقع الأتي على شبكة الانترنت : http://www.moiegypt.gov.eg/Arabic، تاريخ الاطلاع 2018/06/23 على الساعة 18:41 .

[3] تنص (31) من ميثاق المنظمة على ما يأتي:" تحتاج المنظمة لبلوغ أهدافها إلى تعاون دائم ونشط من الأعضاء الذين يتوجب عليهم بذل كافة الجهود المنسجمة مع قوانين بلدانهم للمشاركة في نشاطات المنظمة"، وتنص المادة (32) على ما يأتي : "لتامين هذا التعاون، يعين كل بلد هيئه تعمل فيه كمكتب مركزي وطني....."

[4] عبد الرزاق العري، الإرهاب البيولوجي، مقال منشور على الموقع الأتي على شبكة الانترنت: http://www.omanday.com/20/locat/14.htm، تاريخ الاطلاع 2018/06/23 على الساعة 18:56 .

[5] محمود نجيب حسني، مرجع سابق، ص 193 ، 196

2- تحقيق الاتصال بين أجهزة الشرطة المحلية والأمانة العامة للانتربول في مدينة ليون الفرنسية.

3- استقبال وتوجيه الطلبات التي ترد من مختلف الدول لملاحقة المجرمين الفارين والمطلوب إلقاء القبض عليهم داخل البلاد.

4- متابعة إجراءات محاكمة من يحمل الجنسية الوطنية، ولحين صدور الأحكام وتنفيذها.

5- متابعة قرارات التسليم لمن يحمل الجنسية، واتخاذ الإجراءات التنفيذية حتى يتم التسليم.

وتقوم المكاتب الوطنية بمتابعة مجموعة من القضايا الجنائية، على المستوى الدولي يمكن إيجازها بالاتي:-

1- الأشخاص المطلوبين.

2- الجثث المجهولة الهوية.

3- الغائبين والمفقودين.

4- السيارات المسروقة.

5- الأسلحة المسروقة والمفقودة.

6- الآثار والتحف الفنية المسروقة.

7- جوازات السفر المسروقة والمفقودة.

وللمنظمة الدولية للشرطة الجنائية "الانتربول"، أن تستعين بمستشارين لدراسة المسائل العلمية والفنية، ويكون دورهم استشاري صرف[1]، أي أن رأيهم غير ملزم للمنظمة، ولكن المتعارف عليه أن اللجوء إلى الاستشارة لا يكون إلا للحاجة الماسة والملحة للوقوف على حقيقة أمر ما، أو اتخاذ قرار بشان مسالة معينة، ومن المعلوم أن أصحاب الفن والاختصاص هم الأكثر ميزة ودراية في مجال اختصاصهم، فلهذا يتم اللجوء إلى استشارتهم[2].

ويتم تعيين المستشارين من قبل اللجنة التنفيذية، ولا يكتسب تعيينهم الصفة النهائية إلا بعد المصادقة علية من قبل الجمعية العامة للمنظمة، وفترة تعيينهم تستمر لثلاث سنوات ويتم اختيار المستشارين من بين الأشخاص الذين اكتسبوا شهرة والمعروفين على المستوى الدولي في مجال

[1] نص المادتين (34 -35) من النظام الأساسي للمنظمة (الميثاق).

[2] أحمد فتحي سرور، (الوسيط في قانون الإجراءات الجزائية)، مرجع سابق، ص 494.

اختصاصهم نتيجة قيامهم بأبحاث في إحدى المجالات التي تهم المنظمة ويمكن سحب حقه المستشار بقرار تتخذه الجمعية العامة للمنظمة[1].

## ثانيا: جهود المنظمة الدولية للشرطة الجنائية في مكافحة الإرهاب الالكتروني.

كان للمنظمة الدولية للشرطة الجنائية دور كبير في الكشف عن التنظيمات الإرهابية وتحديد هوية الإرهابيين، وذلك بالتنسيق بين الدول الأعضاء، والإجراءات المتخذة في سبيل القضاء على هذه الجريمة ومنع انتشارها، واعتبرت هذه المنظمة جرائم الإرهاب بكل أنواعها من أخطر الجرائم وخاصة جريمة الإرهاب الالكتروني يجب اتخاذ جميع الوسائل للتصدي لها، حيث كان لها في هذا النطاق إستراتيجية فعالة جسدت من خلال مجال التعاون الشرطي عن طريق مكاتبها المركزية الموجودة في كل دولة من الدول الأعضاء، فعملت على وضع قاعدة للمعلومات والبيانات، وتحليلها عن طريق القيام بدراسات ميدانية من خلال المجهودات التي تقوم بها الأجهزة الساهرة على إنفاذ القانون وتعميمها على الدول الأعضاء للاستفادة منها في مكافحة الإرهاب.

وقد اعتمدت المنظمة سياستين لمكافحة جرائم الإرهاب إحداها قمعية والأخرى وقائية فبالنسبة للسياسة القمعية فقد اتخذت في سبيل ذلك أسلوب الرد الايجابي على الاعتداءات الإرهابية وذلك بالقبض على المتهمين المتورطين في هذه الجرائم، واتخاذ التدابير اللازمة لتسهيل إجراءات تسليمهم وإنشاء مشاريع عملياتية لدراسة وتحليل المعلومات والبيانات المتعلقة بقضايا الإرهاب وتقديم الدعم للأجهزة المختصة بتطبيق القانون، أما بالنسبة للإجراءات الوقائية فان دورها في هذا المجال فلا تختلف عن تلك التدابير التي اعتمدتها الأمم المتحدة في سياستها اتجاه الوقاية من الإرهاب، فقامت بعقد بعض المؤتمرات واللقاءات بهدف التنديد بالعمليات الإجرامية في هذا الإطار، والوصول إلى تحديد معالم إستراتيجية جماعية تجمع بين الدول الأعضاء يتجسد من خلال التعاون الفعال بين جميع الأجهزة الأمنية الفعالة في كل دولة[2] .

[1] نص المادتين (36-37) من النظام الأساسي للمنظمة (الميثاق).

[2] ساعد الهام حورية، مرجع سابق، ص 61.

وبتفاقم ظاهرة الإرهاب وتطورها أخذت طابع الجرائم بالغ الخطورة تغيرت نظرة الانتربول لها وأخرجتها من نطاق القانون العام، كما رفضت اعتبار الجريمة الإرهابية جريمة سياسية[1].

وعملت المنظمة على تأمين التعاون الدولي وتنميته وتوسيع نطاقه بين سلطات الشرطة الجنائية في مختلف الدول الأعضاء، وذلك في حدود القوانين الوضعية ومن خلال إستراتيجية دولية في هذا المجال، واهم مبادئ هذه الإستراتيجية مايلي:

### 01- الاعتماد على نمط تخزين وتحليل المعلومات.

وتعتمد الانتربول على المعلومات الواردة إليها من الدول الأعضاء بواسطة مكاتبها المركزية وتهتم المنظمة بكل معلومة مستخلصة من التحقيقات المستقاة بخصوص الجرائم الإرهابية، حيث تطلب من ممثليها تزويدها بكل المستجدات التي تحدث في هذا الميدان[2]، وبكل المعلومات التي تتعلق بالأشخاص أو المجموعات أو الأدوات التي تم العثور عليها في مسرح الجريمة والأساليب التي يلجأ إليها الإرهابيون لارتكاب جرائمهم، كما تعتمد على المعلومات التي تصل إليها بالنسبة للجرائم المرتبطة بالجرائم الإرهابية بصفة غير مباشرة .

وتشكل المعلومة أهمية كبيرة ولها فائدة جد عظيمة في معرفة تحركات الإرهابيين، مما يسهل عملية الكشف عن التنظيمات وقمعها والوقاية منها، ويجب على المكاتب المركزية عند تقديمها للمعلومات بهذا الخصوص اتخاذ كل الإجراءات الكفيلة بضمان صحة تلك المعلومات، والتمييز بوضوح أثناء الإحالات بين المعلومات الحقيقية وبين الاستنتاجات والخلاصات المستنبطة من الواقع وهذا حتى تستطيع الجهة مستلمة المعلومات من اتخاذ الإجراءات المناسبة، ويمنع على المنظمة أن تنظر في المعلومات المتعلقة بالجرائم السياسية العسكرية، الدينية، والعنصرية[3].

ولكون الجريمة الإرهابية من بين الأهداف الرامية لضرب النظام السياسي القائم وبعث مبادئ إيديولوجية معينة، حاولت المنظمة من خلال دورة لوكسمبورغ سنة 1984 حل الإشكالية المطروحة والتي تثيرها المادة الثالثة سالفة الذكر، وعلى هذا المستوى تم السماح للمكاتب المركزية والأمانة

---

[1] محمد سعد الله، المنظمة الدولية للشرطة الجنائية ودورها في مناهضة الإرهاب الدولي، مذكرة ماجستير في القانون كلية الحقوق، بن عكنون– الجزائر، 2011، ص 78.

[2] حسنين محمد البوادي، مرجع سابق، 175.

[3] تنص المادة الثالثة من النظام الأساسي لمنظمة الشرطة الجنائية الدولية على أنه:" يحظر على المنظمة حظرا باتا أن تنشط أو تتدخل في مسائل أو شؤون ذات طابع سياسي أو عسكري أو ديني أو عنصري"

استغلال المعلومات بغرض الوقاية منها، الأمر الذي سمح للمنظمة باعتماد نمط تحليلي للمعلومات المقدمة في سبيل وضع خطة ردعية ووقائية في جرائم الإرهاب ومنها الإرهاب الالكتروني، إلا أنها في جميع الحالات أوصت باستبعاد النظر والتعاون في الجرائم السياسية والعسكرية، وتلك ذات الطابع الديني أو العنصري كالتعبير عن بعض الآراء المحظورة، أو إهانة السلطات وكذلك الجرائم ضد الأمن الداخلي والفرار من القوات المسلحة والتجسس وممارسة ديانة محظورة أو الانتماء إلى منظمة عنصرية، كما استبعدت التدخل في الجرائم التي يرتكبها السياسيون في نطاق نشاطهم السياسي، وفي هذا الإطار حددت المعيار الواجب اعتماده لتجسيد مبدأ التعاون واتخاذ إجراءات القمع والمنع المتمثل في معيار الأهمية الدولية للفعل المرتكب[1].

في إطار تعميم المعلومات على سلطات إنفاذ القانون عبر أجهزة اتصال فعالة، فتقوم المنظمة باستقبال المعلومة وفق عملية تسلسلية طبقا للبرمجة الموجودة لديها على مستوى الأمانة العامة، تعمل على جمع وتخزين المعلومات الواردة وتتبادلها مع الدول الأعضاء فيما يتعلق بالأفراد والجماعات المشتبه فيهم وعن أنشطتهم وتنسق فيما بينهم، حيث تقوم الجمعية العامة بتعميم هذه المعلومات عبر الدول الأعضاء، وتزويد المنظمات الدولية والإقليمية بها حتى يتسنى للمجموعة الدولية العمل على سياق واحد وهو مكافحة الجريمة الإرهابية وقمعها.

ومن أجل تفعيل دور المعلومات التي يتم تحصيلها وإيصالها بسرعة إلى المكاتب المركزية تم استحداث المكاتب الإقليمية، وبذلك يتم جمع كافة الإحصائيات عن الجرائم الإرهابية المرتكبة في إقليم معين من حيث نوعها وأساليب ارتكابها وأسماء الجناة وجنسياتهم كاستخدام الانترنت في الجريمة الإرهابية، كما تسعى هذه المكاتب إلى تبادل المعلومات في التحقيقات الجنائية بالإضافة إلى المساعدات التي تقدمها إلى المنظمة في التحضير للملتقيات والمؤتمرات الإقليمية والدولية التي تعقد في إحدى الأقاليم، بالإضافة إلى ذلك تقوم بربط العلاقات بين نشاط المنظمة الدولية للشرطة الجنائية ومنظمات دولية أخرى، بغية إعداد برامج لمكافحة جميع أنواع الجرائم ومنها جريمة الإرهاب الالكتروني – محل الدراسة–

التقسيم الإداري للمنظمة تضمن وجود إدارة للمعلومات الجنائية والاتصالات تنقسم إلى عدة فروع ومن بين هذه الفروع يوجد فرع للإرهاب الدولي، ومن اجل تعميم المعلومة أيضا عن طريق المكاتب

[1] ساعد الهام حورية، مرجع سابق، ص 64.

الإقليمية والمركزية اعتمدت المنظمة على أجهزة اتصال فعالة كجهاز "X 400" الذي يعتبر وسيلة فعالة لتبادل المعلومات بين الأمانة العامة والمكاتب المركزية ومنه ربط شبكة المعلومات بهيئة الاتصالات الدولية الموجودة بين دولتين يجري الاتصال بين مكتبيها كما تستخدم المنظمة نظام اتصال آخر يطلق عليه نظام "1-24/7" الذي يمكن الدول الأعضاء من تبادل المعلومات في إطار منظم ومحمي عبر جهاز اتصال فعال ويعتمد هذا النظام على ربط مؤمن مع شبكة الانترنت عن طريق ترقيمات مشفرة متطورة تسمح بنقل عدد كبير من المعلومات السرية، كما يسهل على الدول الأعضاء الدخول إلى شبكة المعلومات الخاصة بالمنظمة، ومن خلال المؤتمر الأفريقي رقم 22 الذي احتضنته الجزائر في مدينة وهران في سبتمبر 2013[1]، وقد أكد هذا المؤتمر أن الجزائر تحتل المرتبة الخامسة في مجال التحكم في قاعدة البيانات التي وضعتها الانتربول، وقد تمت المصادقة في هذا المؤتمر على خطة جديدة في مجال مكافحة الجريمة وعلى توسيع استخدام النظام الموحد للشرطة الجنائية "1-24/7" وهو المخطط المستقبلي الاستراتيجي الذي تم وضعه من قبل الانتربول للفترة مابين 2014 إلى غاية 2016 والذي يتضمن مساعدة رؤساء الشرطة بالمنطقة للكشف عن الأشكال الجديدة للجريمة الإرهابية والتعرف على الجناة ومكافحتهم بفعالية، بالإضافة إلى منح الأولوية لتفكيك الشبكات الإجرامية المنتشرة في أفريقيا وخاصة الإرهابيـــة والتي تستخدم وتستغل الابتكار التكنولـــوجي كما تعطي المنظمة أهمية قصوى لاستخدام قاعدة البيانات التي تعتبره من الأسس الفعالة لبناء خطة شاملة لمكافحة الإرهاب والجرائم المرتبطة به، وقد جاء في المؤتمر رغبة الدول المشاركة في حتمية استخدام التكنولوجية الرقمية في إطار مكافحة الجريمة الإرهابية حتى تناسب وتكافئ تطورها[2] فتسهل هذه الوسيلة عملية الاتصال مع انخفاض قيمة المكالمات[3] .

## 02- الرد الايجابي الفوري للانتربول على الأفعال الإرهابية.

تعمل الانتربول وفق إستراتيجية قمعية للرد على الجرائم الإرهابية، من خلال تسليم المجرمين والقبض عليهم وتحديد هويتهم خاصة بعد تطور هذه الظاهرة لتصبح الكترونية، وقد أكدت على هذا الدور رئيسة المنظمة " ميراي باليسترازي" من خلال الكلمة التي ألقتها في الدورة 82 للمنظمة في الفترة

[1] ساعد الهام حورية، مرجع سابق، ص 66.

[2] تفاصيل المؤتمر منشورة في الموقع:anna:leb.gov.lb/ar/show-news/124673 تاريخ الزيارة 2018/06/24 على الساعة 19:10.

[3] ساعد الهام حورية، مرجع سابق، ص 66 .

بين 21 إلى 24 عام 2013 بكولومبيا بقولها:" على الدول الأعضاء اتخاذ القرارات السديدة لجعل العالم أكثر أمنا، وتمكين المنظمة من مواصلة العمل من اجل تحقيق هذا الهدف، وفي مجال مكافحة الإرهاب أو الاتجار بالمخدرات أو الجريمة الالكترونية أو حماية الحدود سوف يواصل الانتربول عمله الفعال وسيقوم باستحداث استراتيجيات وأدوات وخدمات مبتكرة، وسيضعها حيز التنفيذ بشكل متزامن مع الجهود التي تبذلها بلدانه الأعضاء في هذا الصدد، كما أن الانتربول قد أبصرت النور منذ مائة سنة تقريبا، وأصبحت المنظمة لاعبا أساسيا في مكافحة الجريمة المنظمة والإرهاب، وبالرغم من التطورات التي عرفتها الانتربول مكنتها من إحراز تقدم استثنائي في أكثر من مجال، إلا أنه لابد لمنظمتنا من الحفاظ على قدرتها على الابتكار ليظل بإمكانها الاستجابة لتوقعات بلدانها 190 عضو"[1].

يكمن الدور الأساسي للانتربول في إطار إجراءات ضبط وملاحقة المشتبه فيهم والإرهابيين الهاربين وتسليمهم في التعرف على الإرهابيين وعلى أساليب العمل الإجرامي من خلال جمع المعلومات وتبادلها مع الدول الأعضاء وملاحقتهم والقبض عليهم لتسليمهم وتبدأ إجراءات الملاحقة والضبط بطلب يقدم إلى الأمانة العامة للمنظمة بواسطة المكتب المركزي للدولة طالبة التسليم، ويحتوي على جميع المعلومات اللازمة المتعلقة بالإرهابي الهارب وكل ما يتعلق بالقضية أو الجريمة المتهم بها، ثم تقوم المنظمة ببحث الطلب للنظر فيه وليتحقق من نوع الجريمة، وإذا ثبت أنها جريمة إرهابية فتصدر المنظمة نشرة دولية إلى كافة المكاتب المركزية الوطنية الموجودة في الدول الأعضاء في المنظمة، وفي حالة القبض على الإرهابي في أي من الدول يبلغ المكتب المركزي للدولة طالبة التسليم، فتقوم هذه الأخيرة بإتباع الطرق الدبلوماسية لاستلام الإرهابي المطلوب، كما يحتوي الانتربول على قاعدة بيانات والمعلومات المتعلقة بالإرهابيين الدوليين وأوصافهم ويقوم بنشر جميع المعلومات التي تم تحصيلها عبر نشراته الخاصة لتسهيل عملية الكشف عنهم والقبض عليهم[2].

كما قامت الانتربول بإنشاء مشاريع عملياتية لمكافحة الإرهاب ومنه الإرهاب الالكتروني بمشاركة الدول الأعضاء، ومن هذه المشاريع على سبيل المثال:

[1] تغطية لأشغال الدورة 82 للجمعية العامة للانتربول بقرطاجنة –كولومبيا، مجلة الشرطة، العدد 121، نوفمبر 2013 ص 13.

[2] ساعد الهام حورية، مرجع سابق، ص 68.

1. مشروع "PASSAGE" الهدف منه السعي إلى وضع حد لتمويل المنظمات الإرهابية والكشف عن العلاقات التي تربط بينهم وبين المنظمات الإجرامية العالمية في مجال تزوير وثائق السفر، والعبور الدولي غير الشرعي متخذا بذلك صفة المهاجر أو اللاجئ أو مقيم[1].
2. مشروع "TARGET" الخاص بجمع المعلومات الصادرة من الدول الأعضاء بهدف وضع قائمة كل سنة خاصة بالأشخاص الموقوفين جراء الأعمال الإرهابية ودراستها وتحليلها بشكل معمق ثم توزيعها بعد ذلك على الدول الأعضاء.

بالإضافة إلى مشاريع أخرى مثل مشروع "BAOBAB" الخاص بأفريقيا، ومشروع "PACIFIC" الذي اهتم بدراسة وتحليل والتعرف وتعداد التنظيمات الإرهابية التي تنشط في جنوب شرق آسيا، وكذلك مشرع الخاص بأوروبا والمعروف باسم "NIXOS " والذي كشف عن هوية بعض المتورطين في قضايا الإرهاب[2].

وأبرز دور قامت به المنظمة في هذا الإطار الذي يخص الإرهاب الالكتروني تنديدها بالهجمات الإرهابية التي تعرضت لها الولايات المتحـــدة الأمريكيـــــة في 2001/09/11 ورفضها بشدة لهذه الهجمات، واثر انعقاد موسكو في الفترة بين 10 إلى 2002/04/12 قامت بوضع مبادرة جديدة تمثلت في " قائمة لرصد الإرهاب"، يمكن للدول الأعضاء الوصول إليها والاطلاع عليها، ومازالت جهود المنظمة مستمرة في هذا المجال[3] .

بتطور الجريمة الإرهابية حتى وصلت إلى جريمة الإرهاب الالكتروني الحالية كان لا بد من تطور جهود المنظمة الدولية للشرطة الجنائية، فواصلت التخطيط للمسائل الطارئة في القضايا الإرهابية بكل عقلانية، والاعتماد على مبدأ التنسيق والتعاون بين جميع الأجهزة والسلطات المناهضة للإرهاب التي أصبحت تتمتع بالاحترافية، استحدثت المنظمة وسيلة جديدة تمثلت في نشرية خاصة، وذلك انعقاد الدورة 74 للجمعية العامة في الفترة مابين 19 إلى 22 سبتمبر 2005 بألمانيا، بحضور 600 مشارك يمثلون 155 دولة، بناء على طلب الأمم المتحدة بغية اطلاع أجهزة الشرطة في البلدان الأعضاء بكل

[1] بالإضافة إلى مشاريع أخرى خاصة بالإرهاب النووي، كمشروع "GEIGER"، ومشروع "FAIL SAFE"، ومشروع "CRITP"، وللتفصيل أكثر راجع: عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة – دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2013، ص 187.

[2] نفس المرجع، ص 187.

[3] ساعد الهام حورية، مرجع سابق، ص 70.

ما يتعلق بالإرهاب وتهريب الأسلحة، ففي هذا الاجتماع تم التأكيد على أهمية التنسيق والتعاون بين جميع أجهزة إنفاذ القانون كالجمارك وحراس الحدود ....، وبالتالي ضرورة اطلاعهم على قاعدة بيانات الانتربول والوصول إليها من اجل مكافحة جريمة الإرهاب، والكشف عن وثائق السفر المزورة التي يستعين عليها الإرهابيون في تحركاتهم[1].

وفي مجال الوقاية من الإرهاب الالكتروني ومنع الإرهابيين من استغلال الانترنت كأداة للتجنيد عقدت الانتربول مؤتمر دولي في مدينة "ليون" الفرنسية سنة 2007، حضر هذا المؤتمر 79 دولة ومختصون في مكافحة الإرهاب، ومن خلال هذا المؤتمر أعلنت المنظمة الدولية للشرطة الجنائية قيام الدول الأعضاء بدراسة الوسائل المعتمدة من قبل التنظيمات الإرهابية في مجال التجنيد، وذلك من أجل التحكم في الوضع ومنع تفاقمه، حيث انه في الوقت الحاضر تستعمل التنظيمات الإرهابية شبكة الانترنت للتجنيد واختراق المواقع والهجمات الالكترونية ونشر الأفكار المتطرفة التي تصل إلى جميع الفئات مهما كانت أعمارهم وتأصيلهم التاريخي في وقت قصير.

كما درس هذا المؤتمر طبيعة الفعل الإرهابي وتطوره، واستمرار التهديدات الإرهابية ولكل هذه الأسباب وجب تكثيف الجهود بين الدول الأعضاء في المنظمة من أجل مواجهة جريمة الإرهاب وخاصة الالكتروني، وخلص هذا المؤتمر إلى جملة من التوصيات القيمة لعل أهمها وضع آليات مراقبة على الوسائل التي تستعمل من قبل الإرهابيين كشبكات الانترنت وخطورتها وخاصة في مجال التجنيد، ووضع نبذة خاصة عن الأفراد المرتبطين بالتنظيمات الإرهابية، بالإضافة إلى ضرورة اتخاذ كافة الإجراءات اللازمة لمحاربة استغلال التنظيمات الإرهابية للانترنت في تنفيذ أعمالها[2].

كما اعتمدت المنظمة آليات خاصة بتوثيق المراقبة عبر الحدود في العديد من المؤتمرات الإقليمية وأهمها والذي يدخل في إطار دراستنا المؤتمر العشرون للأمريكيتين المنعقد في أفريل 2009 والذي دعت من خلاله إلى اعتماد أو استخدام تكنولوجيا المعلومات لتشمل موظفي الحدود من أجل التحقق الفوري من جوازات السفر بالاستناد إلى قاعدة بيانات الانتربول المتعلقة بجوازات السفر المسروقة والمفقودة، والتي كثيرا ما يستخدمها الإرهابيون.

---

[1] نفس المرجع، ص 70،71.

[2] بيان الأمين العام للجمعية العامة لمنظمة الانتربول سنة 2007 منشور في الموقع https://www.interpol.int/content/download/.../iaw2007AR تاريخ الاطلاع 2018/06/24 على الساعة 17:36.

وفي الأخير وعموما ففي إطار مكافحة الإرهاب الالكتروني تقوم المنظمة الدولية للشرطة الجنائية بتوفير وسائل الاتصال السريعة والفعالة والكفيلة بتأدية المهام المنوطة بها، والمتمثلة في ربط العلاقات بين الدول الأعضاء وتمرير المعلومات خاصة بين المكاتب المركزية الوطنية للدول الأعضاء، والدور الذي تلعبه في نجال تبادل المعلومات حول الأنشطة الإرهابية، وفي سبيل تحقيق إستراتيجية وقائية من جريمة الإرهاب هذه اعتمدت أسلوب النشرات الخاصة وكذلك توطيد العلاقات مع المنظمات الدولية الحكومية وغير الحكومية

فبالنسبة لإصدار النشرات الدولية لتعميم الدراسات ونشر المعلومات حول الجريمة الإرهابية حيث تبادر الانتربول بإصدار نشرات دولية بغرض الوقاية من الإرهاب ومنه الإرهاب الالكتروني، تقوم من خلالها بنشر المعلومات التي تساعد على فهم الظاهرة وتجنب أخطارها، كما تساعد هذه النشرات على القيام بدراسات في ميدان الجريمة وواقع الإرهاب وتعميمها على الدول الأعضاء، وتصدر هذه النشرات عن الأمانة العامة وتكون بمثابة أداة اتصال بينها وبين المكاتب المركزية الوطنية، وتتنوع حسب الهدف المرجو منها[1]:

1. النشرات الدولية الحمراء تصدر في الجرائم الخطيرة كالجنايات والجنح ذات عقوبة مشددة، وتعتبر أقوى أدوات الملاحقة الدولية التي تلحق بالأشخاص الخطرين في حالة صدور حكم قضائي ضدهم والمطلوب القبض عليهم لصالح الدول الأعضاء في المنظمة، أو في حالة اتهام شخص مطلوب القبض عليه في جناية او جنحة خطيرة، وتصدر هذه النشرة بكل لغات العمل الرسمية الأربعة: الانجليزية– العربية– الفرنسية– الاسبانية.
2. النشرات الدولية الخضراء فتصدر في حالة يكون فيها الشخص مطلوب القبض عليه لكن يكون أقل خطورة من المجرم أو المتهم المطلوب، والمنصوص عليه في النشرة الحمراء والنشرات الدولية مهما كان لونها تحمل نفس بياناتها
3. النشرات الدولية الزرقاء فتتعلق بالأشخاص المطلوبين للملاحقة، إما لصدور أحكام بالإدانة ضدهم أو أمر القبض من طرف السلطات القضائية، لكن لا يطلب من الدولة الموجود فوق أراضيها الشخص المطلوب القبض عليه وتسليمه لكن الإبلاغ بوجوده فوق أراضيها.

[1] ساعد الهام حورية، مرجع سابق، ص 73.

4. النشرة الدولية الصفراء وتصدر في حالة وجود إخطار من المكاتب المركزية في حالة غياب أحد الأشخاص من مواطنيها أو أجنبي، حيث تتضمن مجموعة من البيانات تتعلق باسم الشخص وعلامته المميزة إن وجدت، ورقم جواز السفر وصورته الفوتوغرافية وبصمات أصبعه، واللغات التي يحسنها هذا الشخص والدول التي يحتمل أن يذهب إليها، والدول التي سبق له زيارتها مع ذكر تاريخ آخر مرة شوهد فيها الشخص والملابس التي كان يرتديها يوم غيابه مع رقم المحضر والتاريخ المحرر فيه بالإضافة إلى الإجراء الواجب اتخاذه في حالة العثور عليه أو العثور على جثته والأشخاص الذين يمكن الاتصال بهم في حالة وجوده، فتقوم الأمانة العامة بإخطار المكاتب المركزية الوطنية .

5. النشرات الدولية السوداء تصدر في حالة وجود جثث مجهولة بعد تلقيها إخطار من المكاتب المركزية، وتشمل هذه النشرات البيانات الضرورية حول الطبيعة البدنية للجثث وتاريخ وجودها، مع اخذ صورة للبصمات، وتمكن هذه النشرات التي تصدرها الأمانة العامة لمنظمة الشرطة الجنائية الدولية الدول الأعضاء من اتخاذ الإجراءات اللازمة لمنع الاعتداءات الإرهابية ومنها الالكترونية[1] .

وتقوم الانتربول في مجال تجسيد سياسة التعاون والوقاية من الجريمة الإرهابية بمختلف أشكالها بتوطيد العلاقات مع الكثير من المنظمات الدولية والإقليمية، فحسب ما نص عليه الميثاق فللمنظمة أن تقيم علاقات تعـــــاون مع غيرها من المنظمات الدولية سواء كانت حكومية أو غير حكومية كلما وجدت ذلك مناسبا ومتوافقا والأهداف التي ينص عليها القانون الأساسي، ولا تلتزم المنظمة بأي وثيقة تنص على إقامة علاقات دائمة مع منظمات دولية حكومية أو غير حكومية إلا بعد موافقة الجمعية العامة[2] .

وبموجب ذلك قامت المنظمة بعقد اتفاق تعاون مع منظمة الأمم المتحدة والهيئات التابعة لها كمركز حقوق الإنسان ومجموعة الوقاية من الجريمة والعدالة الاجتماعية، وتعمل على ربط أواصل التعاون في مجال محاربة الجرائم المرتبطة بالإرهاب كالاتجار بالمخدرات وبالبشر وجميع عمليات التهريب التي قد تخصص لتمويل الإرهاب، حيث يسعى المكتب المختص بمكافحة المخدرات والتابع

[1] ساعد الهام حورية، مرجع سابق، ص 74.

[2] المادة 41 من ميثاق المنظمة الدولية للشرطة الجنائية.

للأمانة العامة بالعمل مباشرة على تجسيد برنامج الأمم المتحدة في هذا المجال، ويساهم بفعالية في انجاز برامج التكوين والتعاون.

دائما في إطار جهود الانتربول في مكافحة جريمة الإرهاب الالكتروني، فان المنظمة تقوم ببعض العمليات الشرطية والأمنية المشتركة، فتعاقب مجرمي المعلوماتية عامة وخاصة جريمة الإرهاب الالكتروني، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة[1].

## المبحث الثاني: للتعاون القضائي الدولي لمكافحة الإرهاب الالكتروني.

دعت الأمم المتحدة جميع الدول إلى ضرورة وضع آليات قانونية وذلك في العديد من اللقاءات والمؤتمرات التي عقدتها من أجل دراسة ظاهرة الإرهاب ومكافحتها، بحيث تكون هذه الآليات القانونية مكب تشريعي تلجا له الدول إلى حل المشاكل والعراقيل التي تعترض مسالة التعاون القضائي والأمني فيما بينها في هذا المجال، وتقوم بتعديل تشريعاتها الداخلية طبقا لأحكام هذه الاتفاقيات، وخاصة أن معظم الدول كانت تفتقر إلى الآليات التشريعية في مجال مكافحة الإرهاب وخاصة الإرهاب الالكتروني، ومن المعلوم أن هناك عدة اتفاقيات أبرمت بشان مكافحة جرائم الإرهاب بمختلف أشكالها وصورها منها: اتفاقيات منع الاعتداءات الإرهابية ضد الأفراد، حيث تم إبرام ثلاثة اتفاقيات في هذا المجال بنيويورك كانت الأولى سنة 1973 لمكافحة الاعتداءات ضد البعثات الدبلوماسية، والثانية سنة 1979 والتي خصت تجريم أخــذ الرهائن، وأما الثالثة فكانت سنة 1998 تعلقت بمنع استخدام القنابل

من طرف الإرهابيين ضد الأفراد، وأيضا الاتفاقيات الدولية لمكافحة الاعتداءات الموجهة ضد الطيران المدني، والتي تمثلت في اتفاقية طوكيو لمحاربة جرائم الخطف الجوي لعام 1963 ، وأيضا اتفاقية لاهاي لمحاربة الاستيلاء غير المشروع على الطائرات لسنة 1970، وآخرها في هذا المجال اتفاقية مونتريــال لسنة 1971 ، وبالإضافة للاتفاقية المبرمة لمنع تمويل الإرهاب لعام 1999[2].

ومن أهم الاتفاقيات الدولية التي أبرمت من أجل مكافحة الإرهاب الالكتروني هي اتفاقية بودابست التي أبرمت في 11/23/ 2001 ، وهذا لأن الإرهاب الالكتروني يعتبر صورة من صور الجريمة المعلوماتية، بل إنه يعتبر الصورة الأكثر خطورة، والتي سوف نتعرض إليها بشيء من التفصيل في العناصر القادمة.

[1] يوسف حسن يوسف، مرجع سابق، ص 149 .

[2] ساعد الهام حورية، مرجع سابق، ص (30،48).

والحقيقة أن هذه الاتفاقيات السابقة لم تذكر على سبيل الحصر بل على سبيل المثال وهذا راجع للاهتمام الدولي الكبير وتخوفه من هذه الظاهرة الخطيرة والتي تطورت يوما بعد يوم حتى وصلت الى الصورة المستحدثة والمتمثلة في الإرهاب الالكتروني.

وجميع الاتفاقيات التي أبرمت في هذا الشأن كرست مبدأ التعاون القضائي والأمني بين الدول نظرا لأهمية هذا التعاون في مكافحة الإجرام العابر للحدود بما في ذلك جرائم الإرهاب ونخص منها جريمة الإرهاب الالكتروني.

ومن أجل ذلك سوف نتعرض إلى الآليات التقليدية للتعاون الدولي في مكافحة الإرهاب الالكتروني وبعدها سوف نتعرض إلى الوسائل المستحدثة للتعاون وأهم الصعوبات التي تعترض التعاون الدولي من خلال عنصرين .

## المطلب الأول: الآليات التقليدية للتعاون الدولي مكافحة الإرهاب الالكتروني.

يقصد بالآليات التقليدية في التعاون الدولي في مكافحة أي جريمة كل ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة، وتستجمع الأدلة بمختلف الطرق وهو ما يستغرق وقتاً، ويتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى، ومع التزايد المستمر في نسبة الجريمة واستغلال المنظمات الإجرامية للمناخ الدولي المتسم بالمرونة لتوسيع مجال عملياتها الإجرامية عبر الحدود وذلك إما بطريق مباشر من خلال مد نشاطها الدولي، أو بطريق غير مباشر عن طريق انتشار شبكات دولية للمنظمات الإجرامية تتعاون فيما بينها، فكان من الضروري التفكير في تقييم أداء أجهزة العدالة الجنائية الدولية، وخلق أجهزة نوعية متخصصة ، ورفع كفاءة الأجهزة المختصة بملاحقة الجريمة[1].

جريمة الإرهاب الالكتروني يمكن ارتكابها من أقصى بقاع الأرض بنفس السهولة التي يمكن ارتكابها من اقرب نقطة لمكان التنفيذ وهذا لأنها جريمة الكترونية، كما أن رسالة واحدة تعزز ارتكاب جريمة الكترونية يمكن تمريرها من خلال الكثيرين من مقدمي الخدمات في بلدان مختلفة لها نظم قانونية مختلفة، كما أن الآثار الرقمية التي يمكن تتبعها تكون سريعة الزوال وضعيفة الحجية، ومن

[1] أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، مداخلة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية والقانون، ص 1، متوافرة في الموقع: www.iefpedia.com تاريخ الاطلاع 2018/05/03 على الساعة:23:50.

أجل ذلك وجب اتخاذ إجراءات سريعة، كان يقوم الإرهابيون بشن هجمة الكترونية على بنية حساسة في دولة ما فهنا وجب على الدول اتخاذ إجراءات سريعة بغية منع الجريمة، الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم وطبيعتها، وتطوير الوسائل التقليدية بما يكفل تضامن جهود الدول، وأجهزتها القائمة بمهمة مكافحة الجرائم الإرهابية وخاصة جريمة الإرهاب الالكتروني باعتبارها الصورة المستحدثة والمتطورة لجريمة الإرهاب التقليدية بحيث جمعت بين الجريمة الإرهابية في أهدافها وأغراضها والجريمة المعلوماتية في أسلوب ارتكابها ووسائلها.

وبما أن المكافحة المثلى لجريمة الإرهاب الالكتروني قد تتجاوز الوسائل التقليدية إلى وسائل أكثر جرأة تدعم التعاون الرسمي المتخصص، سواء أكان ثنائيا أم متعدد الأطراف بحيث يسمو على الخلافات السياسية والهيكلية التي تواجهها الحكومات، حيث لا يزال مبدأ السيادة من المبادئ الجوهرية التي تحد من فعالية التعاون الدولي، ويعيق الأسس العلمية للتعاون الدولي اللازم والملائم لمكافحة جريمة الإرهاب الالكتروني[1].

ومن أجل توضيح فكرة التعاون الدولي لمواجهة جريمة الإرهاب الالكتروني، وجب الحديث على التعاون الدولي في مكافحة الجرائم المعلوماتية على اعتبار أن جريمة الإرهاب الالكتروني نوع من أنواع الجرائم المعلوماتية، وتتمثل أهم مظاهر التعاون الدولي هذه في تسليم المجرمين التي سوف نتناولها في عنصر أول، والمساعدة القضائية التي سوف نتناولها في عنصر ثاني.

## الفرع الأول: تسليم المجرمين.

استقر فقه القانون الدولي على عد تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين، وحماية المجتمعات من المخلين بأمنها واستقرارها وحتى لا يفلت هؤلاء الجناة من العقاب، ويعتبر هذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في المجالات كافة ومنها مجال الاتصالات وتقنية المعلومات حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، وإذا شرع المجرم منهم في التحضير لارتكاب جريمته في بلد معين وينفذها في بلد آخر ويفر

[1] نفس المرجع، ص 2.

إلى بلد ثالث هروبا من العقاب، فهنا الجريمة أصبح لها طابع دولي والمجرم أصبح مجرما دوليا وهذا الأمر ينطبق على الجرائم المتعلقة بالانترنت[1] بما فيها جريمة الإرهاب الالكتروني– محل الدراسة–.

وحيث أن أجهزة إنفاذ القانون لا تستطيع تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، كان لا بد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، ولكي تتحقق العدالة ويتم الوصول إلى تعاون دولي ناجح كان واجب على جميع الدول أن تنظم هذا التعاون الدولي في المجال التشريعي والقضائي والتنفيذي، ونظام تسليم المجرمين في يقوم على أساس أن الدولة التي يتواجد على إقليمها مرتكب أحد الجرائم العابرة للحدود كجريمة الإرهاب الالكتروني عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا تعين عليها تسليمه لمحاكمته بمعرفة دولة أخرى مختصة[2].

ففي السابق ولمدة طويلة لم تظهر أي أحكام أو معاهدات دولية بشان تسليم المجرمين أو بشأن الإجراءات الواجب إتباعها لتسليم فار من العدالة إلى دولة طالبة لمحاكمته أو تنفيذ حكم صادر عليه وكان تسليم المجرمين إلى حد كبير يعد من المسائل التي يحكمها مبدأ المعاملة بالمثل، أو حسن المعاملة بين الدول وكان الرأي السائد عموما هو انه في ظل غياب معاهدة دولية ملزمة فإنه لا وجود لالتزام دولي لتسليم المجرمين، ومع ذلك كان هناك اتجاه ينادي بضرورة الاعتراف بوجوب تسليم المجرم أو محاكمته لاسيما في جرائم دولية معينة، وفي حقبة ما بعد الحرب العالمية الثانية كانت الزيادة في عدد المعاهدات والاتفاقيات وخاصة الثنائية منها لتنظيم إجراءات تسليم المجرمين لاسيما عند دول القانون العام إذ استخدمت على نطاق واسع .

فما المقصود بالتسليم؟، وما هي إجراءاته؟

## أولا: مفهوم تسليم المجرمين.

يرجع اصطلاح تسليم المجرمين إلى أصل لاتيني حيث يعبر عن إعادة الشخص المطلوب تسليمه إلى الدولة ذات السيادة والمختصة بمحاكمته، وكان يطلق عليه باللاتينية"Extrodcre" واستخدم مصطلح "تسليم" لأول مرة رسميا في المرسوم الفرنسي الصادر سنة 1791 ، وبعدها استخدم

[1] عمار تيسير بجبوج، مرجع سابق، ص 297 .

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 264.

في اتفاقية كانت فرنسا طرفا فيها في سنة 1828 حيث كان قبل ذلك يستخدم مصطلح "إعادة" أو "رد"، وبعد ذلك استقر استخدام اصطلاح تسليم في مجال العلاقات الدولية عند إجراء تسليم المجرمين[1]

تسليم المجرمين هو إجراء من إجراءات التعاون القضائي الدولي، ويعني قيام إحدى الدول – والتي مطلوب منها التسليم– بتسليم شخص موجود في إقليمها إلى دولة أخرى –أي الدولة طالبة التسليم– بناءا على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها، وبمعنى آخر وبشكل مبسط هو تسليم دولة لدولة أخرى شخص منسوب إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه[2] .

لم تختلف التعريفات المختلفة حول المقصود بالتسليم إلا فالصياغة، أما المضمون فيصب في واد واحد، فقد عرف التسليم بأنه:" أن تتخلى دولة عن شخص موجود في إقليمها إلى دولة أخرى بناءا على طلبها لمحاكمته عن جريمة يعاقب عليها قانونها أو لتنفذ عليه حكم صادر ضده من محاكمها"[3]

كما عرف التسليم بأنه " عمل تقوم بمقتضاه الدولة التي لجأ أرضها شخص متهم أو محكوم عليه في جريمة بتسليمه إلى الدولة المختصة بمحاكمته أو تنفيذ العقوبة عليه"[4].

يتضح من التعريفات السابقة أن نظام التسليم يقوم من جهة على وجود علاقة بين دولتين الأولى تطالب بأن يسلم إليها مرتكب الجريمة لتتخذ بحقه الإجراءات اللازمة لإيقاع العقوبة المناسبة له والثانية يوجه إليها طلب التسليم لتقرر بعد ذلك إما الاستجابة له إذا كان متوافقا مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق يربط بينها وبين الدولة الطالبة، أو الرفض لعدم وجود ذلك التشريع أو تلك الاتفاقية.

ومن جهة أخرى نجده يشمل طائفتين من الأشخاص، طائفة الأشخاص المتهمين الذين تنسب إليهم ارتكاب الجريمة موضوع التسليم إلا أنه لم يصدر في حقهم أحكام بعد، والفرض هنا أن إرهابيا

[1] يوسف حسن يوسف، مرجع سابق، ص 154 ،155

[2] نفس المرجع، ص 156.

[3] محمد الفاضل، محاضرات في تسليم المجرمين، معهد الدراسات العربية العليا، منشورات جامعة حلب، سوريا 1966، ص 22.

[4] جندي عبد المالك، الموسوعة الجنائية، الجزء الثاني، الطبعة الأولى، مكتبة العلم للجميع، بيروت، 2004، ص 590

اقترف جريمة إرهاب الكترونية كان يدمر موقع حساس في الدولة مما يعطل النشاط وينشر الفزع والرعب في نفوس المواطنين، وقبل أن يلقى عليه القبض يفر إلى دولة أخرى، عندها تطلب الدولة المرتكب على إقليمها الجريمة الإرهابية من الدولة التي فر إليها الإرهابي أن تسلمه لها لمحاكمته عما ارتكب من جرم، وأما الطائفة الثانية فهي طائفة الأشخاص المحكوم عليهم والذين صدر في حقهم حكم بالإدانة إلا انه لم ينفذ بعد نتيجة لفرارهم إلى دولة أخرى، والفرض هنا أن هذا الإرهابي الفار قد لوحق جزائيا من قبل قضاء الدولة التي ارتكب فيها الفعل الإجرامي، وصدر بحقه حكما قضائيا إلا أنه وقبل البدء في التنفيذ يفر هاربا إلى دولة أخرى، فتطلب الدولة التي ارتكبت فيها الجريمة استلامه من الدولة التي فر إليها[1] .

يختلف التسليم عن غيره من المفاهيم التي قد تشبهه، فهو لا يعد من قبيل الإبعاد الذي يعد عملا إداريا تستقل باتخاذه الجهة الإدارية في حالات لا يمكن حصرها، كما لا يعتبر من قبيل الطرد الذي تمارسه الدولة بما لها من سيادة على إقليمها متى ما رأت أن بقاء الشخص على إقليمها من شأنه أن يؤثر على وجودها أو أمنها[2].

يتطلب التسليم عنصر الدولية في الفعل، ويخضع لأحكام الاتفاقيات الدولية الثنائية أو المتعددة الأطراف وقد تنص عليه التشريعات الداخلية لبعض الدول،كالتشريع الجزائري بحيث تضمن قانون الإجراءات الجزائية إجراءات وشروط يجب إتبـــاعها في ذلك، فقد أجاز القانون الجزائـــري تسليـــم

الأشخاص الأجانب إلى حكومة أجنبية بناء على طلبها إذا وجدوا في الأراضي الجزائرية واتخذت في حقهم إجراءات متابعة من طرف الدولة الطالبة أو صدرت ضدهم أحكام قضائية من هذه الدول ويشترط لتسليم المجرمين إذا كانت الجريمة محل الطلب و المتابعة قد ارتكبت حسب الحالات التالية :

1. إما في أراضي الدولة الطالبة من أحد رعاياها.
2. وإما خارج أراضيها و من أحد رعايا هذه الدولة.

[1] يوسف حسن يوسف، مرجع سابق، ص 156،157 .

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 265.

3. وإما خارج أراضيها من أحد الأجانب عن هذه الدولة إذا كانت الجريمة من عداد الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر حتى و لو ارتكبت من طرف أجنبي في الخارج

ونص المشرع الجزائر على التسليم لا يعني عدم الالتزام بالاتفاقيات الدولية، فقد تضمن الدستور الجزائري في المادة 132[1] مبدأ سمو الاتفاقيات على القانون الداخلي للدولة، وقد أبرمت الجزائر العديد من اتفاقيات التسليم مع المغرب وتونس وغيرها...ومجمل هذه الاتفاقيات تتبع النموذج الذي جاءت به اتفاقية تسليم المجرمين على مستوى الجمعية العامة للأمم المتحدة بقرار رقم 45-116[2] .

## أولا: مصادر نظام التسليم.

إن مصادر هذا النظام ليست واحدة في كافة التشريعات وإنما تختلف باختلاف الظروف التشريعية لكل دولة، إلا أنه وبشكل عام يمكن ردها إلى ثلاثة مصادر هي:

1. **المعاهدات والاتفاقيات بين الدول:** وتنقسم إلى ثلاثة أنواع، اتفاقيات التسليم الثنائية التي تتم بين دولتين وفقا للشروط والضوابط الموضوعة منهما[3]، واتفاقيات التسليم المتعددة الأطراف، وهي اتفاقيات يكون أطرافها أكثر من دولتين ،أما الاتفاقيات الدولية تتضمن أحكاما متصلة بتسليم المجرمين من دون أن تكون بحد ذاتها اتفاقيات تسليم.
2. القوانين الداخلية التي تنظم تسليم المجرمين.
3. العرف الدولي الذي يطبق في حالة انعدام اتفاقيات أو قوانين داخلية[4].

ويتم التسليم بأحد الأنظمة التالية:

[1] الدستور الجزائري لسنة 1996.

[2] ساعد الهام حورية، مرجع سابق، ص 49 .

[3] وضعت الأمم المتحدة سنة 1990 معاهدة نموذجية لتسليم المجرمين لتكون إطارا يساعد الدول التي بصدد التفاوض على اتفاقيات التسليم الثنائية ، وتتكون من 18 مادة بالإضافة إلى ملحق صدر لها سنة 1997 يتضمن بعض الأحكام التكميلية، كما أن مجلس وزراء الداخلية العرب أقر قانونا نموذجيا لتسليم المجرمين.

[4] يوسف حسن يوسف، مرجع سابق، ص 158.

**01- التسليم القضائي:** يقوم هذا النظام على أساس احترام حقوق الأفراد وصيانة حرياتهم لذا تعد السلطة القضائية هي الجهة الوحيدة المختصة بإصدار قرار التسليم، ولا شأن لجهة الإدارة بهذا الخصوص، والدولة التي تنتهج هذا النظام في التسليم وجب أن تسلك أحد النهجين، الأول أن تكون المحكمة هي الجهة الوحيدة المختصة بإصدار قرار التسليم للدولة طالبة التسليم ولا دخل للنيابة العامة في إصدار هذا القرار، وإنما يقتصر دورها على تلقي طلب التسليم من الجهة المختصة وتعد أوراق الموضوع للعرض على المحكمة المختصة لتتولى هذه الأخيرة عملية إصدار القرار النهائي حول هذا الطلب، أما النهج الثاني فيتمثل في إعطاء النائب العام في الدولة المطلوب منها التسليم سلطة الفصل في إصدار القرار النهائي من عدمه، ويعاب على هذا النظام انه ينقصه القدرة على إحداث نوع من التوازن بين الخبرة القانونية الدولية والأبعاد السياسية الدولية والتي قد لا تتوافر في جميع القضاة بالإضافة إلى طول المدة التي تتخذها إجراءات المحاكمة من شأنها أن تدفع بالمحكمة إلى إصدار أمر بالإفراج المؤقت عن المطلوب تسليمه لحين استكمال الإجراءات وفي هذا فرصة لفرار المطلوب تسليمه[1] .

**02- التسليم الإداري:** ويتم بموجب هذا النظام الفصل في طلبات التسليم على مستوى السلطة التنفيذية إذ يحال طلب التسليم من وزارة الخارجية إلى وزارة العدل التي تبت في الطلب قبولا أو رفضا والتي ترد به إلى وزارة الخارجية لتبليغه للمثل الدبلوماسي للدولة طالبة التسليم ويبرر أنصار هذا النظام بأن إناطة مهمة الفصل في طلب التسليم إلى السلطة التنفيذية كونه يعتبر من أعمال السيادة كما أنه قد يثير مسائل سياسية تكون السلطة التنفيذية كفيلة بمعالجتها، ورغم ما يتميز به هذا النظام من بساطة الإجراءات، إذ يكفي لدراسة ملف التسليم التأكد من مطابقة الهوية الواردة في الطلب مع الشخص الموقوف قيد التسليم وأن الجريمة المتابع بها من الجرائم القابلة للتسليم.

ويعاب على هذا النظام أنه لا يوفر للشخص المسلم الضمانات القانونية الكافية إذ يسلم الشخص دون أخذ رأيه أو الاعتراض على قرار التسليم، كما أن الإجراءات القانونية المتخذة من السلطة

[1] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 266 .

التنفيذية قد تتأثر بالاعتبارات السياسية مما يشوبها عيب الدقة وبالتالي فقد تؤدي إلى خلاف ما يقتضيه التسليم[1].

**03 – التسليم المختلط:** وهو النوع الثالث من التسليم والذي يجمع بين التسليم القضائي والإداري، وهو النظام الأكثر رواجا وانتشارا حيث يحاول الموازنة بيم المصلحتين المتعارضتين مصلحة الدولة طالبة التسليم ومصلحة الشخص المطلوب تسليمه، فيكون من حق السلطة القضائية فحص الطلب، ويمنح الشخص المطلوب تسليمه كل الضمانات القانونية للدفاع، بشرط أن لا تقحم الدولة المطلوب منها التسليم نفسها في فحص وقائع الدعوى، وتكتفي بما يرد إليها من مستندات ووثائق من الدولة الطالبة[2].

وتجدر الإشارة في هذا الشأن أن طلب التسليم ليس ملزم للحكومة وإنما يظل استشاريا لها، أن شاءت الأخذ به وان شاءت لم تأخذ به، فلها مطلق الحرية في التسليم أو أن ترفض هذا الطلب، وهو ما يبرز دور الإدارة أو السلطة التنفيذية في اتخاذ القرار بتسليم الشخص أم لا، ففي حالة قررت المحكمة رفض التسليم فلا يجوز للحكومة عندئذ تسليمه[3].

## ثانيا: شروط وإجراءات تسليم المجرمين.

ينبغي لتسليم شخص مدان أو متهم في دولة ما إلى دولة أخرى أن تتوافر مجموعة من الشروط ليتم التسليم على أكمل وجه، ويمكن تقسيم هذه الشروط كالتالي:

### 01– الشروط المتعلقة بالجريمة.

وتتمثل هذه الشروط في:

– **ازدواج التجريم:** ويقصد بذلك أن يؤلف الفعل المقترف جريمة في تشريع الدولة طالبة التسليم وفي تشريع الدولة المطلوب منها التسليم، والحقيقة يعتبر هذا الشرط منطقي وبديهي، فمن غير المنطق أن تقوم دولة بتسليم شخص موجود على أراضيها دون أن يكون ارتكب فعل مخالف لقوانينها

[1] يوسف حسن يوسف، مرجع سابق، ص 159.

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 268 .

[3] يوسف حسن يوسف، مرجع سابق، ص 161.

وقد أقرت التشريعات الداخلية لمختلف الدول وكذا الدولية هذا الشرط[1]، وقد أجاز القانون الجزائري تسليم الأشخاص الأجانب إلى حكومة أجنبية بناء على طلبها إذا وجدوا في الأراضي الجزائرية واتخذت في حقهم إجراءات متابعة من طرف الدولة الطالبة أو صدرت ضدهم أحكام قضائية من هذه الدول ويشترط لتسليم المجرمين إذا كانت الجريمة محل الطلب و المتابعة قد ارتكبت حسب الحالات التالية[2]:

1. إما في أراضي الدولة الطالبة من أحد رعاياها.
2. وإما خارج أراضيها و من أحد رعايا هذه الدولة
3. وإما خارج أراضيها من أحد الأجانب عن هذه الدولة إذا كانت الجريمة من عداد الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر حتى و لو ارتكبت من طرف أجنبي في الخارج.

أما على المستوى الدولي فان احدث الاتفاقيات الدولية التي كرست شرط التجريم المزدوج هي اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المنعقدة بموجب قرار الأمم المتحدة رقم 25 في نوفمبر سنة 2000 إذ تنص المادة 16 منها في فقرتها الأولى والتي تحدد الجرائم الخاصة لنظام التسليم:"...شريطة أن يكون في الجرم الذي يلتمس بشأنه التسليم معاقبا عليه بمقتضى القانون الداخلي لكل من الدولة الطرف الطالبة والدولة الطرف المتلقية الطلب"، كما أكدت أيضا على هذا الشرط المادة الثانية من المعاهدة النموذجية للأمم المتحدة بشان تسليم المجرمين، والمادة الثالثة من اتفاقية جامعة الدول العربية لتسليم المجرمين، والمادة 40 من اتفاقية الرياض العربية للتعاون القضائي، والمادة 40 من الاتفاقية الأوربية للإجرام المعلوماتي[3]، والتي تنص في الفقرة الأولى منها أن الالتزام بتسليم المجرمين لا ينطبق إلا على الجرائم المعرفة وفقا للمواد من 2 إلى 11 من الاتفاقية والتي يكون معاقب عليها في تشريع كلا الطرفين بعقوبة سالبة للحرية لفترة قصوى لا تقل عن سنة أو بعقوبة اشد، وقد توقع واضعوا الاتفاقية وجود حد أقصى ضئيل بالنسبة للعقوبة وهذا لأنه وفقا لاتفاقية مكافحة الإجرام المعلوماتي يمكن للأطراف أن يعاقبوا على بعض الجرائم بعقوبة الحبس ويكون الحد

[1] محمد الفاضل، مرجع سابق، ص 50،51.

[2] المادة 696 من قانون الإجراءات الجزائية الجزائري.

[3] عمار تيسير بجبوج، مرجع سابق، ص 304

وأيضا يوسف حسن يوسف، مرجع سابق، ص 164 .

الأقصى فيها قصير نسبيا، كما هو الحال بالنسبة للمادة 2 والمتعلقة بالولوج غير القانوني والمادة 4 والمتعلقة بالاعتداء على سلامة البيانات، (وكلا هاتين الجريمتين صورة وأسلوب من أساليب الإرهاب الالكتروني على نحو ما شرحنا سابقا) ومن هذا المنظور لم يشأ واضعوا الاتفاقية أن يفرضوا تسليم المجرمين في كل الجرائم المنصوص عليها في المواد من 02 إلى 12، بل تم وضع عام بمقتضاه أنه لا يتم تسليم المجرمين في الجرائم المعلوماتية إلا في الجرائم التي لا تقل الحد الأقصى فيها عن سنة حبس[1] .

وتجدر الإشارة إلى أن التجريم المزدوج لا يعني التماثل في الوصف القانوني، ولكن يكفي الخضوع لنص التجريم، ويقع على الدولة المطلوب منها التسليم التحقق من توافر شرط الازدواج سواء في قانونها الداخلي أو في قانون الدولة التي تطلب التسليم[2] .

**– أن تكون الجريمة مما لا يحظر التسليم فيها قانونا او عرفا** (استبعاد الجرائم السياسية من نطاق التسليم)**:** استبعدت الاتفاقيات والأعراف الدولية وكذلك القوانين الوطنية بعض الجرائم من نطاق التسليم، ومن ابرز هذه الجرائم المستبعدة وأكثرها شيوعا الجرائم السياسية، وقد أثار هذا الاستبعاد العديد ومن المشاكل والصعوبات وهذا بسبب غموض مفهوم الجريمة السياسية، كما أن الكثير من الفقه يرى أنه لا توجد جريمة سياسية خالصة فغالبا ما تكون مرتكبة على حقين في آن واحد، إحداهما غير سياسي يعتدي فيه الجاني على الحقوق الشخصية والأملاك الخاصة والآخر سياسي[3]، وقد استبعدت الجرائم التي تعتدي على مصلحة سياسية، وباعثها سياسي بحت من نطاق التسليم، وهناك إجماع دولي وكذا وطني في هذا الشأن، وهو الأمر الذي أشارت إليه الاتفاقية الأوروبية للتسليم سنة 1957 حيث نصت في مادتها الثالثة على رفض التسليم في الجرائم السياسية

[1] هلالي عبد اللاه احمد، (المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 250،251 .

[2] عمار تيسير بجبوج، مرجع سابق، ص 304.

[3] وقد انقسم الفقه حول تحديد المقصود بالجريمة السياسية إلى مذهبين:

- المذهب الشخصي: يرى أن معيار تحديد الجريمة السياسية يتمثل في الدافع لارتكاب الجريمة ، فإذا كان الدافع سياسيا عدت هذه الجريمة سياسية، أيا كان موضوعها ومهما كانت المصلحة القانونية المعتدى عليها
- =المذهب الموضوعي: يعتمد على طبيعة المصلحة القانونية محل الاعتداء وموضوعه، فكل اعتداء على كيان الدولة أو نظامها السياسي يعتبر جريمة سياسية.

وقد برر هذا الموقف بأنه وجب أن تعامل الجريمة السياسية معاملة مميزة من حيث العقاب، كونها ترتكب لأسباب وبواعث ليست مشينة بل وتدعو إلى الاحترام، كما أن المجرم السياسي عندما يفر إلى دولة أخرى يكون هذا الفرار بمثابة النفي وهي عقوبة قاسية جدا على رجال السياسة، بالإضافة إلى أن الكثير من دول العالم وليدة الثورة .

المجرمون السياسيون يعاملون معاملة خاصة حتى على المستوى الوطني ليس الدولي فحسب وقد جرى عرف الدول بشكل عام على تشبيه الجرائم التي تعتدي على المصلحة الشخصية والمصلحة السياسية في آن واحد، بالجرائم السياسية كجرائم اغتيال شخصيات سياسية، فتجمع اغلب الاتفاقيات والتشريعات الوطنية على استبعاد هذه الجرائم من نطاق الجرائم السياسية بل إنها تشبهها فقط وبالتالي فإن هذه الجرائم تستوجب التسليم[1].

اتفاقية الرياض للتعاون القضائي بين دول الجامعة العربية لسنة 1983، حيث نصت المادة 41 منها على إخراج الجرائم التالية من نطاق الجرائم السياسية وذلك لما تشتمله من اعتداء على الحقوق الخاصة حتى ولو كان باعثها سياسي:

1. التعدي غلى ملوك ورؤساء الأطراف المتعاقدة أو زوجاتهم أو فروعهم أو أصولهم.
2. التعدي على أولياء العهد أو نواب الرؤساء لدى الأطراف المتعاقدة.
3. القتل العمد والسرقة المصحوبة بالإكراه ضد الأفراد أو السلطات أو وسائل النقل أو المواصلات.

هذه الجرائم تم تصنيفها في زمرة الجرائم الإرهابية المرتبطة بالجرائم السياسية البحتة.

التشريعات الوطنية بدورها ذهبت في هذا الاتجاه كالتشريع السوري[2]، وكذلك التشريع الفرنسي رفض التسليم في حالة الجرائم السياسية البحتة، أو أن التسليم كان غرضه سياسي بحت وتنظر

[1] عمار تيسير بجبوج، مرجع سابق، ص 307 .

[2] المادة 196 من قانون العقوبات السوري استثنت من الجرائم السياسية الجرائم التي تعتبر اشد الجنايات خطورة من حيث الأخلاق والحق العام، كالقتل والجرح الجسيم، والاعتداء على الأملاك كالحرق والنسف والإغراق، والسرقات الجسيمة لاسيما ما ارتكب منها بالسلاح والعنف، وكذلك الشروع في هذه الجنايات، فهذه الجرائم تعتبر صور للجريمة الإرهابية.

المحاكم الفرنسية إلى الحق محل الاعتداء من خلال هذه الجرائم، ويتضح ذلك من خلال القضية "Giovanui Gatti" التي تعتبر مثالا واضحا لهذا الاتجاه[1] .

## ثانيا: شروط متعلقة بالعقوبة.

وتتعلق هذه الشروط إما بجسامة العقوبة أو باستبعادها وهذا حتى تكتمل جميع شروط التسليم وأركانه وينتج أثاره .

**01- جسامة الجريمة:** تشترط اغلب الاتفاقيات الدولية والتشريعات الوطنية المتعلقة بتسليم المجرمين، على أن تنطوي العقوبة المقررة بالجريمة موضوع التسليم، على حد أدنى من الجسامة وجب أن يتوافر في تلك العقوبة، ويختلف هذا التسليم بين ما إذا كان طلب التسليم بهدف المحاكمة أو بهدف تنفيذ الحكم المقرر للعقوبة، ويبدو هذا التفاوت واضحا في التشريع الفرنسي، فبينما تشترط المادة 696 فقرة 3 من قانون الإجراءات الجزائية الفرنسي في حالة طلب التسليم بهدف المحاكمة أن لا تقل العقوبة السالبة للحرية المقررة للجنحة مدة عامين على الأقل، وان لا تقل العقوبة المقررة في حالة تنفيذ الحكم الصادر على شهرين على الأقل[2] .

المشرع الجزائري اخذ بما اخذ به المشرع الفرنسي ويتضح ذلك من خلال المادة 697 والتي تنص على أن الأفعال التي يجيز التسليم فيها سراء كان التسليم مطلوب أو مقبول وهي جميع الأفعال التي يعاقب عليها القانون الدولة الطالبة بعقوبة الجناية، وكذلك الأفعال التي يعاقب عليها قانون الدولة الطالبة بعقوبة جنحة إذا كان الحد الأقصى للعقوبة طبقا لنصوص ذلك القانون سنتين أو أقل إذا تعلق

[1] عندما طلبت حكومة "سان مارينو" تسليم أعضاء احد خلية شيوعية رافضة ما قام به من قبيل الجرائم السياسية معللة بذلك أن الجرائم السياسية ترتكب ضد دستور الدولة، ولا تستمد طابعها السياسي من دافع ارتكابها وإنما من الحق المعتدى عليه، بالإضافة إلى قضية " Francesco piperno " وهو أستاذ فيزياء اتهم بالاشتراك في اختطاف واغتيال رئيس الوزراء الإيطالي الأسبق " Aldo Moro"، وقد وجهت الحكومة الايطالية طلبين منفصلين إلى فرنسا من أجل تسليمه لها متهمة إياه بانضمامه إلى مجموعة محظورة "الألوية الحمراء"، إلا أن فرنسا رفضت طلبها، وبعد مدة وجهت ايطاليا طلب ثاني إلى فرنسا متضمنا 46 اتهام من بينها الاشتراك غي اغتيال رئيس الوزراء الأسبق، وغيرها من الأعمال الإرهابية المرتكبة ضد ايطاليا، حينها وافقت فرنسا على طلب التسليم المقدم من طرف ايطاليا مقررة أن معظم الطلبات متعلقة بالمعتقدات السياسية، إلا أن الاغتيال والاختطاف وغيرها هي جرائم عادية، لأنه وبالنظر إلى خطورتها لا يمكن إعطاؤها الصبغة السياسية.

[2] عمار تيسير بجبوج، مرجع سابق، ص 309.

الأمر بمتهم قضى عليه بالعقوبة إذا كانت العقوبة التي قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تجاوز الحبس لمدة شهرين[1].

وفي إطار المعاهدات والاتفاقيات الدولية فقد كان النص صراحة على الأخذ بهذا الشرط في جميع معاهدات التسليم، ومن ذلك الاتفاق القضائي الموقع بين سوريا ولبنان في 1951/02/25 حيث نصت المادة الثانية منه على أن التسليم يكون واجبا إذا كان الشخص المطلوب تسليمه مطلوبا في جناية أو جنحة معاقب عليه في الدولة طالبة التسليم بعقوبة لا يقل حدها الأعلى عن الحبس لمدة سنة أو كان محكوما بالحبس لمدة لا تقل عن شهرين، أما اتفاقية تسليم المجرمين المعقودة تحت رعاية جامعة الدول العربية في 1952/09/14 فقد اشترطت في مادتها الثالثة أن تكون الجريمة جناية أو جنحة معاقب عليها بالحبس لمدة سنة أو بعقوبة اشد في قوانين كلتا الدولتين الطالبة والمطلوب منها التسليم أو أن يكون المطلوب تسليمه عن مثل هذه الجريمة محكوما عليه بالحبس لمدة شهرين على الأقل[2].

كما تجدر الإشارة إلى أن التسليم لا يتم حتى في الجرائم العادية إذا تعلق الأمر بعقوبة يجهلها قانون أي من الدولتين الطالبة أو المطلوب منها، أو أن تكزن العقوبة قاسية أو ماسة بكرامة الإنسان أو مخلة بالنظام العام في الدولة المطلوب منها التسليم، وقد نصت الكثير من التشريعات الوطنية والاتفاقيات الدولية على هذا الشرط[3]، بالإضافة إلى أن بعض الدول التي ألغت عقوبة الإعدام باتت ترفض التسليم في جرائم تعاقب عليها الدولة طالبة التسليم بالإعدام، كما تضمنت العديد من الاتفاقيات الدولية هذا الشرط من ذلك الاتفاقية المبرمة بين مصر وفرنسا وذلك في مادتها 24 منها[4] .

## 02- عدم انقضاء الدعوى العمومية او العقوبة.

يشترط لجواز التسليم أن لا تكون الدعوى العمومية أو الحكم القاضي بفرض عقوبة قد انقضى بأحد أسباب الانقضاء المحددة في التشريعات الوطنية للدولة طالبة التسليم أو المطلوب منها التسليم

[1] المادة 697 من قانون الإجراءات الجزائية الجزائري.

[2] محمد الفاضل، مرجع سابق، ص (78، 100).

[3] المادة 697 من قانون الإجراءات الجزائية الجزائري، وكذا المادة 4/696 من قانون الإجراءات الجنائية الفرنسي والمادة 34 من قانون العقوبات السوري.

[4] عمار تيسير بجبوج، مرجع سابق، ص 311.

أو الدولة التي ارتكبت الجريمة على أرضها[1]، وعلى مستوى التشريعات الوطنية نجد أن المشرع الجزائري قد نص على هذا الشرط في نص المادة 698 في فقرتها الخامسة بقولها:" 5- إذا كانت الدعوى العمومية قد سقطت بالتقادم قبل تقديم الطلب أو كانت العقوبة قد انقضت بالتقادم قبل القبض على الشخص المطلوب تسليمه وعلى العموم كلما انقضت الدعوى العمومية في الدولة الطالبة وذلك طبقا لقوانين الدولة الطالبة أو الدولة المطلوب إليها التسليم"[2].

إلا أن بعض المعاهدات لم ترفض التسليم في حالة سقوط الدعوى العامة أو العقوبة بالتقادم بمقتضى قانون الدولة المطلوب إليها التسليم، ولكنها تجعل من حقها أن تمتنع أو ترفض هذا التسليم[3].

### ثالثا: الشروط المتعلقة بالشخص المراد تسليمه.

بما أن جنسية الشخص المراد تسليمه تعد محل اعتبار في التسليم فان الشروط المتعلقة بهذا الشخص لا تخرج عن التالي:

### 01- أن لا يكون الشخص المراد تسليمه من رعايا الدولة المطلوب إليها التسليم.

من المبادئ المعروفة والسائدة في المجتمع الدولي والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات الدولية مبدأ عدم تسليم الرعايا أيا كان نوع الجريمة المرتكبة من قبلهم في أي إقليم خارج دولتهم، وقد نص المشرع الجزائري على ذلك في المادة 1/698 وذلك بقولها:" ...إذا كان الشخص المطلوب تسليمه جزائري الجنسية والعبرة في تقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجلها"[4] ، أما قانون الإجراءات الجنائية الفرنسي فقد نص على هذا الشرط من خلال المادة 696 /4، حيث يمنع تسليم الشخص الذي يحمل الجنسية الفرنسية والعبرة وقت ارتكاب الجريمة[5]، أما

[1] يوسف حسن يوسف، مرجع سابق، ص 168.

[2] المادة 698 من قانون الإجراءات الجزائية الجزائري.

[3] إيهاب محمد يوسف، اتفاقيات تسليم المجرمين ودورها في تحقيق التعاون الدولي في مكافحة جرائم الإرهاب، رسالة دكتوراه مقدمة إلى أكاديمية الشرطة، 2003 ، ص 228 .

[4] المادة 698 من قانون الإجراءات الجزائية الجزائري

[5] Article 696 - 4 (inséré par Loi nº 2004 - 204 du 9 mars 2004 art. 17 I Journal Officiel du 10 mars 2004)

المعاهدات والاتفاقيات الدولية المتعلقة بالتعاون القضائي وتسليم المجرمين فقد أشارت بدورها إلى هذا المبدأ ومن الأمثلة عليها اتفاقية الرياض العربية للتعاون القضائي حيث جاء فيها:" يجوز لكل طرف من الأطراف أن يمتنع عن تسليم مواطنيه"[1] .

معاهدة منظمة المؤتمر الإسلامي تضمنت نفس هذا الشرط من خلال المادة السادسة في فقرتها الثامنة منها وذلك بقولها:" إذا كان النظام القانوني للدولة المطلوب إليها التسليم لا يجيز لها تسليم مواطنيها فتلزم الدولة المطلوب إليها التسليم بتوجيه التهام ضد من يرتكب منهم جريمة من الجرائم الإرهابية..."، ويلاحظ من خلال هذا النص أن الاتفاقية لا تحظر التسليم إلا إذا حظره التشريع الداخلي للدولة المطلوب إليها التسليم، والأمر نفسه بالنسبة للاتفاقية العربية، إلا أنه وبالمقابل يوجد عدد كبير من الدول وخاصة الأوربية قد انضمت لآليات دولية لا تتضمن حظر التسليم ومثالها موقف اتفاقية الاتحاد الأوربي للتسليم 1996 وقرار مجلس الاتحاد الأوربي بتاريخ 13 يوليو 2002 بشأن أمر القبض الأوربي إذا خلت هاتين الآليتين من الحظر، إلا أنه تجدر الإشارة إلى أن هذا الحظر لا يمتد إلى تسليم المجرمين إلى المحكمة الجنائية الدولية وهذا ما نص عليه نظامها الأساسي[2] .

## 02- الشخص المطلوب من رعايا الدولة طالبة التسليم.

وهذا الشرط تجيزه كل التشريعات الوطنية والاتفاقيات الدولية، وهذا يعني أن يكون الشخص حاملة لجنسية الدولة طالبة التسليم وهذا الأمر لا يثير أي إشكال لان الدولة سوف تسلم رعايا الدولة طالبة التسليم، لكنها يمكن أن تمتنع عن تسليمه في حالات ضيقة جدا كان يرتكب هذا الشخص جريمة في إقليم الدولة المطلوب إليها التسليم، ففي هذه الحالة ترفض بعض التشريعات الوطنية التسليم[3]، ومن ذلك نص المادة 698 فقرة 3 من قانون الإجراءات الجزائية الجزائري[4]، وكذلك نص

[1] المادة 39 من اتفاقية الرياض للتعاون القضائي بين الدول العربية المصدقة بالقانون رقم 14 بتاريخ 1983/10/10.

[2] عمار تيسير بجبوج، مرجع سابق، ص 313.

[3] محمد الفاضل، مرجع سابق، ص 120.

[4] تنص الفقرة الثالثة من المادة 689 من قانون الإجراءات الجزائية الجزائري:" ..إذا ارتكبت الجناية أو الجنحة في الأراضي الجزائرية"

المادة 4/696 من قانون الإجراءات الجنائية الفرنسي التي تحظر التسليم إذا ارتكبت الجريمة داخل أراضي الجمهورية الفرنسية[1]، فما دام الجرم واقع ضمن صلاحية المحاكم الوطنية فإن بإمكانها أن ترفض تسليمه لأي دولة أخرى وتطبيق قوانينها عليه.

### 03 – الشخص المطلوب تسليمه من رعايا دولة ثالثة.

في هذه الحالة يكون الشخص المطلوب تسليمه لا يحمل جنسية الدولة طالبة التسليم ولا لدولة المطلوب منها التسليم، وهذا الأمر لا يشكل عائق كبير إما التسليم إلا أن بعض الاتفاقيات تقتصر في طلب التسليم على رعايا الدولة الطالبة فقط، وبعض الاتفاقيات الدولية اشترطت حتى يتم التسليم وجب أخذ موافقة الدولة التي يحمل الشخص المطلوب تسليمه جنسيتها، ولهذه الدولة الثالثة أن تطلب استرداد الشخص المطلوب والذي يحمل جنسيتها من اجل محاكمته أمام محاكمها الوطنية.

وفي الحقيقة أن تبليغ الدولة المطلوب منها التسليم الدولة الثالثة التي يحمل الشخص المطلوب جنسيتها يعتبر من قبيل المجاملات الدولية، إذ لا يوجد في القانون الدولي ما يلزم الدولة المطلوب منها التسليم باتخاذ مثل هذا الإجراء[2].

### 04– الشخص الذي يحمل أكثر من جنسية.

تثير هذه المسالة صعوبة كبيرة عندما يحمل الشخص جنسية الدولة طالبة التسليم وجنسية الدولة المطلوب منها التسليم، إلا أن المبدأ المعمول به هو اعتبار أن الشخص يعد من رعايا الدولة التي هو على إقليمها، إما في حالة ما إذا اكتسب الشخص جنسية دولة أخرى أو غير جنسيته بعد طلب التسليم فان اغلب الدول لا ترتب على تغيير الجنسية أي اثر، على اعتبار أن هذا التغيير يعتبر هروبا وتحايلا لا يقره القانون، وعليه يجوز تسليم هذا الشخص حتى بعد تغيير جنسيته، أما إذا كان طالب تغيير الجنسية قبل ارتكاب الجريمة وان هناك دلالات قوية على أن هذا الطلب لم يهدف إلى التحايل

[1] Article 696 - 4 (inséré par Loi nº 2004 - 204 du 9 mars 2004 art. 17 I Journal officiel du 10 mars 2004 L'extradition n'est pas accordée: 3º Lorsque les crimes ou delits ont étécommis sur le territoire de la République

[2] محمد الفاضل، مرجع سابق، ص 152.

أو الهروب من التسليم فتكون بذلك أمام حالة عامة لشخص يحمل جنسيتين ويعامل وفقا لقوانين الدولة الموجود على أرضها[1].

### ثالثا: إجراءات التسليم.

يقصد بمراحل وإجراءات التسليم تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم، وهذا بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته وبين تامين الصالح العام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة بحيث لا يفلت أي مجرم من العقاب.

وإجراءات التسليم تتقاسمها الدولتان الطالبة والمطلوب منها، كما وأنها ليست مطلقة بل مقيدة ببعض الالتزامات الدولية أو التعاهدية[2] .

### 01- إجراءات الدولة طالبة التسليم (طلب التسليم).

يعد طلب التسليم الأداة التي من خلالها تعبر الدولة الطالبة صراحة عن رغبتها في استلام الشخص المطلوب فمن دونه لا يمكن أن ينشأ الحق في التسليم، والأصل أن يكون كتابة، إذ أنه لا يجوز أن يقدم هذا الطلب شفاهة كأن ترسل الدولة الطالبة برقية أو تلغراف أو عن أية طريق من طرق الاتصال الالكتروني إلا في حالات معينة تتميز بصفة الاستعجال وعلى سبيل الاستثناء، وعادة ما يرفق طلب التسليم مجموعة من المستندات الدالة على ارتكاب الشخص المطلوب تسليمه للجرم محل التسليم وبعض مواصفات الشخص المطلوب تسليمه والتي من شأنها إعانة أجهزة الدولة المطالبة بالتسليم على تعقب الشخص المطلوب والقبض عليه[3].

ففي قانون الإجراءات الجزائية الجزائري ووفقا للمادة 702 يقدم طلب التسليم إلى الحكومة الجزائرية بالطريق الدبلوماسي و يرفق بحكم الإدانة أو بأوراق الإجراءات الجزائية التي صدر بموجبها

[1] إيهاب محمد يوسف، مرجع سابق، ص 93.

[2] يوسف حسن يوسف، مرجع سابق، ص 168.

[3] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 270.

الأمر بإحالة المتهم على القضاء الجزائي ، و على الدولة الطالبة أو تقدم في الوقت ذاته النصوص المطبقة على الفعل الموصوف بالجريمة وكذا بيان لوقائع الدعوى[1].

## 02- الجهات المنوط بها إعداد طلب التسليم.

يعد إعداد طلب التسليم من الأعمال التي تتصل بالنظام القضائي للدول، ففي مصر نجد أن النيابة العامة تتولى إعداد طلب التسليم من خلال مكتب المحامي العام الأول ، أما في الولايات المتحدة الأمريكية فإن إجراءات التسليم تبدأ من إدارة العدل مكتب الأعمال الخارجية، إذ يقدم الطلب بصفة أساسية من محاكم الولاية طالبة التسليم أو من المحامي العام لهذه الولاية، أو النائب المحلي الخاص بها، وفي فرنسا يعد طلب التسليم وكيل النائب العام الذي يرسله إلى النائب العام فيتولى هذا الأخير إرساله إلى وزارة العدل لتقوم هذه الأخيرة بإرسال ملف التسليم كاملا إلى وزارة الخارجية التي تتولى عبر القنوات الدبلوماسية إرسال الملف إلى سفارتها إلى الدولة الطالبة[2].

## 03- إجراءات الدولة المطلوب منها التسليم.

تتمثل هذه الإجراءات في تلقي الطلب واتخاذ إجراءات التحري وجمع الاستدلالات والقبض على الشخص المطلوب، كما يستجوب المقبوض عليه ويحبس احتياطيا، أو يطلق سراحـــــه بكفالة أو بدونها أو منعه من مغادرة إقليم الدولة المطلوب منها التسليم، إلى أن يتم الفصل في الطلب الوارد بشأنه وهي من اختصاص الادعاء العام في معظم الدول، وأخيرا يتم فحص الطلب من طرف المحكمة المختصة والبت بالقبول أو رفض طلب التسليم، ففي الجزائر يتولى وزير الشؤون الخارجية تحويل طلب التسليم بعد فحص المستندات إلى وزير العدل الذي يتحقق في صحة الطلب ، ويقوم النائب العام باستجواب الأجنبي للتحقيق من شخصيته ويبلغه بالمستند الذي قبض بموجبه وينقل بموجبه وينقل الأجنبي في أقرب وقت ويحبس بسجن العاصمة وخلالها تحول المستندات المقدمة والمؤيدة للطلب إلى النائب العام لدى المحكمة العليا الذي يتولى بدوره استجواب الأجنبي ويحرر بعد ذلك محضرا خلال أربعة وعشرين ساعة ( 24 ) وترفع المحاضر وسائر المستندات إلى الغرفة الجنائية بالمحكمة العليا ، ويمثل الأجنبي أمامها خلال ثمانية أيام اعتبارا من تاريخ تبليغ المستندات

[1] المادة 703 من قانون الإجراءات الجزائية الجزائري.

[2] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 270، 271.

وتسمع أقواله في الغرفة الجنائية بالمحكمة العليا ويمثل الأجنبي أمامها خلال ثمانية أيام اعتبارا من تاريخ تبليغ المستندات. وتسمع أقوال النيابة العامة وصاحب الشأن ويمكنه الاستعانة بمحامي ومترجم ، وإذا أصدرت المحكمة العليا رأيا مسببا برفض طلب التسليم يكون نهائيا وغير قابل للمعارضة ، ويمكن الإفراج عن الشخص الذي قبض عليه مؤقتا طبقا للشروط المنصوص عليها في المادة 702 إذا لم تتلقى الحكومة الجزائرية المستندات المذكورة بالمادة سالفة الذكر خلال خمس وأربعين ( 45 ) يوما من تاريخ إلقاء القبض عليه[1] .

بالإضافة إلى ذلك فانه يجب عند تسليم الشخص محل التسليم أن تسلم معه كل ما كان في حوزته أثناء القبض عليه، وكل ما يمكن أن يكون دليلا على الجريمة ويجوز الاحتفاظ بها إذا رأت الدولة المطلوب إليها التسليم لزوما لذلك، أو أن تحتفظ بحق استرجاعها مستقبلا، وفيما يتعلق بنفقات التسليم الأموال التي تدفع لنقل الشخص المطلوب تسليمه ومحصلات الجريمة وأحيانا لترجمة الوثائق والمستندات المطلوبة فانه ووفقا لما هو مستقر عليه تكون على الدولة الطالبة التسليم ما لم يتم الاتفاق على غير ذلك[2].

على الصعيد الدولي ظهرت عدد من الاتفاقيات متعددة الأطراف بشأن تسليم المجرمين، فهناك اتفاقية البلدان الأمريكية لتسليم المجرمين 1981 في إطار منظمة الدول الأمريكية، وكذلك اتفاقية جامعة الدول العربية لتسليم المجرمين 1952، وهناك الاتفاقية الأوربية المتعلقة بتسليم المجرمين 1957، وبروتوكولاتها الإضافية 1975، 1978، وهناك اتفاقية تبسيط إجراءات تسليم المجرمين بين الدول الأعضاء في الاتحاد الأوربي، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000.

كما أنه يوجد نوع آخر من مظاهر التعاون الدولي في مجال تسليم المجرمين يتمثل في الاعتراف المتبادل بأوامر القبض أو الحبس أو التوقيف وبمقتضاه تصدر السلطة المختصة بإحدى الدول أمرا بالقبض أو الحبس أو التوقيف وتعترف بصلاحيته دولة أخرى أو أكثر ويتعين تنفيذه[3].

[1] المواد من 703 إلى 713 من قانون الإجراءات الجزائية الجزائري.

[2] يوسف حسن يوسف، مرجع سابق، ص 172.

[3] أمير فرج يوسف، (مكافحة جريمة الإرهاب الالكتروني)، مرجع سابق، ص 271.

مما سبق يتضح انه للتسليم أهمية بالغة في جرائم الإرهاب عموما وجريمة الإرهاب الالكتروني بشكل خاص، ويرجع ذلك إلى خطورة الفعل في حد ذاته وتطوره، إلا أن بعض الدول تتمسك بعدم التسليم على أساس أن الجرائم الإرهابية من قبيل الجرائم السياسية، التي لا يجوز فيها التسليم، وهناك أيضا من يتمسك بالعرف الدولي الذي مفاده "عدم تسليم الدولة لرعاياها"، ودولة أخرى ترفض التسليم لعدم وجود اتفاقية للتسليم المتبادل، إلا أن هذه الحجج واهية وخاصة حجة الطابع السياسي لجريمة الإرهاب لا يمكن التمسك بها وهذا لأنه تم إخراج الجريمة الإرهابية من نطاق الجرائم السياسية في مضمون الاتفاقيات والمعاهدات الدولية وكذلك التشريعات الداخلية للدول –على نحو ما وضحناه في شروط التسليم–، كما أن الجريمة الإرهابية بشكل عام تختلف عن الجرائم السياسية من حيث طبيعتها على الرغم من كونها نوع من العنف السياسي إلا أن قواعدها الموضوعية تجعلها تنفرد بإطار خاص بها، الأمر الذي تأكد من قبل مجلس الأمن في قراره رقم 1373 السالف الذكر، والذي دعا من خلاله أعضاء المجتمع الدولي إلى رفض الإرهاب بمختلف أشكاله وأنواعه، وعدم اتخاذ الدول لأراضيها مسرحا للعمليات الإرهابية وعدم الاحتجاج بالطابع السياسي لرفض التسليم، وهو المبدأ الذي نصت عليه جميع الاتفاقيات المتعلقة بالإرهاب[1] .

## الفرع الثاني: المساعدة القضائية في جريمة الإرهاب الالكتروني.

الانترنت شبكة عالمية تمتاز بأنها دولية، وأنها عابرة للحدود، أي أنه لا للحدود الجغرافية معنى وبالتالي فان الجرائم المتصلة بها هي الأخرى عالمية ، وذات طابع دولي، وأثرها يمتد لأكثر من دولة ولأن جريمة الإرهاب الالكتروني جريمة إرهابية متصلة بالانترنت فانه يتعين علينا أولا أن نتعرف على مفهوم المساعدة القضائية وأهم المبادئ العامة المتعلقة بها، وبعدها إجراءاتها.

### أولا: مفهوم المساعدة القضائية وأهميتها.

تعتبر المساعدة القضائية المتبادلة في المسائل الجنائية إحدى الوسائل الإجرائية في مجال التعاون القضائي الدولي الجنائي، وتتمثل في المحاكمة التي تجري في دولة طرف في معاهدة أو اتفاقية لتبادل المساعدة بشان جريمة مرتكبة تدخل في اختصاص سلطتها القضائية، ويقتضي الأمر طلب المساعدة من دولة أخرى طرف في هذه المعاهدة من أجل استظهار وجه الحق والحقيقة في هذه

[1] الهام ساعد حورية، مرجع سابق، ص 50.

المحاكمة[1]، كما تعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[2].

## أهمية المساعدة القضائية المتبادلة في جريمة الإرهاب الالكتروني.

كثيرا ما يتعدى أثر جريمة الإرهاب الالكتروني حدود الدول، فقد يكون مرتكب الهجوم في بلد ما ويتم شن الهجوم من حواسيب موجودة في بلد آخر، وتقع الآثار المترتبة على ذلك في بلد ثالث، وقد يرتكب الإرهابي جميع مراحل جريمته في دولة لم تطأها قدماه أصلا من قبل لذا تقتضي فعالية التحقيق والملاحقة القضائية تتبع اثر النشاط الإجرامي من خلال تقفي اثر قنوات الاتصالات بالحواسيب مصدر الهجوم، وحاسوب الضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات الانترنت في دول مختلفة، ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة التحقيق الاعتماد على سجلات التاريخية التي تبين متى أجريت توصيلات مختلفة ومن أين، ومن الذي أجراها، وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع اثر التوصيل وقت إجرائها، وقد يصطدم المحققون أثناء ذلك بصعوبات قانونية تنجم عن مشاكل الحدود والولايات القضائية عندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية الإقليمية لهم وهو ما يحدث في أغلب الأحيان ، وهنا تظهر أهمية المساعدة القضائية المتبادلة بين سلطات التحقيق في الولايات القضائية في مختلف الدول، فقديما كانت المساعدة القضائية المتبادلة تقليدية وغير فعالة، حيث يستغرق اتخاذ الإجراء شهورا، الأمر الذي لا يتناسب مع ضرورة توخي السرعة في التعامل مع الأدلة الرقمية غير الملموسة وسريعة الزوال[3] .

كما تتجلى أهمية المساعدة القضائية المتبادلة في أن غيابها أو الإبطاء فيها يؤدي إلى أن يجري المحققون في إحدى الدول التي تسعى إلى الحصول على المعلومات في حواسيب موجودة في دولة أخرى عمليات بحث عابرة للحدود تكون هي الأخرى غير مرخص بها في النظم الحاسوبية[4] .

---

[1] شبلي مختار، مرجع سابق، ص 295.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 142.

[3] محمد كمال محمود الدسوقي، مرجع سابق، ص 142، 143.

[4] تدابير مكافحة الجرائم المتصلة بالحواسيب، ورقة عمل مقدمة في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك 18-25 أفريل 2005، ص 17.

انطلاقا من هذه الأهمية لابد من اعتماد آليات للتعاون وتبادل المساعدة تتلاءم مع طبيعة الجرائم المعلوماتية كجريمة الإرهاب الالكتروني، بحيث تمكن المحققين في تلك الجرائم من الحصول على المعلومات بصورة عاجلة، ومن الأمثلة العملية التي تبين أهمية التعاون والمساعدة القضائية المتبادلة قضية معروفة بعملية "**كاتريك Catterick** "[1] ، وقد تطلب التحقيق في هذه القضية التنسيق بين سلطات التحقيق في كل من الولايات المتحدة الأمريكية والمملكة المتحدة، هذا وقد أسفرت التحريات التي تمت بين أجهزة الشرطة في البلدين إلى وجود أشخاص مشتبه بهم في دولة "لاتفيا"، فتم تقديم طلب الإنابة القضائية إلى السلطات في لاتيفيا وعليه قام جهاز الشرطة فيها بعملية مراقبة سرية أسفرت عن إلقاء القبض على 10 أشخاص يشتبه في تورطهم في عمليات غسل الأموال، وفي وقت لاحق تم تحديد موقع جهاز كمبيوتر تم اختراقه، وتم اخذ نسخة من الشفرة الخبيثة الموجودة عليه مما قاد المحققين إلى قناة محادثة عبر الانترنت، وقام رجال الشرطة بمراقبة غرف المحادثة هذه وتوصلوا إلى أن المتحكم في شبكة البوت نت المستخدمة في جريمة حجب الخدمة الموزعة يدخل عادة هذه القناة لشن هجومه، وتم تحديد الأفراد الأعضاء في هذه القنوات.

من خلال هذه القضية تلخص لنا مدى أهمية وضرورة التعاون وتبادل المساعدة في مجال مكافحة الجرائم المعلوماتية التي تعتبر جريمة الإرهاب الالكتروني من أخطرها، الأمر الذي بات فرضا ولزاما لا خيارا بحكم طبيعة تلك الجرائم[2] .

[1] تتلخص وقائع قضية كاتريك في قيام احد شركات القمار بعملية ابتزاز عبر شبكة الانترنت في فترة من شهر ماي إلى شهر أكتوبر من عام 2004، وقد نفذ هذه العملية عدد من المجموعات الإجرامية التي تنشط الإجرام الالكتروني وكان أفراد هذه المجموعات يقومون بمراسلة إحدى الشركات لمطالبتها بمبلغ من المال يهددونها بأنه في حالة امتناعها عن دفع المبلغ المطلوب فسيقومون بشن هجوم على موقعها الالكتروني بهدف حجب خدماتها( هجمات حجب الخدمة الموزعة وتسمى أيضا بهجمات الحرمان من الخدمات – DDOS) أي إغراق الموقع بسيل من البيانات غير اللازمة عن طريق أجهزة مصابة ببرامج تسمى DDOS-ATTACKS ، وقد نفذت هذه المجموعة الإجرامية هجماتها باستخدام شبكة البوت نت، وهي عبارة عن شبكة من أجهزة الكمبيوتر المصاب بفيروس يتحكم فيها المخترق بتنشيط هذه الأجهزة وإجبارها على زيارة موقع معين في الموقع نفسه، دون أن يدرك أصحابها أنهم يشتركون في هذا العمل الإجرامي، وقد تعرض إلى هذا الهجوم حوالي 57 شركة في مختلف أنحاء العالم وأدت إلى خسائر جسيمة، فضلا عن الضرر الذي تتعرض له المواقع ذاتها حيث أن مقدار البيانات التي يتم توجيهها عبر قسم الوصلات الرئيسية لشبكة الانترنت يكاد يتسبب في تدمير هذه المواقع.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص (143 ،145).

ومن المبادئ العامة التي تنظم الإلزام بتقديم المساعدة القضائية المتبادلة وفقا للمادة 25 في فقرتها الأولى من اتفاقية بودابست، وهذا الالتزام وجب أن يتوافر إلى أقصى حد ممكن، وعليه فان المساعدة المتبادلة من حيث المبدأ يجب أن تكون واسعة المدى، كما يجب أن يتم تقييد العوائق وتحديدها، بالإضافة إلى ذلك فان الالتزام بالتعاون ينطبق من حيث المبدأ على كل من الجرائم المتعلقة بنظم الحاسوب[1]، مثل الجرائم المقررة في المادة 14، في فقرتها الثانية تقسيم (أ–ب)، وتجميع الدليل في هيئته الالكترونية الناجم عن الجرائم، ولقد تم الاتفاق على تقرير الالتزام بالتعاون على هذا النحو الواسع للجرائم لأن هناك حاجة مماثلة لآلية انسيابية للتعاون الدولي لهاتين الهيئتين، وعليه فإن المادة 24 والمادة 35 تسمح للأطراف بتقديم نطاق مختلف لتنفيذ هذه الإجراءات[2].

## ثالثا: مجالات المساعدة القضائية المتبادلة.

تتنوع وتتعدد مجالات المساعدة القضائية المتبادلة في مجال مكافحة الجريمة ويمكن تقسيمها إلى مجالات عامة تستهدف مختلف الجرائم، والتي غالبا ما تتضمنها اتفاقيات عامة مثل معاهدة الأمم المتحدة النموذجية بشان نقل الإجراءات في المسائل الجنائية، والاتفاقية الأوربية لنقل الإجراءات الجنائية، النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي 2003، واتفاقية الرياض العربية للتعاون القضائي 1983، ومجالات خاصة تتطلبها طبيعــة

الجريمة المستهدفة مكافحتها، مثل مكافحة الجرائم الإرهابية، كجريمة الإرهاب الالكتروني –محل الدراسة–، وعادة ما ترد هذه المجالات ضمن الاتفاقيات الدولية أو الإقليمية التي أبرمت لغرض مكافحتها مثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000، واتفاقية بودابست المتعلقة بالجريمة الالكترونية 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

مما سبق يمكن حصر مجالات المساعدة القضائية المتبادلة فيما يلي:

### 01 – نقل الإجراءات.

[1] المادة 23 من اتفاقية بودابست.

[2] هلالي عبد اللاه احمد، (المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 258.

يقصد بنقل الإجراءات قيام دولة ما بناءا على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة، ومن أهمها التجريم المزدوج، الذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات.

فضلا عن شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن الجريمة نفسها، وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بما كان، بحيث تؤدي دورا مهما في الوصول إلى الحقيقة[1] .

العديد من الاتفاقيات الدولية والإقليمية أقرت نقل الإجراءات بوصفها إحدى صور المساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000 وذلك في المادة 21 منها، ونفس الشيء نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999 في المادة 09 منه.

### تبادل المعلومات.

تبادل المعلومات يشتمل على تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم.

[1] علي حسن طوالبة، التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية، بحث منشور في الموقع الالكتروني :www.policemc.gov.bh، تاريخ الاطلاع 2018/06/11 على الساعة 00:52.

التبادل قد يشمل السوابق القضائية للجناة، ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبير في الكثير من الاتفاقيات[1] .

ويتم تبادل المعلومات من خلال تعزيز قنوات الاتصال بين سلطات الدول وأجهزتها ودوائرها المختصة بمكافحة الجرائم، مثل الأجهزة المختصة بمكافحة الجرائم المعلوماتية، ويعتبر إنشاء مثل تلك القنوات ضرورة وذلك من اجل تيسير تبادل المعلومات بصورة مأمونة وسريعة بشأن كل ما يتعلق بتلك الجرائم مثل[2] :

1. هوية الأشخاص المشتبه في ضلوعهم في تلك الجرائم، وأماكن وجودهم وأنشطتهم، أو أماكن الأشخاص الآخرين المعنيين.
2. حركة عائدات الجرائم أو الممتلكات المتأتية من ارتكاب تلك الجرائم.
3. حركة الممتلكات أو المعدات أو الأدوات الأخرى المستخدمة أو المراد استخدامها في ارتكاب تلك الجرائم.
4. تبادل المعلومات عن الوسائل والأساليب المحددة التي تستخدمها الجماعات الإجرامية المنظمة في ارتكاب جرائمها، ووسائل وأساليب إخفاء أنشطتها.
5. تبادل المعلومات وتنسيق التدابير الإدارية وغير الإدارية المتخذة حسب الاقتضاء لغرض الكشف المبكر عن الجرائم .
6. كما يمكن أن تقوم الجهة المختصة في دولة ما بإرسال إلى الجهة المختصة لدى دولة أخرى وهي بصدد النظر في جريمة ما بيانات عن الأحكام القضائية النهائية الصادرة ضد مواطني الأخيرة أو الأشخاص المولودين أو المقيمين في إقليمها والإجراءات التي اتخذت ضدهم والمقيدة في صحف الحالة الجنائية لدى الدولة المرسلة.

ومما سبق يتضح أن لهذه الصورة من صور المساعدة القضائية المتبادلة أهمية كبيرة خاصة في مكافحة جريمة الإرهاب الالكتروني التي يلجا مرتكبوها إلى التخفي على الشبكات الالكترونية خلف شخصيات وهمية وبأسماء مستعارة، وهو ما يتطلب تعاونا بين الدول خاصة في حالة توزع النشاط

[1] يوسف حسن يوسف، مرجع سابق، ص 150.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 147.

الإجرامي بين أكثر من دولة لتحديد هوية الأشخاص المشتبه في ضلوعهم في تلك الجرائم، وتحديد أماكن وجودهم تمهيدا للقبض عليهم، فضلا على أن تبادل الدول المعلومات بالنسبة للوسائل والأساليب التي يستخدمها مرتكبي تلك الجرائم في ارتكاب جرائمها والتي تتسم بالتطور السريع والمستمر، يسهل من مهمة التصدي لتلك الجرائم[1]

ويجب أن يتم تبادل تلك المعلومات بشكل أكثر سرعة دون انتظار عقد اجتماعات ومؤتمرات لعرض تلك المعلومات واستعراض هذه الأساليب، حيث أنه على سبيل المثال بالإمكان إصدار نشريه دورية شهرية تتضمن احدث الوسائل والأساليب في مجال الجرائم الإرهابية، على أن يتم تبادلها على مستوى الدول إما بطريقة مباشرة (من دولة إلى دولة) أو من خلال المنظمة الدولية أو الإقليمية، والتي بدورها تقوم بتعميمها على الدول الأعضاء بها أو بطرحها على المواقع الالكترونية الخاصة بها أو عقد الاجتماعات عن بعد بواسطة الشبكات، ومناقشة تلك الخبرات، وهذه الفكرة مقتبسة من مجرمي المعلومات ذاتهم الذين لا يدخرون جهدا ولا يتوانون عن تبادل خبراتهم في مجال الاختراق والتجسس المعلوماتي سواء من خلال مؤتمراتهم عبر شبكات الانترنت، أو من خلال منتدياتهم المخصصة لهذا الغرض[2] .

### 03- تبادل المعلومات التلقائي.

قد يحدث أن يتوافر لدى إحدى الدول معلومات هامة تتعلق بمسائل جنائية تخص دولة أخرى ويمكن أن تحقق تلك المعلومات فائدة للأخيرة أو تساعدها على القيام بالتحريات والإجراءات الجنائية أو إتمامها بنجاح والتي لا تعلم بوجودها الدولة ذات العلاقة، ففي هذه الحالة تقوم الدولة التي تحوز تلك المعومات بالاتصال بالدولة ذات العلاقة والتنسيق معها لتبادل تلك المعلومات دون انتظار أن تتلقى طلبا بذلك، إلا انه في هذه الحالة عادة ما تعطي الاتفاقيات التي تنص على هذه الحالة الحق للدولة الحائزة للمعلومات باشتراط أن تظل المعلومات وخاصة الحساسة سرية ولو مؤقتا، أو أن

[1] محمد كمال محمود الدسوقي، مرجع سابق، ص 148.

[2] نفس المرجع، ص 149.

تستخدم وفقا لشروط معينة حيث أن السرية قد تكون مطلوبة ولازمة في بعض القضايا التي تكون فيها مصالح الدولة مقدمة المعلومات معرضة للخطر جراء البوح بهذه المعلومات[1].

إلا أن هذا لا يمنع الدول الأطراف من أن تفشي معلومات من أجل تبرئة شخص متهم، وفي هذه الحالة تقوم الدولة المتلقية بإخطار الدولة المحيلة قبل إفشاء تلك المعلومات وتتشاور مع الدولة الطرف المحيلة إذا ما طلب منها ذلك، في حالة استثنائية إذا تعذر توجيه إشعار مسبق قامت الدولة الطرف المتلقية بإبلاغ الدولة الطرف المحيلة بذلك الإفشاء دون إبطاء[2].

## 04- التحقيقات المشتركة.

إن طبيعة الجرائم العابرة للحدود مثل جريمة الإرهاب الالكتروني تفترض هذا النوع من التعاون حيث يتطلب التحقيق في هذا النوع من الجرائم تشكيل فرق مشتركة بين الجهات المختصة في كل دولة من الدول التي وقعت فيها جزء من الجريمة.

ويرى جانب من الفقه انه للتحقيق في الجرائم المعلوماتية وخاصة الأكثر خطورة منها كجريمة الإرهاب الالكتروني وكشف الغموض الذي يعتريها بشكل سريع وفعال يتطلب عناصر بشرية مؤهلة علميا وتقنيا وهذا من اجل تحليل أدلتها وحفظها، وهو ما قد لا يكون متاح لإحدى الدول، مما يشكل عقبة أمامها وقد يترتب عليه إفلات الجناة لو قامت بهذا التحقيق منفردة، مما يجعل من تشكيل فرق تحقيق مشتركة مع دول أكثر تقدما في هذا المجال حلا لها.

وتجدر الإشارة إلى أن تشكيل هذه الفرق للتحقيق لا يقتصر فقط على الدول، إنما يمكن تشكيل مثل هذه الفرق من أعضاء دولة معينة وأعضاء من المنظمات الدولية أو الإقليمية المتخصصة في مجال مكافحة الجريمة بشكل عام والجرائم العابرة للحدود بشكل خاص، مثل الانتربول، الأوروبول والمكتب العربي للشرطة الجنائية،الأوروجست وغيرها، حيث أن دعم الدول ومساندتها في مجال مكافحة جريمة الإرهاب الالكتروني وغيرها من الجرائم والتحقيق فيها وكشف وملاحقة مرتكبيها، يشكل

[1] هلالي عبد اللاه احمد، (المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 262.260.

[2] المادة 4/18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والمادة 26 من اتفاقية بودابست.

جزء أساسي من مهام هذه المنظمات، كما وجب التنويه أن هذا النوع من التعاون يتم في حدود الاحترام التام لسيادة الدولة الطرف التي سيجري التحقيق داخل إقليمها[1].

## 05- الإنابة القضائية الدولية.

الإنابة القضائية الدولية بوصفها صورة من صور التعاون القضائي الدولي بل ومن أهمها في مجال مكافحة الجريمة ومنها جريمة الإرهاب الالكتروني- محل الدراسة-، تتم على المستوى القضائي دون التشريعي بين الدول على اعتبار على أنها تعاون بين الأجهزة القضائية المختلفة للدول.

### أولا: تعريف الإنابة القضائية الدولية.

تعرف الإنابة القضائية في المسائل الجنائية عموما بأنها عمل بمقتضاه تفوض المحكمة محكمة أخرى للقيام مكانها أو في دائر اختصاصها بأحد أو ببعض إجراءات التحقيق أو الإجراءات القضائية الأخرى التي يقتضيها فصل الدعاوى المرفوعة أمامها والتي تعذر عليها مباشرتها بنفسها بسبب بعد المسافة أو أي مانع آخر[2] .

كما تعرف الإنابة القضائية بأنها طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية كانت أو دبلوماسية أساسه التبادل، ومفاده اتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج وكذلك أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسالة المثارة أو المحتمل أثارتها في المستقبل أمام القاضي المنيب الذي ليس بمقدوره القيام به في دائرة اختصاصه[3] .

تعتبر الاتفاقيات الدولية المتعلقة بالمساعدة القضائية بين الدول أساسا قانونيا للإنابة القضائية فالاتفاقية الدولية بعد التصديق عليها تصبح سارية المفعول وملزمة شانها في ذلك شأن القوانين الداخلية، حيث تتمتع بالقوة التنفيذية التي تلزم بها السلطات القضائية الوطنية عند عرض المسالة عليها، وفي حالة ما إذا رفضت دولة ما طلب المساعدة القضائية في مسالة معينة فإنه يستوجب

[1] محمد كمال محمود الدسوقي، مرجع سابق، ص 150، 151.

[2] ادوارد عيد، الإنابات والإعلانات القضائية وفقا للقانون الدولي الخاص واتفاقية الدول العربية في عام 1953، معهد البحوث والدراسات العربية، 1969، ص 9.

[3] عكاشة محمد عبد العال، الإنابات القضائية في العلاقات الخاصة الدولية، دار المطبوعات الجامعية، الإسكندرية 1994، ص 16.

عليها تسبيب رفضها وإيضاح بواعثها من هذا الرفض، وعادة ما تحتج الدول في رفضها لطلب الإنابة القضائية بمبدأ سيادة الدولة وأمنها، حيث تتضمن اغلب الاتفاقيات الدولية شرطا أساسيا يجعل تنفيذ الإنابة القضائية رهنا بإرادة الدولة المنفذة، وهذا الشرط هو أن لا تنطوي هذه المساعدة على المساس بسيادة الدولة أو نطاقها أو مصالحها[1]، وقد تطرقت اتفاقية التعاون القضائي الموقعة بين الدول العربية في عام 1983 إلى موضوع الإنابة القضائية عندما نصت المادة 14 منها على انه:" لكل طرف متعاقد أن يطلب إلى أي طرف متعاقد أخر أن يقوم في إقليمه نيابة عنه بأي إجراء قضائي متعلق بدعوى قائمة وبصفة خاصة سماع شهادة الشهود وتلقي تقارير الخبراء ومناقشتهم وإجراء المعاينة وطلب تحليف اليمين ..."[2].

وتتناول الإنابة القضائية استماع الشهود المقيمين في البلد المناب أو تحليفهم اليمين أو تعيين خبير أو تدقيق مستندات، لكن لا يجوز أن تتضمن الإنابة إعمالا تنفيذية كتنفيذ الأحكام الأجنبية، لأن ذلك سيتعدى نطاق الإجراءات المتعلقة بدعوى لم تزل قيد النظر أمام المحكمة المنيبة، فلا يمكن أن يشمل إجراءات التنفيذ التي تخرج عن نطاق سير الدعوى[3] .

وقد عرفت المادة الثالثة من القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية الإنابة القضائية بأنها:" قيام الجهة الطالبة بتفويض الجهة القضائية المختصة في الجهة المطلوب إليها لاتخاذ إجراء أو أكثر من إجراءات التحقيق أو من إجراءات تتعلق بالجريمة المطلوب التعاون بشأنها"[4] .

## ثانيا: شروطها

[1] عمار تيسير بجبوج، مرجع سابق، ص 341.

[2] وافق على هذه الاتفاقية مجلس وزراء العدل العرب بموجب قراره رقم 01 المؤرخ 1983/04/06 في دورة انعقاده الأولى في الرياض ودخلت الاتفاقية حيز النفاذ ابتداءا من تاريخ 1985/10/30 .

[3] عكاشة محمد عبد العال، مرجع سابق، ص 58.

[4] القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية، اعتمده مجلس وزراء العدل العرب في دورته الثانية والعشرون بموجب القرار رقم 653- 22 بتاريخ 2006/11/29، بالقاهرة.

للإنابة القضائية الدولية شروط لازمة وجب توافرها لتنفيذها في الدولة المطلوب منها وتتمثل هذه الشروط فيما يلي:

1. **الاختصاص:** حتى تكون الإنابة القضائية الدولية صحيحة لابد أن يكون الفصل في الواقعة موضوع الإنابة من اختصاص الدولة الطالبة،وان يكون هناك صلة بين هذه الدولة والقضية أو الجرم المطلوب من أجله تنفيذ الإنابة، وللدولة المطلوب منها تنفيذ الإنابة أن ترفض إذا رأت إن هذا الاختصاص غير مقبول وفقا لقواعد القانون الدولي أو وفقا للمبادئ الأساسية التي تحكم تطبيق القانون الجنائي من حيث المكان والمتمثلة في مبدأ الإقليمية،ومبدأ الشخصية ومبدأ العينية.

ولا يكفي اختصاص قانون الدولة الطالبة في الواقعة موضوع الإنابة وإنما يلزم أيضا لقبول طلب الإنابة أن تكون السلطة القضائية هي المختصة في الواقعة موضوع الإنابة وبالتالي لا تقبل طلبات الإنابة إذا كانت الواقعة من اختصاص جهة إدارية في الدولة الطالبة[1].

وعليه فانه من غير الممكن تنفيذ الإنابة القضائية في الدولة المطلوب منها إذا كان الإجراء المطلوب لا يدخل في اختصاص الجهة التي وجه إليها الطلب، وقد أكدت اتفاقية الرياض للتعاون القضائي العربي على ذلك، حيث نصت في المادة 15 منها في فقرتها الأولى على أنه إذا تبين عدم اختصاصها فللجهة المطلوب إليها تنفيذ الإنابة أن تحيل الطلب من تلقاء نفسها إلى الجهة المختصة، وإذا تعذر عليها ذلك تحيلها إلى وزارة العدل وتخطر فورا الجهة الطالبة بما تم في الحالتين،وان اختلا ل شرط الاختصاص يؤدي إلى وجود عيب شكلي في إجراءات وسير الدعوى[2].

2. **عدم تعارض تنفيذ الإنابة مع النظام العام:** فتنفيذ الإنابة القضائية الدولية وجب أن لا يكون خارقا للنظام العام في الدولة المطلوب منها التنفيذ، فإذا رأت الدولـــــة أن هـــذا التنفيذ

يتعارض مع نظامها العام كان لها أن ترفضه، وتتجه الاتفاقيات الدولية والقوانين الوطنية إلى النص صراحة على هذا الشرط بالنسبة للدولة المطلوب منها تنفيذ الإنابة، وذلك إذا اتضح لها أن

[1] عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دار النهضة العربية، القاهرة، 2001، ص 59.

[2] عمار تيسير بجبوج، مرجع سابق، ص 343.

في التنفيذ مساس بنظامها العام أو بمصالحها الجوهرية،وقد أشارت الاتفاقية العربية لمكافحة جرائم الإرهاب إلى هذا الشرط صراحة عندما نصت على أن تلتزم كل من الدول المتعاقدة بتنفيذ الإنابات القضائية المتعلقة بالجرائم الإرهابية، ويجوز لها رفض طلب التنفيذ إذا كان تنفيذ الطلب من شأنه المساس بسيادة الدولة المكلفة بتنفيذه أو بأمنها أو بالنظام العام فيها.

كما نصت الاتفاقية الأوربية للمساعدة القضائية لعام 1959 على هذا الشرط من خلال مادتها الثانية فقرة "ب"، بأنه يمكن رفض طلب المساعدة إذا قدرت الدولة المطلوب منها التنفيذ أن تنفيذ الطلب من شأنه إحداث اعتداء على النظام العام أو أية مصالح أساسية أخرى.

وعلى الرغم من أن فكرة النظام العام تخضع لتقدير الدولة المنفذة إلا أنها في حال رفضت طلب الإنابة تلتزم بتبيان أسباب هذا الرفض وهذا ما أشارت إليه الاتفاقية العربية لمكافحة جرائم الإرهاب عندما نصت على أن كل رفض للإنابة القضائية يجب أن يكون مسببا، وهو ما نصت عليه أيضا المادة 19 من الاتفاقية الأوربية للمساعدة القضائية[1].

3. **مراعاة الشروط الشكلية:** يتعين على السلطات القضائية عند تقديم طلب الإنابة أن تلتزم بشكل معين في الإجراءات وذلك من اجل صحتها، حيث توجه الإنابة بطلب مكتوب من السلطة القضائية، إما إلى وزارة العدل في بلدها والتي تحيلها بدورها إلى وزارة الخارجية التي تتولى إرسالها بالطريق الدبلوماسي إلى وزارة الخارجية في البلد المطلوب توفير الإنابة فيه ومنها إلى وزارة العدل فإلى المحكمة المنابة، وغالبا ما تتبع هذه الطريقة في حالة عدم وجود اتفاق قضائي بين الدولتين، أي على سبيل المجاملة الدولية أو مبدأ المعاملة بالمثل، ولوزارة العدل في هذه الحالة أن تقوم بفحص الطلب وتدقيقه قبل إرساله وتتأكد من استيفاء جميع الشروط الشكلية والموضوعية فيه، وإما يتم طلب الإنابة بالطريقة القضائية الخالصة حيث يتم الاتصال بين السلطتين القضائيتين بشكل مباشـر من الدولة الطالبة والدولـــــة المطلوب منها

[1] عمار تيسير بجبوج، مرجع سابق، ص 343،344.

تنفيذ الإنابة القضائية، حيث يوجه هذا الطلب مباشرة من المحكمة المنيبة إلى المحكمة المنابة، وتتميز هذه الطريقة بأنها أكثر سرعة واشد فعالية ، وغالبا ما تتم هناك اتفاق قضائي بين الدولتين[1] .

وقد بين قانون الإجراءات الجنائية الفرنسي من خلال المادة 694 الأسلوب الذي يتوجب إتباعه، ففي حالة ما إذا طلبت السلطات القضائية الفرنسية المساعدة القضائية فانه يتوجب عليها تقديم الطلب عبر وزارة العدل إلى السلطة القضائية للدولة الأجنبية، أما في حالة ما إذا تلقت السلطات القضائية الفرنسية طلب المساعدة القضائية فان ذلك يتم عبر القنوات الدبلوماسية، وفي حالة الاستعجال يمكن أن تنتقل طلبات المساعدة التي تطلبها السلطات الفرنسية أو الأجنبية إلى سلطات الدولة المختصة، بشكل مباشر دون اللجوء إلى القنوات الدبلوماسية ما لم ينص أي اتفاق دولي على خلاف ذلك.

أما على صعيد مكافحة جرائم الإرهاب فقد جاءت الاتفاقية العربية لمكافحة جرائم الإرهاب مسايرة للأخذ بالطريقتين حيث نصت على أن يوجه طلب الإنابة القضائية من وزارة العدل في الدولة الطالبة إلى وزارة العدل في الدولة المطلوب منها، ويعاد بنفس الطريقة، وفي حالة الاستعجال يوجه طلب الإنابة القضائية مباشرة من السلطة القضائية في الدولة الطالبة إلى السلطات القضائية في الدولة المطلوب منها، وترسل صورة هذه الإنابة في نفس الوقت إلى وزارة العدل في الدولة المطلوب منها، وتعاد الإنابة مصحوبة بالأوراق المتعلقة بتنفيذها بالطريقة المنصوص عليها في البند السابق كما يمكن أن يوجه طلب الإنابة القضائية مباشرة من الجهات القضائية إلى الجهة المختصة في الدولة المطلوب منها، ويجوز أن تحال الردود مباشرة عن طريق هذه الجهة، وهو نفس الأمر الذي نصت عليه الاتفاقية الأوربية للمساعدة القضائية في المسائل الجنائية، حين نصت المادة 15 منها على أن طلبات الإنابة القضائية ترسل من وزارة العدل في الدولة الطالبة إلى وزارة العدل في الدولة المطلوب منها تنفيذ الإجراءات، ويتم إعادتها بالطريق ذاته[2]، وفي حالة الاستعجال فان طلبات الإنابة يتم إرسالها مباشرة عن طريق السلطات القضائية في الدولة الطالبة إلى السلطات القضائية للدولة

[1] عمر سالم، مرجع سابق، ص 85.

[2] عمار تيسير بجبوج، مرجع سابق، ص 347.

المطلوب منها التنفيذ، وتتم إعادة هذه الإنابات مصحوبة بالأوراق المتعلقة بالتنفيذ بالطرق العادية أي عن طريق وزارة العدل في الدولتين، كما يمكن تنفيذ هذه الإنابات عن طريق منظمة الشرطة الدولية[1] .

4. **أن لا تكون الجريمة موضوع الإنابة من الجرائم المستبعدة من نطاق الإنابات القضائية الدولية:** تنص اغلب القوانين الوطنية والاتفاقيات الدولية المتعلقة بالمساعدة القضائية عموما، والإنابات القضائية بشكل خاص على استبعاد بعض الجرائم من نطاقها التي نفسها الجرائم المستبعدة من نطاق تسليم المجرمين –كما سبق توضيحه في عنصر التسليم– كالجرائم السياسية والجرائم العسكرية .

وقد خلت الاتفاقية العربية لمكافحة جرائم الإرهاب من هذا الاستثناء حيث اكتفت في تحديد حالتين يجوز فيهما للدولة رفض طلب الإنابة القضائية، أولهما حالة ما إذا كانت الجريمة موضوع الطلب محل اتهام أو تحقيق أو محاكمة لدى الدولة المطلوب منها تنفيذ الإنابة، وثانيها إذا كان الطلب من شأنه المساس بسيادة الدولة المكلفة بتنفيذه أو بأمنها أو بالنظام العام فيها[2].

## رابعا: مجالات المساعدة المتبادلة الخاصة بمواجهة الجرائم المعلوماتية.

إن الطبيعة السريعة للجرائم المعلوماتية تجعل من الإجراءات الرسمية الواردة باتفاقات المساعدة القانونية المتبادلة القائمة تتسم بنوع من التعقيد والبطء، ومن اجل ذلك كان من اللازم استحداث وسائل أخرى للتعاون أكثر سرعة وفاعلية للتصدي لهذا النوع من الجرائم ومن هذه الوسائل اتفاقية بودابست المتعلقة بالجريمة الالكترونية2001، والاتفاقية العربية لمكافحة جريمة تقنية المعلومات لسنة 2010.

فبالإضافة إلى مجالات التعاون الدولية التي تضمنتها اتفاقيات التعاون القضائي الدولية والإقليمية، فقد تضمنت كل من اتفاقية بودابست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات بعض الصور لمجالات التعاون القضائي والتي تتناسب مع طبيعة الجرائم المعلوماتية.

**01– المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة:** وتشمل المجالات التالية:

[1] عمار تيسير بجبوج، مرجع سابق ، ص 347.

[2] المادة 10 من الاتفاقية العربية لمكافحة الإرهاب

### أ- التحفظ العاجل على بيانات الحاسوب المخزنة[1].

تناولت هذا الإجراء المادة 29 من اتفاقية بودابست والتي تقابلها المادة 37 من الاتفاقية العربية لمكافحة جريمة تقنية المعلومات، فهذه المساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي حسب المادتين السابقتين أمر ضروري تستلزمه طبيعة الأدلة في الجريمة المعلوماتية، وذلك لتفادي أي تغيير في هذه الأدلة، أو نقلها أو إتلافها ومحو أثار الجريمة، خلال المدة التي تستغرقها إجراءات طلب المساعدة المتبادلة للحصول على تلك البيانات بالطرق التقليدية والتحفظ هو إجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدية، بالإضافة إلى ما يتميز به هذا الإجراء من سرعة، فانه يعد أقل تدخلا حيث أن هذا الإجراء لا يتطلب من سلطات الدولة الموجه إليها طلب المساعدة نزع البيانات من الجهة القائمة عليها والاستحواذ عليها، وإنما مضمون هذا الإجراء أن تقوم هذه السلطات باتخاذ الإجراءات التي تضمن أن الجهة التي بحوزتها المعلومات موضوع طلب المساعدة، وهذه الجهة غالبا ما تكون مزود الخدمة أو شخص ثالث، ولا تقوم بمحو هذه البيانات لحين صدور تحويلها إلى سلطات إنفاذ القانون فيوقت لاحق.

كما يتسم هذا الإجراء أيضا بعدم مساسه بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب، فلا يتم كشفها ولا فحصها من قبل سلطات إنفاذ القانون إلا في بعض الحالات ووفقا للشروط المقررة قانونا بما يكفل حق الشخص المعني بالمعلومات في الخصوصية بسرية[2].

ومن خلال البند الثالث من المادة 29 من اتفاقية بودابست لم تستلزم كشرط مسبق لتبادل المساعدة في هذا المجال تحقيق مبدأ التجريم المزدوج بمعنى أن يكون الفعل المراد تبادل المساعدة بشأنه يشكل جريمة في النظام القانوني للدولتين، وذلك لان تطبيق هذا الشرط لن يكون منتجا في مواد التحفظ، إلا انه يوجد اتجاه نحو استبعاد قاعدة التجريم المزدوج بالنسبة لكل الوسائل الإجرائية ماعدا الأكثر تطفلا أو تدخلا في الحياة الخاصة كالتفتيش والتنصت، والتحفظ على البيانات والمعلومات المخزنة الكترونيا لا يعد – حسب راي واضعي الاتفاقية- من قبيل التطفل أو التدخل في الحياة

[1] هلالي عبد اللاه أحمد، (المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 279.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 105 .

الخاصة، حيث أن كل ما يفعله الحارس على البيانات أو القائم عليها هو المحافظة على تلك البيانات بأن تبقى في حيازته بشكل قانوني وان يحافظ عليها من المحو والإتلاف، وان لا يتم الكشف عنها أو فحصها من قبل سلطات الدولة مقدمة الطلب إلا بعد تقديم طلب المساعدة، ووفقا للإجراءات الرسمية بهدف الكشف عن سرية هذه البيانات والمعلومات، وحسب البند الرابع من المادة سالفة الذكر فانه يحق للدول الأطراف الحق في اشتراط أو التمسك بمبدأ التجريم المزدوج استثناء للرد على طلب المساعدة المتبادلة في هذا المجال، إلا أن هذا الاستثناء مقيد بالجرائم الواردة في المواد من 2 إلى 11 من اتفاقية بودابست[1]، أي أن هذا الاستثناء يمكن أن يطبق بالنسبة للحالات التي تكون فيها الجريمة مرتكبة باستخدام نظام معلوماتي أو بالنسبة للجرائم التي تكون فيها الجريمة لم ترتكب بواسطة نظام معلوماتي ولكن يمكن أن تكون محلا لجمع أدلة ذات شكل الكتروني، فالجرائم السابقة حسب هذه الاتفاقية تفترض أن شرط التجريم المزدوج قد تم استيفاؤه بطريقة آلية بين الطرفين[2].

### ب – الإفشاء العاجل لسرية بيانات المرور المتحفظ عليها.

هذا المجال من التعاون يكمل المجال السابق، فهو إجراء يظهر بمناسبته، وقد نصت على هذا الإجراء كل من المادتين 30 من اتفاقية بودابست والمادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وحسب هاتين المادتين فانه عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور المتعلقة بنقل الاتصال بواسطة مزودي الخدمة، فملا لو افترض أنه من خلال تتبع مصدر الاتصال لتحديد هوية مرتكب الجريمة أو تجميع الأدلة على ذلك، قد يكتشف أثناء ذلك أن بيانات المرور التي وجدت في إقليمه تشيـــر إلى أن الاتصال قد تم إرسالـــه من خلال مزود خدمات في إقليم دولة ثالثة أو حتى في إقليم الدولة مقدمة الطلب، فإنه في هذه الحالـــــة يجب على

[1] وهذه الجرائم هي جريمة الولوج غير القانوني والاعتراض غير القانوني، والاعتداء على سلامة البيانات، والاعتداء على سلامة النظام وإساءة استخدام أجهزة الحاسب ومعداته، والتزوير المعلوماتي والغش المعلوماتي والجرائم المتصلة بالمواد الإباحية، والجرائم المتصلة بالمواد الإباحية الطفولية، والجرائم الواقعة على الملكية الفكرية والحقوق المجاورة، والشروع والاشتراك ، بالإضافة إلى تجميع الأدلة تحت شكل الكتروني للجريمة الجنائية، المواد من 2 إلى 11 من اتفاقية بودابست.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 106 .

الدولة المقدم إليها الطلب أن تكشف للدولة الطالبة على القدر الكافي من البيانات من خط سير البيانات الذي يمكنه من التعرف على مزود الخدمة هذا، والمسار الذي سلكه الاتصال، وفي ذلك فائدة للدولة مقدمة الطلب حيث تتمكن من خلال هذه المساعدة معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن التحفظ على البيانات والمعلومات المخزنة في النظام المعلوماتي، وهكذا حتى يتم الوصول إلى المصدر الحقيقي للاتصال[1] .

## 02- المساعدة القضائية المتبادلة في مجال سلطات التحقيق.

وتشمل المجالات الآتية:

**أ- المساعدة المتبادلة الخاصة بالولوج إلى البيانات المعلوماتية المخزنة:** نصت على هذا النوع من المساعدة المادة 31 من اتفاقية بودابست، والتي تقابلها المادة 39 من الاتفاقية العربية لمكافحة جريمة تقنية المعلومات، وتتشابه هاتين المادتين مع البند "ج" من الفقرة الثانية من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والخاصة بتقديم المساعدة القانونية المتبادلة بمقتضى قوانين الدولة متلقية الطلب ومعاهداتها واتفاقاتها وترتيباتها ذات الصلة بشأن تنفيذ عمليات التفتيش والضبط والتجميد، وبمقتضى المادة 31 والمادة 39 السالفتي الذكر يحق لإحدى الدول الأطراف في الاتفاقية بمناسبة تحقيقات تجريها في جريمة ما إن تطلب من دولة طرف أخرى يقع على إقليمها النظام المعلوماتي تفتيش هذا النظام والدخول إليه والتحفظ أو مصادرة البيانات المخزنة بداخله لمصلحة الدولة مقدمة الطلب، تماما كما هو الحال بالنسبة لعمليات التفتيش والضبط التي تجريها الدولة المقدم إليها الطلب على البيانات والمعلومات المخزنة الكترونيا في النظم المعلوماتية الموجودة في إقليمها، وهو ما يفرض على الدول الأطراف أن تكون مؤهلة لتلبية تلك الطلبات من الناحية الفنية والتقنية، ووفقا للبند الثاني من المادة 31 السابقة فانه يسري بشان هذا الطلب الشروط المقررة في المعاهدات والاتفاقيات والتشريعات الوطنية المطبقة في هذا الخصوص[2] .

[1] هلالي عبد اللاه أحمد،(المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 279 ،280.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 160، 161.

**ب- الدخول عبر الحدود إلى البيانات المعلوماتية المخزنة بتصريح أو من خلال إتاحتها للجمهور:** يعد هذا المجال الذي تضمنته المادة 32 من اتفاقية بودابست والتي تقابلها المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من مجالات المساعدة القضائية المتبادلة أفرزته طبيعة الجرائم المعلوماتية، وقد أثار نص المادة 32 السالفة الذكر نقاش مطول بين واضعي هذه الاتفاقية قبل إقراره بحالته، حيث كان موضوع النقاش هو متى يكون مسموحا لأي دولة أن تدخل بشكل منفرد إلى بيانات ومعلومات مخزنة على إقليم دولة أخرى، ولقد توصلوا من خلال مناقشتهم لعدة حلول مختلفة إلى تحديد الحالات التي يمكن أن يقبل فيها الدخول بشكل فردي، وتلك التي لا يجوز أن تكون مقبولة، وفي الخير وصلوا إلى اتفاق مفاده ما نصت عليه المادة 32 من اتفاقية بودابست التي تضمن حالتين، الأولى عندما تكون المعلومات والبيانات التي تم الوصول إليها متاحة للجمهور أصلا، والثانية عندما يتم الوصول إلى هذه البيانات المخزنة خارج النطاق الإقليمي لدولة طرف أو تلقيها من خلال نظام معلوماتي يقع على إقليمه، وذلك بناء على موافقة قانونية أو إرادية من شخص يملك سلطة قانونية للكشف عنها[1] .

يعرف الشخص الذي يملك سلطة قانونية للكشف عن البيانات والمعلومات الالكترونية بأنه كل شخص طبيعي أو معنوي له كافة السلطات الممكنة بموجب قانون أو اتفاق على البيانات والمعلومات المخزنة الكترونيا بحيث يحق له استعماله واستغلاله والتصرف فيه[2] فإذا كان الأمر يتعلق بالتحقيق في جريمة إرهاب الكتروني، وكانت المعلومات المراد الاطلاع عليها مخزنة في نظام معلوماتي يقع خارج إقليم الدولة التي تجري التحقيق، ففي هذه الحالة يكون في مقدور هؤلاء الأشخاص استعادة البيانات شريطة أن يكون لديهم سلطة قانونية تخولهم ذلك، بالإضافة إلى سلطة الكشف عنها، وذلك بمحض إرادتهم لسلطات إنفاذ القانون، أو أن يسمحوا لهذه السلطات بالدخول إلى هذه البيانات، ويرى الدكتور محمد كمال محمود الدسوقي، أنه من باب احترام سيادة الدول والمجاملات الدولية ولتفادي أي إشكالية قد تثور بين الدول الأطراف بشان تفتيش نظام معلوماتي يقع على إقليم إحداهما أن يتم إضافة شرط بالنسبة للحالة التي تقوم فيها سلطات الدولة بالدخول إلى النظام المعلوماتي، الموجود في إقليم الدولة

[1] هلالي عبد اللاه أحمد،(المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 288.

[2] محمد كمال محمود الدسوقي، مرجع سابق، ص 162.

أخرى وتفتيشه وضبط ما بداخله من معلومات، ومفاد هذا الشرط إخطار الدولة التي يقع على إقليمها النظام المعلوماتي المراد تفتيشه، وإحاطتها علما بعملية الدخول وموافقة صاحب السلطة القانونية على تلك المعلومات والبيانات على ذلك[1] .

**ج- المساعدة المتبادلة بخصوص جمع بيانات المرور[2] في الوقت الفعلي:** في كثير من الأحيان قد لا يكون بإمكان سلطات التحقيق ضمان تتبع خط سير الاتصال للوصول إلى مصدر الاتصال لإتباع أثره من خلال التسجيلات الخاصة برسائل سابقة، وذلك نتيجة قيام مزود الخدمة بحذف بيانات المرور بشكل إلي من حلقات الاتصال التي تمر بها عملية نقل الرسالة، لذا فانه من الضروري بالنسبة لسلطات التحقيق في كل دولة أن يكون لديها القدرة على الحصول على بيانات المرور خلال الوقت الفعلي بالنسبة للاتصالات التي تمر من خلال نظام معلوماتي لدى دولة أخرى.

حسب نص المادة 33 من اتفاقية بودابست والتي يقابلها المادة 41 من الاتفاقية العربية لمكافحة جريمة تقنية المعلومات يكون كل طرف ملزم بتجميع خط سير البيانات بصورة عاجلة وفي الوقت الفعلي لمصلحة الطرف الآخر، ولما كان تجميع بيانات المرور بصورة عاجلة وفي الوقت الفعلي قد يكون الوسيلة الوحيدة الجوهرية لتحديد هوية مرتكب الجريمة المعلوماتية، وحيث أن هذا الإجراء اقل تطفلا أو تدخلا، فان الفقرة الثانية من المادة 33 سالفة الذكر قد استخدمت مصطلح "على الأقل" لجميع الدول الأطراف للسماح بأوسع نطاق ممكن للمساعدة المتبادلة بهذا الشأن حتى في ل غياب مبدأ التجريم المزدوج[3] .

**د- المساعدة المتبادلة في مسالة اعتراض بيانات المحتوى:** نصت المادة 24 من اتفاقية بودابست على أن الأطراف يقدمون المساعدة المتبادلة لبعضهم البعض فيما يتعلق بتجميع أو تسجيل محتوى البيانات بصورة عاجلة، والتي تتعلق باتصالات محددة يتم نقلها بواسطة نظام كمبيوتر وذلك بالحد الذي تجيزه الاتفاقيات والقوانين الوطنية واجبة التطبيق .

---

[1] محمد كمال محمود الدسوقي، مرجع سابق، ص 162.

[2] يقصد ببيانات المرور بيانات الكمبيوتر المتعلقة باتصال عن طريق منظومة كمبيوتر، والتي تنشأ عن منظومة كمبيوتر تشكل جزء من سلسلة اتصالات، توضح مصدر الاتصال، والوجهة المرسلة إليها، والطريق الذي تسلكه، ووقت وتاريخ وحجم ومدة ونوع الخدمة المذكورة، وهذا وفقا لما جاء في المادة الأولى من اتفاقية بودابست السالفة الذكر.

[3] محمد كمال محمود الدسوقي، مرجع سابق، ص 164 .

ونظرا لما يشكله هذا الإجراء من مساس بحقوق الأفراد في الخصوصية حيث أنه ينطوي على تجميع وتسجيل البيانات التي يتم نقلها بواسطة نظام معلوماتي معين، فقد تم تحديد الالتزام بتوفير المساعدة المتبادلة المتعلقة بهذا الخصوص، كما أنه يجب أن يكون تقديم المساعدة المتبادلة في الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة لدى الدول الأطراف[1] .

والملاحظ أن هذا الإجراء مماثل لمراقبة المحادثات والمراسلات السلكية واللاسلكية أو تسجيل الأحاديث المنصوص عليه في المادة الرابعة من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والذي تمت إحاطته بشروط أهمها أن يتم هذا الإجراء إذا كانت له فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس، وان يتخذ هذا الإجراء بعد إذن صادر من القاضي المختص وان يكون قرار ضبط المراسلات أو المراقبة أو التسجيل مسببا[2].

## المطلب الثاني: الوسائل الحديثة للتعاون الدولي لمكافحة الإرهاب الالكتروني.

أمام تطور الجريمة الإرهابية واستغلال الإرهابيين لشبكة الانترنت للقيام بهذه الجريمة لأنها الأقل تكلفة والأكثر ضمانا لإفلات الإرهابيين من العقاب، كما أنها الصورة الأكثر خطورة وفتكا بالأفراد والمجتمعات من صور الإرهاب التقليدية الأخرى، ومن أجل ذلك كان لزاما على مختلف الدول تطوير وسائل المكافحة والتعاون من اجل مكافحة وقمع هذه الجريمة الخطيرة لأن الطرق التقليدية أصبحت غير مجدية ولا فعالة في القضاء على هذا النوع المتطور من الجريمة الإرهابية.

وللتفصيل أكثر عن هذه الوسائل المتطورة في التعاون قسمنا هذا العنصر إلى فرعين فرع خصص للتحقيق الجنائي عن بعد، وفرع ثاني خصص لإنشاء قواعد البيانات الخاصة بالإرهاب.

[1] هلالي عبد اللاه أحمد، (المواجهة التشريعية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست)، مرجع سابق، ص 292 .

[2] رشيدة بوكر، مرجع سابق، ص374.

## الفرع الأول: التحقيق الجنائي عن بعد في جريمة الإرهاب الالكتروني.

اتجه مرفق العدالة الجزائية في الآونة الأخيرة إلى إرساء قواعد قانونية جديدة تواجه المشكلات التي أسفر عنها التطور التكنولوجي والمعرفي الكبير، وذلك من خلال الأخذ بمعطيات التكنولوجيا الحديثة في الكشف عن الجرائم وملاحقة مرتكبيها ومحاكمتهم، دون الإخلال في الوقت ذاته بحقوق المتهم أو غيره من أطراف الخصومة الجزائية. وتجلى ذلك بشكل واضح من خلال استخدام تقنية الاتصال المرئي المسموع "videoconference" في مجال التحقيق أو المحاكمة الجزائية عن بعد حيث تبنت العديد من دول العالم استخدام هذه التقنية، للمزايا والفوائد الكبيرة التي يمكن أن تحققها .

وقد شكل استخدام هذه التقنية مرحلة جديدة من مراحل تطور الإجراءات الجزائية، بشكل يعكس الرغبة في الاستفادة من المعطيات التكنولوجية الحديثة في مجالات تطوير مرافق العدالة الجزائية ويعتبر البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجزائية من أهم الاتفاقيات التي وضعت قواعد لاستخدام هذه التقنية في مجال التعاون الدولي في مكافحة الجريمة وهذا نظرا للدور الذي يمكن أن تلعبه هذه التقنية وإمكانية تسخيرها في التعاون الدولي في مكافحة الجريمة الإرهابية ومنها جريمة الإرهاب الالكتروني[1]، فما مفهوم التحقيق عن بعد، وما هي أهميته في مكافحة جريمة الإرهاب الالكتروني.

### 1 أولا: مفهوم التحقيق الجنائي عن بعد"Videoconference ".

إن تقنية الاتصال المرئي المسموع أو ما يعرف في اللغة الأجنبية بمصطلح "Videoconference" وهي: "وسيلة أو آلية حديثة لمباشرة إجراءات التحقيق أو المحاكمة الجزائية عن بعد، يتم الاستعانة بها، في بعض الحالات، لسماع شهادة الشهود والمتعاونين مع العدالة لكشف غموض الجرائم الخطيرة لاسيما المنظمة منها، بل وكذلك محاكمة المتهمين، رغم تواجدهم داخل المؤسسة العقابية، أمام محكمة قد تبتعد عن هذه المؤسسة أو تلك المؤسسات مئات الأميال"[2] .

[1] صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال"Videoconference"، مجلة علوم الشريعة والقانون، المجلد 42، العدد الأول، جامعة الأردن، 2015، ص 353.

[2] عادل يحيى، التحقيق والمحاكمة عن بعد، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006، 27.

استخدمت هذه التقنية لأول مرة في ايطاليا سنة 1992 بموجب المرسوم رقم 306 لسنة 1992 وقد قصرت المادة 147 مكرر والخاصة بتطبيق مواد الإجراءات الجزائية الايطالي التحقيق عن بعد في سماع الشهود فقط، وبعد ذلك اتسع نطاق تطبيقها نظرا للنتائج الايجابية التي حققتها، وذلك بموجب المرسوم رقم 11 لسنة 1998، لتشمل إجراءات محاكمة المجرمين الخطرين وهو داخل المؤسسات العقابية التي تقع في مكان بعيد عن قاعة المحكمة، وهذا دون المساس بحقوق الدفاع وانتقل استخدام هذه التقنية وتوسع فقد استخدمته الولايات المتحدة الأمريكية على المستوى الداخلي وكذلك في مجال المساعدة القضائية الدولية المتبادلة في المسائل الجنائية عند وجود اتفاقية دولية حيث توجد 94 نيابة من النيابات الفدرالية الأمريكية مجهزة بتقنية" Video conference " الحديثة.

كما أقرت بعض الدول ككندا واستراليا ونيوزلندا استخدام هذه التقنية في مجال محاكمة الأحداث وهذا لتفادي الأضرار النفسية التي قد تلحق بالأحداث جراء حضرهم الشخصي لجلسات المحاكمة، كما أقرت دولة بلجيكا استخدام هذه التقنية في إطار المساعدة القضائية الدولية في المجال الجنائي، لكنها لم تقر استخدامها على المستوى الداخلي[1]

فالتحقيق الجزائي وفقا لهذه الطريقة وباستخدام هذه الوسيلة التقنية المتطورة يعد خروجا على القاعدة العامة في جلسات التحقيق والمحاكمة والتي تتم في نطاق جغرافي واحد بخصوص المتهمين والشهود أو غيرهم من أطراف الخصومة، بحيث يكون لكل منهم دوره في سير جلسات المحاكمة أو التحقيق من خلال مشاركته فيها[2]، وباللجوء إلى استخدام تقنية ال" Video conference" في مجال التحقيق الجزائي أصبح من الممكن امتداد النطاق الإقليمي لجلسة التحقيق أو المحاكمة بحيث يشمل عدة أماكن إقليمية داخل الدولة الواحدة أو أماكن إقليمية في دول متعددة، وبحيث تكون سلطة التحقيق في دولة، والمتهم الذي يتم التحقيق معه في دولة أخرى، وقد يكون الشهود في دولة ثالثةً ومن الواضح أن هذه الوسيلة من الممكن أن تلعب دورا كبيرا ومهما في التعاون الدولي في مكافحة الجرائم بشكل عام وجرائم الإرهاب بشكل خاص وجريمة الإرهاب الالكتروني بشكل أخص لأنها الأكثر تطورا وتعتمد على نفس التكنولوجية التي يعتمد عليها التحقيق الجنائي هذا، إلا أنها تحتاج من الناحية الفنية والتقنية توافر شبكة اتصال مرئي ومسموع على مستوىٍ عال من التطور بين قاعة الجلسة التي تتم

[1] عادل يحيى، مرجع سابق، ص 16.

[2] صفوان محمد شديفات، مرجع سابق، ص 354.

فيها إجراءات التحقيق والمكان أو الأماكن التي يتواجد فيها المتهم أو الشهود، بحيث تؤمن الرؤية المتبادلة الواضحة والصوت الواضح دون انقطاع، ومن ثم فإن أي من الدول التي لا تتوافر فيها تلك التقنيات يحق لها رفض استخدام هذا النظام[1]، إلا إذا قامت الدولة الطالبة بوضع هذه التقنية بين يدي الدولة المنفذة ويمكن التمييز في هذا الصدد بين أربعة نظم مختلفة للتحقيق الجزائي عن بعد Videoconferenceوهي[2]:

**1) – نظام الاتصال من نقطة إلى أخرى.**

يتم بمقتضى هذا النظام الاتصال المباشر، المرئي والمسموع، بين قاعة المحكمة ومكان آخر يوجد فيه المتهم أو أحد الشهود، ويعد هذا النظام أبسط أنظمة الاتصال المرئي والمسموع وأقلها إثارة للمشكلات التقنية والفنية.

**2) –نظام السويتش أو المتحدث النشط.**

حيث تتعدد الأماكن التي يتم بينها الاتصال عبر الـ "Videoconference" ،كأن تكون المحكمة في دولة والشهود في دولة والمتهم في دولة ثالثة، ويتطلب هذا النظام أن يتم إعداد هذه الأماكن إعدادا تقنيا، بحيث يبدو هؤلاء الأطراف وكأنهم في مكان واحد، ولا تظهر شاشة العرض الموجودة في جميع هذه الأماكن، إلا صورة واحدة هي صورة الشخص الذي يتكلم سواء إلى القاضي أو المتهم أو الشاهد، وفي حالة تكلم أكثر من شخص في نفس الوقت فإن الاتصال المرئي المسموع يتم أوتوماتيكيا مع المكان الذي يوجد فيه الشخص صاحب الصوت الأعلى[3].

**3) نظام الحضور المستمر الثابت أو الموحد.**

ويتم الاتصال، وفقا لهذا النظام، بواسطة الـ "Videoconference"، بين خمسة أماكن مختلفة وبعيدة عن بعضها جغرافيا، والأماكن هي قاعة المحكمة التي تنعقد فيها جلسة المحاكمة، وأربعة أماكن أخرى يوجد فيها باقي أشخاص الدعوى من شهود ومتهمين وغيرهم.

[1] عمار تيسير بجبوج، مرجع سابق، ص 373.

[2] صفوان محمد شديفات، مرجع سابق، ص 355.

[3] سالم عمر، مرجع سابق، ص 176.

ويوجد في كل مكان شاشة عرض الغرض منها عرض الصورة إلى هؤلاء الأشخاص بالإضافة إلى أجهزة دقيقة يتم بواسطتها سماع صوت من يتكلم من المشاركين بهذه الجلسة.

**4) نظام الحضور المستمر المتقدم.**

وفق لهذا النظام يتم الاتصال المرئي المسموع الـ "Videoconference"بين القاعة الرئيسية التي تجري فيها إجراءات التحقيق، وبين عدد كبير من الأماكن الأخرى البعيدة عنها، ويعد هذا النظام من أحدث النظم التطبيقية لتقنية الـ"Videoconference" ،حيث يتم تزويد الأماكن التي تتطلب وجود هذه التقنية بشاشات عرض لصورة وأجهزة الصوت التي يتكلم من خلالها المشاركين.

ويتم تقسيم شاشة عرض الصور الموجودة في كل مكان من هذه الأماكن إلى أربعة أقسام، يتم تثبيت القسم الأول لعرض بانوراما عامة للقاعة التي تتم فيها المحاكمة، وقسمين آخرين في مكانين من الأماكن المتصلة بهذه القاعة، أما القسم الرابع من شاشة العرض فتنتقل آليا بصورة تلقائية إلى صورة الشخص الذي يشارك، ويتكلم بصوت أعلى من غيره من المشاركين في جلسة التحقيق أو المحاكمة.

**ثانيا:أهمية التحقيق الجنائي عن بعد.**

سبق القول أن إلى أن تقنية الـ "Videoconference" تمثل إحدى الوسائل الحديثة للتحقيق الجزائي، والتي اقتضتها ضرورة الاستعانة بالمعطيات التكنولوجية الحديثة، بغية تطوير أداء مرفق العدالة الجزائية ودعم وإضافة وسيلة جديدة إلى وسائل التعاون الدولي في مكافحة الإجرام الخطير بما فيه جريمة الإرهاب الالكتروني الخطيرة، وتتجلى أهمية هذه التقنية فيما يلي[1]:

**1. سرعة الإجراءات وخفض النفقات.**

تتجه العديد من التشريعات الجزائية الحديثة، من خلال الاتفاقيات الدولية، إلى تعزيز التعاون الدولي في مكافحة الجرائم، من خلال اتخاذ التدابير التشريعية والعملية لرفع كفاءة أجهزة العدالة الجناية وتطوير أدائها.

وتمثل الاستعانة بالوسائل التكنولوجية الحديثة في ميدان البحث والتحقيق الجزائي أحد أهم هذه التدابير في جميع مراحل الدعوى الجزائية، وتعد تقنية "Videoconference" وسيلة هامةُ من وسائل التحقيق والمحاكمة الجزائية لما لها من دور كبير في تبسيط وتسريع إجراءات العدالة الجزائية.

[1] عادل يحيى، مرجع سابق، ص 37.

فإذا ما تمت المقارنة ما بين إجراءات التحقيق عن بعد عبر الـ "Videoconference"مع إجراءات الإنابات القضائية مثلا يلاحظ أن الإنابة القضائية تتسم بالبطء والتعقيد، حيث يتم إرسالها عبر الطرق الدبلوماسية في الدولة المطلوب فيها التنفيذ، ومن ثم إلى وزارة العدل فالمحكمة المختصة ومن ثم العودة بذات الطريق حتى تصل إلى الجهة القضائية في الدولة الطالبة، وهذا كله يتصف بطول الإجراءات وزيادة التكاليف[1]، وطول هذه الإجراءات قد يؤدي إلى الإفراج عن المهتمين المحبوسين إذا لم تتم محاكمتهم خلال مدة محددة احتياطي.

لذلك فاللجوءً إلى التحقيق عن بعد قد يحول دون طول هذه الإجراءات ومن ثم تجنب الإفراج عن المتهمين لانتهاء المدة الواجبة في الحبس المؤقت، زيادة على ذلك فان نقل المتهمين من أماكن فضلا على أن نقل المتهمين من أماكن الاحتجاز إلى الأماكن التي تنعقد فيها جلسات التحقيق أو المحاكمة تؤدي إلى زيادة النفقات التي تترب على ذلك.

فالتحقيق عن طريق الـ "Videoconference" يوفر عناء الإجراءات ويخفف من النفقات حيث تكفل هذه التقنية حقوق الدفاع المقررة للمتهم، من خلال السماح له برؤية وسماع ومناقشة سلطة التحقيق أو هيئة المحكمة وسائر الخصوم والشهود، بما يحقق قاعدتي شفوية المرافعة والمواجهة بين الخصوم، كما تساهم هذه التقنية في التحقيق الجنائي في الوقت نفسه في الحد من نفقات وعناء نقل المتهمين من أماكن احتجازهم إلى أماكن جلسات التحقيق أو المحاكمة[2].

كما أن الدول التي تمتنع عن تسليم مواطنيها للتحقيق أو المحاكمة يمكنها السماح لمواطنيها بالإدلاء بشهاداتهم أو مواجهتهم بالتهم المنسوبة إليهم عن طريق هذه التقنية[3].

## 2. تعزيز الوسائل المتبعة في التعاون الدولي لمكافحة الجريمة.

تقنية الاتصال المرئي "Videoconference" تعد وسيلة مستحدثة وإضافية من وسائل التعاون الدولي في مكافحة الجرائم والمساعدات القضائية المتبادلة بين الدول، ولا سيما في مجال استجواب المتهمين وسماع الشهود عندما يكونون مقيمين في إقليم دولة غير تلك الدولة التي تقوم بالتحقيق أو المحاكمة.

[1] سالم عمر، مرجع سابق، ص 185.

[2] صفوان محمد شديفات، مرجع سابق، ص 355.

[3] عادل يحيى، مرجع سابق، ص 54.

حيث يكفل اللجوء إلى هذه التقنية الوصول إلى حل توافقي للمشكلات الناتجة عن اختلاف النظام الإجرائي للدولتين الطالبة والمطلوب منها التنفيذ، على اعتبار أنه سوف يكون هناك قانون واحد واجب التطبيق هو قانون الدولة الطالبة، التيً تباشر الإجراءات وفقا لما هو منصوص عليها في قانونها[1].

### 3. حماية الشهود والمجني عليهم.

تتجلى أهمية تقنية الـ "Videoconference" باعتباره إحدى الوسائل الفعالة التي تضمن حماية أطراف النزاع أو الدعوى القضائية كالشهود والمجني عليهم وأي شخص آخر من الأشخاص المتعاونين مع العدالة، حيث يرى بعض الباحثين والكتاب ضرورة استخدام هذه التقنية في سماع الشهود والمتهمين التائبين المتعاونين مع العدالة، لكي يتم الحصول على إفاداتهم المتعلقة بالعصابات الإجرامية المنظمة أو الجماعات الإرهابية المسلحة حول مخططاتهم الإجرامية المستقبلية وغيرها من المعلومات التي تفيد العدالة الجزائية في القبض عليهم.

فتستخدم هذه التقنية لعدم كشف هذه الجماعات الإجرامية لأماكن تواجد الشهود وتحركاتهم وذلك حماية لهم من الانتقام الذي قد يتعرضون له، كما تتجه بعض التشريعات الجزائية الحديثة إلى استخدامها في مجال التحقيق والمحاكمات الجزائية الخاصة بالأحداث القاصرين وذلك لتفادي الآثار النفسية الضارة التي تصاحب حضور القاصر بشخصه لجلسات المحاكمة وأمام الجميع[2]، وهو ما تقوم به كل من كندا وأستراليا ونيوزيلندا.

وتجدر الإشارة في هذا الشأن إلى أن النظام الأساسي للمحكمة الجزائية الدولية قد سمح أن يتم إجراء التحقيق أو سماع الشهود بوسائل غير المواجهة المباشرة وجها لوجه، في إشارة إلى إمكانية استخدام تقنية ال "Videoconference"، وذلك حرصا على سلامة الشهود أو المتهمين، حيث نصت المادة 68 في فقرتها الثانية على أنه:" استثناء من مبدأ علنية الجلسات المنصوص عليه في المادة 67 لدوائر المحكمة أن تقوم– حماية للمجني عليهم والشهود أو المتهم – بإجراء أي جزء من المحاكمة في جلسات سرية أو بالسماح بتقديم الأدلة بوسائل إلكترونية أو بوسائل خاصة أخرى، وتنفذ

[1] صفوان محمد شديفات، مرجع سابق، ص 356.

[2] عادل يحيى، مرجع سابق، ص 59.

هذه التدابير بشكل خاص في حالة ضحية العنف الجنسي أو الطفل الذي يكون مجنيا عليه أو شاهدا ما لم تأمر المحكمة بغير ذلك مع مراعاة كافة الظروف ولاسيما آراء المجني عليه أو الشاهد"[1]

وعلى الرغم من المزايا العديدة التي تقدمها هذه التقنية في ميدان التحقيق والمحاكمة فإن بعض الفقه يرى أنها لا تخلو من أوجه القصور كغيرها من الوسائل التي يستعان بها في التحقيق الجنائي ومحاولة الوصول إلى الحقيقة، فمن ناحية أولى قد لا توفر هذه التقنية مستوى عالي من الواقعية والجدية في مجال التحقيق، فمن أهم الأمور التي يمكن أن يستفيد منها القاضي لكشف الحقيقة، هي تقييم لغة الجسد وطريقة التعبير لدى الشاهد أو المتهم فلا يستطيع القاضي أن يستنبط ردة فعل المستجوب على سؤال معين قد يكون محرجا بالنسبة له، حيث إن استخدام هذه التقنية تمنح المتهم فاصلا زمنيا حتى يستوعب السؤال ويقدم الإجابة عليها.

وزيادة عن كل ما سبق فان هذه التقنية لا تسمح لأطراف المحاكمة بالقيام بمداخلات متكررة بشكل مريح وسلس كما هو الحال في الجلسات العادية، مما يخدش النزاهة في الإجراءات، ويشكك في دستوريتها في بعض الحالات التي لا تتوفر فيها كامل الاحتياجات المتعلقة بسير الدعاوى[2].

## ثالثا: قواعد التحقيق والمحاكمة عن بعد عبر الـVideoconference .

بتوقيع الدول الأوروبية على البروتوكول الإضافي الثاني للاتفاقية الأوربية للمساعدة المتبادلة في المسائل الجزائية في ستراسبورغ في 2001/11/08 ودخلت حيز النفاذ في 2004/02/01 سعت إلى توسيع نطاق آليات ووسائل التعاون القضائي فيما بينها بغية الاستفادة من الإمكانيات والوسائل التكنولوجية الحديثة في التحقيق والبحث الجزائي، بحيث تكفل سرعة أكبر ومرونة أعلى وفاعلية أشد لهذا التعاون، وبما لا يتعارض مع حقوق الإنسان وسيادة القانون، وبهدف ضمان مواجهة قانونية وقضائية فعالة[3]، وسريعة للجرائم الخطيرة التي باتت تهدد الدول الأوربية ومنها جريمة الارهاب التي تفاقمت خاصة في السنوات الأخيرة.

[1] عمار تيسير بجبوج، مرجع سابق، ص 377.

[2] صفوان محمد شديفات، مرجع سابق، ص 356.

[3] Tokson, Matthew J., Virtual Confrontation: Is (5) Videoconference Testimony by an Unavailable Witness Constitutional?, University of Chicago Law Review, Vol 74, No 4, June 11, 2007, 1613.

وقد تم تبني الإنجازات التكنولوجية في هذه الاتفاقية تلبية لاحتياجات المساعدة القضائية في المسائل الجزائية، وأهم هذه المظاهر تجلى في اللجوء إلى تقنية الاتصال المرئي والمسموع ال "Videoconference".

وقد تضمنت المادتان التاسعة والعاشرة من البرتوكول الإضافي بيانا تفصيليا لكيفية استخدام هذه التقنية، بحيث جاءت بحلول تفصيلية للعديد من المشكلات العملية والقانونية التي قد تعترض استخدامها في مجال التحقيق الجزائي، مراعية تحقيق التوازن بين كفالة فعاليتها في المساعدة والتعاون القضائي بين الدول الأوروبية من جهة، وبين حماية الحريات والحقوق التي تمنحها القوانين الوطنية والدولية للأفراد[1] .

ومن خلال التعرض إلى هذا البروتوكول سوف يتم توضيح شروط تطبيق هذه التقنية وكذلك الإجراءات المتبعة في تطبيقها، كما نتعرض لأهم تطبيقاتها في مكافحة جرائم الإرهاب ومنها جريمة الإرهاب الالكتروني، كما يلي:

## أ- شروط تطبيق تقنية ال "Videoconference" في البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجزائية.

تضمنت المادة التاسعة من البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية المتبادلة في المسائل الجزائيةً شروطا معينة يتوجب التقيد بها عند استخدام تقنية ال**"Videoconference"** في التحقيق الجزائي الدولي، حيث استلزمت عدم تعارض استخدامها مع المبادئ الأساسية لقانون الدولة المنفذة، كما يتوجب توفير الإمكانيات الفنية التي تمكنها من استخدام هذه التقنية، وحصر استخدامها في مجال سماع الشهود والخبراء.

[1] صفوان محمد شديفات، مرجع سابق، ص 356.

### 1. عدم تعارض استخدام تقنية ال "Videoconference"مع قانون الدولة المطلوب منها التنفيذ.

اشترطت الفقرة الثانية من المادة التاسعة من البروتوكول الإضافي ألا ينطوي استخدام هذه التقنية على تعارض مع المبادئ الأساسية في الدولة المنفذة، ومن ثم فإن للدولة رفض الاستخدام إذاً قدرت أنه يؤدي إلى إهدار المبادئ الأساسية لقانونها[1] .

فاستخدام هذه التقنية في سماع شاهد أو خبير أو استجواب متهم يتواجد في إقليم الدولة المنفذة، وهو في الأصل مباشرة لاختصاص قضائي يدخل في اختصاص تلك الدولة، ومن ثم فإن مباشرة دولة أخرى لهذا الاختصاص عن طريق التحقيق الجزائي عن بعد بواسطة ال **"Videoconference"** يستوجب موافقة الدولة المنفذة التي يوجد فيها الشخص المطلوب منه الإدلاء بأقواله، ولهذه الدولة أن تقدر مدى تعارض هذا الإجراء مع المبادئ الأساسية لقانونها الداخلي[2]

### 2. توافر الوسائل والإمكانيات التي تمكن الدولة المنفذةً من استخدام هذه التقنية.

تشترط الفقرة الثانية من المادة التاسعة من البروتوكول الإضافي الثاني للاتفاقية الأوروبية الجديدة للمساعدة القضائية، لاستخدام تقنية ال **"Videoconference"** في مجال التحقيق الجزائي عن بعد أن تتوافر لدى الدولة المطلوب منها التنفيذ الإمكانيات والوسائل الفنية التي تمكنها من ذلك، وفي حال عجزها عن توفير تلك هذه الإمكانيات وتلك الوسائل يمكن لها أن ترفض استخدام هذه التقنية[3] .

---

[1] Article 9 - 2: The requested Party shall agree to the (25) hearing by video conference provided that the use of the video conference is not contrary to fundamental principles of its law and on condition that it has the technical means to carry out the hearing. If the requested Party has no access to the technical means for video conferencing, such means may be made available to it by the requesting Party by mutual agreement, http://conventions.coe. int/Treaty/en/Treaties/Word/ 182.doc,(26/06/2018 13:58. )

[2] عادل يحيى، مرجع سابق، ص 97.

[3] سالم عمر، مرجع سابق، ص 197.

فقد يكون في استخدام تقنية ال **"Videoconference"** في مجال التحقيق الجزائي في بعض الأحيان مكلف نسبيا للدولة المطلوب منها التنفيذ، من حيث توفير المعدات اللازمة لذلك، مما ينطوي عليه نفقات مالية باهضة[1].

وفقد أجازت الاتفاقية للدولة الطالبة في حال عجز الدولة المطلوب منها التنفيذ من توفير الإمكانيات الفنية والتقنية اللازمة لاستخدام هذه الوسيلة أن تعرض عليها المساعدة في توفير ما يلزم من معدات أو خبرات لاستخدام هذه التقنية سواء على سبيل الإعارة أو الهبة.

### 3. حصر استخدام هذه التقنية في مجال سماع الشهود ثالث والخبراء.

يقتصر استخدام تقنية ال **"Videoconference"** وفقا للمادة العاشرة من الاتفاقية الأوروبية الجديدة للمساعدة القضائية، على سماع الشهود وإفادات الخبراء، حيث يمكن للسلطات القضائية لإحدى الدول المتعاقدة طلب سماع شخص يتواجد على إقليم دولة متعاقدة أخرى – بصفته شاهد أو خبير– عبر هذه التقنية متى ثبت استحالة أو عدم ملائمةً مثول هذا الشخص بنفسه أمامها.

والملاحظ أن واضعوا الاتفاقية أرادوا من خلال هذا الشرط أن يحصروا استخدام هذه التقنية في الإجراءات التي لا تثير الكثير من المشكلات القانونية، كما يتبين أيضا انه من خلال نص الفقرة الأولى من المادة العاشرة، أن اللجوء لتقنية ال **"Videoconference"** في التحقيق الجزائي يتم بصورة احتياطية لا أصلية، فنص هذه المادة يحظر استخدامها إلا في الحالات التي يثبت فيها عدم ملاءمة انتقال الشاهد أو الخبير إلى الدولة الطالبة للمثول أمام سلطاتها القضائية.

ومفاد ذلك انه يجوز وفقا لهذه الاتفاقية انتقال الشهود أو الخبراء إلى الدولة الطالبة متى اقتضى ذلك، وضمن الشروط التي وضعتها المادة الثانية عشر من الاتفاقية الأوروبية للمساعدة القضائية الموقعة سنة 1959، والتي تنص على عدم جواز ملاحقة الأشخاص أو احتجازهم أو فرض أي قيود أخرى على حريتهم الشخصية في إقليم الطرف الطالب، وذلك بالنسبة للأفعال أو أحكام الإدانة السابقة لمغادرته إقليم الدولة متلقية الطلب[2].

ومن ثم فإن التحقيق عن بعد عبر ال **"Videoconference"** هو وسيلة احتياطية يمكن اللجوء إليها إذا تعذر اللجوء إلى استدعاء الشخص المطلوب أو إرسال إنابة قضائية للسلطة القضائية

[1] صفوان محمد شديفات، مرجع سابق، ص 357.

[2] المادة 12 من الاتفاقية الأوربية للمساعدة القضائية 1959/04/20 متوافرة في الموقع: . http://conventions.coe.int/Treaty/en/Treaties/Wor d/030.doc

في الدولة المطلوب منها لسماع الشهادة نيابة عنها، ومن ثم إرسال نتائج الإنابة مرة أخرى للدولة الطالبة.

فعند استنفاد هاتين الوسيلتين وعدم إمكانية استخدامهما في التحقيق، يجوز للسلطات القضائية أن تطلب القيام بهذا التحقيق عبر هذه التقنية الحديثة[1]

## ب- إجراءات تطبيق تقنية ال "Videoconference" كوسيلة للتحقيق الجزائي في البروتوكول الإضافي الثاني للاتفاقية الأوروبية للمساعدة القضائية في المسائل الجزائية.

نصت البروتوكول الإضافي الثاني للاتفاقية الأوربية للمساعدة القضائية في المسائل الجزائية على إجراءات معينة يتوجب على الدول الأطراف الالتزام بها، لتطبيق هذه التقنية الحديثة في مجال التحقيق الجزائي عن بعد، سواء من قبل الدولة الطالبة، أو من قبل الدولة المطلوب منها التنفيذ، النحو التالي:

### 3. إجراءات السلطة القضائية في الدولة الطالبة.

يتوجب على السلطات القضائية في الدولة الطالبة أن تلتزم في حال رغبت في مباشرة إجراء تحقيق جزائي عبر ال **"Videoconference"** أن تقدم طلب للدولة التي يتواجد على إقليمها الأشخاص المطلوب سماعهم أو استجوابهم.

ويجب أن يشتمل الطلب على اسم السلطة مقدمة الطلب وكذلك موضوعه وسببه وتحديد هوية الشخص المطلوب التحقيق معه أو استجوابه وجنسيته، والتهمة الموجهة له، مع عرض مختصر للوقائع، وعند الاقتضاء يتعين ذكر اسم وعنوان الجهة الموجه إليها الطلب كما أوجبت الفقرة الثالثة من المادة التاسعة أن تبين في الطلب السبب الذي استندت إليه في اعتبار أن انتقال الشهود أو الخبراء إليها مستحيل أو غير مرغوب فيه، واسم السلطة القضائية ومن الأشخاص الذين سيتم إجراء جلسة ال **"Videoconference"** معهم[2] .

[1] سالم عمر، مرجع سابق، ص 194.

[2] الفقرة الأولى من المادة 14 من الاتفاقية الأوروبية للمساعدة القضائية الموقعة عام 1959.

وبعد إتمام الإجراءات المتعلقة بالطلب المقدم، تباشر السلطات القضائية في الدولة الطالبة إجراءات التحقيق الجزائي، سواء بنفسها أو تحت إشرافها، والتي تتمثل في سماعً الشهود أو إفادات الخبراء أو استجواب المتهم وذلك وفقا لقانونها الوطني[1].

وتقع جميع النفقات المالية اللازمة لوضع هذه التقنية موضع التطبيق الفعلي على عاتق الدولة الطالبة، حيث تتحمل هذه الدولة النفقات المالية، وكذلك أجور المترجمين والتعويضات التي يتم دفعها للشهود والخبراء ومصاريف انتقالهم داخل الدولة المنفذة، فإذا ما تحملت هذه الأخيرة أي جزء من النفقات، كان لها الرجوع إلى الدولة الطالبة لتعويضها بكل ما تكبدته من مصاريف[2].

### 4. إجراءات السلطة القضائية في الدولة المطلوب منهاً التنفيذ.

تلتزم السلطة القضائية التي رفع إليها طلب تنفيذ إجراء ال **"Videoconference"**بإخطار الشاهد أو الخبير أو المتهم بهذا الطلب، وذلك بهدف تنفيذه في الموعد المحدد، ويتم هذا الإخطار وفقا للإجراء أو الشكل الذي ينص عليه قانون الدولة المطلوب منها التنفيذ وليس قانون الدولة الطالبة[3].

ويتعين حضور ممثل الدولة المنفذة في المكان الذي يتواجد فيه الشخص الذي يتم سماعه أو استجوابه بواسطة السلطات القضائية للدولة الطالبة، وكذلك إحضار مترجم متى دعت الحاجة إلى ذلك، حيث يقتصر دور ممثل السلطة القضائية للدولة المنفذة على التأكد من شخصية الشاهد أو الخبير أو المتهم، وضمان احترام المبادئ الأساسية لقانون الدولة المنفذة، وبالتالي لا يحق له توجيه الأسئلة أو الاستجواب أو إبداء الملاحظات[4].

وفي حال اتضح له عدم احترام المبادئ الأساسية للقانون، كان له اتخاذ الإجراءات اللازمة حتى يتم توافق إجراءات التحقيق مع تلك المبادئ.

كما تلتزم السلطة القضائية في الدولة المنفذة، عقب الانتهاء من سماع شهادة الشاهد أو إفادة الخبير أو استجواب المتهم من قبل السلطة القضائية للدولة الطالبة، إعداد محضر يتضمن، تاريخ ومكان انعقاد الجلسة، وهوية الشخص الذي تم سماع أقواله، وهويات بقية الأشخاص الذين شاركوا في

[1] صفوان محمد شديفات، مرجع سابق، ص 358 .

[2] سالم عمر، مرجع سابق، ص 204.

[3] صفوان محمد شديفات، مرجع سابق، ص 357.

[4] عادل يحيى، مرجع سابق، ص 104.

الجلسة، والظروف التقنية التي تم فيها اتخاذ الإجراء، ويتم إحالة هذا المحضر إلى السلطة القضائية في الدولة الطالبة[1].

## ج- إمكانية تطبيق تقنية التحقيق الجزائي عن بعد في مكافحة جرائم الإرهاب الالكتروني.

لم تستخدم تقنية ال **"Videoconference"** بشكل واسع فيما يتعلق بالتعاون القضائي في مكافحة جرائم الإرهاب، ولعل حادثة اغتيال الوزير البلجيكي Cools Andre هي أشهر الحوادث الإرهابية التي استخدمت فيها هذه التقنية للتحقيق والمواجهة مع المتهمين.

فمن المعروف أن الاعتداء على الأشخاص المتمتعين بحماية دولية، حسب اتفاقية منع ومعاقبة الجرائم الموجهة ضد الأشخاص المحميين دوليا الموقعة في نيويورك عام 1973 تمثل إحدى صور الإرهاب التي جرمتها الاتفاقية، وقضت بأن تجرم كل دولة طرف الاعتداء على شخص يتمتع بحماية دولية بالقتل عمدا، أو بالاختطاف، أو الهجوم على شخصه أو مس بحريته، أو ارتكاب هجمات خطرة على أماكن عمله الرسمية، أو على مراسلاته الخاصة، أو وسائل تنقله، أو التهديد بالقيام بتلك الهجمات أو محاولة القيام بها، وبأن تجعل تلك الأفعال مستوجبة لعقوبات مناسبة تأخذ في الاعتبار طبيعتها الخطرة واعتبار من يهدد بتلك الهجمات أو يحاول القيام بهاً شريكا في تلك الاعتداءات[2].

وبالاستناد إلى ما سبق فإن حادثة اغتيال رئيس الحزب الاشتراكي الوزير البلجيكي "Cools Andre " سنة 1991، وتمثل جريمة إرهابية حسب هذه الاتفاقية، وقد ألزمت المادة الثامنة منها الدول الموقعة على اعتبار هذا النوع من الجرائم جرائم تستوجب التسليم، لكن مع مراعاة الأحكام الإجرائية والشروط الأخرى المنصوص عليها في قانون الدولة التي يقدم إليها الطلب[3] .

وقد توصلت سلطات التحقيق البلجيكية إلى أن بعض المتهمين في هذه القضية هم من الرعايا التونسيين الذين غادروا البلاد وقبض عليهم بالفعل في تونس، واعترفوا بارتكاب الجريمة، ولما كان الدستور التونسي يحظر تسليم المواطنين، فقد كان من المستحيل على السلطات التونسية أن تستجيب لطلب السلطات البلجيكية، فلم يتم تسليمهم إليها، ونظرا لوجود بعض المشتبه في مشاركتهم هذه الجريمة في بلجيكا، فقد أرادت السلطات القضائية البلجيكية إجراء مواجهة بين المتهمين التونسيين

[1] المادتين 5 و6 من الاتفاقية الأوروبية للمساعدة القضائية.

[2] المادة الثانية من اتفاقية الجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية، الموقعة في نيويورك عام 1973.

[3] صفوان محمد شديفات، مرجع سابق، ص 359.

وهؤلاء المشتبه فيهم، ولم يكن أمامهم سوى اللجوء إلى تقنية التحقيق عن بعد عبر ال **"Videoconference"** لإجراء هذه المواجهة وبالفعل تم ذلك بين المتهمين رغم اختلاف أماكن تواجدهم[1] .

وهذا إن دل، فإنما يدل على أنه يمكن أن تكون هذه الوسيلة الحديثة إحدى الوسائل الفعالة والبديلة للوسائل التقليدية كالإنابات القضائية، أو طلب استجواب الشاهد أو المتهم في ا لاعتباراتً ا ما يواجه بالرفض نظرً البلد الطالبة له، والذي غالب السيادة، فتسهم هذه الوسيلة بشكل كبير في التعاون القضائي بين الدول في مجال كشف الجرائم الإرهابية ومعاقبة مرتكبيها.

وفي الأخير يمكن القول انه بما انه أمكن للدول الأوربية تطبيق هذه التقنية على جريمة الإرهاب التقليدية فمن المؤكد إمكانية تطبيقها على جريمة الإرهاب الالكتروني وهذا لما تحققه هذه التقنية من السرعة في إجراءات التحقيق والمحاكمة الجزائية نتيجة التقدم العلمي الهائل في مجال تقنيات المعلومات ، وأضحى من الصعوبة بمكان الاستغناء عن خدمات الانترنت اللامحدودة، وبما أن بعض الأشرار استغلوا المخترعات العلمية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المستحدثات أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الآخرين على وجه الخصوص، بصورة أدت إلى بزوغ فجر ظاهرة إجرامية جديدة، بجريمة الإرهاب الالكتروني، وبالتالي فلا بد من مواجهة هذا التطور بأنظمة متطورة من اجل السرعة في اكتشاف المجرم ومعاقبته من خلال التحقيق عن بعد عن طريق ال **"Videoconference"** عند تعذر النيابة العامة عن خصوصا الانتقال إلى مكان يبعد عن مكان التحقيق أو مواجهتها لصعوبة في ذلك[2].

## الفرع الثاني: إنشاء قواعد البيانات الدولية الخاصة بجريمة الإرهاب الدولي والإرهاب الالكتروني .

إن هذا الإجراء يشمل جميع أنواع وصور الجرائم الإرهابية ويبدأ حصر هذه البيانات انطلاقا من جريمة الإرهاب الدولي وصولا للإرهاب الالكتروني كأحدث صورة للجرائم الإرهابية بل وأخطرها.

[1] سالم عمر، مرجع سابق، ص 184 .

[2] نفس المرجع، ص 185.

وقد فرضت قواعد البيانات المتعلقة بالإرهاب ومنها الإرهاب الالكتروني نفسها بقة في عصر المعلوماتية باعتبارها تكنولوجيا حديثة تهدف إلى استخلاص المعلومات المخبأة حول أي جريمة ومكافحتها، نظرا لمل تحتويه من معلومات مهمة للغاية بالنسبة لأجهزة إنفاذ القانون الوطنية الملقى على عاتقها عبء مكافحة الجرائم.

وبالفعل نجحت العديد من الدول وخاصة الأوربية وكذلك المؤسسات الأكاديمية من إنشاء قواعد خاص بمكافحة الإرهاب، غايتها جمع أكبر قدر ممكن من المعلومات بغية اكتشاف الأنماط الحقيقية والمستحدثة لهذه الجريمة وتحليل اتجاهاته وكشف أسبابه وعواقبه ورسم السياسات اللازمة للوقاية منه وبيان مدى نجاح تلك السياسات[1] .

وتتجلى أهمية إنشاء هذه القواعد بأنها توفر للمؤسسات وأجهزة الأمن في جميع المجالات القدرة على بناء التنبؤات المستقبلية واستكشاف والسلوك والاتجاهات، مما يسمح بتقدير القدرات الصحيحة واتخاذها في الوقت المناسب.

فبعد الحادي عشر من سبتمبر عام 2001 تفجرت موجة عارمة من الإرهاب الدولي لم تقتصر علي استهداف الدول الغربية بل تعدتها لتطال أيضًا الدول العربية والإسلامية وتلا ذلك انقسام عميق في المجتمع الدولي حول تعريف الإرهاب الدولي فعلى الرغم من أن الأفعال الإرهابية تشمل تهديدًا لأمن وسلامة واستقرار المجتمع الدولي والعالمي وعاملًا من عوامل التوتر في العلاقات الدولية مما يجعل من الضروري اعتبار هذه الأفعال بمثابة جرائم دولية ضد أمن وسلامة البشرية إلا أنه ما زال هناك تباين شديد في وجهات النظر بين أعضاء المجتمع الدولي حول تعريف المقصود بمصطلح الإرهاب الدولي .

وليس هذا وحسب بل إنها لم تحرز أي تقدم نحو تعريف الإرهاب الدولي أو التوصل إلى اتفاق بشأن مواجهة الأعمال الإرهابية ومكافحتها فقد تضمنت قرارات الجمعية العامة للأمم المتحدة ذات الصلة عبارات عامة لا يمكن بموجبها التوصل إلى صيغة مشتركة لتوحيد الإجراءات التي يجب

[1] ذياب بن موسى البداينة، مرجع سابق، ص 2.

اتخاذها في مواجهة الإرهاب– على النحو الذي تم توضيحه سابق– ولعل ذلك يرجع إلى التباين الشديد في وجهات نظر الدول فيما يتعلق بالجوانب القانونية للإرهاب الدولي وعدم اتفاقها على العناصر المكونة لتلك الجريمة[1].

ورغم الدعوات المتكررة التي صدرت من معظم العواصم العالمية ورغم أن الإرهاب بات يهدد كل القوى الكونية دون استثناء فإن أي مؤتمر جدي لمكافحة الإرهاب على المستوى الدولي لم ينجح في الالتئام لأن عواصم صناعة القرار في العالم أغرقت نفسها عن عمد في لعبة المفاهيم بحيث مزجت ما بين المقاومة وما بين الإرهاب رغم أن الفارق بينهما واضح ولا يحتاج لكثير من الدلائل أو من البراهين[2].

وانطلاقا من هذه الحقائق، وحرصا على ضرورة تظافر الجهود الدولية للتصدي للإرهاب واقتلاعه من جذوره ومنع أسباب استفحاله وتجفيف مصادر تمويله، ودعت المملكة العربية السعودية إلى عقد مؤتمر دولي لمكافحة الإرهاب تعزيزا للمساعي الدؤوبة لمواجهة الإرهاب عبر بلورة جهود واسعة النطاق تشمل العديد من الدول المتضررة منه وتبادل الآراء والخبرات والتجارب، والخروج بالتوصيات والمقترحات المناسبة لمواجهة هذه الآفة الخطيرة.

وقد تقدمت المملكة العربية السعودية بقائمة لتوصياتها الأولية المقترحة خلال المؤتمر، وكان أهمها:" إنشاء مركز دولي لتطوير آليات تبادل المعلومات والخبرات بين الدول في مجال مكافحة الإرهاب، ولربط المراكز الوطنية المختصة بقاعدة بيانات يمكن تحديثها باستمرار، ذلك أن مكافحة الإرهاب هي مسئولية مشتركة تتطلب أعلى درجات التنسيق والتعاون بين الدول والاستعداد الكامل لتبادل المعلومات الاستخباراتية والأمنية بأسرع ما يمكن بين الأجهزة المختصة عبر وسائل آمنة .

[1] حسن بن أحمد الشهري، أهمية القواعد الخاصة بمكافحة الإرهاب– بناء قاعدة بيانات دولية لمكافحة الإرهاب – مشروع مقترح ، بحث مقدم للندوة العلمية لمركز الدراسات والبحوث– قسم الندوات واللقاءات العلمية، في الفترة من 25– 27 ماي 2009، ص 02.

[2] نفس المرجع، ص 02.

وتتشابه هذه التوصية بشكل كبير مع التوصيات التي اقترحها وفد الانتربول خلال المؤتمر بشأن توصل المجتمع الدولي إلى أفضل السبل الممكنة لتبادل المعلومات بشأن الإرهابيين وتنظيماتهم بأكبر قدر ممكن من التفاصيل وعلى نحو يتيح للدول تعقب تحركاتهم فور حدوثها، وكذلك بشأن تبادل معلومات معيارية حول الجوازات ووثائق السفر المفقودة والمزورة.

كما اقترح عدد من الوفود أن هناك حاجة لمراكز إقليمية إلى جانب المركز الدولي المقترح وأنه يمكن ربط المراكز الإقليمية بمركز موحد افتراضي عبر تقنيات اتصال آمنة في حين اقترحت وفود أخرى تلبية حاجات تبادل برامج التدريب والتنظيم والتقنيات بين أجهزة مكافحة الإرهاب، وتبادل الخبرات بشأن التشريعات الملائمة وتقوية مؤسسات إنفاذ القانون مع الحفاظ على حقوق الإنسان وحكم القانون[1].

وأخيراً أشارت بعض الوفود أن المركز الدولي المقترح يمكنه تسهيل تبادل الخبرات بشأن توعية المعلمين والإعلاميين بمخاطر الإرهاب وضرورة محاربته.

## أولا: قواعد بيانات متخصصة في مجال الحوادث الإرهابية في أوروبا، واستراليا.

سوف نتعرض في هذا العنصر أولا للقواعد الخاصة بأوربا ثم استراليا كتالي:

### 1. ألمانيا

أقر مجلس الوزراء بألمانيا إنشاء قاعدة بيانات مكافحة الإرهاب تحتوي أسماء كل من يثبت تورطه في عمليات إرهابية داخل أو خارج ألمانيا تستخدم من قبل الأجهزة الألمانية الأمنية كقاعدة بيانات مشتركة، وتقابل بمعارضة شديدة نظرا للخلفية التاريخية لألمانيا في الحرب العالمية الثانية[2].

[1] حسن بن أحمد الشهري، مرجع سابق، ص 03.

[2] عمار تيسير بجبوج، مرجع سابق، ص 418.

### 2. أستراليا.

أنشأت الحكومة الاسترالية قاعدة بيانات تحتوي بيانات بأسماء متورطين في عمليات إرهابية، مع نشر صورهم وتفاصيل الحادثة الإرهابية وحملتها على شبكة الانترنت ليسهل الاطلاع على من تراهم ضالعين في عمليات إرهابية[1].

### 3. بريطانيا.

أنشأت بريطانيا قاعدة بيانات سمتها قاعدة بيانات الأخ الكبير للتلفون والبريد الالكتروني ( Big brother database for phone and e-mails)، وتخطط الحكومة البريطانية في إجراء يحد من العمليات الإرهابية وذلك بإنشاء قاعدة بيانات ضخمة تشمل تدوين جميع المكالمات التلفونية والرسائل الالكترونية.

ويلاحظ أن هذه القاعدة للبيانات تم إنشاؤها لمكافحة جريمة الإرهاب الالكتروني والتي يعتبر البريد الالكتروني أهم وسيلة من وسائل الإرهاب الالكتروني .

ويتم الاحتفاظ بهذه المعلومات لمدة عام كامل وبإمكان أجهزة الأمن المختصة استخدامها عند موافقة المحاكم[2] .

### 4. قاعدة بيانات أمريكية بريطانية مقترحة.

تخطط كل من الولايات المتحدة الأمريكية وبريطانيا في إنشاء قاعدة بيانات دولية متخصصة في مجالات الإرهاب، ومن المتوقع انضمام كل من كندا واستراليا ونيوزيلندا للمشاركة في هذا المشروع الخاص بمكافحة الإرهاب.

[1] حسن بن أحمد الشهري، مرجع سابق، ص 8.

[2]. Anderson, T. and C. Hsiao (1981). "Estimation of Dynamic Models with Error-Components Journal of the American Statistical Association 76: 598-606 https://amstat.tandfonline.com/doi/abs/.../01621459.1981(27/06/2018 à 20:04)

هذه القاعدة المقترحة لا تزال في طور التصميم وعند اكتمالها سوف تحتوي على معلومات بأخطر الإرهابيين والحوادث الإرهابية في كافة أنحاء العالم[1].

**ثانيا: قواعد البيانات التي أنشئت بالولايات المتحدة الأمريكية والخاصة بالحوادث الإرهابية.**

### 1. قاعدة معلومات مونتريه للإرهاب.

قاعدة بيانات تحتوي على أسماء أشخاص وجماعات ومنظمات متورطة في عمليات إرهابية وتستخدم فقط من قبل الموظفين الحكوميين المحليين والفدراليين وأفراد القوات المسلحة في الولايات المتحدة الأمريكية[2].

### 2. قاعدة المعرفة للعمليات الإرهابية .

أنشئت في سنة 2004 وتخصصت في تسجيل الحوادث الإرهابية، من جماعات وقيادات وقضايا إرهابية، وتحتوي على أكثر من 29 ألف حالة إرهابية وملفات لأكثر من 900 مجموعة إرهابية.

كما تضمن هذه القاعدة على سيرة ذاته لأكثر من 1200ارهابي، وتدعم هذه القاعدة من قبل إدارة الأمن الوطني[3] .

---

[1] حسن بن أحمد الشهري، مرجع سابق، ص 9.

[2] Lafree,G.&Dugan L,(2006).GTD II User Guide,STRAT Study of Terrorism and response to Terrorism,available at: http//www.start.umd.edu/start/data/gtd,(27/06/2018 à22:57).

[3] حسن بن أحمد الشهري، مرجع سابق، ص 9.

### 3. قاعدة بيانات راند العالمية للحوادث الإرهابية.

أنشئت في سنة 1972، وتحتوي معلومات عن عمليات إرهابية حدثت في جميع أنحاء العالم وتتكون من قاعدتين للمعلومات :

أ- الأولى تحتوي معلومات عن حوادث إرهابية عالمية حدثت في الفترة بين 1968 إلى غاية 1997.

**ب**- الثانية تحتوي معلومات عن حوادث إرهابية محلية وعالمية حدثت في الفترة بين 1998 وحتى يومنا هذا.

ورصدت هذه القاعدة أكثر من 36 ألف حالة إرهابية موثقة توثيقا كاملا[1].

### 4. قاعدة هوية وبيئة الإرهاب.

أنشئت في سنة 2004 وتتبع هذه القاعدة مركز مكافحة الإرهاب الوطني الأمريكي وتضم أكثر من 564 ألف اسم حتى سنة 2009 يسجل في هذه القاعدة أسماء كل من يعرف أو يشتبه في ضلوعه في أي نشاط إرهابي.

وتتسبب هذه القاعدة في تأخير عدد كبير من المسافرين لتطابق أو تشابه أسمائهم[2] .

### 4. قاعدة بيانات متغيرات إرهابية عالمية .

تحتوي على أكثر من 12000 حادثة إرهابية عالمية، وتعتبر من القواعد الضخمة والمفتوحة للأبحاث .

---

[1] عمار تيسير بجبوج، مرجع سابق، ص 419.

[2] مصطفى فؤاد عبيد، تقنيات التنقيب في قواعد البيانات واستكشاف المعلومات المخبأة فيها، بحث منشور في الموقع: www.itns.org.sa/ItnsMedia/26.ppt تاريخ الاطلاع 2008/06/27 على الساعة 23:34.

### 5. قاعدة بيانات الإرهاب العالمية.

أنشئت هذه القاعدة في سنة 2001 عندما حصل الباحثين في جامعة مريلاند على قاعدة بيانات ضخمه سبق جمعها بواسطة The Pinkerton Global Intelligence Servicesالذي قام بين العامين 1970الى 1997 هو ومجموعة من متقاعدي القوات الجوية برصد وتسجيل جميع الحوادث الإرهابية في جميع أنحاء العالم دون استثناء.

وقد أنهى فريق جامعة "مريلاند" بناء القاعدة في العام 2007 ، بعد أن تلقى دعما من إدارة الأمن الوطني وبصدد توحيد القاعدتين **GTD2, GTD1** التي تم إنشائها في فترتين مختلفتين.

في هذه القاعدة تحتوي كل معلومة على نوعها ومكان وتاريخ وقوعها، وطبيعة الهدف وعدد الضحايا والمجرمين عند توفر أسمائهم.

وتتبع هذه القاعدة للمركز الوطني لدراسة الإرهاب **( START)** وتتميز هذه القاعدة بمجموعة من الخصائص التالية[1]:

- تحتوي على أكثر من 80000 هجوم إرهابي .
- تحتوي كل معلومة على نوعها ووقت حدوثها وعدد القتلى، والمجموعة المتبنية للهجوم.
- تحتوي على معلومات لأكثر من 27000 تفجير و 13000 اغتيال و2800 اختطاف
- يعمل في جمع المعلومات ما يقارب من 75 مختص.
- تخضع معلومات هذه القاعدة لرقابة 12 باحث متخصص.
- جمعت معلومات القاعدة من أكثر من 2000000 مقال موثق ، وأكثر من 2500 مصدر.

[1] مصطفى فؤاد عبيد، مرجع سابق.

- تضع القاعدة معلوماتها في تصرف موظفي ووكالات الحكومة في أي وقت وتسمح للباحثين بعد سنة من جمعها، وتعتبر أكبر وأشمل قاعدة متخصصة في القواعد الإرهابية[1]

### ثالثا: قاعدة بيانات الإرهاب في أوربا الغربية.

تغطي هذه القاعدة تسعة عشرة دولة أوربية وهي: النمسا- بلجيكا- الدانمارك- فلندا- فرنسا- ألمانيا- اليونان- أيسلندا- ايرلندا- ايطاليا- لوكسمبورغ- هولندا- النرويج- البرتغال- اسبانيا- السويد سويسرا- بريطانيا- ايرلندا الشمالية.

وتصنف هذه القاعدة نوع الإرهاب الذي يقع في أوروبا الغربية ضمن سياق النظام السياسي لهذه الدول، وتستثنى من هذه البيانات الحوادث الإرهابية التي تقع خارج الدول سابقة الذكر، إلا في الحالات التي تكون فيها إحدى العناصر التي تكون الجريمة ترتبط بهذه الدول كجنسية الجاني، أو المجني عليه أو طبيعة المصلحة المعتدى عليها

وتعرف هذه القاعدة الإرهاب بقولها:" أنه شكل من أشكال العنف يقع ضد أهداف معينة من الجمهور وذلك للتأثير على طرف ثالث لتغير موقفها من قضية معينة"

وقد جمعت هذه القاعدة البيانات في الفترة الممتدة من سنة 1950 إلى سنة 2004 حيث بلغ مجموع الأحداث التي تم تسجيلها وفق قاعدة (TWEED) 11026 حادثة، قامت بها 200 جماعة إرهابية سجلت 2959 حالة وفاة ناتجة عن أعمال تلك الجماعات[2].

### رابعا: قاعدة البيانات الصينية.

تعتزم الصين إنشاء قاعدة بيانات سكانية وطنية مرتبطة بمعلومات الهوية والسجلات الائتمانية كجزء من حملة واسعة لتعزيز المراقبة والأمن، وفقا لما ذكرته وسائل الإعلام الرسمية، وتهدف من وراء هذه البيانات حصر قائمة للإرهابيين والمتطرفين.

[1] حسن بن أحمد الشهري، مرجع سابق، ص 11.

[2] عمار تيسير بجبوج، مرجع سابق، ص 419.

وكانت الصين اتخذت بالفعل سلسلة من التدابير الرامية إلى منع وقوع هجمات من قبل متطرفين، بما في ذلك خطط لقانون مكافحة الإرهاب من شأنه أن يمنح الحكومة سلطات مراقبة أوسع.

وذكرت شينخوا أن السلطات سوف تحتاج إلى الهوية عند التسجيل في الفنادق، والتجارة في السلع المستعملة، و"خدمات الترفيه"، دون تحديد نوع الترويح عن النفس.

وتشمل أحدث الخطوات أيضا تخصيص المزيد من قوات الأمن لوسائل النقل العام، بما في ذلك الحافلات والقطارات ومترو الأنفاق، فضلا عن المدارس والمؤسسات المالية والمستشفيات، بحسب ما ذكرته وكالة أنباء الصين (شينخوا) الرسمية نقلا عن بيان صادر عن اللجنة المركزية للحزب الشيوعي الحاكم، ومجلس الوزراء الصيني.

وجاء في بيان الحزب الشيوعي الصيني أن الإجراءات الجديدة ستساعد على "منع العنف والهجمات الإرهابية أو الأحداث المتطرفة[1].

## خامسا: قواعد البيانات في الدول العربية.

تضمنت الاتفاقية العربية لمكافحة الإرهاب النص على إنشاء قواعد البيانات في الدول العربية وذلك بقولها:" تقوم كل دولة من الدول المتعاقدة بإنشاء قاعدة بيانات لجمع وتحليل المعلومات الخاصة بالعناصر والجماعات والحركات والتنظيمات الإرهابية ومتابعة مستجدات ظاهرة الإرهاب، والتجارب الناجحة في مواجهتها، وتحديث هذه المعلومات، وتزويد الأجهزة المختصة في الدول المتعاقدة بها وذلك في حدود ما تسمح به القوانين والإجراءات الداخلية لكل دولة"[2].

---

[1] الصين.. إنشاء قاعدة بيانات عامة لمكافحة الإرهاب، مقالة منشورة في الموقع: www.skynewsarabia.com بتاريخ 2015/04/14 على الساعة 11:01 .

[2] الاتفاقية العربية لمكافحة الإرهاب التي اعتمدها مجلس وزراء الداخلية العرب يوم 1998/04/22.

وعلى الرغم من أن الاتفاقية تضمنت النص على إنشاء قواعد للبيانات خاصة بالدول العربية كتدبير حديث للتعاون الدولي في مكافحة الإرهاب بمختلف أنواعه ومنها الإرهاب الالكتروني، إلا أن المنطقة العربية مازالت تفتقد إلى قواعد بيانات وطنية، رسمية أو خاصة تعنى بجرائم الإرهاب.

ومع ذلك فان بعض المؤسسات العالمية قامت بعمل إحصائيات في كثير من الدول العربية، وهذه الإحصائيات تعامل بتكتم كبير على مستوى الدولة الواحدة، نظرا لاختلاف معايير تصنيف الحوادث الإرهابية في المفهوم العربي عنه في المفهوم الغربي[1]

وبدراسة قواعد البيانات السابقة والمتخصصة في رصد وتسجيل الحوادث والهجمات الإرهابية اتضح أنها جميعا بدأت بمجهودات ومبادرات خاصة، وأغلب هذه المبادرات نشأت في أحضان الجامعات والمراكز البحثية، وقام عدد من دول العالم بدعم مثل هذه الجامعات والمراكز البحثية.

وبما أن كل قاعدة صممت على انفراد ، آخذة في الاعتبار الاحتياجات والمتطلبات الوطنية فإن فوائدها محلية لم تعكس طبيعة الجريمة الإرهابية التي تتمتع بخاصية هامة، هي أن لا دين ولا حدود ولا وطن لهذه الجريمة، وقد نشأت هذه القواعد منفصلة وغير مترابطة وجمعت معلوماتها من مصادر متنوعة وصممت أنظمتها الفنية بطرق مختلفة.

ويقول "قيري لافري" مدير قاعدة البيانات الدولية التابعة للمركز الوطني لمكافحة الإرهاب بجامعة "ميريلاند" بالولايات المتحدة الأمريكية في معرض نقده لقواعد البيانات الإرهابية المفتوحة إلي أن هناك عيوبا تشترك فيها جميع قواعد البيانات الإرهابية الكبرى المفتوحة لخصها في ثلاثة عيوب هي[2]:

1. اعتمدت في جمع معلوماتها من مصادر إخبارية لكبريات الصحف والمجلات والمحطات الإخبارية، والتي يحتمل انحياز البعض منها مما يفقدها المصداقية بالإضافة إلى أن هناك العديد من الحوادث الإرهابية التي حدثت ولم تغطى من قبل هذه المصادر، وينتج عن ذلك عدم رصد مثل هذه الحوادث.

[1] دياب بن موسى البداينة، مرجع سابق، ص 13.

[2] حسن بن أحمد الشهري، مرجع سابق، ص 13.

**2.** هناك نقص معلومات لبعض القضايا الهامة المتعلقة بالإرهاب، ويرى البعض أن هناك ندره في معلومات عدد من المنظمات الإرهابية، وكذلك إرهاب الدولة ضد مواطنيها.

ويستنتج من ذلك إلى أنه من المهم الاعتراف أن المعلومات التي جمعت لهذه القواعد تبقى محدودة.

**3.** يضيف "قيري لا فري" في سياق نقده لقواعد البيانات الإرهابية المفتوحة إلى احتمال ضياع معلومات هذه القواعد كما حصل لبعض معلومات القاعدة التي يديرها.

مما تقدم فان بعض الباحثين في هذا الشأن يرون انه من الممكن مواجهة مثل هذه التحديات باستخدام هذه القواعد كبنية تحتية لخلق نظام أشمل وأوسع وموحد[1].

وتجدر الإشارة أن مختلف قواعد البيانات العالمية تعتمد بشكل مفرط على المصادر الإعلامية التي قد تكون غير دقيقة نظرا لتحيزها وانعدام الموضوعية في تقييمها ووصف الحالات، فضلا عن أنها لا تتضمن في غالبيتها معلومات أو إحصائيات عن إرهاب الدولة ضد مواطنيها أو ضد الدول الأخرى.

ومن أجل ذلك تبدو الحاجة ملحة اليوم لاعتماد قواعد بيانات عربية وطنية، تقوم بعمل إحصائيات دقيقة وموضوعية حول الجرائم الإرهابية التي تحصل في منطقتنا العربية، وتكون مواكبة لتطور هذه الجريمة وتتناسب مع طبيعتها وتحيط بجميع أبعادها.

كما أن مكافحة الإرهاب تعد مسؤولية مشتركة تتطلب أعلى درجات التعاون والتنسيق بين الدول والاستعداد الكامل لتبادل لمعلومات الاستخباراتية والأمنية بأسرع ما يمكن بين الأجهزة المعنية وعبر وسائل آمنة، وضرورة وجود مركز أو هيئة دولية لتبادل المعلومات والخبرات بين الدول في مجال مكافحة الإرهاب ولربط المراكز الوطنية عبر قاعدة بيانات موحدة يمكن تحديثها باستمرار وتتيح تبادل المعلومات المطلوبة في الوقت المناسب.

[1] حسن بن أحمد الشهري، مرجع سابق، ص 14.

ويعمل كذلك على إيجاد وسائل مشتركة آمنة للتبادل الطوعي للمعلومات المتعلقة بالإرهابيين والمجموعات الإرهابية بأكبر تفصيل ممكن وعلى نحو يدعم جهداً تعاونيا لتعقب تحركاتهم بشكل فوري وللمساعدة على اعتراض تحركاتهم وعملياتهم، وتسهيل تبادل المعلومات المعيارية حول الجوازات ووثائق السفر المفقودة والمزورة، وتطوير قواعد بيانات يمكن البحث المشترك فيها بسرعة.

كما تساعد القواعد على التنسيق مع المراكز الإقليمية والدولية المختصة لإيجاد شبكة من الروابط عبر وسائل اتصال آمنة تشكل بمجموعها مركزا افتراضيا.

وكذلك تحقيق تبادل المعلومات حول سبل تطوير الأساليب والتدريبات والتشريعات والتقنيات والتنظيمات والأنشطة التي من شانها تدعيم القدرات الوطنية في مجال مكافحة الإرهاب وتنفيذ المعاهدات الدولية ذات الصلة وتقوية مؤسسات إنفاذ القانون مع الحفاظ على حقوق الإنسان وحكم القانون[1].

كما أن الأمم المتحدة في مواجهتها للإرهاب وفي الإطار الاستراتيجي نصت خطة العمل في قرار الجمعية العامة – كما سبق توضيحه–

وقد جاء في الفقرة 36 من التقرير النهائي للمؤتمر الدولي لمكافحة الإرهاب المنعقد في الرياض في الفترة 5–8 فيفري 2005م، الذي تمت الدعوة من خلاله إلى إنشاء مركز دولي لمكافحة الإرهاب، الذي سوف يضطلع من بين أمور أخرى بتنمية آلية لتبادل المعلومات والخبرات بين الدول في مجال مكافحة الإرهاب.

وربط المراكز الوطنية لمكافحة الإرهاب من أجل مكافحة الإرهاب مع وجود قاعدة بيانات كفيلة باستكمال السريع للمعلومات الممكنة مع الأخذ في الاعتبار بأن مكافحة الإرهاب تعتبر بمثابة جهد جماعي يتطلب أقصى درجة من التعاون والتنسيق بين الدول والاستعداد الكامل لتبادل المعلومات الأمنية الاستخباراتية على الفور بين الأجهزة المتخصصة من خلال معدات آمنة.

[1] حسن بن أحمد الشهري، مرجع سابق، ص 15.

وعليه ومما سبق فإنه لا يوجد قاعدة بيانات دولية متخصصة في الحوادث الإرهابية وإن وجود قاعدة بيانات شاملة وموحدة تضم جميع قواعد البيانات المتخصصة في كل ما يتعلق بالإرهاب لتبادل المعلومات والخبرات بين أعضاء المجتمع الدولي[1].

وفي الأخير يمكن القول انه وعلى الرغم من أن إنشاء قواعد بيانات خاصة بالإرهاب كإحدى الوسائل المستحدثة في التعاون الدولي لمكافحة مختلف أنواع الإرهاب إلا انه يعيبها أنها متباينة مع بياناتها تبعا لتعريفها الإجرائي للإرهاب، كما أنها أنشئت بطريقة مستقلة ودون تنسيق مع غيرها من القواعد المخصصة لنفس الغرض، كما أن بعض القواعد لم يأخذ في الاعتبار عند التصميم مدى أهليتها للربط مستقبلا مع غيرها من القواعد مما يؤدي إلى تقليل الفائدة من هذه القواعد نظرا لانحصارها في محيطها.

[1] حسن بن أحمد الشهري، بناء قاعدة بيانات دولية لمكافحة الإرهاب– مشروع مقترح، المجلة العربية للدراسات الأمنية والتدريب، المجلد 26، العدد 51،الرياض، ص 257، 258 .

## خلاصة الباب الثاني.

مما سبق يتضح وأنه على الرغم من أن هناك جهود لمكافحة الإرهاب الالكتروني سواء على المستوى الدولي أو الإقليمي، وسواء كانت جهود علمية أم عملية إلا أن هذه الجهود تبقى محتشمة وغير كافية لمواجهة هذه الجريمة الخطيرة وهذا لان هناك جملة من الصعوبات التي تواجه مكافحة جريمة الإرهاب الالكتروني كسهولة إخفاء الدليل ونقص الخبرة لدى جهاز الشرطة وكذا الجهات القضائية في مجال تكنولوجيا المعلومات .

كما أنه من الصعب بأي حال من الأحوال الوصول إلى مرتكبي أغلب الجرائم المعلوماتية لسهولة اختبائهم وعدم الكشف هن هويتهم الحقيقية .

هذا بالإضافة إلى انه ومن الناحية العملية في ميدان المكافحة نلاحظ غياب اتفاق عام مشترك بين الدول حول الأفعال الجرمية وخاصة المستحدثة منها، ويمكن أن يكمن السبب في اختلاف المفاهيم المتعلقة بهذه الجرائم وخاصة الإرهابية منها .

# خاتمة

مما سبق يتضح أن الإرهاب الالكتروني أصبح خطرا يهدد العالم بأسره فهو لم يفرق بين مجتمع وآخر ولا بين دين وآخر، فكل الشعوب أصبحت عرضة للهجمات الإرهابية عبر الانترنت في أي وقت وفي كل مكان من العالم فباتت التقنية الحديثة لوحدها غير كافية ولا قادرة على حماية المجتمع من هذا الخطر ومن أجل ذلك حاولت جميع الدول التصدي لهذه الجريمة التي فتكت بالدول والمجتمعات.

ولأن الإرهاب الالكتروني هو ظاهرة عالمية جد خطيرة تستهدف الدول على نطاق عالمي الأمر الذي استدعى تضافر الجهود وإنشاء آليات متخصصة لمكافحته دون إغفال النتائج الايجابية المترتبة عن إقامة شراكة قانونية أمنية بين أهم الأجهزة في الدولة منها القضاء والأمن والدرك قصد تضييق الخناق على ممارسي مثل هذا النوع من الجرائم الالكترونية .

ومن أهم النتائج التي توصلنا إليها من خلال هذه الدراسة –المتواضعة– ما يلي:

- إن الإرهاب الالكتروني صورة متطورة من صور الإرهاب التقليدي، حيث وضعت له العديد من التعريفات – كما سبق وتعرضنا لها بشيء من التفصيل– سواء على المستوى العربي أو الغربي، وسواء على الصعيد الإقليمي أو الدولي.
- تشترك جريمة الإرهاب الالكتروني مع جريمة الإرهاب التقليدي في أسباب النشأة والانتشار كالأسباب السياسية والاقتصادية والاجتماعية ..الخ كما تشترك معها في الأهداف المرجوة من خلال هذه الجريمة، إلا أنها تختلف عن جريمة الإرهاب التقليدي من حيث الأساليب والأشكال المختلفة لها (صور الإرهاب الالكتروني).
- كما يعتبر الإرهاب الالكتروني صورة من صور الجرائم المعلوماتية (الالكترونية) ،حيث أن الإرهابي في جريمة الإرهاب الالكتروني يتخذ من الفضاء الالكتروني نطاقا يمارس من خلاله عمله الإرهابي، متخذا من الانترنت وسيلة إعلامية أو وسيلة اتصال وتنسيق بين الجماعات الإرهابية ...
- في جريمة الإرهاب الالكتروني يتغلب الجانب المعنوي المتعلق بالمعارف والخبرات والأساليب اللازمة في العمل الإرهابي في البيئة الالكترونية على الجانب المادي المتعلق بالمواد المستخدمة في التنقل أو الاتصال .

- إذا كان لا يتصور شروع في الجريمة الإرهابية التقليدية على النحو الذي سبق وشرحناه فإنه لا يتصور شروع في جريمة الإرهاب الالكتروني وذلك من ناحيتين، الأولى هو أن الإرهاب الالكتروني ما هو إلا شكل متطور وحديث للجريمة الإرهابية، فما تغير في جريمة الإرهاب الالكتروني سوى أن الوسيلة المستخدمة في هذه الجريمة تطورت وأصبحت وسيلة تقنية حديثة، وأما الناحية الثانية هو أن جريمة الإرهاب الالكتروني هي في أصلها جريمة معلوماتية (الكترونية)، ففي الجريمة الالكترونية حتى الأعمال التحضيرية تعتبر جرائم في حد ذاتها فشراء برامج الاختراق يعتبر عمل تحضيري ولكنه في نفس الوقت جريمة قائمة بذاتها.
- من خلال دراسة أركان جريمة الإرهاب الالكتروني توصلنا إلى نتيجة مفادها أن جريمة الإرهاب الالكتروني تشترك مع جريمة الإرهاب التقليدي في الركن المعنوي حيث أن للجريمتين نفس القصدين العام والخاص، كما أنه في كلتا الجريمتين لا يمكن تصور الخطأ فجريمة الإرهاب الالكتروني جريمة عمدية شأنها في ذلك شأن جريمة الإرهاب التقليدي، في حين تشترك جريمة الإرهاب الالكتروني مع الجريمة المعلوماتية في الركن المادي، وهذا الاشتراك يكون في الأداة الجرمية وهي المواقع الالكترونية والفيروسات ..الخ.
- آليات مكافحة الإرهاب الالكتروني انقسمت إلى آليات قمعية وأخرى وقائية، ويظهر ذلك جليا في جهود هيئة الأمم المتحدة من خلال الاتفاقيات التي تم إبرامها في هذا الصدد وكذلك استراتيجياتها العالمية التي تضمنت توصيات مهمة وكثيرة في هذا المجال، بالإضافة إلى الجهود الإقليمية والتي تمثلت في إبرام الاتفاقيات الإقليمية في مكافحة الإرهاب الالكتروني وكذلك الاستراتيجيات الإقليمية.
- من خلال دراستنا للإرهاب الالكتروني في المنطقية العربية تم التوصل إلى نتيجة مفادها تدني المستوى الأمني والتقني للبيئة الالكترونية العربية.
- من خلال دراستنا لدور المنظمات الإقليمية في مكافحة الإرهاب الالكتروني نجد أنها كانت سبب تشريعي هام للدول الأعضاء، حيث قامت الدول الأعضاء بتعديل تشريعاتها الوطنية بما يتماشى مع الاتفاقيات المبرمة، كما سايرت الاتفاقيات الإقليمية أحكام الاتفاقيات العالمية الصادرة عن الأمم المتحدة ، وعملت على تطبيق القرارات الأممية في هذا المجال.
- على الرغم من النتيجة السابقة هناك فراغ كبير في نصوص القوانين العربية فيما يخص بالجريمة المعلوماتية عموما وجريمة الإرهاب الالكتروني خاصة وكذلك بخصوص مكافحتها

**المقترحات.**

في ختام هذا الموضوع وبعد أن تعرضنا إلى مجموع النتائج السابقة يمكن اقتراح بعض التوصيات والمقترحات التي تعتبر ضرورية من وجهة نظرنا، والتي يمكن إيجازها فيما يلي:

– وجوب إيجاد مفهوم موحد لجريمة الإرهاب الالكتروني وذلك من خلال إبرام اتفاقية دولية شاملة لمكافحة الإرهاب بمختلف صوره وأشكاله ومنها وأهمها جريمة الإرهاب الالكتروني، وبموجب هذه الاتفاقية تتحمل جميع الدول الأعضاء الالتزامات المفروضة على عاتقها بمنع وقمع الجريمة الإرهابية وخاصة الالكترونية وعدم مساندتها أو التحريض عليها.

– وجوب أن توحد جميع الدول سياساتها التشريعية والأمنية في مجال مكافحة الإرهاب الالكتروني على اعتباره أكثر صور الإرهاب خطورة وفتكا بالمجتمعات والدول .

– ضرورة استخدام التقنيات الحديثة في مكافحة الإرهاب الالكتروني كالأجهزة الالكترونية وهذا للتمكن من مجابهة الإرهاب وصده بطريقة فعالة ونهائية .

– ضرورة تكوين وتأهيل المحققين وكذلك ضباط الشرطة القضائية في مجال الجريمة الإرهابية والجريمة الالكترونية وخاصة منها جريمة الإرهاب الالكتروني .

– العمل على الوقاية من الإرهاب الالكتروني وذلك عن طريق الحملات التحسيسية وضرورة مشاركة أعضاء المجتمع المدني من جمعيات وأحزاب وجميع القوى الفعالة في الدول في هذه الحملات من أجل وقاية أكثر فعالية.

– ضرورة التصدي لعملية تبييض الأموال وتمويل الإرهاب، وذلك بإنشاء أجهزة فعالة على مستوى كل البنوك والمصارف في جميع الدول، حيث تعمل على مراقبة مصادر الأموال ومختلف العمليات المتعلقة بحركات رؤوس الأموال، وهذا لأن تبييض والتمويل من أكثر المصادر التي يستغلها الإرهابيون لتأمين الأجهزة المستخدمة في الإرهاب الالكتروني.

– ضرورة الاستخدام الصحيح لوسائل الإعلام وتوجيهه لمحاربة الإرهاب بمختلف أنواعه وإظهار حقيقته البشعة للناس كافة .

– إن الدول مهما امتلكت من الإمكانيات والوسائل لا يمكنها مكافحة الإرهاب الالكتروني بصفة منفردة بل يجب تضافر كافة الجهود سواء داخل الدولة الواحدة من أسرة وأجهزة الأمن والقضاء والتعليم وبين الدول كالمنظمات .

– ضرورة تبادل الخبرات في ميدان تكنولوجيا المعلومات بين مختلف الدول من أجل تحقيق الأمن المعلوماتي وتضييق الخناق أمام الجماعات الإرهابية ومنعها من استغلال شبكات الانترنت لتحقيق أغراضهم الإرهابية.

– تعزيز التعاون والتنسيق بين المؤسسات الوطنية والمنظمات الدولية لمواجهة هذه الجريمة الجد خطيرة.

– وجوب وضع إستراتيجية عربية فعالة لحماية البيئة الالكترونية ومكافحة جريمة الإرهاب الالكتروني

# قائمة المراجع

**القرآن الكريم.**

## أولا : المصادر

### I. النصوص الرسمية.

**1.** الدستور الجزائري لسنة 1996.

أ/ **الاتفاقيات.**

**1.** النظام الأساسي للمنظمة الدولية للشرطة الجنائية 13 تموز 1956 .

**2.** اتفاقية الجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية، الموقعة في نيويورك عام 1973.

**3.** اتفاقية مناهضة اخذ الرهائن الموقعة في 1979/12/18 في نيويورك، وقد اعتمدت هذه الاتفاقية قبل صدور القرار 1461/34 من قبل الجمعية العامة للأمم المتحدة، وبحلول نهاية عام 1980 كان قد تم التوقيع عليها من قبل 39 دولة ودخلت حيز التنفيذ في 3 يونيو 1983 بعد أن صدقت عليها 22 دولة، واعتبارا من ديسمبر 2014 فإن اتفاقية أصبحت تضم 174 دولة.

**4.** اتفاقية الرياض للتعاون القضائي بين الدول العربية المصدقة بالقانون رقم 14 بتاريخ 1983/10/10، وقد وافق على هذه الاتفاقية مجلس وزراء العدل العرب بموجب قراره رقم 01 المؤرخ 1983/04/06 في دورة انعقاده الأولى في الرياض ودخلت الاتفاقية حيز النفاذ ابتداءا من تاريخ 1985/10/30 .

**5.** اتفاقية ماسترخت سنة 1992 التي دخلت حيز التنفيذ سنة 1993، وتم الاتفاق عليها من قبل المجلس الأوروبي في مدينة ماسترخت الهولندية في ديسمبر 1991، ودخلت هذه المعاهدة، التي تم توقيعها في 7 فبراير 1992 في ماسترخت، حيز التنفيذ في الأول من نوفمبر 1993.

**6.** الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 والتي اعتمدها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك بالقاهرة يوم 1998/04/22 ودخلت حيز النفاذ بتاريخ 1999/05/07.

**7.** اتفاقية المعاقبة على تمويل الإرهاب لسنة 1996، والتي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 54 109/ المؤرخ في 9 كانون الأول/ديسمبر 1999.

**8.** اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، التي اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم (25) في الدورة الخامسة والخمسون بتاريخ 2000/11/15، منشورات الجمعية العامة للأمم المتحدة 2001/01/08.

**9.** اتفاقية بودابست لسنة 2001 ، حيث تم اعتماد الاتفاقية وتقريرها التفسيري من طرف لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة في 2001/11/08 وفتح باب التوقيع عليها في 2001/11/23 بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.

**10.** الاتفاقية العربية لمكافحة تقنية نظم المعلومات التي وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بالقاهرة بتاريخ 1432/01/15 هـ الموافق لـ 2010/12/21، وقد وقعت عليها الجزائر في 2010/12/21.

**ج/ القرارات الدولية**

**1.** قرار مجلس الأمن رقم 883 المؤرخ في 11 نوفمبر 1993 المتعلق بقضية لوكربي الليبية .

**2.** قرار مجلس الأمن رقم 1044، الصادر في الجلسة رقم 3627 المنعقدة في 21 جانفي 1996 .

**3.** قرار مجلس الأمن رقم 1373 الصادر بتاريخ 28 سبتمبر 2001.

**4.** القرار رقم 1566 لسنة 2004 .

**5.** قرار مجلس الأمن رقم 2322 لسنة 2016.

**د/ القوانين الوطنية**

**1.** الأمر 66-156 المؤرخ في 18 صفر 1386هـ الموافق لـ 8يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

**2.** الأمر 66-155 المؤرخ في 18 صفر 1386هـ الموافق لـ 8يونيو 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم.

**3.** قانون رقم 03/2000 مؤرخ في: 05 جمادى الأولى عام 1421 ﻫ الموافق لـ 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية واللاسلكية، جريدة رسمية، عدد48، ص03، (2000/08/06).

**4.** قانون رقم 03/2000 مؤرخ في: 05 جمادى الأولى عام 1421 ﻫ الموافق لـ 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمراسلات السلكية واللاسلكية، جريدة رسمية، عدد48، ص03، (2000/08/06).

**5.** قانون 01/05 المؤرخ في 2005/02/06 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والذي عدل بموجب القانون 06/15 المؤرخ في 2015/02/15، الجريدة الرسمية عدد 8 الصادرة بتاريخ 2015/02/15 ص 4

**6.** قانون رقم 04/09 مؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد 47، الصادرة في 16 غشت 2009، ص6.

**7.** مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة 1435 هـ الموافق لـ 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 2010/12/21، جريدة رسمية للجمهورية الجزائرية العدد 57، الصادرة بتاريخ 4 ذو الحجة 1435 هـ الموافق لـ 28 سبتمبر 2014 م ص 4.

**8.** المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53 في 8 أكتوبر 2015.

**ج/ القوانين الأجنبية.**

**1.** القانون58 لسنة 1937 المتضمن قانون العقوبات المصري المعدل والمتمم.

**2.** قانون رقم 148 لسنة 1949 المتضمن قانون العقوبات السوري المعدل.
**3.** القانون رقم 16 لسنة 1960 المتضمن قانون العقوبات الأردني، والمعدل بموجب القانون رقم 12 لسنة 2010.
**4.** قانون رقم 16 لسنة 1960 المتضمن قانون الجزاء الكويتي.
**5.** القانون 111 لسنة 1969 المتضمن قانون العقوبات العراقي، مجلة الوقائع العراقية، عدد 1778 ، بتاريخ 1969/09/15.
**6.** القانون الفرنسي رقم 96-392 المتعلق بمكافحة تبييض الأموال والاتجار في المخدرات والتعاون الدولي في مجال حجز ومصادرة متحصلات الجريمة.
**7.** القانون رقم 97-1159 المؤرخ في 19 ديسمبر 1997 المتضمن قانون العقوبات الفرنسي.
**8.** القانون رقم 2004-575 المؤرخ في 2004/06/21 المتعلق بالثقة بالاقتصاد الوطني الفرنسي.
**9.** قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة 2004 والذي اعتمده مجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم 417 سنة 2004 .
**10.** القانون رقم 13 لسنة 2005 المتضمن مكافحة الإرهاب العراقي ، الوقائع العراقية عدد 4009 بتاريخ 2005/11/09.
**11.** قانون الإجراءات الجزائية الفرنسي لسنة 2009.
**12.** قانون رقم 30 لسنة 2010 المتضمن جرائم أنظمة المعلومات الأردني.
**13.** القانون العربي الاسترشادي للتعاون القضائي الدولي في المسائل الجنائية اعتمده مجلس وزراء العدل العرب في دورته الثانية والعشرون بموجب القرار رقم 653- 22 بتاريخ 2006/11/29، بالقاهرة.
**14.** قانون رقم 94 لسنة 2015 الصادر في 30 شوال 1436 هـ الموافق لـ 15 أغسطس 2015 م المتضمن قانون مكافحة الإرهاب المصري، الجريدة الرسمية عدد 33 مكرر، للسنة الثامنة والخمسون.

## ثانيا: المراجع

### 1)باللغة العربية

**I. الكتب.**


1. إبراهيم حامد طنطاوي، المواجهة التشريعية لغسيل الأموال في مصر- دراسة مقارنة، دار النهضة العربية، القاهرة 2003.
2. إبراهيم القماز، الشهادة كدليل إثبات في المواد الجزائية –دراسة قانونية ونفسية- الطبعة الأولى، علم الكتاب، القاهرة، 1980.
3. إبراهيم أحمد خليفة، القانون الدولي الدبلوماسي والقنصلي، دار الجامعة الجديد الإسكندرية، 2007.
4. أحمد إبراهيم مصطفى سليمان، الإرهاب والجريمة المنظمة- التجريم وسبل المواجهة، الطبعة الأولى، دار الشروق القاهرة، 2004.
5. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي الإسكندرية، 2006.
6. أحمد فتحي سرور، حكم القانون في مواجهة الإرهاب، الدار الجامعية بيروت،2005.
7. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الجزء الثالث، دار النهضة العربية، القاهرة، 1980.
8. ادوارد عيد، الإنابات والإعلانات القضائية وفقا للقانون الدولي الخاص واتفاقية الدول العربية في عام 1953، معهد البحوث والدراسات العربية، 1969.
9. أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية،الطبعة الثانية، دار الثقافة عمان-الأردن، 2014.

**10.** أسامة أحمد شتات، قانون العقوبات المصري، دار الكتب القانونية، القاهرة، 2004.

**11.** أسامة حسين محي الدين، جرائم الإرهاب على المستوى الدولي والمحلي، المكتب العربي الحديث، الإسكندرية 2009.

**12.** أشرف توفيق شمس الدين، مبادئ القانون الدولي الجنائي، المؤسسة الجامعية للطباعة، بيروت، 1990.

**13.** أغادير عرفات حويجان، محمد عوض الترتوري علم الإرهاب- الأسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب، الطبعة الأولى، دار الحامد عمان- الأردن، 2006.

**14.** السيد محمد حسن الشريف، النظرية العامة للإثبات الجنائي، دار النهضة العربية القاهرة،2002.

**15.** أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومة، الجزائر، 2007.

**16.** أمير فرج يوسف، مكافحة جريمة الإرهاب الالكتروني- في ظل اتفاقية مجلس التعاون لمكافحة الإرهاب، دار الكتب والدراسات العربية، الإسكندرية 2015.

**17.** أمير فرج يوسف، مكافحة الإرهاب، الطبعة الأولى، مكتبة الوفاء القانونية الإسكندرية، 2011.

**18.** أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2009.

**19.** أمير فرج يوسف، الجريمة المنظمة عبر الوطنية، دار المطبوعات الجامعية الإسكندرية، 2008.

**20.** إمام حسانين خليل، الجرائم الإرهابية في التشريعات المقارنة، الطبعة الأولى مركز الخليج للنشر والتوزيع، القاهرة 2008.

**21.** إمام حسانين عط الله، الإرهاب- البنيان القانوني للجريمة، دار المطبوعات الجامعية، الإسكندرية، 2004.

**22.** إيناس محمد البهجي، يوسف المصري، الجريمة في القانون الدولي والشريعة الإسلامية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2013.

**23.** العيش فضيل، شرح قانون الإجراءات الجزائية، مطبعة البدر، الجزائر، 2008.

**24.** بغدادي جيلالي، التحقيق -دراسة مقارنة- نظرية تطبيقية، الطبعة الأولى، الديوان الوطني للأشغال التربوية الجزائر، 1999.

**25.** جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2002.

**26.** جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2001.

**27.** جمال محمد مصطفى، التحقيق والإثبات في القانون الجنائي، مطبعة الزمان بغداد، 2004.

**28.** جندي عبد المالك، الموسوعة الجنائية، الجزء الثاني، الطبعة الأولى، مكتبة العلم للجميع، بيروت، 2004.

**29.** حسنين محمدي البوادي، إرهاب الانترنت الخطر القادم، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

**30.** حسين المحمدي البوادي، الوسائل العلمية الحديثة في الإثبات الجنائي الإسكندرية، 2005.

**31.** حسين محمود عبد الدايم، البصمة الوراثية وحجيتها في الإثبات- دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي، الطبعة الأولى، دار الفكر العربي، الإسكندرية، 2008.

**32.** خالد حازم الإبراهيمي، دور الأجهزة الأمنية في الإثبات الجنائي في الجرائم المتعلقة بشبكة المعلومات الدولية " الانترنت"– دراسة مقارنة ، ،(د د ن)، (د م ن) 2014.

**33.** خالد حمد محمد الحمادي، الإرهاب الالكتروني– دراسة في التشريع الاتحادي لدولة الإمارات العربية المتحدة أكاديمية الاتصالات، الشارقة، 2007.

**34.** خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي الإسكندرية، 2009.

**35.** خليل حسين، التنظيم الدولي– النظرية العامة والمنظمات العالمية، دار المنهل اللبناني، بيروت، 2010.

**36.** رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت– لبنان، 2012.

**37.** رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الفكر العربي القاهرة، 2005.

**38.** رؤوف عبيد، جرائم الاعتـــداء على الأشخاص والأموال، الطبعة السابعـة، دار الفكر العربي، القاهـــرة، 1985.

**39.** سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية،2011.

**40.** سامي حامد عياد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية، 2008.

**41.** سمير الأمين، مراقبة التلفون والتسجيلات الصوتية والمرئية، الطبعة الثالثة، دار الكتاب الذهبي، القاهرة، 2000.

**42.** سهيل حسين الفتلاوي، الإرهاب الدولي وشرعية المقاومة، دار الثقافة، عمان– الأردن، 2009.

**43.** شلبي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة ، الجزائر 2013.

**44.** طارق عبد العزيز حمدي، المسؤولية الدولية الجنائية والمدنية عن جرائم الإرهاب الدولي، دار الكتب القانونية، القاهرة 2008.

**45.** طارق عزت رخا ، المنظمات الدولية المعاصرة ، دار النهضة العربية ، القاهرة ، 2006.

**46.** طه أحمد طه، التحقيق الجنائي وفن استنطاق مسرح الجريمة، منشأة المعارف الإسكندرية، 2000.

**47.** عادل صادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015.

**48.** عادل يحيى، التحقيق والمحاكمة عن بعد، الطبعة الأولى، دار النهضة العربية القاهرة، 2006.

**49.** عبد الحليم موسى يعقوب، الإعلام الجديد والجريمة الالكترونية، الطبعة الأولى الدار العالمية للنشر والتوزيع، القاهرة، 2014.

**50.** عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة- دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، دار الفكر الجامعي الإسكندرية، 2008.

**51.** عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجزائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2007.

**52.** عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي الإسكندرية، 2006.

**53.** عبد الفتاح مصطفى الصيفي، وآخرون، الجريمة المنظمة- التعريف والأنماط والاتجاهات، أكاديمية نايف للعلوم الأمنية، الرياض، 1999.

**54.** عبد الفتاح مصطفى الصيفي، الاعتداء الواقع على أمن الدولة والأموال- قانون العقوبات اللبناني، دار النهضة العربية، بيروت، 1972.

**55.** عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، طبعة الثانية، دار النهضة العربية القاهرة، 2001.

**56.** عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت-الجرائم الالكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت-لبنان، 2007.

**57.** عبد المنعم متولي، الوجيز في قانون المنظمات الدولية، دار النهضة العربية القاهرة، 2008.

**58.** عثمان علي حسن، الإرهاب الدولي ومظاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام،الطبعة الأولى مطبعة مناره، هه ولير-كردستان،2006.

**59.** عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة القاهرة، 2005.

**60.** عكاشة محمد عبد العال، الإنابات القضائية في العلاقات الخاصة الدولية، دار المطبوعات الجامعية، الإسكندرية 1994.

**61.** عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة – دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2013.

**62.** علاء الدين راشد، الأمم المتحدة والإرهاب قبل وبعد 11 سبتمبر، دار النهضة العربية، القاهرة، 2005.

**63.** علي بن عبد الله عسيري، الإرهاب والقرصنة البحرية، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.

**64.** علي عدنان الفيل، الإجرام الالكتروني- دراسة مقارنة، الطبعة الأولى، مكتبة زين الحقوقية والأدبية، لبنان، 2011.

**65.** عماد مجدي عبد الملك، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية الإسكندرية، 2011.

**66.** عمر السعيد رمضان، مبادئ قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، القاهرة، 1993.

**67.** عمر بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي- المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، (مكان النشر غير موجود)، (سنة النشر غير موجودة) .

**68.** عمر سالم، الإنابة القضائية الدولية في المسائل الجنائية، دار النهضة العربية القاهرة، 2001.

**69.** فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة – دراسة مقارنة دار الثقافة، عمان- الأردن، 2006.

**70.** كوركيس يوسف داود، الجريمة المنظمة، الدار العلمية، عمان- الأردن، 2001.

**71.** ماهر عودة الشمايلة، وآخرون، الإعلام والإرهاب الالكتروني، الطبعة الأولى دار الإعصار العلمي، عمان- الأردن 2015.

**72.** محمد الفاضل، محاضرات في تسليم المجرمين، معهد الدراسات العربية العليا منشورات جامعة حلب، سوريا، 1966.

**73.** محمد بن عبد الله آل فايع العسيري، حسين بن احمد الشهري، استعمال الانترنت في تمويل الإرهاب وتجنيد الإرهابيين- الإرهاب الالكتروني وبعض وسائله والطرق الحديثة لمكافحته، مركز البحوث والدراسات- جامعة نايف للعلوم الأمنية، الرياض 2012.

**74.** محمد حزيط، مذكرات في قانون الإجراءات الجزائية، دار هومة، الجزائر 2005.

**75.** محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي الإسكندرية، 2006.

**76.** محمد سامي الشوا، الجريمة المنظمة وصداها على الأنظمة العقابية، دار النهضة العربية، القاهرة، 2001.

**77.** محمد صبحي نجم، شرح قانون العقوبات–القسم العام، دار الأوائل، عمان–الأردن، 2000.

**78.** محمد عزيز شكري، الإرهاب الدولي –دراسة قانونية ناقدة، الطبعة الأولى، دار العلم للملايين،(دون مكان نشر).

**79.** محمد سامي النيراوي، شرح الأحكام العامة لقانون العقوبات الليبي، الطبعة الثالثة، منشورات جامعة قار يونس بنغازي، ليبيا، 1995.

**80.** محمد سيد عرفة، تجفيف مصادر تمويل الإرهاب، أكاديمية نايف للعلوم الأمنية الرياض، 2009.

**81.** محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية الرياض، 1419هـ.

**82.** محمد فتحي عيد، واقع الإرهاب في الوطن العربي، أكاديمية نايف للعلوم الأمنية، الرياض، 1999.

**83.** محمد فريد قورة، نائلة عادل، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت 2005

**84.** محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية الطبعة الأولى، دار الفكر والقانون، القاهرة، 2015.

**85.** محمد منصور الصاوي، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية (سنة النشر غير مذكورة).

**86.** محمد مؤنس محي الدين، الإرهاب في القانون الجنائي على المستويين الوطني والدولي، المكتبة الانكلو– مصرية مصر،(دون سنة نشر).

**87.** محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة عمان–الأردن، 2009 .

**88.** محمود شريف بسيوني، الوثائق الدولية المعنية بحقوق الإنسان، المجلد الثاني، دار الشروق، القاهرة، 2003.

**89.** محمود صالح العادلي، الجريمة الدولية– دراسة مقارنة، دار الفكر الجامعي الإسكندرية، 2004.

**90.** محمود صالح العادلي، موسوعة القانون الجنائي للإرهاب– المواجهة الجنائية للإرهاب، الجزء الأول، دار الفكر الجامعي، الإسكندرية، 2003.

**91.** محمود عبد العزيز محمد، الإرهاب النفق المظلم في تاريخ البشرية وعلاقته بالأديان السماوية، دار الكتب القانونية القاهرة، 2013.

**92.** محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول النظرية العامة، الطبعة الأولى الكتاب الجامعي، القاهرة، 1977.

**93.** محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الجزء الثاني، دار النهضة العربية، القاهرة، 1995.

**94.** محمود نجيب حسني، شرح قانون العقوبات –القسم الخاص، دار النهضة العربية القاهرة، 1994.

**95.** مختار حسين شبيلي، التعاون الدولي لمواجهة الجريمة المنظمة، جامعة نايف للعلوم الأمنية، الرياض، 2013.

**96.** مصطفى محمد موسى، الإرهاب الالكتروني– دراسة قانونية–أمنية– نفسية– اجتماعية، سلسلة اللواء الأمنية في مكافحة الجريمة الالكترونية، مطابع الشرطة،(دون مكان نشر)، 2009.

**97.** مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية القاهرة، 2005

**98.**مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب والوثائق القانونية، القاهرة، 2003.

**99.**مصطفى مصباح دبارة، الإرهاب- مفهومه وأهم جرائمه في القانون الدولي الجنائي، منشورات جامعة قار يونس، بن غازي- ليبيا، 1995.

**100.** مصطفى يوسف كافي، وآخرون، الإعلام والإرهاب الالكتروني، الطبعة الأولى، دار الإعصار العلمي،2015.

**101.** ممدوح عبد الحميد عبد المطلب، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، مكتبة دار الحقوق، الشارقة 2001.

**102.** ممدوح محمد الجنبيهي، منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006.

**103.**منتصر سعيد حمودة ، المنظمة الدولية للشرطة الجنائية ، الانتربول ، دار الفكر الجامعي، الإسكندرية، 2008 .

**104.** نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات- دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2013.

**105.** هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة،(سنة النشر غير مذكورة).

**106.** هشام فريد محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى مكتبة الآلات الحديثة، أسيوط- مصر، 1994.

**107.** هلالي عبد اللاه احمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني على ضوء اتفاقية بودابست، الطبعة الثانية، دار النهضة العربية القاهرة 2013.

**108.** هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.

**109.** ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية الإسكندرية، 2009.

**110.** يقدح دارين، هنوني نصر الدين، الضبطية القضائية في القانون الجزائري دار هومة، الجزائر، 2009.

**111.** يوسف حسن يوسف، الجرائم الدولية للانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة 2011.

**112.** يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الإستراتيجية، السليمانية- العراق، 2007.

## II. الأطروحات والمذكرات

### أ/ الأطروحات.

**1.** أحمد محمد أبو مصطفى، الإرهاب ومواجهته جنائيا، أطروحة دكتوراه في القانون،كلية الحقوق، جامعة القاهرة 2007/2006.

**2.** إيهاب محمد يوسف، اتفاقيات تسليم المجرمين ودورها في تحقيق التعاون الدولي في مكافحة جرائم الإرهاب، رسالة دكتوراه مقدمة إلى أكاديمية الشرطة، 2003.

**3.** بخاوية إدريس، جريمة غسل الأموال ومكافحتها في القانون الجزائري، أطروحة دكتوراه في القانون الجنائي الخاص، جامعة أبو بكر بلقايد، تلمسان،2011 /2012.

**4.** بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة دكتوراه في القانون الجنائي والعلوم الجنائية، جامعة الجزائر1، 2015.

**5.**حسين محمد إبراهيم، الحماية الجنائية لحق المؤلف عبر الانترنت، رسالة دكتوراه في القانون –كلية الحقوق- جامعة عين شمس،2000.

**6.** ديش موسى، النظام القانوني لتعويض ضحايا الجرائم الإرهابية- دراسة مقارنة رسالة دكتوراه في القانون العام، كلية الحقوق، جامعة تلمسان 2016/2015.

7. ساعد إلهام حورية، وسائل مكافحة الإرهاب، أطروحة دكتوراه في القانون العام كلية الحقوق –سعيد حمدين– يوسف بن خدة، جمعة الجزائر01 2016/2015.
8. عبد الله علي عبو سلطان، دور القانون الدولي الجنائي في حماية حقوق الإنسان أطروحة دكتوراه في القانون العام كلية الحقوق، جامعة الموصل–العراق 2004/2003.
9. عمار تيسير بجبوج، التعاون الدولي في مكافحة جرائم الإرهاب، أطروحة دكتوراه في الحقوق، جامعة القاهرة– قسم القانون الجنائي، 2010.
10. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس، 2004.
11. محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي الإسكندرية، 2006.
12. محمد عبد الكريم عيسى العفيف، جرائم الإرهاب في قانون العقوبات الأردني– دراسة مقارنة، رسالة دكتوراه في فلسفة القانون العام، جامعة عمان العربية للدراسات العليا الأردن، 2006/2005.
13. يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه في القانون الخاص، جامعة باجي مختار، عنابة، 2016.

**ب/ مذكرات الماجستير**

1. أسمهان بوضياف، دور الدول والمنظمات العالمية والإقليمية في مكافحة الإرهاب الدولي والعلاقات الدولية، مذكرة ماجستير في القانون، جامعة بن عكنون– الجزائر، 2009.
2. حسن عزيز نور الحلو، الإرهاب في القانون الدولي–دراسة مقارنة، مذكرة ماجستير في القانون العام، الأكاديمية العربية المفتوحة، هلسنكي–فنلندا، 1427هـ/2007.
3. ذياب موسى البداينة، الإرهاب المعلوماتي، مذكرة ماجستير في القانون، كلية التدريب، جامعة نايف للعلوم الأمنية، 2008.

4. صابرة شعنبي، حق الدفاع الشرعي في القانون الدولي الجنائي، مذكرة ماجستير في القانون العام، جامعة عباس لغرور – خنشلة– قطب تبسة، 2012/2011.
5. ضيف الله بن شيب الجيلي، المساهمة التبعية في ارتكاب الجريمة الإرهابية وعقوبتها، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2009.
6. عادل عبد الصادق محمد الجخة، أثر الإرهاب الالكتروني على مبدأ استخدام القوة في العلاقات الدولية، مذكرة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في العلوم السياسية، كلية الاقتصاد والعلوم والسياسية –قسم العلوم السياسية، القاهرة، 2009.
7. محمد سعد الله، المنظمة الدولية للشرطة الجنائية ودورها في مناهضة الإرهاب الدولي، مذكرة ماجستير في القانون كلية الحقوق، بن عكنون– الجزائر، 2011.
8. مصطفى سعد حمد خلف، جريمة الإرهاب عبر الوسائط الالكترونية –دراسة مقارنة بين التشريعين الأردني والعراقي مذكرة ماجستير في القانون العام، كلية الحقوق جامعة الشرق الأوسط، كانون الثاني 2017.
9. نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الالكتروني مذكرة مكملة لنيل شهادة الماجستير في القانون الدولي العام، كلية الحقوق والعلوم السياسية– جامعة مولود معمري– تيزي وزو.
10. نسيب نجيب، التعاون الدولي في مكافحة الإرهاب، مذكرة مكملة لنيل الماجستير في القانون ،كلية الحقوق والعلوم السياسية –جامعة مولود معمري– تيزي وزو، 2009

## III. المقالات والأبحاث العلمية.

1. إبراهيم نايل عيد، السياسة الجنائية لمكافحة الإرهاب الالكتروني، بحث مقدم للحلقة العلمية بعنوان" الانترنت والإرهاب" في الفترة 15–2008/11/19، عين شمس – القاهرة.
2. آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الالكتروني بالجزائر، مداخلة في الملتقى الدولي

حول "الإجرام السيبراني –المفاهيم والتحديات، في الفترة 11-2017/04/12 جامعة 08 ماي 1945 قالمة- الجزائر.

**3.** إلياس أبو جودة، الإرهاب والجهود الدولية والإقليمية في مكافحته، مجلة منشورات الجيش اللبناني، العدد 91، 15 كانون الثاني 2015، بيروت- لبنان.

**4.** أيسر محمد عطية ، الآليات الحديثة للحد من الجرائم المستحدثة- الإرهاب الالكتروني وطرق مواجهته، ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، عمان- الأردن، في الفترة من 2-2014/09/4.

**5.** بوعناد فاطمة الزهرة، مكافحة الجريمة إلالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول مركز الدراسات القانونية، الجزائر، 2013.

**6.** جبار علي صالح، الجهود العربية لمكافحة الإرهاب، مجلة دراسات دولية مركز الدراسات الإستراتيجية والدولية بغداد العدد السادس والأربعون، 2010.

**7.** جميل عبد الباقي لصغير، مدى كفاية نصوص قانون العقوبات والإجراءات الجنائية لمواجهة الانترنت عبر الانترنت بحث مقدم في الحلقة العلمية بعنوان "الانترنت والإرهاب"، في الفترة 15-2008/11/19، عين شمس- القاهرة.

**8.** جميلة محلق، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار –عنابة عدد 42 ، جوان 2015 .

**9.** حسن بن أحمد الشهري، أهمية القواعد الخاصة بمكافحة الإرهاب- بناء قاعدة بيانات دولية لمكافحة الإرهاب – مشروع مقترح ، بحث مقدم للندوة العلمية لمركز الدراسات والبحوث- قسم الندوات واللقاءات العلمية، في الفترة من 25-27 ماي 2009.

**10.** حسن بن أحمد الشهري، بناء قاعدة بيانات دولية لمكافحة الإرهاب- مشروع مقترح، المجلة العربية للدراسات الأمنية والتدريب، المجلد 26، العدد 51،الرياض.

**11.** ذياب موسى البداينة، الإرهاب المعلوماتي،أبحاث الحلقة العلمية حول "الانترنت والإرهاب"، كلية التدريب جامعة نايف للعلوم الأمنية بالتعاون مع جامعة عين شمس، 2008.

**12.** رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، مقالة مقدمة في الدورة التدريبية الموسومة بالعنوان:" توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب"ن خلال الفترة 13-2012/04/17 إلى غاية 23-2013/02/27 الرياض، 2013.

**13.** ربيعي حسين، المراقبة الالكترونية وحق الفرد في الخصوصية داخل الفضاء الرقمي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 01-2016 لسنة 2016.

**14.** سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، بحث مقدم إلى جامعة كربلاء، 1437 هـ/ 2016 م.

**15.** صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال"Videoconference"، مجلة علوم الشريعة والقانون، المجلد 42، العدد الأول، جامعة الأردن، 2015.

**16.** طارق محمد الجميلي، الدليل الرقمي في مجال الإثبات الجنائي، مقالة مقدمة في المؤتمر المغربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا طرابلس-ليبيا في الفترة الممتدة من: 28-2009/10/29.

**17.** عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الانترنت، المنعقد في القاهرة في من 2 إلى 4 يونيو 2008، القاهرة.

**18.** عبد الرحمان السند، وسائل الإرهاب الالكتروني-حكمها في الإسلام وطرق مكافحتها، بحث مقدم للجنة العلمية للمؤتمر العالمي عن موقف الإسلام من الإرهاب جامعة الإمام محمد بن سعود الإسلامية، 2004.

**19.** عبد الفتاح مصطفى الصيفي، الاعتداء الواقع على أمن الدولة والأموال- قانون العقوبات اللبناني، دار النهضة العربية، بيروت، 1972.

**20.** عبد الله حامد الكيلاني، جهود مكافحة الإرهاب النووي على الصعيد العربي مداخلة في قمة جامعة الدول العربية الرياض، في الفترة بين 3-5 جوان 2013.

**21.** عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة القاهرة، 2005.

**22.** علي عدنان الفيل، جريمة الإرهاب الالكتروني، مجلة الملحق القضائي، العدد 44، المعهد العالي للقضاء، المملكة المغربية، 2011.

**23.** فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراء تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة 01، عدد 33، جوان 2010.

**24.** فهد يوسف الكساسبة، الإرهاب الالكتروني في التشريع الأردني، مجلة العلوم القانونية والسياسية، جامعة عمان العربية، العدد التاسع، 2015.

**25.** ماجد الحموي، قضية لوكربي بين السياسة والقانون- العلاقة بين محكمة العدل الدولية ومجلس الأمن، مجلة جامعة دمشق، المجلد السابع عشر، العدد الثاني سوريا، 2001 .

**26.** مأمون سلامة، إجرام العنف، مجلة القانون والاقتصاد ، العدد الثاني للسنة الرابعة والأربعون، جويلية 1974.

**27.** ماهر الجنيدي، النصر للأقوى والذكي والقذر، مجلة انترنت العالم العربي، العدد 36، نوفمبر 1999.

**28.** محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستخدمة ، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، في الفترة 25-1993/10/28، القاهرة.

**29.** محمد صبحي نجم، شرح قانون العقوبات-القسم العام، دار الأوائل، عمان-الأردن، 2000.

**30.** محمد مؤنس محي الدين، الإرهاب في القانون الجنائي على المستويين الوطني والدولي، المكتبة الانكلو- مصرية مصر،(دون سنة نشر).

**31.** مقني بن عمار بوراس عبد القادر، التنصت على المكالمات الهاتفية واعتراض المراسلات كآلية للوقاية من جرائم الفساد ، مداخلة مقدمة للملتقى الوطني حول الآليات القانونية لمكافحة الفساد، جامعة ورقلة، في الفترة من 2-2008/12/3.

**32.** وليد عاكوم، التحقيق في جرائم الحاسوب، مداخلة ألقيت في الملتقى العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، المنعقد بأكاديمية شرطة دبي(ا.ع.م) في الفترة من(28/26 أفريل 2003).

**33.** يونس زكور، الإرهاب وإشكالية تحديد المفهوم، مقالة منشورة في مجلة الحوار المتمدن، العدد 1785 2006/12/08.

**34.** يونس عرب، صور الجرائم الالكترونية واتجاهاتها وتبويبها، بحث مقدم في مؤتمر مجموعة عرب للقانون، 2-4 نيسان، مسقط-عمان، 2006.

**35.** أعمال الندوة 32 لمجلس وزراء الداخلية العرب، مجلة الشرطة ، العدد 126 مارس 2015.

**36.** تغطية لأشغال الدورة 82 للجمعية العامة للانتربول بقرطاجنة -كولومبيا، مجلة الشرطة، العدد 121، نوفمبر 2013 .

**VI. المقالات الالكترونية.**

**1.** أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، مداخلة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية والقانون، متوافرة في الموقع: www.iefpedia.com.

**2.** باخوية إدريس، جرائم الإرهاب في دول المغرب العربي- تونس، الجزائر المغرب نموذجا، مقالة منشورة في مجلة الحقوق والعلوم السياسية، العدد 11 لسنة 2014 جامعة ورقلة متوافرة في موقع: www.revues /ouargla.dz.

**3.** بول روجرز، حماية أمريكا ضد الإرهاب عبر الانترنت، مقالة منشورة في موقع وزارة الخارجية الأمريكية، متوافرة على الرابط:

.http//usinfo.state.gov/journals/itps/1101/ijpa/focus4.htm

**4.** حسين بن سعيد، جرائم الإرهاب الالكتروني، بحث منشور في الموقع: .www.moheet.com

**5.** حسين بن سعيد الغافري، جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الانترنت، مقالة منشورة على الموقع:www.hussain- alghafri.blogspot.com .

**6.** خالد ممدوح، معاينة مسرح الجريمة الالكتروني، مقالة منشورة على الرابط: .ttps://kenanaonline.com/users/KhaledMamdouh/posts/81659

**7.** خلدون غسان سعيد، الإرهاب والجرائم المعلوماتية– اختطاف وتسميم يومي لمواقع والملفات، منشورة في الموقع: www.aawsat.com.

**8.** ضياء عبد الله عبود الجابر، وآخرون، المنظمة الدولية للشرطة الجنائية، بحث مقدم إلى مركز آدم للدفاع عن الحقوق والحريات منشور في الموقع: www.annabaa.org

**9.** عبد الرزاق العري، الإرهاب البيولوجي، مقال منشور على الموقع الأتي على شبكة الانترنت: http://www.omanday.com/20/locat/14.htm.

**10.**علي حسن طوالبة، التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية، بحث منشور في الموقع الالكتروني :www.policemc.gov.bh.

**11.** غسان ضياء المظفر، الاتفاق الجنائي، مجلة الحوار المتمدن، العدد 3621 2012/01/28، منشورة في الموقع: www.alhewar.org.

**1.** ليلى حسين، فعالية القوانين الوطنية والدولية في مكافحة الجرائم الالكتروني بحث في العلوم القانونية، قسم القانون في الأكاديمية العربية في الدانمارك، منشورة في موقع المنهل: https://platform.almanhal.com

**2.** محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية دار الناشري للنشر الالكتروني 2012، (متوافرة في الموقع www.nashiri.net).

**3.** محمد فارس، أخطر عشرة فيروسات في التاريخ، مقالة منشورة يوم 2011/08/18 في الموقع:http//itwadi.com/node/1928.

**4.** محمد بن علي كومان، تقرير حول دور مجلس وزراء الداخلية العرب في مكافحة الإرهاب، متوافرة على الرابط: .www.aim-coucil.org/SiteCollectionDocuments/2.pdf

**5.** مصطفى فؤاد عبيد، تقنيات التنقيب في قواعد البيانات واستكشاف المعلومات المخبأة فيها، بحث منشور في الموقع: www.itns.org.sa/ItnsMedia/26.ppt.

**17.** الجريدة الرسمية الأردنية رقم 2010/5056 الصادرة في 2010/09/16 متوافرة في الموقع: www.lawjo.net/vb/showthread.php?.

**18.** شرح قانون جرائم المعلوماتية السوداني لسنة 2007، مقالة منشورة في الموقع:http://ibrahimtahaa.blogspot.com/2013/07/2007.

**19.** قانون مكافحة الإرهاب المصري الصادر في 15 أغسطس 2015 منشور في الموقع:http//www.aljazeera.net/encyclopedia/events/2015/8/17.

**20.** مشروع قانون الجريمة الالكترونية المصري، منشور في جريدة الوطن متوافر في الموقع:http://Fr.scribd.com/document/266804184 .

**21.** ما هي أشهر فيروسات الحواسيب التي هددت العوالم الرقمية؟، مقالة منشورة في الموقع:www.alwasatnews.com/news/1126869.

**22.** مقالة منشورة في الموقع: www.desconceils.com.

**23.** إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، مقالة منشورة في موقع وكالة الأنباء الجزائرية، الأربعاء 14 ديسمبر 2016، على الرابط: www.aps.dz/sante.science.

**24.**الجزائر تبحث تحصين مؤسساتها من هجمات الإرهاب الالكتروني"، جريدة البلاد، على الموقع: www.elbilad.nd/article65620.

**25.**منظمة الدول الأمريكية، منشور في موقع ويكيبيديا: https://ar.wikipedia.org.

**26.** منظمة الدول الأمريكية، مقالة منشورة في موسوعة الجزيرة فضاء من المعرفة الرقمية، متوفرة في الموقع: http://www.aljazeera.net

**27.** مجموعة الثماني G8، منشورة في موقع ويكيبيديا: https://ar.wikipedia.org/wiki.

**28.**نتائج وتوصيات قمة مجموعة الثماني بمادلينا– أكيلا– ايطاليا، 2009، موقع قمة مجموعة الثماني :www.g8italia2009.it.

**29.**كيف تكافح أوروبا الإرهاب... وماذا تتضمّن "أجندة" 2015؟، مقالة منشورة في موقع النهار: https://newspaper.annahar.com.

**30.** الإعلان الختامي للمؤتمر الإقليمي حول الأمن المعلوماتي في قطر، متوافر على الرابط : http//ituarabic.org/2008/CIIP/Doha_Declaration.pdf

**31.** التقرير السنوي للاتحاد الدولي للاتصالات السلكية واللاسلكية لسنة 2007، متوافرة في الرابط:
https://www.mpttn.gov.dz/sites/.../Decret%20pres%20n°07-377.pdf

**32.**المنظمة العالمية للملكية الفكرية، مقالة منشورة على موقع الجزيرة : http://www.aljazeera.net..

**33.**البند السابع من القرار ق/296- دع/40-2007/6/20 في دورة انعقاده العادي الواحد والأربعون في 19 يونيو 2008 ، متوافر على الرابط:
www.arableagueonline.org/las/picture gallery/awards19june08.pdf.

**34.**ورقة جامعة الدول العربية في الملتقى العلمي :أثر الإرهاب على السلم والأمن العالمي، الرباط، في الفترة من 14-16 أكتوبر 2014 متوافرة على الرابط:
https://repository.nauss.edu.sa.

**35.** إجراءات قانونية للتعامل مع القنوات المسيئة- وزراء الإعلام العرب يضعون إستراتيجية مكافحة الإرهاب 2030 مقالة منشورة في الموقع عاجل الالكترونية:https://www.ajel.sa/local/1910531.

**36.** موقع مجلس وزراء العدل العرب متوافر على الرابط:
http//www.arablegalnet.org/ArabMinisters/ArabMinDecList.aspx?ID=24.

**37.**الرسالة الموجهة إلى رئيس مجلس الأمن(S/2005/309) من المراقب الدائم لجامعة الدول العربية لدى الأمم المتحدة المؤرخة في 10 ماي 2005، والتي تتضمن توصيات الندوة الإقليمية حول مكافحة الإرهاب المعقودة يومي 16-17 فيفري 2005 متوافرة على الرابط: http//daccess-ods.un.org/TMP/712647.html

**38.** مجلس وزراء العدل العرب يطالب بالحيلولة دون استغلال الإرهابيين تكنولوجيا المعلومات، مقالة منشورة في موقع القدس العربي:
http://www.alquds.co.uk/?p=635412

**39.**مجلس وزراء العدل العرب": مكافحة الإرهاب يتصدر أهم المشاريع..العمل على منع استغلال العناصر الإرهابية لتكنولوجيا المعلومات..ومحاربة غسل الأموال على أجندة الأولويات"، الدورة 59 بتاريخ 22 نوفمبر 2016 ، منشورة في موقع انفراد: http://www.innfrad.com/News/14/456518.

**40.**تنفيذي وزراء العدل العرب" يدعو للمصادقة على اتفاقية مكافحة الإرهاب"، الدورة الستين لمجلس وزراء العدل العرب القاهرة في 2017/05/17 منشور في موقع اليوم السابع: https://www.youm7.com/story/2017/5/1789 .

**41.**إستراتيجية جامعة الدول العربية في مكافحة الإرهاب متوافرة على الرابط: https://repository.nauss.edu.sa.

**42.**وثيقة المؤتمر الدولي حول تعزيز التعاون في مجال مكافحة الإرهاب المنعقد بباكو عاصمة أذربيجان 2013 متوافرة في الموقع: http://www.albawabhnews.com.

**43.**تقرير الأمين العام للأمم المتحدة حول "إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: أنشطة منظومة الأمم المتحدة لتنفيذ الإستراتيجية"، الأمم المتحدة، الدورة الثانية والستون، نيويورك، 7 تموز 2008، A/62/898 متوافرة في الموقع: https://www.lebarmy.gov.lb/.

**44.**ميثاق الأمم المتحدة، متوافر في الموقع :http://www.un.org .

**45.**مقالة حول قضية لوكربي منشورة في الموقع الالكتروني: المرجع الالكتروني للمعلوماتية: http://almerja.net.

**46.**أعمال الإرهاب، مقالة منشورة في موقع : المكافآت من أجل العدالة: www. rewardsforjustice.net.

**47.**الجرائم الإرهابية والجريمة المنظمة والاتجار بالمخدرات والرقيق والأعضاء البشرية، وغسيل الأموال والاتجار بالأسلحة، وتخريب وتعطيل وسائل المواصلات والاتصالات، منشورة في الموقع: http://www.aljazirah.com.

**48.**مؤتمرات الانتربول منشور على موقع المنظمة على شبكة الانترنت: http://www.interpol.int.

**49.**نص المادتين (14 – 16) من النظام الأساسي للمنظمة (الميثاق) وينظر أيضا الموقع الآتي: على شبكة الانترنت: http://www.Interpol.int/public/icpo/GeneralAssembly/defaultAr.asp.

**50.**مقررات اجتماع مجموعة دمج جهود مكافحة الإرهاب في الشرق الأوسط في 10/ ديسمبر / 2007 منشور على الموقع الأتي على شبكة الانترنت : .http://www.moiegypt.gov.eg/Arabic

**51.**بيان الأمين العام للجمعية العامة لمنظمة الانتربول سنة 2007 منشور في الموقع: .https://www.interpol.int/content/download/.../iaw2007AR

**52.**الاتفاقية الأوربية للمساعدة القضائية 1959/04/20 متوافرة في الموقع: . .http://conventions.coe.int/Treaty/en/Treaties/Wor d/030.doc

**53.**الصين.. إنشاء قاعدة بيانات عامة لمكافحة الإرهاب، مقالة منشورة في الموقع: .www.skynewsarabia.com

**IV.المعاجم والقواميس.**

**1.** ابن منظور، لسان العرب، الجزء الثاني، دار المعارف، مصر.

**2.** محمد الزبيدي، تاج العروس من جواهر القاموس، الجزء الثاني.

**3.** مختار الصحاح، طبعة الحادية عشرة، 1962.

**deuxièmes: les références en français**

**I. ouvrages.**

**1.** Bruce Middletion, Cyber crime investigator's field guide auevbach publication, New- York, 2000.

**2.** Dan Verton, Black ice-The Invisible Threat of Cyber-Terrorism, New York,McGraw-Hill,Osborne,2003.

**3.** David Bain Bridge, Introduction to Computer Law, Forth Edition, Longman, England, 2000.

**4.** Hans G.Nilsson, computer crimes and other crime against 1 information technology within the working programmer of the council of Europer R I D P Vol.64 1 st et 2 end tremesters, 1993

**5.** Information Security, Emerging Cyber Security Issues Thereaten Federal information systems, Washington, GAO,2005.

**6.** Jean Paul, masseron manuel, Pratique de la procédure policière, préface de robe, poplawsky, paris, 1946.

**7.** Jean Pradel, Les infractions de terrorisme, un nouvel exemple de L'eclatement du droit penal, Recual Dalloze Sirey, 7e chaier-chronque .

8. Joseph Léa NKALWO NGOULA, L'Union Africaine à l'épreuve du terrorisme : forces et challenges de la politique africaine de sécurité Cameroun, avril 2016.
9. Laqueur WALTER, Age of terrorism-Boston, Little, brown and CO-USA, 1987.
10. Linanatx AVIER et Allan HOLLANDE, pratique de droit informatique,4eme édition, Delmas,1998.
11. Pascal DE GENDT, L'Union Africaine face aux défit du continent, analyses et etudes politique international, 2016.
12. Pitter BELLEY, Hached attacked,Abused digital crime exposed,London,Regan page, 2002.
13. Silvia Cattori» ,**La Stratégie de la Tension : Le Terrorisme non revendiqué de l'OTAN** ,«Voltaire Edition Internationale, Zurich (Suisse), Décembre 2006.
14. Steven FURNEL, cyber crime vandalizing the information society,London, Addison cuesely,2002.
15. Thierry Meyssan,11septembre2001, L'effroyable imposture, Ed Carnot, Paris.
16. Tokson, Matthew J., Virtual Confrontation: Is (5) Videoconference Testimony by an Unavailable Witness Constitutional?, University of Chicago Law Review, Vol 74, No 4 June 11, 2007.
17. Webster desk, dictionnary English language portland house, new York 1990.
18. Yam padova, un aperçu de la lutte contre la cybercriminalité en franc, revue de science criminelle et droit pénal compare, 03/02/2002.


## II. les rapports.


1. rapport de la Réunion, à Washington (États-Unis d'Amérique), par l'Organisation des États américains (OEA) et son Comité Interaméricain contre le Terrorisme (CICTE); 7 octobre 2003, sur le site Comité contre le terrorisme du Conseil de sécurité de l'ONU
2. African Centre for the Study and Research on Terrorism (ACSRT), The African union terrorism situation analysis report (AU-TSAR) 2014 January-December 2014
3. Stratégie de l'Union Européenne visant à lutter contre le terrorisme ,«Le Monde, 5 décembre 2005.

## IV. Les Dictionnaires

**1.** oxford,word power, dictionnary of English language, Oxford University press, Oxford,1981.

**2.** Webster desk, dictionnary English language portland house, new York, 1990.

**3.** Faruq: Faruqi's law dictionary –English –Arabic ,forth revised Libraine Dul Harith Suleiman Ban– Beirut, 2003.

## III. les cites électroniques.

**1.** B.Collin, "THE FUTURE OF CYBER TERRORISM: Where the physical and virtual worlds converge", 11 the annual international symposium on criminal justice issues, 1996 http//www.irsem.defense.gouv.fr

**2.** Conseil de l'Union Européenne, Plan d'action pour lutter contre le terrorisme- Le Monde Diplomatique, 13 février 2006: www.consilium.europa.eu/media.

**3.** Les Ennemis d'internet 2014- rapport publier par l'organisation Reporters Sans Frontières a l'occasion de la journée mondiale contre la cyber-censure-12 Mars 2014- p 03 ,04. disponible sur internet- date de consultation : le 01 /11/2015. lien directe : www .12Mars .rsf .org.

**4.** .Macdonald Raegen- liberté sur internet et droit a la vie privée protection des données a caractère personnel et respect des formes l égales – Rapport présenté pour la Conférence des ministres du conseil de l'Europe responsable des medias et de la sécurité de l'information – Belgrade-Serbie- le 7 – 8 Novembre 2013-p 08 disponible sur internet – date de consultation 01 /11/2015. lien directe:

http://www.coe.int/t/dghl/standardsetting/media/belgrade2013/MCM (2013)008_Rapport_MacDonald_fr.pdf.

**5.** Muskoka Huntsville Canada, 25-26 juin 2010, L'Aquila (anciennement La Maddalena), Italie, 8-10 juillet 2009, Hokkaido, Japon, 7-9 juillet 2008, Heiligendamm, Allemagne, 6-8 juin 2007, Saint-Petersbourg, Russie, 15-17 juillet 2006, Gleneagles, Écosse, Royaume Uni, 6-8 juillet 2005, Sea Island, Georgie, Etats-Unis, 8-10 juin 2004, Evian, France, 1-3 juin 2003, Kananaskis, Canada, 26-27 juin 2002, Gênes, Italie, 20-22 juillet 2001, voir le Centre d'information sur le G8, sur le site http// www.g8.fr.

**6.** Mathieu OLIVIER, Kadhafi, Obiang, Mugabe… ces présidents de l'Union africaine qui font polémique, http://www.jeuneafrique.com, 02 février 2015.

**7.** Nick Heath,Nato- Cyber terrorism as dangerous as missile attack: http//software.silicon.com/security/0.39024655.39170300.00.htm.

**8.** Anderson, T. and C. Hsiao (1981). "Estimation of Dynamic Models with Error-Components Journal of the American Statistical Association 76: 598-606 https://amstat.tandfonline.com/doi/abs/.../01621459.198.

**9.** Lafree,G.&Dugan L,(2006).GTD II User Guide,STRAT Study of Terrorism and response to Terrorism,available at: http//www.start.umd.edu/start/data/gtd.

# فهرس المحتويات

# فهـــرس المحتويـــات

Summary.

As the development of the ICT world has had an unprecedented impact, as this development has had its advantages, it has had the disadvantages of reaching the possibility of destroying societies and the whole world. This is because of the development of serious crimes, the most important of which is the crime of terrorism The subject of this study.

Since all States are vulnerable to cyber-terrorist attacks at any time, anywhere and from any place, confronting and eradicating this crime is a fundamental objective pursued by all countries of the world with all their capabilities, structures and mechanisms. This is because of this great damage to societies and peoples.

In order to combat the crime of electronic terrorism and to rid humanity of its ravages and destructive effects, all countries have made commendable efforts individually, through the amendment of their national legislation in line with the reduction of this crime or in cooperation among themselves through the conclusion of international conventions in this field. For this crime through regional and international organizations.

Finally, we say that the efforts of all States to combat the crime of electronic terrorism continue to evolve and continue in an attempt to eliminate this crime, which threatens all aspects of economic, social, cultural and political life