# موقف التشريع الجزائري من جريمة الإرهاب الالكتروني

# The Attitude Of Algerian Legislation On The Crime Of Cyber Terrorism.

**محمد خميخم [1]**

[1] كلية الحقوق سعيد حمدين ، جامعة الجزائر -1- (الجزائر)، m.khmmikhem@univ-alger.dz

تاريخ الإرسال: 2019/01/31 تاريخ القبول:2020/05/08 تاريخ النشر: جوان2020

**الملخص**

يعتبر الإرهاب الالكتروني من أخطر الظواهر الإجرامية التي تهدد أمن الدول ، فهو الصورة المستحدثة للإرهاب التقليدي الذي استغل التكنولوجيا ووسائل الاتصال الحديثة ، و ما وفرته من مزايا لبث الرعب و الخوف في نفوس الأفراد و الاعتداء على أمن الدول و استقرارها ، و ذلك عن طريق استخدام شبكة الانترنت للقيام بالعمليات الإرهابية ، سواء من خلال إنشاء المواقع الالكترونية التي تبث الأفكار الضالة و الهدامة و المتطرفة و ببث البيانات و التصريحات و الأفلام المصورة التي تعلم كيفية استعمال الأسلحة و صنع المتفجرات و القيام بالعمليات الانتحارية ، أو من خلال تدمير البنى التحتية للدول و المؤسسات الدولية ، و هذا عن طريق اختراق الشبكات السلكية و اللاسلكية بواسطة الفيروسات و البرامج الخبيثة ، من أجل تحقيق أغراض سياسية أو دينية أو إيديولوجية أو اقتصادية أو غيرها.

**الكلمات المفتاحية** : جريمة ، إرهاب ، الكتروني ، موقف ، التشريع ، الجزائري .

**Abstract**

Cyber terrorism is a dangerous phenomenon that threatens the security of states to achieve political, economic, ideological and religious purposes.

Essentially, it is a new form of terrorism which takes advantage of media , technology and modern means of communication to spread terror among individuals and states. Modern means of communication like internet offer a range of opportunities to such terrorism.

Cyber terrorists use websites to broadcast statements and films inciting hatred , extremism and violence. Or else , they aim to destroy the infrastructure of institutes and states through spreading malwares, hacking networks, encrypting malicious programs and viruses.

**Key words** : crime , terrorism, electronic, the attitude , legislation, Algerian.

*المؤلف المرسل: محمد خميخم ، الإيميل المهني:* -m.khmmikhem@univ-alger.dz

**مقدمة**

أدت ثورة المعلومات و الاتصالات الحديثة ، و ما رافقها من تطور علمي و تكنولوجي رهيب إلى ظهور أشكال جديدة من الإجرام ، و التي من بينها الإرهاب الالكتروني الذي يعتبر النسخة الالكترونية للإرهاب التقليدي .

حيث استغل المجرمون المزايا التي توفرها البيئة التقنية لتنفيذ شتى العمليات الإرهابية ، سواء كان ذلك عن طريق استخدام شبكة الانترنت ووسائل التواصل الاجتماعي لتجنيد الأشخاص و تدريبهم أو إنشاء المواقع الالكترونية التي تثبت الأفكار الضالة و الهدامة أو ببث البيانات و التصريحات و الأفلام المصورة التي تعلمهم كيفية صناعة الأسلحة و المتفجرات والقيام بالعمليات الانتحارية ، أو من خلال القيام بتدمير البني التحتية للدول و المنظمات ، و هذا عن طريق اختراق الشبكات السلكية و اللاسلكية ، و ذلك بنشر الفيروسات و البرامج الخبيثة لتدمير الأنظمة المعلوماتية الخاصة بها أو توقيفها عن العمل ، وهذا من أجل بث و نشر الرعب و الخوف للإخلال بالوضع الأمني أو الاستقرار السياسي أو الوحدة الوطنية أو إدخال الخوف و الفزع بين المواطنين ، لتحقيق أغراض سياسية أو عقائدية أو إيديولوجية أو اقتصادية .

هذا ما استلزم من الدول إلى اتخاذ إجراءات و ابتكار وسائل و تقنيات من شأنها أن تحد من الإرهاب الالكتروني ، كما قامت بإصدار تشريعات تجرم أشكاله و صوره و تعاقب كل شخص تسول له نفسه القيام بذلك ، حيث سيتم تناول موضوع الإرهاب الالكتروني من خلال هذا البحث .

**أهمية البحث**

- حداثة وخصوبة البحث في موضوع ظاهرة الإرهاب الالكترونية باعتبار أنه موضوع جديد ظهر وتطور في كنف التقنيات الحديثة.
- خطورة ظاهرة الإرهاب الالكتروني، نظرا لأنه يهدد أمن و استقرار الدول و الشعوب في كافة أنحاء المعمورة.
- صعوبة الكشف عن مرتكبيه ، وتعدد وسائله ومظاهره وصعوبة حصره وتحديد حجم الخسائر التي يخلفها على الممتلكات العامة والخاصة .
- معرفة موقف التشريعات المقارنة من الظاهرة الإرهاب الالكتروني وموقف المشرع الجزائري من ذلك .

**أهداف البحث**

- محاولة التعرف على ظاهرة الإرهاب الالكتروني .
- توضيح أهم خصائص ومظاهر الإرهاب الالكتروني .
- محاولة تبيان مواقف التشريعات المقارنة من الإرهاب الالكتروني .
- الخروج ببعض التوصيات التي من شأنها أن تقلل أو تحول دون وقوع الإرهاب الالكتروني.

**مشكلة البحث**

تدور إشكالية موضوع هذا البحث حول جريمة الإرهاب الالكتروني، وذلك بتعريف هذه الجريمة وتناول خصائصها، ومحاولة البحث عن موقف التشريعات المقارنة منها و موقف التشريع الجزائري من ذلك، وهذا بطرح الإشكالية التالية: **ما مفهوم الإرهاب الالكتروني ؟ وما موقف التشريعات المقارنة منه ؟** حيث تتفرع عن الإشكالية الرئيسية الأسئلة الفرعية الآتية:

- ما هي التعريفات التشريعية و الفقهية لظاهرة الإرهاب الالكتروني ؟
- وما هي خصائصه و أشكاله ؟
- وما موقف التشريعات المقارنة منه ؟
- وما موقف المشرع الجزائري من ظاهرة الإرهاب الالكتروني ؟

**خطة البحث**

سيتم معالجة موضوع هذا البحث وفق الخطة الآتية: المبحث الأول ماهية الإرهاب الالكتروني، وفي المبحث الثاني موقف التشريعات المقارنة من الإرهاب الالكتروني، ثم خاتمة، تتضمن أهم النتائج والتوصيات التي تم التوصل إليها.

**المبحث الأول: ماهية جريمة الإرهاب الالكتروني وأركانها.**

صاحب الانتشار الواسع لشبكة الانترنت و التطور السريع في وسائل الاتصال و التقنيات الحديثة ظهور أشكال مستحدثة للإجرام الالكتروني ، وأصبحت تهدد أمن الأفراد والدول ، مستفيدة من طبيعة البيئة الالكترونية المفتوحة لوسائل الاتصال أين انتهز بعض الأشخاص ذلك للإضرار بالغير و القيام بأعمال إجرامية ، أطلق عليها الإرهاب الالكتروني ، مما اضطر الدول والمنظمات إلى البحث عن الآليات القانونية والفنية لمحاربة هذه الظاهرة والحد من آثارها ، وعليه سأسلط الضوء على دراسة هذه الجريمة ، وذلك بتناول مفهومها ( المطلب الأول ) ودراسة أركانها ( المطلب الثاني ) .

**المطلب الأول : مفهوم جريمة الإرهاب الالكتروني .**

اختلفت وتباينت التعريفات التي أعطيت لجريمة الإرهاب الالكتروني ويرجع ذلك إلى الاختلاف في وجهات النظر الدولية والاتجاهات السياسية ، وهذا تبعا للاختلاف في الإيديولوجيات و المصالح الدولية ، فما يراه البعض إرهابا ، يراه البعض الآخر عملا مشروعا ، ولذلك سأستعرض بعض التعريفات التشريعية

و الفقهية التي عرفت الإرهاب الالكتروني ( الفرع الأول ) ، وذكر الخصائص التي تميزه عن الجرائم الأخرى ( الفرع الثاني).

**الفرع الأول: تعريف جريمة الإرهاب الالكتروني.**

بالرغم من التباين والاختلاف في إعطاء تعريف جامع مانع لجريمة الإرهاب الالكتروني، إلا أنه كانت هناك محاولات تشريعية وفقهية لتعريف جريمة الإرهاب الالكتروني، والتي تتمثل في التعريفات التالية .

**أولا - التعريف التشريعي لجريمة الإرهاب الالكتروني :** عرفت بعض التشريعات المقارنة جريمة الإرهاب الالكتروني ، و هذا مثل ما نص عليه المشرع الأردني في المادة الثانية و الفقرة الخامسة من القانون منع الإرهاب رقم 55 لسنة 2006 ، حيث نصت على ما يلي : " **كل عمل مقصود يرتكب بأي وسيلة كانت تؤدي إلى قتل أي شخص أو التسبب بإيذائه ....**" [1].

أما الفقرة الخامسة من المادة الثالثة من نفس القانون السابق ، فتنص على : " مع مراعاة أحكام قانون العقوبات أو أي قانون آخر ، تعتبر الأعمال التالية في حكم الأعمال الإرهابية المحظورة ،... **استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع الكتروني لتسهيل القيام بأعمال إرهابية** أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل الأردني من شأنه تعريض الأردنيين أو ممتلكاتهم ...".

كما عرف القانون الجنائي الاسترالي لسنة 1995 المعدل و المتمم لسنة 2002 ، الإرهاب الالكتروني ، بأنه : " **كل عمل أو تهديد يسبب أذى جسمانيا جسيما أو يسبب الوفاة لشخص أو يعرض حياة شخص للخطر أو يحمل مخاطر جسيمة للصحة والسلامة العامة أو الممتلكات أو تدخلا خطيرا في الأنظمة الالكترونية ، على أن يكون القيام بالعمل أو ممارسة التهديد بقصد فرض مبدأ سياسي أوديني أو أيديولوجي ، أو لحمل الحكومة الاسترالية أو حكومة أجنبية و التأثير عليها على القيام بأمر ما أو بترويع الجمهور أو جزءا منه** "[2] .

كما أن هيئة الأمم المتحدة ، قد عرفت الإرهاب الالكتروني ، وهذا خلال شهر أكتوبر لسنة 2012 ، بأنه : " **استخدام الانترنت لنشر الأعمال الإرهابية** "[3].

أما المشرع الجزائري ، فقد تناول تعريف الإرهاب الالكتروني ، خلال نص المادة 87 مكرر 11 الفقرة الرابعة من قانون العقوبات الجزائري ، بأنه : " **استخدام تكنولوجيا الإعلام و الاتصال من أجل ارتكاب الأفعال الإرهابية ...**"[4] .

فمن خلال التعريفات المذكورة أعلاه ، ألاحظ أنها تناولت تعريف الإرهاب الالكتروني ، وقد أصابت في ذلك إلى حد بعيد ، خاصة المشرع الأردني والاسترالي ، أما بخصوص تعريف الأمم المتحدة ، فقد

جاء فضفاضا و لم يحدد التفاصيل اللازمة ، وبالنسبة للمشرع الجزائري فيبدو أنه قد أصاب في تعريفه ، إلا أنه ما يؤخذ عليه نصه حالة تخصيص الإرهاب الالكتروني في حالة السفر أو محاولة السفر للجزائري أو الأجنبي ، ولذلك أدعو المشرع الجزائري لتعديل نص المادة 87 مكرر 11 ، الفقرة الرابعة لتستوعب كل أشكال الإرهاب الالكتروني الأخرى ، إلا أن المادة الثانية من الفقرة الأولى من القانون رقم: 04/09 ، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ممكن أن تستوعب هذه الأشكال إلى حين تدخل المشرع و تعديل ذلك[5].

**ثانيا- التعريف الفقهي للإرهاب الالكتروني:** بالرغم من الاختلاف والتباين في إعطاء تعريف دقيق ومتفق عليه لجريمة الإرهاب الالكتروني ، إلا أنه قد كانت هناك العديد من المحاولات الفقهية لإعطاء تعريف مناسب لها ، حيث يعرفها جانب من الفقه ، بأنها : " استخدام التقنيات الرقمية ومهاجمة نظم المعلومات لإخافة و إخضاع الآخرين بدوافع سياسية أو عرقية أو دينية ."[6]، كما يعرفها جانب آخر ، بأنها : " استخدام الانترنت من أجل التسبب في إلحاق الضرر و الشلل بالأنظمة المعلومات و الاتصالات المدنية و العسكرية ، و قطع الاتصال بين الشبكات المختلفة ، و تعطيل أنظمة الطيران و الدفاع الجوي و اختراق النظام المصرفي وإرباك حركة المسافرين برا و جوا وشل محطات الطاقة الكهربائية و محطات تنقية المياه ، أو حتى مهاجمة القواعد الإستراتيجية المهمة مثل المواقع النووية "[7] .

بينما يعرفها طرف ثالث ، بأنها : " هجوم الكتروني عرضه تهديد أو العدوان على الحكومات ، و هذا من أجل تحقيق أهداف سياسية أو دينية أو إيديولوجية ، وأن ينتج عن هذا الهجوم أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب "[8].

وبذلك فلكي ينعت السلوك المرتكب بواسطة تقنيات المعلومات أو عن طريق شبكات الاتصال المختلفة بأنه سلوك إرهابي ، فلابد أن ينتج عليه عنف ضد الممتلكات أو الأشخاص ، أو يؤدي إلى إحداث الخوف والرعب أو إلحاق الضرر بالأفراد و الحكومات .

**الفرع الثاني: خصائص جريمة الإرهاب الالكتروني.**

تتميز جريمة الإرهاب الالكتروني ببعض الخصائص التي تميزها عن غيرها من الجرائم في هذا المجال، و التي تمثل فيما يلي:

**أولا- أنها جريمة عابرة للحدود الوطنية:** كان لربط العالم بشبكة الاتصالات من خلال الأقمار الصناعية والانترنت الأثر الكبير في انتشار جريمة الإرهاب الالكتروني، حيث أصبحت لا حدود جغرافية بين الدول و هذا نظرا لارتباط العالم بشبكة واحدة[9].

لذا نجد أن جرائم الإرهاب الالكتروني ترتكب من خلال شبكة الانترنت التي لا تحدها حدود ولا تعترف بعنصر المكان أو الزمان[10]، ونتج عن ذلك العديد من المشاكل القانونية الإجرائية حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة ، و كذا القانون الواجب التطبيق[11] .

**ثانيا - خفاء هذه الجريمة و سرعة تطورها :** إن جريمة الإرهاب الالكتروني التي تقع عبر الانترنت هي جريمة مخفية و مستترة في أغلبها ، لأن الضحية لا يمكن له أن يلاحظها رغم أنها تقع أثناء تواجده على شبكة الانترنت[12] ، فالجاني الذي يقوم بارتكابها يتمتع بقدرات فنية و تقنية تمكنه من إخفاء معالم هذه الجريمة و صعوبة الاحتفاظ الفني بآثارها إن و جدت[13] .

**ثالثا - أنها من الجرائم المتجددة:** جرائم الإرهاب الالكتروني من الأنماط الإجرامية المستحدثة، و هذا نظرا للأشكال المتعددة التي تأخذها في وقتنا الحاضر ما صعب مواكبتها و كشفها[14].

وتكمن خطورة هذه جريمة في كونها لا تأخذ شكلا أو نمطا أو أسلوبا معينا، وإنما تكشف تلك الأنماط و الأساليب بعد مرور حينا من الوقت على ارتكابها[15].

**رابعا - اعتبارها من الجرائم غير العنيفة[16] :** لا تتطلب جرائم الإرهاب الالكتروني عنفا لتنفيذها أو مجهودا كبيرا ، فهي تتميز بأنها من الجرائم الهادئة بطبيعتها[17] ، فكل ما يجب توفره من لوازم لارتكابها ، هو القدرة على التعامل مع جهاز الحاسوب أو الهواتف الذكية بمستوى تقني عالي ، إضافة إلى ربطه بشبكة الانترنت ، و توفر مجرم يوظف خبرته و قدرته على التعامل مع الشبكة للقيام بجرائم الإرهاب الالكتروني[18].

فمن هذا المنطلق تعد هذه الجريمة المرتكبة عبر الانترنت من الجرائم الناعمة ، فلا آثار لها في استعمال العنف أو القوة ، و إنما مجرد أرقام و بيانات يتم تغييرها من السجلات الالكترونية في ذاكرة الحواسيب ، و ليس لها أي أثر خارجي مادي[19].

**خامسا - صعوبة إثباتها :** يصعب على المحقق التقليدي التعامل مع هذه الجريمة ، فهي تتسم بالغموض و صعوبة الإثبات ، وهذا نظرا لافتقاد وجود الآثار التقليدية للجريمة ، و غياب الدليل الفيزيقي ( بصمات ، تخريب ، شواهد مادية ) ، و سهولة محو الدليل ، أو تدميره في زمن متناه في القصر[20]، لذا فإن معظم أشكال هذه الجريمة يتم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها [21]

**سادسا - اعتبارها من الجرائم الخطيرة :** تتسم جرائم الإرهاب الالكتروني بخطورتها البالغة ، و التي تتمثل في الخسائر الناجمة عنها تكون كبيرة جدا مقارنة بالجرائم التقليدية ، و تكلفتها المالية الضخمة وتعاظم آثارها على الدول والمجتمعات ، و هذا من حيث حجم الضحايا و الدمار الذي يصيب البنى التحتية والممتلكات و الآليات المستخدمة في شتى القطاعات[22] ، كما أنها ترتكب من فئات متعددة تجعل من الصعب التنبؤ بالجاني في هذه الجرائم[23] .

**المطلب الثاني: أركان جريمة الإرهاب الالكتروني.**

تتخذ جريمة الإرهاب الالكتروني من الفضاء الإلكتروني مسرحا لها ، مما يجعلها تتميز بخصوصيات تنفرد بها كما ذكرت سابقا ، إلا أن ذلك لا ينفي عدم وجود تشابه بينها و بين الجريمة المرتكبة في العالم المادي ، فهي مثلها مثل باقي الجرائم التي ترتكب عبر الانترنت ، و بالتالي فلا بد لها من وجود الركنين المادي والمعنوي الذي تقوم عليهما كل جريمة ، و بذلك سأوضح عناصر الركن المادي لجريمة الإرهاب الالكتروني (الفرع الأول) لأنتهي إلى تحديد الركن المعنوي فيها (الفرع الثاني) .

**الفرع الأول: الركن المادي لجريمة الإرهاب الالكتروني.**

حتى يقوم الركن المادي لهذه الجريمة لا بد له من توفر العناصر التالية، السلوك الإجرامي ( أ ) والنتيجة الإجرامية ( ب ) و العلاقة السببية بينهما (ج ).

**أ - السلوك الإجرامي :** يتطلب السلوك الإجرامي لجريمة الإرهاب الالكتروني وجود بيئة رقمية و اتصال بشبكة الانترنت ، حيث يتخذ السلوك الإجرامي في هذه الجريمة صورا متنوعة و متجددة مسايرة للتقدم التكنولوجي في هذا المجال ، سأحاول التركيز على أهمها و التي تتمثل في ما يلي :

**-تدمير المواقع و البيانات و النظم الالكترونية :** تتمثل هذه الصورة في قيام الإرهابيين و المنظمات الإرهابية بتبني الهجومات الكترونية من خلال شبكة الانترنت تستهدف تدمير المواقع و البيانات و النظم الالكترونية المتعلقة بالمؤسسات العامة و الخاصة ، إلحاق الضرر بالبنى التحتية و تدميرها أو توقيفها عن العمل كليا أو مؤقتا [24]، و هذا من خلال الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية تكون متصلة بشبكة الانترنت ، أو ما يعرف بنظام (Sever-pc) ، أو مجموعة أنظمة مترابطة شبكيا (Intranet) بهدف تخريب أو تعطيل نقطة الاتصال أو النظام[25] .

مما يحدث آثارا مادية و اقتصادية وسياسية كبيرة ، لأن ذلك يؤدى إلى توقف المرافق الحيوية عن النشاط ، كالحكومة الالكترونية وأجهزة الاتصال ووسائل النقل العامة ، وإلحاق الضرر بالأسواق المالية والبنوك[26] ، ويتم ذلك باستخدام الفيروسات[27]، وهذا من أجل الحصول على المعلومات التي لها علاقة بالأماكن و المنشآت الحيوية لاستهدافها بالعمليات الإرهابية ، أو عن بعد إذا كانت فيه إمكانية لذلك[28] .

**-التجسس الالكتروني :** هو عبارة عن التلصص وسرقة المعلومات من الأفراد والمؤسسات العامة و الخاصة و الدول و المنظمات ، وهذا من أجل معرفة الحالة الاقتصادية و المالية و السياسية التي تعيشها الدولة[29] ، ومن ثم استغلالها من طرف التنظيمات الإرهابية للقيام بعمليات إرهابية أو بيعها لدول معادية للدولة المستهدفة[30].

ومن بين طرق التجسس الالكتروني المستعملة أسلوب الاستيلاء على المعلومات الحساسة الهامة عن طريق إرفاق الرسائل الالكترونية مجهولة المصدر ببرامج وتطبيقات الكترونية من أجل فتح ثغرات الكترونية في حاسوب الضحية أو الشبكة الالكترونية المستعملة من طرفه[31] .

**-إنشاء المواقع الالكترونية الإرهابية :** تتمثل هذه الصورة في إنشاء وتصميم المنظمات الإرهابية لمواقع الكترونية لهم على شبكة الانترنت من أجل الوصول إلى أكبر شريحة من الناس للتأثير عليهم فكريا ونفسيا ، ومن ثم تجنيدهم أو الاستفادة منهم ماليا عن طريق التحويلات المالية التي يقدمونها تضامنا مع هذه التنظيمات الإرهابية[32] ، أو الاستفادة من المواقع الالكترونية لتلقين الأفراد المنظمة كيفية التدريب أو صناعة المتفجرات أو استعمال الأسلحة المختلفة أو شرح طرق الاختراق البريد الالكتروني أو تدمير المواقع الالكترونية أو الدخول إلى المواقع المحجوبة أو صناعة الفيروسات ونشرها[33] .

كما يمكن استعمال المواقع الالكترونية من قبل المنظمات الإرهابية في نشر بياناتها المختلفة، التي تأخذ أشكالا مختلفة فأحيانا تقدم الأهداف و الخطط العامة التي يسعى التنظيم الإرهابي لتحقيقها، و أحيانا أخرى تكون في شكل تهديد ووعيد بشن هجومات إرهابية على المصالح الحيوية للدول أو منظمات معينة، كما تستعمل هذه المواقع الالكترونية لإعلام المجتمعات و بتبني و تنفيذ عمليات إرهابية محدد أو إصدار بيانات التأكيد و النفي و التعليق على الأخبار والتصريحات الصادرة من الجهات الحكومية المختلفة[34] .

**-التهديد والترويع الالكتروني** : يتم استعمال المواقع الالكترونية التابعة للتنظيمات الإرهابية من أجل التأثير على نفسية الأفراد ، وذلك من خلال اللجوء إلى التهديد و الوعيد بقتل الشخصيات السياسية أو الدينية أو المؤثرة في المجتمعات الإنسانية، أو بالتهديد بتفجير المنشآت الحيوية أو الإستراتيجية في الدولة أو التهديد بتعطيل أو إتلاف الأنظمة الالكترونية للمنشآت القاعدية للدولة ،أو الخلق الضرر و الدمار بالشكات الالكترونية أو الأنظمة المعلوماتية [35]، بل وصل ببعض المنظمات الإرهابية إلى ابتزاز و تهديد رجال المال و الأعمال وإخضاعهم لمطالبها و ذلك بتقديم الأموال لها[36] .

**ب- النتيجة :** تعتبر النتيجة العنصر الثاني من عناصر الركن المادي في جريمة الإرهاب الالكتروني فهي تمثل الأثر المادي المترتب على السلوك الإجرامي والذي يحدث في العالم الخارجي أو المادي ، أي ما يسببه الجاني من ضرر أو خطر من شأنه أن يصيب أو يهدد مصلحة يحميها القانون[37] .

وبذلك فتتحقق النتيجة في جريمة الإرهاب الالكتروني متى كانت هناك حالة خطر عام، وهذا مثل خلق حالة من الفزع و الخوف في نفوس الأفراد ، أي من شأنه المساس بالاستقرار الذي يعيشه الناس داخل مجتمعهم ، وهذا مثل ما نص عليه المشرع الجزائري في نص المادة87 مكرر من قانون العقوبات الجزائري[38]، أومن شأن الفعل الإجرامي أن يؤدي إلى حدوث ضرر جسيم ، وهذا مثل الإضرار بالأفراد أو البنى التحتية و الإستراتجية للدولة أو المساس بالمؤسسات العامة و الخاصة وتدميرها أو تعطيلها عن العمل، و هذا بالاعتماد على شبكة الانترنت أي وجود بيئة رقمية مرتبطة بالشبكة المعلوماتية .

**ج-العلاقة السببية :** تمثل العلاقة السببية العنصر الثالث و الأخير من عناصر الركن المادي في جريمة الإرهاب الالكتروني ، حيث لا يكتمل هذا الركن إلا إذا قامت علاقة ما بين فعل الإرهاب الالكتروني و تحقق النتيجة ، و المتمثلة في إيجاد حالة من الخوف والذعر بين الأفراد أو الإخلال بالأمن العام أو الإضرار بالبنى التحتية الإستراتيجية للدولة[39].

ولذلك يجب لقيام جريمة الإرهاب الالكتروني أن تكون هناك رابطة مابين السلوك الإجرامي و النتيجة الإجرامية المحققة.

**الفرع الثاني: الركن المعنوي لجريمة الإرهاب الالكتروني.**

يعتبر الإرهاب الالكتروني جريمة عمدية تتطلب توافر القصد الجنائي العام فيها ، و الذي يتمثل في اتجاه إرادة الجاني إلى إحداث النتيجة الإجرامية ، و علمه بعناصر هذه الجريمة[40] ، وبذلك فهي لا تقع بطريق الخطأ ، إضافة إلى القصد الجنائي الخاص ، و المتمثل في انصراف إرادة الجاني إلى إيجاد حالة من الذعر و الخوف بين الأفراد أو الإخلال بالمن العام أو الضرار بالبنية التحتية للدولة أو الاعتداء على المؤسسات العمومية أو الخاصة[41].

وبذلك فإن القصد الجنائي في جريمة الإرهاب الالكتروني يمكن أن يكون الهدف منه الإضرار المعنوي و هو خلق الخوف و الذعر بين الناس أو الإخلال بالأمن العام ، وما لذلك من آثار كبيرة على الدولة ، كما يمكن أن يهدف إلى الإضرار المادي و المتمثل في تدمير أو الاعتداء على البنى التحتية والإستراتيجية للدولة أو المؤسسات الخاصة فيها [42].

**المبحث الثاني: موقف التشريع من جريمة الإرهاب الالكتروني.**

أصبحت جرائم الإرهاب الالكتروني هاجسا يؤرق مضجع الدول و الشعوب و المنظمات الدولية كافة ، حيث استغل الإرهابيون و الجماعات المتطرفة التقنية الحديثة ، وعلى رأسها شبكة الانترنت لتنفيذ الهجمات و ممارسة أنشطتها الإرهابية من أي مكان في العالم مخلفة بذلك أضرارا جسيمة على الأفراد و الدول ، و لذلك سعت العديد من الدول إلى اتخاذ التدابير القانونية و التقنية لمواجهة هذه الظاهرة الإجرامية ، حيث نصت على تجريمها و العقاب عليها ، و هذا ما سأحاول تبيانه من خلال تناول موقف التشريع المقارن من هذه الظاهرة (المطلب الأول ) وموقف التشريع الجزائري منها ( المطلب الثاني ) .

**المطلب الأول: موقف التشريع المقارن من ظاهرة الإرهاب الالكتروني .**

نصت العديد من التشريعات المقارنة على تجريم ظاهرة الإرهاب الالكتروني و اختلفت في النص على ذلك، سواء في قانون العقوبات أو القوانين الخاصة بالجرائم الالكترونية ونظم المعلومات.

حيث نص قانون مكافحة الإرهاب الأسترالي في المادة الأولى منه على تجريم الإرهاب الالكتروني و العقاب عليه[43] ، كما نص القانون الأمريكي المتعلق بالاحتيال و إساءة استخدام الحاسب الآلي و المعروف بـ: CFAA[44] ، على تجريم الإرهاب الالكتروني ، وهذا من خلال تجريم الأفعال التي ترتكب

ضد الحكومة الأمريكية ، أو ما يعرف بـ : Crime Against The Gouverment ، و تشمل جرائم تعطيل الأعمال الحكومية ، وتهديد السلامة العامة و الإرهاب الالكتروني و الأنشطة التأثيرية و العقاب عليه ، أما التشريع الفرنسي ، فقد جرم الإرهاب الالكتروني و عاقب عليه من خلال نص المادتين 323 و421-1 من قانون العقوبات الفرنسي النافذ [45].

وبخصوص التشريعات العربية ، فقد نصت على تجريم ظاهرة الإرهاب الالكتروني ، باعتبار أنها فرضت نفسها في الواقع ، حيث جرم المشرع الأردني في قانون منع الإرهاب هذه الظاهرة وعاقب عليها [46] ، كما جرم أيضا ذلك في المادة 10 من قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 [47].

أما المشرع السعودي، فقد جرم صور الإرهاب الالكتروني و عاقب عليه من خلال نص المادة الثالثة و الخامسة من المرسوم الملكي والمتعلق بقانون مكافحة الجرائم المعلوماتية [48].

كما جرم المشرع التونسي الإرهاب الالكتروني في الفصل الخامس و السادس و الثلاثون من قانون مكافحة الجرائم الإرهابية[49]، وإضافة إلى ما سبق ، نجد أن كل من التشريع الكويتي والإماراتي ، المتعلق بمكافحة جرائم تقنية المعلومات، قد نصا على تجريم بعض صور الإرهاب الالكتروني و العقاب عليه[50].

**المطلب الثاني: موقف التشريع الجزائري من ظاهرة الإرهاب الالكتروني.**

عانت الجزائر من ظاهرة الإرهاب ، لذلك كانت سباقة في النص على تجريم هذه الظاهرة الخطيرة وهذا من خلال نص المادة 87 مكرر من قانون العقوبات الجزائري ، إلا أنه وأمام ثورة تكنولوجيا المعلومات وما نتج عنها من تعاظم لمخاطر الإرهاب واتساع نطاقه ومجالاته إلى درجة أن أصبح ظاهرة عالمية تهدد كل المجتمع الدولي ، لذلك كان لزاما على المشرع الجزائري أن يواكب التطور التشريعي في هذا المجال ، وهذا من خلال تجريمه لظاهرة الإرهاب الالكتروني ، سواء من خلال نص المادة394 مكرر3 من قانون العقوبات ، أومن خلال المادة 87 مكرر11 ، الفقرة الرابعة ، وكذا المادة 87 مكرر12 الفقرة الأولى[51] ، وهي ترجمة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات[52] ، أومن خلال القانون رقم : 04/09 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال وبمكافحة[53].

إلا أن ما يعاب على المشرع الجزائري في هذا الجانب عدم وجود نص صريح يجرم الإرهاب الالكتروني و يعاقب عليه ، وهذا مثل ما نص عليه المشرع الأردني في المادة 10 من القانون رقم 30 لسنة 2010 والمتعلق بجرائم أنظمة المعلومات[54] ، خاصة وأن الجزائر متجهه إلى إنشاء الحكومة الالكترونية و استعمال أغلب المؤسسات سواء العامة أو الخاصة لتكنولوجيا الإعلام و شبكات الاتصال الالكترونية ، خاصة في القطاعات الحيوية مثل قطاع النقل بأنواعه وقطاع العدالة و الدفاع الوطني ، وغيرها من القطاعات الأخرى .

**خاتمـة**

يعتبر الإرهاب الالكتروني من أخطر الجرائم المستحدثة التي تهدد أمن الدول و الشعوب ، و هذا نظرا لتعدد أشكالها و تنوع أساليبها و اتساع مجال أهدافها ، مستفيدة بذلك مما وفرته تكنولوجيا الإعلام و الاتصال و التقنية الحديثة ، حيث يمكن ارتكابها عن بعد و دون اللجوء إلى العنف مع توفر قدر كبير من السلامة و الأمان لمرتكبيها ، لذلك نجد أن العديد من الدول قد سعت إلى اتخاذ الإجراءات القانونية و التدابير التقنية اللازمة لمواجهة هذه الظاهرة ، إلا أنها تبقى قليلة مقارنة بالأخطار و الأضرار التي يمكن أن تسببها للدول و الشعوب .

حيث خلصت من خلال دراسة جريمة الإرهاب الالكتروني إلى بعض النتائج و التوصيات، و التي أوجزها في النقاط التالية:

**أولا :** لا يوجد هناك اتفاق على تعريف قانوني جامع مانع للإرهاب الالكتروني في القانون الدولي ، ويرجع ذلك إلى نظرة كل دولة لهذه الظاهرة ، فالبعض يعتبره سلوكا إجراميا ويعاقب عليه ، بينما البعض الآخر يعتبره مقاومة مشروعة ، كما أن هناك تداخل لمفهوم الإرهاب الالكتروني مع غيره من المفاهيم الأخرى ، و هذا مثل الجريمة المنظمة الالكترونية و جريمة التجسس الالكتروني و القرصنة المعلوماتية .

**ثانيا:** يعتبر الإرهاب الالكتروني امتداد للجريمة الإرهابية التقليدية، ويكمن الفرق في الوسيلة المستعملة، والتي تتمثل في استغلال الوسائل الالكترونية و التقنية وشبكة الانترنت لارتكاب هذه الجريمة الخطيرة على الدول و الشعوب.

**ثالثا:** تتميز جريمة الإرهاب الالكتروني بعدة خصائص، و هذا مثل أنها من الجرائم العابرة للحدود، كما أنها ترتكب عن بعد و لا يتم اكتشافها إلا بعد فوات الأوان.

**رابعا :** تتنوع وتتمايز صور الإرهاب الالكتروني ، فمن إنشاء المواقع الالكترونية الإرهابية إلى استهداف البنية التحتية للدول عن طريق شبكة الانترنت ، و هذا مثل البنى الاقتصادية ووسائل الاتصال و المواقع العسكرية و المؤسسات العامة و الخاصة .

**خامسا :** اختلفت التشريعات المقارنة في تجريم ظاهرة الإرهاب الالكتروني و العقاب عليها ، فالبعض نص على تجريمها بطريقة غير مباشرة من خلال تجريم الدخول على المواقع الالكترونية أو تعطيلها أو إتلافها ، و البعض الآخر نص على تجريمها بطريقة مباشرة من خلال تجريم استعمال وسائل تكنولوجيا المعلومات في الإرهاب أو تسهيله أو تمويله أو تجنيد الأفراد للقيام بالأعمال الإرهابية .

**التوصيات**

**أولا:** ضرورة سن التشريعات التي تسد كافة حالات وصور الإرهاب الالكتروني من طرف المشرع الجزائري وتوضيح طرق التحقيق وجمع الأدلة وحفظها، و تسليم المجرمين والتعاون الدولي في هذا المجال.

**ثانيا:** تنسيق الجهود ما بين الجهات المختلفة في الدولة ، و ذلك باتخاذ الإجراءات الفنية و التقنية لحماية شبكات الاتصال المختلفة و الأنظمة المعلوماتية والمواقع الالكترونية الرسمية و المهمة من الاختراقات الالكترونية.

**ثالثا :** إنشاء فرق أمنية متخصصة من أجل مراقبة و متابعة الأعمال الإرهابية الالكترونية و تحديد موقعها ، وكذا القائمين بها تحت إشراف هيئات قضائية متخصصة في ذلك ، و العمل على تطوير قدرات الأجهزة الأمنية ،سواء المادية أو البشرية وذلك بتوفير التكوين العالي و المتخصص للعاملين في هذه الأجهزة من أجل التعامل مع هذا النوع من الإجرام الالكتروني .

**رابعا :** محاولة إنشاء مواقع الكترونية تتميز بالوسطية و الاعتدال ومحاربة التطرف الديني والفكري تحت إشراف هيئات علمية ودينية متخصصة ، والاستفادة من أفكار الكفاءات العلمية المتحكمة في تقنية المعلومات من أجل حماية هذه المواقع الالكترونية .

**خامسا :** ضرورة تعزيز التعاون و التنسيق بين الدول و المؤسسات الدولية المختلفة وتوحيد الجهود ، وذلك من خلال عقد الاتفاقيات الدولية لمحاربة جرائم الإرهاب الالكتروني ، وتحديد كافة الإجراءات اللازمة لتبادل المعلومات و الأدلة في هذا الشأن وتحديد طرق تسليم مرتكبي هذه الجرائم .

**الهوامش**

1- **قانون منع الإرهاب** رقم 55 لسنة 2006 ، المعدل و المتمم بالقانون رقم 18 لسنة 2014 ، الجريدة الرسمية العدد : 3365 الصادرة بتاريخ : 2014/06/01 : " كل عمل مقصود يرتكب بأي وسيلة كانت يؤدي إلى قتل أي شخص أو التسبب بإيذائه جسديا أو إيقاع أضرار".

2- رائد العدوان، **المعالجة الدولية لقضايا الإرهاب الالكتروني**، الدورة التدريبية الخاصة بتوظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ، المنعقد من طرف قسم البرامج التدريبية ، خلال الفترة 23-2013/02/27 ، الرياض ، السعودية ، ص : 06 .

3- علي مطر ، **الإرهاب الالكتروني في القانون الدولي** ، مقال منشور على الموقع الالكتروني : https:www.assakina.com/news/news1/31803.html ، تاريخ التصفح 2018/02/14، الساعة 18:30.

4 - المادة 87 مكرر 11 من القانون رقم 66-156 والمتعلق **بقانون العقوبات**، المعدل و المتمم بالقانون رقم: 16-02، الصادر بتاريخ: 2016/06/19 الجريدة الرسمية العدد: 37، الصادرة بتاريخ: 22 /2016/06

5- تنص المادة الثانية من الفقرة الأولى من القانون رقم : 04/09 المتعلق **بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال** ، المؤرخ في : 2009/08/05 ، الجريدة الرسمية العدد : 47 الصادرة بتاريخ : 2009/08/16 ، على ما يلي : " يقصد في مفهوم هذا القانون ، بما يأتي : الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية ....."

6- عبد العزيز بن حميدان الثمالي ، **تأثير الإرهاب الالكتروني وسبل مكافحته** ، مداخلة مقدمة ضممن فعاليات المؤتمر الإسلامي العالمي" **مكافحة الإرهاب** "من طرف رابطة العالم الإسلامي ، المنعقد بمكة ، السعودية ، بتاريخ 25/22 فبراير 2015 ، ص : 05

7- حسن بن أحمد الشهري ، **الإرهاب الالكتروني – حرب الشبكات –** المجلة العربية الدولية للمعلوماتية ، المجلد الرابع ، العدد 2 ، 2015 ،ص : 3 و 4.

8-Mehmet Yayla ,Cyber terrorism From The Criminal Law Perspective , Law And Justice Review , Volume: 5 , Issue: 1, June 2014 , p : 132-133

9- ذياب موسى البداينة ، **الأمن الوطني في عصر العولمة** ، جامعة نايف للعلوم الأمنية ، الرياض ، ط 1 ، 2011 ، ص : 92 .

10- حسين بن سعيد الغافري، **جهود السلطنة في مواجهة جرائم الانترنت**، ص: 03 ، متوفر على الموقع الالكتروني : http://www.eastlaws.com ، تاريخ التصفح : 2018/01/20 ، الساعة: 17:30 .

11- صغير يوسف ، **الجريمة المرتكبة عبر الانترنت** ، مذكرة ماجيستر في القانون ، تخصص قانون دولي للأعمال ، مدرسة الدكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2013 ، ص : 17 .

12 - ذياب موسى البداينة ، **مرجع سابق** ، ص : 91 .

13 - دويب حسين صابر ، **القوانين العربية و تشريعات تجريم الجرائم الإلكترونية و حماية المجتمع** ، مداخلة مقدمة ضمن فعاليات المؤتمر السادس لجمعية المكتبات و المعلومات ، **أمن المعلومات** ، ص : 06 .

14- بدر بن ناصر التميمي ، **الاحتيال في عقود التأمين و عقوبته** ، رسالة ماجيستر في العدالة الجنائية ، كلية الدراسات العليا ، جامعة نايف للعلوم الأمنية ، 2010 ، ص : 57 .

15- أحسن مبارك طالب ، **جرائم الاحتيال و العوامل الاجتماعية و النفسية المهيئة لها** ، جامعة نايف للعلوم الأمنية ، الرياض ، 2007 ، ص : 25 .

16- يطلق عليها البعض من الفقه ، الجرائم الناعمة لأنها لا تتطلب العنف لارتكابها ، لمزيد من التفصيل ، ذياب موسى البداينة ، **مرجع سابق** ، ص: 92 .

17- صغير يوسف ، **مرجع سابق** ، ص : 16.

18- سيناء عبد الله محسن ، **المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية** ، الندوة الإقليمية حول **الجرائم المتصلة بالكمبيوتر** ، الدار البيضاء ، المملكة المغربية ، أيام 10-20 جوان 2007 ، ص : 52.

19- صغير يوسف ، **مرجع سابق** ، ص : 16.

20- ذياب موسى البداينة ، **مرجع سابق** ، ص : 93 .

21- دويب حسين صابر ، **مرجع سابق** ، ص : 06.

22- عبد الله على عبد الله القحطاني، **إدارة امن المعلومات ودورها في الحد من الإرهاب الالكتروني بكلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة**، كلية العلوم الإدارية، جامعة نايف للعلوم الأمنية، 2017 ، ص : 36 .

23- حسين بن سعيد الغافري ، **جهود السلطنة في مواجهة جرائم الانترنت** ، **مرجع سابق** ، ص : 30.

24- عبد الرحمن المسند ، **وسائل الإرهاب الالكتروني ، حكمها في الإسلام وطرق مكافحتها** ، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب ، الجزء 1 ، الرياض، 2004 ، ص : 147 .

25- عبد الله على عبد الله القحطاني ، **مرجع سابق** ، ص :49 .

26-علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، 1999، ص: 56.

27- يعرف الفيروس بأنه عبارة عن برنامج الكتروني يلحق ضررا بنظام المعلومات والبيانات و له القدرة على التضاعف والانتشار بشكل رهيب ، والانتقال من جهاز إلى آخر بكل سهولة ، عبد الله على عبد الله القحطاني ، **مرجع سابق** ، ص :49 .

28- مايا حسن ملا خاطر ، **الإطار القانوني لجريمة الإرهاب الالكتروني** ، مجلة جامعة الناصر ، المجلد الأول ، العدد 5 ، يناير - يونيو ، 2015 ، ص : 135 .

29- جسن بن احمد الشهري، **مرجع سابق**، ص:15.

30- محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسوب الالكتروني ، دار الثقافة للطباعة والنشر ، 1997 ، ص : 71 .

31- عبد الله على عبد الله القحطاني ، **مرجع سابق** ، ص :51 .

32- حسن بن احمد الشهري ، **مرجع سابق** ، ص : 16 .

33- عبد العزيز بن حميدان الثمالي ، **مرجع سابق** ، ص : 14.

34- مايا حسن ملا خاطر ، **مرجع سابق** ، ص :136 .

35- عبد العزيز بن حميدان الثمالي ، **مرجع سابق** ، ص : 12.

36- حسن بن احمد الشهري ، **مرجع سابق** ، ص : 16 .

37- ضيف مفيدة ، **سياسة المشرع في مواجهة ظاهرة الإرهاب** ، مذكرة ماجيستر في قانون العقوبات والعلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة الإخوة منتوري ، قسنطينة ، 2010/2009 ، ص : 50 .

38- تنص المادة87 مكرر من قانون العقوبات الجزائري على ما يلي : " يعتبر فعلا إرهابيا أو تخريبيا، في مفهوم هذا الأمر، آل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي :

- 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،

-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 ،

–تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل ،

-إتلاف منشآت الملاحة الجوية أو البحرية أو البرية ،

-تخريب أو إتلاف وسائل الاتصال ،

-احتجاز الرهائن ،

-الاعتداءات باستعمال المتفجرات أو المواد البيولوجية أو الكيميائية أو النووية أو المشعة ،

-تمويل إرهابي أو منظمة إرهابية.

39- منال مروان منجد ، **المواجهة الجنائية الجرائم الإرهاب في القانون السوري – دراسة تحليلية-** ، مجلة مروان دمشق للعلوم الاقتصادية و القانونية ، المجلد: 70 ، العدد : 2 ، 2014 ، ص : 111 .

40-عبد الله بن محمد كريري، **الركن المعنوي في الجرائم المعلوماتية في النظام السعودي– دارسة تأصيلية–** رسالة ماجيستر، قسم العدالة الجنائية، كلية الدراسات العليا جامعة نايف للعلوم الأمنية، الرياض، 203،ص:45 .

41- مسلط ماجد على أبو ثنين ، **التحقيق والمحاكمة في جرائم الإرهاب في النظام السعودي – دراسة مقارنة -** ، رسالة ماجستير في الشريعة و القانون ، قسم الشريعة ، كلية العدالة الجنائية ، جامعة نايف للعربية للعلوم الأمنية .، 2017 ، ص : 47 .

42- منال مروان منجد ، **مرجع سابق** ، ص :111 .

43- قانون مكافحة الإرهاب الاسترالي، متوفر موقع الالكتروني: http :www.lawfoundation.net.au ، تاريخ الصفح : 2018/02/24 ، الساعة 11.00.

44-The Computer Fraud And Abuse Act ; 18 U.S.C. § 1030

45-Article 323 **de code pénal français** : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende » et Article : 421-1 : «Constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur, les infractions suivantes :……..
- 2° Les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique définis par le livre III du présent code ;……. ».

46- **قانون منع الإرهاب الأردني رقم : 55 لسنة 2006 ، المعدل و المتمم بالقانون رقم : 18 لسنة 2014** ، الصادر بتاريخ :2014/06/01 ، الجريدة الرسمية العدد: 3365.

47- تنص المادة 10 من **القانون الأردني المتعلق بجرائم أنظمة المعلومات** رقم : 30 لسنة 2010 ، الصادر بتاريخ : 2010/09/16 ، الجريدة الرسمية العدد: 5056 ، على ما يلي : " **كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو أنشأ 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 " .

48- المرسوم الملكي رقم م 17 ، الصادر بتاريخ : 1428/03/08 **والمتعلق بقانون مكافحة الجرائم المعلوماتية .**

49- قانون أساسي رقم 26 لسنة 2015 بتاريخ : 2015/08/07 و**المتعلق بمكافحة الإرهاب ومنع غسل الأموال** ، الرائد الرسمي ، عدد 63 الصادر بتاريخ 2015/08/07 ، ص : 2163 .

50- نص المشرع الكويتي على تجريم الإرهاب الالكتروني من خلال نص المادة العاشرة من القانون رقم : 63 لسنة 2015 و **المتعلق بمكافحة جرائم تقنية المعلومات** ، أما المشرع الإماراتي فقد نص على ذلك من خلال نص المادة 26 من القانون الاتحادي رقم : 05 لسنة 2012 و **المتعلق بمكافحة جرائم تقنية المعلومات** .

51- تنص المادة 87 مكرر 11 ، الفقرة الرابعة ، على ما يلي : " يعاقب بالسجن المؤقت من خمس سنوات إلى عشر سنوات و بغرامة من 100.000دج إلى 500.000 دج كل جزائري أو أجنبي .....**يستخدم تكنولوجيات الإعلام و الاتصال لارتكاب الأفعال المذكورة في هذه المادة** " ، و تنص المادة 87 مكرر 12 ، على ما يلي : " يعاقب بالسجن المؤقت من خمس سنوات إلى عشر سنوات و بغرامة من 100.000دج إلى 500.000 دج **كل من يستخدم تكنولوجيات الإعلام و الاتصال** لتجنيد الأشخاص لصالح إرهابي أو جمعية أو

تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة الأحكام هذا القسم ، أو ينظم شؤونها أو يعدم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة ".

52- تم التصديق "عليها بموجب المرسوم الرئاسي رقم 252/14 المؤرخ في : 2014/09/08 ، و الصادر ج رع 57 ، بتاريخ : 2014/08/28 ، ص : 04 .

53- تنص المادة 02 الفقرة الأولى من القانون رقم: 04/09 ، والمتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ، المؤرخ في 2009/08/05 ، و الصادر بتاريخ : 2009/08/16 ، الجريدة الرسمية العدد : 74 ، ص : 05 على ما يلي : ' الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات **و أي جريمة أخرى ترتكب أو يسهل ارتكابها منظومة أو نظام للاتصالات الالكترونية**...." .

54 - تنص المادة 10 من القانون الأردني رقم : 30 لسنة 2010 ، و المتعلق بجرائم أنظمة المعلومات ، و الصادر بتاريخ : 2010/09/16 ، الجريدة الرسمية العدد: 5056 ، على ما يلي : " **كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو أنشأ 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 " .