وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور –خنشلة–
كلية الحقوق و العلوم السياسية
قسم الحقوق
نيابة العمادة للدراسات وشؤون الطلبة

السياسة الجنائية لمكافحة الارهاب الالكتروني في التشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر تخصص:قانون جنائي

من إعداد الطالب:
موساوي محمد

تحت إشراف الأستاذ:
سلامي نـــادية

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الاصلية	الصفة
بدر الدين خلاف	أستاذ محاضر "أ"	جامعة عباس لغرور– خنشلة	رئيسا
نادية سلامي	أستاذ محاضر "ب"	جامعة عباس لغرور– خنشلة	مشرفاو مقررا
نجوى كواشي	أستاذ مساعد "أ"	جامعة عباس لغرور– خنشلة	عضوا ممتحنا

السنة الجامعية:2019/2018

مقدمـــــــــــة

أولا : التعريف بالموضوع:

إن عصر المعلوماتية والثورة المعلوماتية كما عرفها ألفيت توفلر [1] التي يشهدها العالم الحديث أدى إلى ظهور وتطور تقنية المعلومات وظهور الحاسبات الآلية التي قدمت للإنسان حياة أفضل سواء في القطاع الاقتصادي أو الفكري أو التربوي ...الخ ما يجعل من الصعوبة بمكان الاستغناء عن هذه التقنيات التي بفضلها حققت التواصل الإنساني والتي بفضلها أيضا أصبح العالم قرية صغيرة يتصل فيها الأشخاص والجماعات بعضهم ببعض رغم ألاف الكيلومترات التي تفصل بينهم، إلا أن هذا الوجه المشرق للتكنولوجيا قابله وجه مظلم لا يخلو من المخاطر يتمثل في ظهور نمط جديد للسلوك الإجرامي والذي عرف اليوم بما يسمى بالإرهاب الالكتروني حيث ظهر بأنماط وسلوكات مختلفة كثيرة المخاطر تستهدف غايات معينة. وتميز هذا النوع من الإرهاب عن غيره من أنواع الجرائم بالطريقة العصرية جاعلا من الموارد المعلوماتية والوسائل الالكترونية والبنية التحتية المعلوماتية هدف له وبحكم أن الجزائر هي الأخرى تشغل حيزا من هذا الفضاء الافتراضي فهي ليست بمنأى من هذا الخطر المتنامي الذي أصبح من الممكن أن يخترق الأنظمة والشبكات المعلوماتية وان يستخدمها أيضا في تدمير البنية التحتية المعلوماتية لحكومتها ومؤسساتها العامة وشركاتها الاقتصادية الكبرى. لذا توجب على المشرع الجزائري أن يوجد الآليات التي من خلالها يتم التصدي لهذا النوع من الإرهاب ومن اجل ذلك اخترت أن يكون موضوع بحثي في هذه المذكرة الموسومة بـ: **السياسة الجنائية لمكافحة الإرهاب الالكتروني في التشريع الجزائري.**

[1] الفين توفلر: **ولد سنة** 1928 **كاتب وعالم اجتماع** أمريكي **مؤلف "صدمة المستقبل** 1970" عرف بأعماله في مناقشة الثورة الرقمية وثورة الاتصالات .

ثانيا:أهمية الموضوع :

إن تحول الحديث عن ذلك الإرهاب التقليدي والعنف المحدود، المفهوم التفسير والتأثير إلى هذا النوع الجديد من الإرهاب الذي يمارسه الأفراد والجماعات والدول، بشكل حتم الاهتمام بهذه الظاهرة من قبل علماء ينتمون إلى مختلف صنوف العلوم الإنسانية وتقنيون من مختلف التخصصات سعيا وراء فهم هذا النوع من الجريمة ومحاولة منهم تقنينها وتقعيدها وصولا لفهمها وضبطها بما يضمن فعالية التصدي لها والحد من أثارها ومن هنا تتجلى أهمية هذا الموضوع وحاجة البحث العلمي و حاجتنا الماسة للكشف عن العناصر والمميزات التي تتميز بها هذه الظاهرة التي تتطور مع التطور الهائل في الأدوات والوسائل مازاد من عظم التحدي الذي تواجهه الأجهزة المكلفة بمحاربتها وتتطلب تكاتف جهود وتعبئة موارد وتكامل رؤى جهات متعددة على المستوى المحلي ، الإقليمي والدولي وكذا سن منظومة قانونية رادعة لهذا النوع من الإرهاب.

ثالثا:الإشـــكـــاليـة:

من جهة أخرى فالقانون الجنائي غير قابل للتطبيق إلا وفقا للتفسير الضيق للمواد الجزائية كمبدأ من مبادئ شرعية الجرائم والعقوبات وبالتالي لا يجوز للقاضي تحت أي غطاء أو تفسير واسع خلق جرائم تخرج عن نطاق نص القانون كما لا يجوز القياس في حالة الجرائم التقليدية المرتكبة بواسطة المعلوماتية بالنصوص التقليدية إلا إذا توافرت الأركان التي حددتها هذه النصوص [1] وفي سبيل الخروج من هذا اللبس فالإشكال الذي يمكن طرحه هو : **ما مفهوم الإرهاب الالكتروني وما مدى فعالية الآليات التي أرساها المشرع الجزائري للتصدي له ؟**

[1] أحسن بوسقيعة : الوجيز في القانون الجزائي العام ، الطبعة الأولى ،طبعة 2002 ، الديوان الوطني للأشغال التربوية (الجزائر) ،ص 58.

رابعا:أسباب اختيار الموضوع:

يعود السبب في اختيار هذا الموضوع كونه حديث متزامن مع التطور التكنولوجي لوسائل الاتصال والإعلام من جهة ومن جهة أخرى نظرا لكونه من بين المواضيع الأكثر تعقيدا سواءا من جانب ضبط مفهومه أو من جانب مكافحته بالنظر إلى المحيط الذي ترتكب فيه الجريمة وكذا فيما يخص التكييف الصحيح لكل تصرف في مجال المعلوماتية الذي جرمه القانون والذي غالبا ما كان غامضا من خلال نصوصه القانونية وصعب الإثبات .

أيضا اختيار هذا الموضوع لم يأت صدفة بل لوجود رغبة الاطلاع على مجال المعلوماتية من الناحية التقنية كما أن الموضوع يدخل في اختصاصي الدراسي .

خامسا:أهداف الموضوع:

يهدف هذا الموضوع إلى الوقوف على ماهية هذه الجريمة التي تتميز عن غيرها بالطريقة العصرية والوسائل الالكترونية الحديثة لارتكابها ومحاولة معرفة الأهداف التي تحاول هذه الجريمة ضربها وذلك من خلال الأنظمة الالكترونية والبنية التحتية المعلوماتية للدول والحكومات وكذا تجنيد الأفراد والجماعات وغيرها من الأهداف الإجرامية العابرة للحدود الإقليمية والدولية .

كما يهدف هذا الموضوع الى معرفة آليات السياسة الجنائية للمشرع الجزائري والدور الذي يلعبه في التصدي لهذا الخطر المتنامي من خلال التطرق للآليات الموضوعية والإجرائية في ظل القانون الجزائري لمكافحة الإرهاب الإلكتروني مع توضيح جهات الحكم المختصة بالفصل في هذا النوع من الإجرام .

سادسا:الصعوبـــــات:

إن من بين الصعوبات التي واجهة الدراسة هي بيان ماهية الإرهاب الالكتروني من حيث تقديم مفهوم محدد له وهذا البعد يتصل بالجانب النظري لغياب مفهوم عالمي واضح بسبب اختلاف الأطر الإيديولوجية وتضارب المصالح الدولية التي تنتفي معها الحيادية في تفسير الظاهرة الإرهابية الالكترونية بالإضافة إلى أن الإرهاب قد استفاد من التطور التكنولوجي مما

أدى إلى ظهور إشكالات غير تقليدية من الأعمال الإرهابية تكمن في استعمال وسيلة الانترنت التي لا تتطلب ربط حزام ناسف بالجسد، هذا التعقيد في التقنية صاحبه تعقيد في أسلوب المكافحة (التشريع).

ولعل من أهم الصعوبات هي قلة الأحكام والاجتهادات القضائية والبحوث الفقهية خاصة الوطنية إذا ما قارنها بالقوانين الدولية الأخرى التي تعرف ثراء سواء في الجانب النظري أو العقابي لما وصلت له هذه الدول من تطور وهو الأمر الذي جعلني أقوم بتحديد مجال الدراسة بما يتوافق وموضوع المذكرة الذي يقتصر على بيان ماهيتها وحصرها في السياسة الجنائية التي أتى بها المشرع الجزائي الجزائري قصد مكافحتها .

سابعا: المنهـــج.

لقد تم اعتماد المنهج الوصفي التحليلي في هذه الدراسة كونه منهج يعتمد على دراسة الظاهرة كما توجد في الواقع ويهتم بوصفها وصفا دقيقا سواء بالتطرق لتعريفها وكذا خصائصها ومميزاتها وتحليل النصوص القانونية التي تحكم وتنظم هذه الظاهرة أو الجريمة.

ثامنا:الخطـــة.

كما سبق وان قلنا في الإشكال القانوني **ما المقصود بالإرهاب الالكتروني وما هي الآليات التي أرساها المشرع الجزائري للتصدي للإرهاب الالكتروني؟** ولمحاولة الإجابة والإحاطة بالإشكال فقد تم تقسيم هذه المذكرة إلى فصلين:

الفصل الأول: الإطار ألمفاهيمي للإرهاب الالكتروني واحتوى ثلاثة مباحث رئيسية جاء فيها على التولي:

المبحث الأول: تعريف الإرهاب وهو المبحث الذي تم تقسيمه إلى ثلاثة مطالب وهي: المطلب الأول:تعريف الإرهاب لغة واصطلاحا المطلب الثاني: تعريف الإرهاب الالكتروني المطلب الثالث: وسائل الإرهاب الالكتروني.

المبحث الثاني: الجريمة الالكترونية، وتم تقسيمه إلى مطلبين جاء في المطلب الأول: تعريف الجريمة الالكترونية وذلك بالتطرق إلى خصائصها ومميزاتها وكذا أنواعها أما

المطلب الثاني فتناول الأسباب الدافعة لارتكاب الجريمة وكذا أهداف المجرم الالكتروني منها كما تناول أيضا صعوبة إثباتها باعتبارها جريمة عابرة للحدود .

المبحث الثالث:الإرهاب الالكتروني وصفحات التواصل الاجتماعي وتم تقسيمه إلى مطلبين جاء في المطلب الأول: تعريف مواقع التواصل الاجتماعي وذلك بالتطرق إلى مميزات الشبكات الاجتماعية وكذا أنواعها أما **المطلب الثاني** فتناول التجنيد عبر شبكات التواصل وكذا مدلول عملية التجنيد ، والانترنت كبيئة للتجنيد ، وفئة الشباب المستهدفة بالتجنيد.

الفصل الثاني: تناول آليات مكافحة الإرهاب الالكتروني في التشريع الجزائري واحتوى ثلاثة مباحث رئيسية جاء فيها على التولي:

المبحث الأول: الآليات الموضوعية لمكافحة الإرهاب الالكتروني وتم تقسيمه إلى مطلبين جاء في المطلب الأول: التجريم وذلك بالتطرق إلى النصوص القانونية التقليدية وكذا المستحدثة أما المطلب الثاني فتناول العقوبات المقررة لجرائم الإرهاب الالكتروني من خلال العقوبات المقررة على الشخص المعنوي والطبيعي .

المبحث الثاني:تناول الآليات الإجرائية لمكافحة الإرهاب الالكتروني وتم تقسيمه الى ثلاثة مطالب تناولت على التوالي مرحلة البحث والتحري ، أساليب التحري الخاصة وتم اختتام المبحث بالتطرق إلى الإجراءات الخاصة بالبحث والتحري الالكتروني .

المبحث الثالث:الآليات الإجرائية في ظل القانون 04/09 وتم تقسيمه إلى مطلبين المطلب الأول تم التطرق فيه إلى الأحكام الخاصة بالوقاية من جرائم الإعلام والاتصال من خلال تبيان الإجراءات الجديدة في قانون الإجراءات الجزائية وتوضيح إستراتيجية الجزائر في التعامل مع جرائم الإعلام والاتصال فيما تناول المطلب الثاني القوانين والهياكل الخاصة للتصدي للجرائم الالكترونية ، المطلب الثاني :القوانين والهياكل للتصدي للجرائم الالكترونية وكذا النتائج المحققة في إطار مكافحة الإرهاب.

وانتهت المذكرة بخاتمة تضمنت أهم النتائج المتوصل إليها من خلال الدراسة بالإضافة إلى بعض الاقتراحات.

الفصل الأول: الإطار ألمفاهيمي للإرهاب الالكتروني.

لقد تم تقسيم الفصل الى ثلاثة مباحث رئيسية من خلال التطرق إلى تعريف

الإرهاب التقليدي في المبحث الأول ، ثم التعريف بالجريمة الالكترونية في المبحث الثاني ليختتم الفصل بمبحث ثالث تناول الإرهاب الالكتروني وصفحات التواصل الاجتماعي

المبحـــث الأول: تعريف الإرهاب.

لم يتفق المجتمع الدولي على تعريف للإرهاب حتى غدا المفهوم من المشاكل التي تعترض الفكر السياسي والقانوني، والسبب ليس غموض المصطلح فقد تداولته العامة فضلا عن المتخصصين ولا لقصور المعاجم اللغوية عن تقديم المفردات لتعريفه ،ولكن حيث يجب أن يتطابق المفهوم مع مصادقه الخارجية ، اختلفت الإرادات السياسية تبعا لاختلاف مصالحها وأيديولوجياتها وما تريد الوصول إليه من عدم الاتفاق .

المطلب الأول: تعريف الإرهاب لغة واصطلاحا.

على الرغم من وجود أكثر من مائة تعريف للإرهاب [1]. ولكننا اقتصرنا على ما هو آت من خلال التطرق الى تعريفه في اللغة والاصطلاح .

الفرع الأول :الإرهاب في اللغة:

الإرهاب مصدر أرهب يرهب إرهابا وترهيبا، وأصله مأخوذ من الفعل الثلاثي رهب بالكسر– يرهب رهبة ورهبا –بالضم و بالفتح وبالتحريك – أي خاف، ورهب الشيء خافه، وأرهبه واسترهبه أخافه، وترهبه توعده، والرهبة الخوف والفزع [2]. قال ابن فارس [3]: الراء والهاء والباء أصلان: أحدهما يدل على خوف، والآخر على دقة وخفة. وجاء في تاج العروس: الإرهاب بالكسر – الإزعاج والإخافة[4].

---

[1] محمد عبد المطلب: تعريف الإرهاب الدولي بين الاعتبارات السياسية والاعتبارات الموضوعية، دار الجامعة الجديدة، الإسكندرية، مصر، ط 2007، ص 48.

[2] ابن فارس: هو احمد بن فارس القزويني الرازي أبو الحسين ، مقاييس اللغة، دار الفكر، 1979 م.

[3] ابن فارس: مجمل اللغة لأبن فارس، مؤسسة الرسالة، بيروت، ط/2، 1989 ص79.

[4] الزبيدي محمد :تاج العروس من جواهر القاموس. دار الهداية ، ص 538

و من خلال ما تقدم يتبين أن معنى الإرهاب في اللغة يدل على الإخافة والتفزيع والترويـــــع.

الفرع الثاني:الإرهاب في الاصطلاح:

لقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه، فما يراه البعض إرهابا يراه الآخر عملا مشروعا كما بذلت في هذا الشأن جهود مشكورة من أهل العلم والإنصاف، ومن بعض المجامع الإسلامية والعربية، وكذلك حاولت بعض الاتفاقيات الدولية أو الإقليمية تحديد المراد من هذا المصطلح، كما قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب، ويمكننا ذكر أهم التعاريف لهذا المصطلح:

فقد عرف مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي الإرهاب بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دينه ودمه وعقله وماله وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصور الحرابة وإخافة السبيل 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 أموالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة، أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها [1].

وعرفت الاتفاقية العربية لمكافحة الإرهاب بأنه: كل فعل من أفعال العنف أو التهديد به أية كانت دوافعه 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

[1] علي محيى الدين القره داغي: الإرهاب الدولي، دراسة فقهية تحليلية، ، الحلقة 3 تعريف معاهدة منظمة المؤتمر الإسلامي للإرهاب، موقع الاتحاد العام للعلماء المسلمين.

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

كما عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م الإرهاب بأنه: الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة[2] .وكذلك عرف الإتحاد الأوربي عام 2002م الإرهاب بأنه: أعمال ترتكب بهدف ترويع الأهالي أو إجبار حكومة أو هيئة دولية على القيام بعمل أو الامتناع عن القيام بعمل ما، أو تدمير الهياكل الأساسية السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو هيئة دولية، أو زعزعة استقرارها[3].

إن عدم الاتفاق على تعريف واضح للإرهاب هي أولى المشاكل في مواجهته، فكيف تواجه شيء لا تعرفه.!

المطلب الثاني: تعريف الإرهـاب الإلكتـــــروني:

ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة، ويستهدف غايات معينة، ويتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين. إن الإرهاب الإلكتروني يشير إلى عنصرين أساسيين هما: **الفضاء الافتراضي Cyber Space والإرهاب** Terrorism، إضافة إلى ذلك هناك كلمة أخرى تشير إلى الفضاء الإلكتروني وهي العالم الافتراضي World Virtual والذي يشير إلى التمثيل الرمزي والزائف والمجازي للمعلومات، وهو المكان الذي تعمل فيه أجهزة وبرامج الحاسوب والشبكات المعلوماتية، كما تتنقل فيه البيانات الإلكترونية، ونظرا لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية، فقد زادت الخطورة الإجرامية

[1] http://www.mokarabat.com visite le 04/05/2019 à 10h :39

[2] مفيد شهاب: موقع السياسة الدولية، دور المجتمع الدولي في مكافحة الإرهاب، http://www.siyassa.org.eg

[3] الاتحاد الدولي في مواجهة الإرهاب، http://arabic. euronews.com visite le 04/05/2019 à 11h :15

للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة. كما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وهناك ما يشير إلى إمكانية انهيار البنى التحتية للأنظمة والشبكات المعلوماتية في العالم كله، وليس في بعض المؤسسات والشركات الكبرى أو في بعض الدول المستهدفة فالإرهاب الإلكتروني أصبح خطرا يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره، حيث يقوم مستخدمه بعمله الإرهابي وهو مسترخ في منزله أو في مكتبه أو في غرفته الفندقية، وبعيدا عن أنظار السلطة والمجتمع. وتجدر الإشارة إلى أن تدمير شبكة معلوماتية تقدر خسائرها اليومية بأضعاف مضاعفة من انهيار مبنى أو قصف منشأة أو تفجير جسر أو اختطاف طائرة، وعندما انقطع الكابل البحري الذي يربط أوروبا بالشرق الأوسط في نهاية شهر يناير عام 2008م، وما أعقبه من انقطاع آخر للكابل القريب من ساحل دبي وخليج عمان، قدرت الخسائر المتولدة من ذلك والتي لحقت بقطاع الاتصالات والتعاملات الإلكترونية بمئات الملايين من الدولارات، ولا تزال الأسباب مجهولة من وراء ذلك الانقطاع المفاجئ. إن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال، فبدلا من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية. وتأسيسا على ما سبق يمكننا القول بأن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم؛ نظرا لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى، مع توفير

قدر كبير من السلامة والأمان للإرهابيين، ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب، وفي ضوء التعريفات السابقة يمكن القول بأن أفضل التعارف الاصطلاحية للإرهاب وأقربها إلى الصواب؛ هو من قصر ألفاظه وإيجاز عباراته، وشموله مختلف أنواع الإرهاب وأشكاله. وتأسيسا على ما سبق يمكننا تعريف الإرهاب الإلكتروني 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 الإلكترونية بشتى صنوف العدوان وصور الإفساد. فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم[1].

الفرع الأول: تاريخ الإرهـــاب:

أولا :يعود تاريخ العمل الإرهابي إلى ثقافة الإنسان بحب السيطرة وزجر الناس وتخويفهم بغية الحصول على مبتغاه بشكل يتعارض مع المفاهيم الاجتماعية الثابتة، والعمل الإرهابي عمل قديم يعود بنا بالتاريخ مئات السنين ولم يستحدث قريبا في تاريخنا المعاصر ،يظهر الإرهاب في العهد القديم للكتاب المقدس، وكانت هناك حوادث كثيرة من جرائم القتل السياسية، وحتى الاغتيالات المنهجية، في التاريخ اليوناني والروماني. وقد شغلت جريمة قتل يوليوس قيصر، على سبيل المثال لا الحصر، الكتاب والفنانين على مدى الألفي سنة التالية. وشغل التساؤل حول ما إذا كان قتل المستبد كما فعل وليام تيل، البطل القومي في الروايات السويسرية الزاخرة بأعمال البطولة مسموحا به، أجيالا من علماء اللاهوت والفلاسفة. ولم يكن هناك إجماع تام في الرأي، إلا أن رأي الأغلبية كان أن الإرهاب مسموح به في ظروف معينة. فعندما لا يترك ظالم مستبد – طاغية – هو عدو للبشرية جمعاء، ومنتهك للقوانين الإلهية والعدالة الإنسانية، سبيلا آخر أمام ضحاياه للخلاص من القمع غير المحتمل، فإن ارتكاب

[1] عبد الله بن عبد العزيز بن فهد العجلان: الإرهاب الإلكتروني في عصر المعلومات، بحث منشور.
http://icacc.ccis-imsiu.edu.sa visite le 04/05/2019 à 12h :39

عمل إرهابي يصبح عندها السهم الأخير، الملاذ الأخير للمظلومين بعد استنفاد جميع الوسائل الأخرى.

إلا أن الفلاسفة وعلماء اللاهوت كانوا يدركون، حتى آنذاك، وجود خطر كبير مقلق بإساءة استخدام مبدأ قتل المستبد المبرر، لإمكانية ادعاء اللجوء إلى استخدام الحجة الأخيرة أو السهم الأخير، عندما لا يكون هناك في الواقع سبب مبرر للقتل كما كان الحال لدى قتـــــل الملك هنري الرابع في فرنسا أو حين تكون هناك طرق أخرى متوفرة للتعبير عن الاحتجاج والمقاومة.

في هذه الأثناء، ظهرت مجموعات صغيرة انخرطت في الإرهاب المنهجي على امتداد فترات طويلة، كطائفة الحشاشين [1] السرية، المنبثقة عن الإسماعيليين المسلمين، التي قامت بعملياتها مما يعرف الآن بالعراق وإيران من القرن الثامن حتى القرن الرابع عشر ميلادي، وقامت بقتل الحكام والولاة والخلفاء وأحد ملوك القدس الصليبيين. وكان الحشاشون روادا في الإرهاب الانتحاري – وكان سلاحهم دائما الخنجر، وبما أن ضحاياهم كانوا يتمتعون دائما بحراسة جيدة، فقد كانت فرص الفرار معدومة فعليا. وحتى اللغة التي استخدموها ما زالت باقية حتى الآن، فقد كان المقاتل فدائيا، وهو تعبير يستخدم حتى يومنا هذا[2].

[1] طائفة الحشاشين أو الحشاشون أو الحشيشية أو الدعوة الجديدة كما أسموا أنفسهم هي طائفة إسماعيلية نزارية، انفصلت عن الفاطميين في أواخر القرن الخامس هجري / الحادي عشر ميلادي لتدعو إلى إمامة نزار المصطفى لدين الله ومن جاء من نسله، واشتهرت ما بين القرن 5 و 7 هجري الموافق 11 و 13 ميلادي، وكانت معاقلهم الأساسية في بلاد فارس وفي الشام بعد أن هاجر إليها بعضهم من إيران .أسس الطائفة الحسن بن الصباح الذي اتخذ من قلعة الموت في فارس مركزة لنشر دعوته؛ وترسيخ أركان دولته. ينظر :أبو الفتح محمد بن عبد الكريم بن أبي بكر أحمد الشهرستاني المتوفى: 548هـ الملل والنحل، مصر سنه 1846، م 2 ص 32-33

[2] وولتر لاكير: دراسات الإرهاب ،مقال منشور على موقع مرافئ www.marafea.org visite le 04/05/19

واستمر النشاط الإرهابي عبر نهاية القرون الوسطى وحتى العصر الحديث، وإن يكن على مستوى أقل إلى حد ما. وكان هذه العصر هو عصر الحروب الكبرى، كحرب الثلاثين عاما 1918 – 1998 والحروب النابليونية 1799 – 1815وفي مثل هذه الفترات الزمنية حين كان يتم قتل وجرح عدد كبير من الناس في ساحات المعارك، لم يكن أحد يعير اهتماما كبيرة لحادث عنف إرهابي يقع هنا وهناك على نطاق ضيق.

الفرع الثاني:أنـــواع الإرهاب:

1- إرهاب عقدي.

2- إرهاب عملي.

3- إرهاب فكري.

4- إرهاب أخلاقي.

5- **الإرهاب الفردي:** وهو الذي يقوم به الأفراد لأسباب متعددة

6- **الإرهاب الجماعي غير المنظم:** وهو الإرهاب الذي ترتكبه جماعات غير منظمة من الناس تحقيقا لمآرب خاصة.

7- **الإرهاب الجماعي المنظم:** الذي يتمثل في جماعات الإرهاب التي تديرها وتشرف عليها دول غير ظاهرة أو مؤسسات أو هيئات مختلفة.

8- **الإرهاب الدولي:** وهو الإرهاب الذي تقوم به دولة واحدة أو أكثر. فهو إما أن يكون إرهابا دوليا أحاديا وهو الذي ترتكبه دولة واحدة، أو إرهابا ثنائيا وهو الذي ترتكبه دولتان، أو إرهابا جماعيا وهو الذي ترتكبه مجموعة من الدول أو يقع من دولة واحدة ولكن بدعم من دول أو حلف من الدول الأخرى[1].

[1] حنا عيسى: الإرهاب تاريخه وأنواعه وأسبابه. http://www.abouna.org visite le 04/05/2019

المطلب الثالث: وسائل الإرهاب الالكتروني.

نظرا لتطور السريع لتكنولوجيا المعلوماتية ووسائلها فقد استمد الإرهاب الالكتروني وسائله منها معتمدا بذلك على العديد من الخدمات التي توفرها هذه الأخيرة

الفرع الأول:البريد الإلكتروني:

خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وتعد هذه الخدمة من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما تمثله من سرعة في إيصال الرسالة وسهولة الإطلاع عليها في أي مكان، فلا ترتبط الرسالة الإلكترونية المرسلة بمكان معين، بل يمكن الاطلاع عليها وقراءتها في أي مكان من العالم.

وعلى الرغم من أن البريد الإلكتروني E-mail أصبح أكثر الوسائل استخداما في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمنا وسرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين له[1].

الفرع الثاني :إنشاء مواقع على الإنترنت:

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك.

[1] وسائل الإرهاب الالكتروني، المكتبة الشاملة. http://shamela.ws visite le 04/05/2019

والموقع هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل Hyper textmark up language HTML ولأجل رؤية هذه الصفحات يتطلب استعراض شبكة المعلومات العنكبوتية WWW Browser ويقوم بحل رموز HTML وإصدار التعليمات لإظهار الصفحات المتكونة[1]. وتسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الإنترنت في شهر أكتوبر 2000م إلى أكثر من 22 مليون موقع[2].

الفرع الثالث:اختراق المواقع

يستطيع قراصنة الحاسب الآلي **Hackers** التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي[3].

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، أو عن طريق نشر الفيروسات وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي [4].

---

[1] سايمونكولن: التجارة على الإنترنت، ، نقله إلى العربية يحيى مصلح، بيت الأفكار الدولية بأمريكا 1999م، دط ،ص29

[2] موقع: www.yahoo.com .

[3] سهير حجازي: التهديدات الإجرامية للتجارة الإلكترونية ، مركز البحوث والدراسات ، شرطة دبي ، دولة الإمارات العربية المتحدة ، العدد91.

[4] موزة المزروعي : الاختراقات الإلكترونية خطر كيف نواجهه ، مجلة آفاق اقتصادية ، دولة الإمارات العربية المتحدة ، العدد التاسع ، سبتمبر 2000م ، ص 54.

المبحث الثاني: الجريمة الالكترونية:

لقد تم التطرق في هذا المبحث إلى تعريف الجريمة المعلوماتية من خلال إبراز أهم خصائصها وكذا مميزاتها وأنواعها مع إبراز الدوافع لارتكابها وأهداف المجرم منها

المطلب الأول: تعريف الجريمة الإلكترونية.

جاءت غالبية قوانين العقوبات الحديثة خالية من تعريف للجريمة ومن هذه القوانين قانون العقوبات العراقي والمصري والايطالي والفرنسي والسوري واللبناني والكويتي والليبي والأردني والسوداني[1].

في حين ذهبت قوانين أخرى باتجاه احتوائها على تعريف عام للجريمة كقانون العقوبات الاسباني الصادر عام 1928م والبولوني الصادر 1932م والسويسري الصادر 1937م الصادر عام 1958م وقانون العقوبات السويدي الصادر عام 1965م الذي عرف الجريمة " التصرف الذي يتبعه عقاب منصوص عليه في هذا القانون أو أي قانون آخر[2]. وعرفها آخرون " هي كل فعل أو نشاط يتم بطريقة غير مشرعة [3]"، بمعنى كل نشاط مخالف للقوانين العرفية والوضعية المتعارف عليها والمعمول بها عبر مختلف دول العالم.. هذا النشاط إذا ما استخدمت فيه وسائط تقنية علمية، أصبح الفعل جريمة إلكترونية، فالجريمة إلكترونية " هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها"[4].

---

[1] علي حسين الخلف و.سلطان عبد القادر الشاوي :المبادئ العامة في قانون العقوبات ،بيروت2012 ،د ط، ص130.

[2] المصدر نفسه ص 131.

[3] وليد محمد حجاج: شرح قانون العقوبات القسم العام كلية الحقوق جامعة أسيوط 2006،د ط ،ص112.

[4] تعريف خبراء منظمة التعاون الاقتصادي والتنمية وتم مناقشة هذا التعريف في اجتماع المنظمة بباريس عام 1983.

وعرفها آخر" هي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات[1].

ونعتت الجريمة الالكترونية بعدة مسميات منها : جرائم الحاسب الآلي ، وجريمة الكمبيوتر والانترنت، وجريمة إساءة استخدام تقنية المعلومات، الجريمة السايبرية وهناك من يطلق عليها الجرائم المستحدثة[2].

وجاء تعريف الجريمة الإلكترونية في الإطار العربي حينما أقامت الجامعة العربية الندوة العربية في 1998/02/01في إطار تعريف الجريمة المنظمة وجاء تعريف الجريمة المنظمة بأنها كل سلوك إجرامي ترتكبه مجموعة من الأشخاص يحترفون الإجرام بشكل مستمر لتحقيق أهدافهم ضمن نطاق أكثر من دولة من المعلوم أن كلمة تكنولوجيا Technology كلمة أصلها يوناني وهي تتكون من مقطعين Techno وتعني الفن أو الصناعة، والمقطع الثاني logos وتعني الدراسة أو العلم، وبالتالي يكون معنى كلمة تكنولوجيا علم الفنون – أو علم الصناعة أو دراسة الفنون أو الصناعة، ومع كثرة استخدام لفظ التكنولوجيا في اللغة العربية اكتسب مع مرور الزمن لفظة عربية أو سمة عربية لأن هناك صعوبة في إيجاد كلمة معربة تدل تماما على المعنى، وقد تم عرض لفظ تكنولوجيا على مجمع اللغة العربية المصري فانتهى إلى أن لفظ تكنولوجيا يقابل في اللغة العربية لفظ "التقنية" بكسر التاء وسكون القاف وكسر النون، ويفضل بعض الفقهاء تعريف كلمة التكنولوجيا على كلمة التقنية ذلك لأن كلمة التقنية والإتقان مشتقة من الفعل تقن وإتقان الأمر إحكام[3].

---

[1] هلال بن محمد: الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دراسة قانونية وفنية مقارنة ،دار النهضة العربية، مصر 2009 ، ص 21.

[2] عبد الفتاح بيومي: مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي ، ص20.

[3] محمد السيد اليماني: الجوانب القانونية لدور براءة الاختراع في نقل التكنولوجيا، د ط ، ص 09.

أما عن التعريف القانوني لمصطلح التكنولوجيا، فقد عرفت بأنها "مجموعة معلومات تتعلق بكيفية تطبيق نظرية علمية أو اختراع ويطلق عليها في الاصطلاح حق المعرفة[1].

فالتكنولوجيا منهج علمي جديد قوامه أعداد الأجهزة التي يمكن بها نقل العلم النظري إلى التطبيق العملي، ونخلص من كل ما سبق إلى أن الجريمة تكون إلكترونية إذا ثبت لجهات التحقيق والتحري أنها تعتمد على النهج العلمي والمعرفة العلمية وأدواتها وأساليب التقنية الحديثة، وإلا سقط عن هذه الجريمة صفة إلكترونية، وبالتالي لا يحق أن تلقى المعاملة العقابية التي قررها المشرع العقابي للجريمة الإلكترونية في قانون الجرائم المعلوماتية لسنة 2007م.

الفرع الأول:خصائص الجريمة الالكترونية

أولا: تتمحور خصائص الجريمة الالكترونية بالمحاور التالية:

1) الدافع على الارتكاب.
2) موضوعها من مراحل تشغيل نظام المعالجة للبيانات.
3) التواطؤ والتعاون على الإضرار.
4) دور المخالطة الفارقة.
5) إعراض النخبة.
6) الإضرار.
7) صعوبة الاكتشاف.

[1] محسن شفيق: نقل التكنولوجيا من الناحية القانونية، جامعة القاهرة ،طبعة 1984م ، ص 04.

الفرع الثاني:مميزات الجريمة الالكترونية

تتجلى أهم مميزات الجريمة الالكترونية فيما يلي :

1. عابرة للدول بصعوبة الإثبات
2. مغرية للمجرم
3. ناعمة.

1-1 عابرة للدول:

في عصر الجريمة الالكترونية ومع انتشار شبكة المعلومات العالمية الانترنت مما أدى إلى ربط إعداد هائلة لا حصر لها من الحواسيب عبر العالم ، حيث يغدو أمر التنقل والاتصال فيما بينها أمرا سهلا وان سبب تميزها بعابرة الدول إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر[1]

1-2 صعوبة الإثبات:

إن المجرم والجريمة في تقدم مستمر فمجرم الأمس ليس كمجرم اليوم وبالتالي جريمة الأمس ليست كجريمة اليوم وان صعوبة حصر تلك الجرائم التي تستهدف قواعد المعلومات المحوسبة يرجع إلى تطورها المستمر. وان استعمال وسائل فنية تقنية معقدة في كثير من الأحيان والتباعد الجغرافي بين الجاني والمجني عليه وافتقار إلى الدليل المادي التقليدي دم، شعر، بصمة مما يزيد الأمر صعوبة ضعف خبرة الشرطة ومعرفتهم الفنية بأمور تكنولوجيا المعلومات[2].

---

[1] محمد محي الدين عوض: مشكلات السياسة الجنائية المعاصرة جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993،ص 06.

[2] رستم، هشام محمد فريد: الجوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، أسيوط، مصر، مكتبة الآلات الحديثة 1994، ص 82.

2-2 مغرية للمجرم:

كون الجريمة الالكترونية جرائم سريعة التنفيذ إذ غالبا يتمثل الركن المادي فيها بضغط زر معين في الجهاز مع إمكانية تنفيذ ذلك عن بعد ولا يشترط التواجد المادي في مسرح الجريمة ، ومع ضخامة الفوائد والمكاسب التي يملك الجاني المعلوماتي تحقيقها باقتراف مثل هذه الجرائم دون جهد يذكر ودون أن يكتشف أمره.

3- ناعمة:

الجريمة بالصورة المعروفة لدى العامة تحتاج في الأغلب إلى مجهود عضلي من نوع ما كجرائم القتل والسرقة والاغتصاب، فأن الجريمة الالكترونية على العكس من ذلك فهي لا تحتاج إلى مجهود عضلي ، بل ترتكز على الدراية الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات التكنولوجيا والمعلومات.

الفرع الثالث:أنواع الجريمة الالكترونية.

لقد أقرت وزارة العدل الأمريكية سنة 2000 إحدى عشرة نوع وهي:

- السطو على بيانات الكمبيوتر.
- الاتجار بكلمة السر.
- عمليات الهاكرز ... القرصنة[1].
- سرقة الأسرار التجارية باستخدام الكمبيوتر.
- تزوير الماركات التجارية.
- تزوير العملة باستخدام الكمبيوتر.

[1] عودة عبد القادر، التشريع الجنائي الإسلامي، مؤسسة الهالة، بيروت، د ط ،ص 75.

- الصور الجنسية باستغلال الأطفال.

-الاحتيال عبر شبكة الانترنيت.

-الإزعاج عن طريق شبكة الانترنيت.

تهديدات القنابل بواسطة الانترنيت.

- الاتجار بالمتفجرات و الأسلحة النارية أو المخدرات و غسل الأموال عبر شبكة الانترنيت [1].

أما تصنيف مكتب التحقيقات الفدرالي الأمريكي FBI بحيث يصنفها إلى:

- اقتحام شبكات الهواتف العامة أو الرسمية.

- اقتحام المواقع الرسمية.

- انتهاك سرية بعض المواقع.

- التجسس.

-البرامج المسروقة[2].

المطلب الثاني:الأسباب الدافعة لارتكاب الجريمة وأهداف المجرم منها.

[1] عبد الفتاح بيومي حجازي: الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر 2002 ص07

[2] داود حسن طاهر : نظم المعلومات ، أكاديمية نايف الأمنية ، الرياض 1420 هـ، ص 90.

اختلفت الأسباب الدافعة لارتكاب الجريمة واهداف المجرم منها وتعددت ولعل من أهمها ما يلي:

الفرع الاول: الأسباب الدافعة لارتكاب الجريمة الإلكترونية.

من بين الاسباب الدافعة لارتكاب الجريمة الالكترونية هو ما يختلج المجرم الالكتروني وما يصبوا إليه ولعل من أهمها مايلي :

1- الولع في جمع المعلومات وتعلمها .

2-حب المغامرة والإثارة.

3- الدوافع الشخصية فغالبا ما يرتكب المبرمج جرائم الكمبيوتر نتيجة احساسه بالقوة والذات، وبقدرته على اقتحام النظام، فيندفع تحت تأثير الرغبة القوية في تحقيق الذات.

4- تحقيق مكاسب مالية.

5- الفضول لدى الكثيرين[1].

الفرع الثاني: أهداف المجرم الالكتروني

من بين الأهداف المجرم الالكتروني التي تتعدد هي الأخرى كتعدد الأسباب الدافعة له لارتكاب الجريمة نذكر اهمها:

1-التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.

2-التمكن من الوصول عن طريق الشبكة العنكبوتية الى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

3-الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

[1] عبد الفتاح بيومي حجازي:المرجع السابق، ص 08.

4-الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية[1].

الفرع الثالث: صعوبة إثبات الجريمة الالكترونية كونها عابرة للحدود.

أولا : نظرا للخصائص المميزة التي تتسم بها الجريمة الالكترونية في كونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر، الى جانب السرعة في تنفيذها والسرعة في اتلاف الأدلة ومحو آثارها، ناهيك عن كونها ترتكب من طرف أشخاص غير عاديين يتمتعون بذكاء خارق وتقنية عالية في التعامل مع التقنية المعلوماتية

وأجهزة الحاسب، كل هذه العوامل تشكل عائقا حقيقيا أمام مهمة المحققين في التوصل إلى ضبط الدليل الرقمي[2] للإثبات والإدانة للجناة، إلى جانب كونها تقع في بيئة افتراضية عابرة للحدود، حتى وصفت أحيانا بالجرائم التخيلية والخلاعة التخيلية كالإباحة الجنسية والتشهير والتحريض على تعاطي الرذيلة ، مما يصعب في اغلب الحالات إثبات هذا النوع من الجرائم ، نظرا لسهولة التخلص وإتلاف الأدلة المادية وبسرعة فائقة ،حيث أن معظم الجرائم التي تم الكشف عنها ومعالجتها تمت عن طريق الصدفة لا غير ،خاصة وانها عـــادة ما تقترن بنوع من الخصوصية أو الحرية الشخصية وتتعدى إقليمية الاختصاص [3].

ثانيا :أن الشبكة العنكبوتية (الانترنت) لا تستأثر بها دولة بعينها ، ويسمح لمستخدميها ولوجها من أية مكان في العالم تقريبا من خلال جهاز الكتروني يكون متصلا بها . باعتبارها موزعة على أرجاء الكرة الأرضية-لا تحدها حدود- والأمر كذالك- تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة ، وهذا يستنتج- عدم إمكان خضوعها لسلطان قانون جنائي معين-افتراضا-

[1] احمد سعد جوهر: التقنيات وأساليب مكافحة الإرهاب ، ، جامعة نايف ، المملكة العربية السعودية ، دورة تدريبية http://icacc.ccis-imisiu.edu.sa visite le 09/05/2019 à09h :30

وعملا بمبدأ الإقليمية ، فان كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها ، والذي يستتبع بالضرورة تنازع الاختصاص ، وبالذات فيما يتصل بالجرائم عبر الوطنية التي ترتكب عبر شبكة الانترنت . فجريمة السب مثلا عبر الرسائل الالكترونية E. mails تقع أحيانا في بلد ويتلقاها الضحية في بلد آخر. وهنا ينبغي أن نشير إلى أن هذه الرسائل وغيرها من أدوات الاتصال عن بعد بواسطة هذة الشبكة تمر في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد المستقبل . ناهيك أن بعض الأفعال التي تبث من خلال الانترنت، تعد أحيانا جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة.

ومن الأمثلة التي يسوقها المشرع على ذالك أن المراهنات على كرة القدم ، فهي غير مشروعة في بلد كفرنسا ، وجائزة في بلدان أخرى كما هو الحال في انجلترا .. [1]

ومما يزيد من حدة المشكلة انعدام أو ضعف الرقابة على الرسائل الالكترونية ، وغياب قانون محدد يجري أعماله على مثل هذه الأفعال ، ما من شأنه أن يبعث على التساؤل عن القانون الواجب التطبيق على المواقع الالكترونية على شبكة الانترنت .

---

[1] جمال عبد الباقي الصغير :الجوانب الإجرائية للجرائم المتعلقة بالانترنت ص 43 -44.

وتطبيقا للقواعد التي تحكم الاختصاص المكاني ، فان جرائم الانترنت العابرة للحدود Transnational crimes تخضع في كثير من الأحيان لأكثر من قانون ،فاذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر فان كلا البلدين يكون قانونه واجب التطبيق على الواقعة ، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة السلوك أو النتيجة ، فيكفي ليكون قانون البلد واجب التطبيق

تلقي الضحية الرسالة الالكترونية المجسدة لجريمة السب أو التهديد مثلا في نطاقه ولو كان الفعل ذاته غير معاقب عليه في بلد المنشأ.

وبتطبيق ذالك على جريمة نسخ المصنفات ينعقد الاختصاص للدولة التي تم فعل النسخ على اقليمها ، باعتبار أن النسخ عن بعد يعد أحد العناصر المكونة لجريمة التقليد. وثمة أمر آخر يزيد الأمر تعقيدا وصعوبة في تحديد الاختصاص في جرائم الانترنت عبر الوطنية بالذات ألا وهو تباين المعايير الوطنية فيما يتعلق بتحديد الاختصاص ، الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم .

أي أن الفعل يتنازعه قانونان ، قانون دولة الإقليم على أساس مبدأ الإقليمية ، وفي الوقت ذاته قد يخضع لقانون دولة الجاني عملا بمبدأ الشخصية الايجابية . ليس هذا فحسب،بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسة بمصالحها الحيوية وفقا لمبدأ العينية[1] .وحتى على فرض إمكانية إيجاد حل لهذه المشكلة من الزاوية القانونية ، فإنها تضل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة التي يلزم إتباعها لمحاكمة الجاني الذي ارتكب أيا من هذه الجرائم ، وكانت اقامته خارج البلد الذي تتم فيها محاكمته ، والأمر ينسحب أيضا على تنفيذ الأحكام الصادرة بالخارج . ومن العوائق في ذالك مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين ، وكذالك عدم جواز تسليم الوطنيين.

وقد طرحت مثل هذه المشاكل على القضاء المقارن، وتصدى لها في أكثر من مناسبة. ففي القضاء الأمريكي، تشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو عرضتها للخطر، تأسيسا على مبدأ الاختصاص الشخصي. من ذالك ماقضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة . والمبدأ ذاته كان قد طبق في واقعة أخرى مؤداها قيام إحدى الشركات بولاية بنسلفانيا بالادعاء على احد مزودي

[1] - جمال عبد الباقي الصغير: **المرجع السابق**

الانترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في الولاية الأولى ، وقد أسست المحكمة حكمها على أن قضاء بنسلفانيا ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الانترنت له مشتركون في الولاية.

بعبارة أخرى ، فان القانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الامريكية[1].

المبحث الثالث:الإرهاب وصفحات التواصل الاجتماعي

تتسم شبكات التواصل الاجتماعي بأنها شبكات عالمية فرضت نفسها – وبقوة – داخل المجتمعات العربية خاصة في السنوات العشر الأخيرة، وذلك لأن أغلب تلك الشبكات متاحة للجميع وبالمجان ولأنها صممت أساسا لتكون سهلة الاستخدام وبدون تعقيدات، ولأنها

[1] USA V. Thomas.no.cr-94-20019-9 w.d.tenn.1994

عمر محمد بن : الجرائم الناشئة عن استخدام الانترنت ،ص 918

عملت على تكوين مجتمعات افتراضية جديدة جمعت لأول مرة بين النص المكتوب والمقطع المرئي وهذا ساعد في تحويل المستخدم لها من متلقي للمعلومات كما في وسائل الإعلام التقليدية، إلى منتج للمعلومات ومشارك فيها. ونجد أن الكثير من الشباب يستخدم شبكات التواصل الاجتماعي للدردشة، ولتفريغ الشحنات العاطفية، ومن ثم أصبح الشباب يتبادلون وجهات النظر الثقافية والفكرية عبر تلك الشبكات حيث إنها مصدر جديد للحصول على المعلومات فمواقع التواصل الاجتماعي وسائل يستخدمها من يشاء وقت ما يشاء وأين ما يشاء ، لنشر الأخبار والآراء بشكل حر للتعبير عن وجهات نظره لأنها وفرت مساحات كبيرة للشباب للتعبير عن وجهات نظرهم؛ بعيدا عن مقص الرقيب، وهذا لم يكن متاحا من قبل للشباب.

ذلك خلق فظاءات مفتوحة للشباب، بداية من التمرد على الخجل والانطواء، وانتهاء بالدخول والتجنيد لمنظمات إرهابية.

وينظر بعضهم إلى موقع اليوتيوب على أنه بمثابة سجل أرشيفي موثق عبر شبكة الإنترنت، يمكن الاستفادة منه في توثيق المعلومات بالصوت والصورة. وتذكر التقارير بأن 80 % من الذين انتسبوا إلى تنظيم داعش تم تجنيدهم عبر وسائل التواصل الاجتماعي[1].

المطلب الأول:مواقع التواصل الاجتماعية:

تعتبر أعوام التسعينات الأولى من القرن الماضي، هي البداية الحقيقية لظهور المواقع الاجتماعية، أو التي تسمى شبكات التواصل الاجتماعي على الإنترنت، حين صمم **راندي**

[1] http://www.assakina.com visite le 09/05/2019 à09h :12

كونرادز موقعة اجتماعية للتواصل مع أصدقائه وزملائه في الدراسة في بداية عام 1995، وأطلق عليه إسم Classmates.com ، وبهذا الحدث سجل أول موقع تواصل إلكتروني افتراضي بين سائر الناس[1].

ماهي المواقع الاجتماعية " إنها مواقع إلكترونية اجتماعية على الإنترنت، وإنها الركيزة الأساسية للإعلام الجديد أو البديل، التي تتيح للأفراد أو الجماعات التواصل فيما بينهم عبر هذا الفضاء الافتراضي" .

لقد أتاحت المواقع الاجتماعية لمتصفحيها إمكانية مشاركة الملفات والصور وتبادل مقاطع الفيديو، وكذلك مكنت مستخدميها من إنشاء المدونات الإلكترونية وإجراء المحادثات الفورية وإرسال الرسائل، وتصدرت الشبكات الاجتماعية هذه ثلاثة مواقع هامة ورئيسية هي: **الفيس بوك وتويتر** وموقع مقاطع الفيديو **اليوتيوب**. ونتيجة لتنامي وتطور هذه المواقع الاجتماعية، فقد أقبل عليها ما يزيد عن ثلثي مستخدمي شبكة الإنترنت.

تقدم شبكات التواصل الاجتماعي خدمات عديدة لمستخدميها ممن لديهم اهتمامات متشابه سواء أكانوا زملاء دراسة أو عمل أو أصدقاء جدد، وتوجز موسوعة ويكيبيديا الحرة هذه الخدمات بالتعريف التالي: "معظم الشبكات الاجتماعية الموجودة حالية هي عبارة عن مواقع ويب، تقدم مجموعة من الخدمات للمستخدمين مثل المحادثة الفورية والرسائل الخاصة والبريد الإلكتروني والفيديو والتدوين ومشاركة الملفات وغيرها من الخدمات.

هذه المواقع ظهرت تباعا في منتصف التسعينات من القرن الماضي، واستمر ظهورها حتى أوائل القرن الواحد والعشرين، لكنها لم يكتب لها النجاح بالرغم من التشابه الكبير في الخدمات التي تقدمها، حتى ظهرت مواقع جديدة سجلت نجاحات ملموسة مثل: **ماس سبيس**

[1] فهد بن ناصر العبود:الشبكات الاجتماعية على الانترنت، مقال منشور في جريدة الرياض بتاريخ 30/يناير 2010 العدد 15195.

وتويتر وفيس بوك، التي استطاعت أن تستقطب أعداد كبيرة من متصفحي الإنترنت، وتعاظم دورها في السنوات الأخيرة وخصوصا : **الفيس بوك وتويتر واليوتيوب**.

تقدم الشبكات الاجتماعية أو صفحات الويب خدمات عديدة لمتصفحيها، فهي تتيح لهم حرية الاختيار لمن يريدون في المشاركة معهم في اهتماماتهم، وبظهور شبكات التواصل الاجتماعي مثل **الفيس بوك** وغيره، توسعت الخدمات المرجوة من هذه الشبكات ومنحت متصفحيها إمكانيات واسعة في تبادل المعلومات في مجالات التعليم والثقافة والرياضة وغيرها. وهذه الشبكات هي عبارة عن مواقع إلكترونية اجتماعية.

وهي مواقع انتشرت في السنوات الأخيرة بشكل كبير وأصبحت أكبر وأضخم مواقع في فضاء الويب ولازالت مستمرة في الانتشار الأفقي المتسارع و هي مواقع تقدم خدمة التواصل بين الأعضاء المنتسبين لها، حيث يمكن لأحد المستخدمين الارتباط بأحد الأصدقاء عبر الموقع ليصل جديد ما يكتب ويضيف ذلك الصديق إلى صفحة صديقه. كما أنها تمكن المستخدم من التحكم بالمحتوى الذي يظهر في صفحته، فلا يظهر إلا ما يضيفه الأصدقاء من كتابات وصور ومقاطع. أما أشهر تلك المواقع فهما : **فيس بوك وتويتر**" ومن الخدمات التي تقدمها هذه الشبكات هي: إتاحة المجال للأفراد في الدخول إلى المواقع الاجتماعية والتعريف بأنفسهم، ومن ثم التواصل مع الآخرين الذين تربطهم بهم اهتمامات مشتركة. وتنقسم المواقع الاجتماعية إلى قسمين رئيسين هما: القسم الأول: هي مواقع تضم أفراد أو مجاميع من الناس تربطهم إطارات مهنية أو اجتماعية محددة، وتعتبر هذه المواقع مغلقة ولا يسمح بالدخول إليها من عامة الناس، عدا من هم أعضاء في هذه المواقع التي تتحكم فيها شركات أو مؤسسات معينة، وهي من تقوم بدعوات المنتسبين إليها. القسم الثاني: هي مواقع التواصل الاجتماعي المفتوحة للجميع ويحق لمن لديه حساب على الإنترنت، الانضمام إليها واختيار أصدقائه والتشبيك معهم وتبادل الملفات والصور ومقاطع الفيديو وغيرها، ومن هذه المواقع شبكة الفيس بوك.

الفرع الأول:ميزات الشبكات الاجتماعية:

تتيح هذه الشبكات [1]الإمكانية لمستخدميها بإرفاق الملفات والكتابة حول مواضيع محددة ومعينة، تهم المشتركين الآخرين في نفس الصفحة وتخدم مصالحهم المشتركة، ففي كل المواقع الإجتماعية تتوفر إمكانية التعليق على المواضيع المطروحة فيها، وهذا ما يدفع زائري تلك الشبكات للمشاركة بعد التعريف بأنفسهم وكتابة شيء عنهم كالمهنة والاختصاص والاهتمام.

هناك مواقع اجتماعية متخصصة بمجالات محددة مثل: منتديات إعلامية أو ثقافية أو تربوية وغيرها تهم مجموعة محددة من الناس، كما توجد مواقع اجتماعية خاصة بالتجارة والتسوق، وهي أيضأ تهم شريحة معينة من الناس يرتادونها ويتفاعلون معها، يضاف إلى ذلك نوع جديد من الشبكات الاجتماعية، التي يتواصل فيها مرتاديها من خلال الهواتف النقالة، وتكوين صداقات وإجراء محادثات ونقاشات وتبادل المعلومات عبر شاشات الهواتف النقالة.

الفرع الثاني:أنواع شبكات التواصل الاجتماعي

شهد العالم في السنوات الأخيرة نوعا من التواصل الاجتماعي بين البشر في فضاء إلكتروني افتراضي، قرب المسافات بين الشعوب وألغى الحدود وزاوج بين الثقافات، وسمي هذا النوع من التواصل بين الناس شبكات التواصل الاجتماعي، وتعددت هذه الشبكات واستأثرت بجمهور واسع من المتلقين، ولعبت الأحداث السياسية والطبيعية في العالم دورة

[1] http://www.assakina.com visite le 09/05/2019 à09h :12

بارزة في التعريف بهذه الشبكات، وبالمقابل كان الفضل أيضا لهذه الشبكات في إيصال الأخبار السريعة والرسائل النصية ومقاطع الفيديو عن تلك الأحداث، الأمر الذي ساعد في شهرة وانتشار هذه الشبكات وأهمها: **الفيس بوك، تويتر، واليوتيوب.**

1- الفيس بوك:

هو شبكة اجتماعية استأثرت بقبول وتجاوب كبير من الناس خصوصا من الشباب في جميع أنحاء العالم، وهي لا تتعدى حدود مدونة شخصية في بداية نشأتها في شباط عام2003، في جامعة هارفارد في الولايات المتحدة الأمريكية، من قبل طالب يدعى مارك **زوكربيرج**، وكانت مدونته **الفيس بوك** محصورة في بدايتها في نطاق الجامعة وبحدود أصدقاء **زوكربيرج**، الطالب المهووس في برمجة الكمبيوتر، ولم يخطر بباله هو وصديقين له إن هذه المدونة ستجتاح العالم الافتراضي بفترة زمنية قصيرة جدا، فتخطت شهرتها حدود الجامعة وانتشرت في مدارس الولايات المتحدة الأمريكية المختلفة، وظلت مقتصرة على أعداد من الزوار ولو أنها كانت في زيادة مستمرة. إلا أن هذه المدونة لم تحقق تميزا على المواقع الاجتماعية الأخرى التي سبقتها مثل موقع **ماي سبيس** وغيره، حتى عام 2007، حيث حقق القائمون على الموقع إمكانيات جديدة لهذه الشبكة ومنها، إتاحة فرصة للمطورين مما زادت هذه الخاصية من شهرة موقع **الفيس بوك**، بحيث تجاوز حدود الولايات المتحدة الأمريكية إلى كافة دول العالم، وتجاوز عدد المسجلين في هذه الشبكة في الأول من تموز 2010 النصف مليار ش خص، يزورنها باستمرار ويتبادلون فيما بينهم الملفات والصور ومقاطع الفيديو، ويعلقون على ما ينشر في صفحاتهم من آراء وأفكار ومواضيع متنوعة وجديدة، يضاف إلى ذلك المشاركة الفعالة وغالبا ما تكون في المحادثات والدردشات. وتحتل

شبكة **الفيس بوك** حاليا من حيث الشهرة والإقبال المركز الثالث بعد موقعي **غوغل ومايكروسوفت**، وبلغ عدد المشتركين فيها أكثر من 800 مليون شخص[1].

2- تويتر:

"هو أحدى شبكات التواصل الاجتماعي، التي انتشرت في السنوات الأخيرة، ولعبت دورة كبيرة في الأحداث السياسية في العديد من البلدان، وخاصة في منطقة الشرق الأوسط، وتصدرت هذه الشبكات في الآونة الأخيرة ثلاثة مواقع رئيسية، لعبت دورا مهمة جدا في أحداث ما يسمى بثورات الربيع العربي وهي: **فيس بوك** – **تويتر** – **يوتيوب**. وأخذ **تويتر** أسمه من مصطلح **تويت** الذي يعني التغريد، وأتخذ من العصفورة رمزا له، وهو خدمة مصغرة تسمح للمغردين إرسال رسائل نصية قصيرة لا تتعدى 140 حرفا للرسالة الواحدة، ويجوز للمرء أن يسميها نصا موجزا مكثفة لتفاصيل كثيرة".

ويمكن لمن لديه حساب في موقع **تويتر** أن يتبادل مع أصدقائه تلك التغريديات والتدوينات، من خلال ظهورها على صفحاتهم الشخصية، أو في حالة دخولهم على صفحة المستخدم صاحب الرسالة، وتتيح شبكة **تويتر** خدمة التدوين المصغرة هذه، إمكانية الردود والتحديثات عبر البريد الإلكتروني، كذلك أهم الأحدث من خلال خدمة **RSS** عبر الرسائل النصية **SMS**.كانت بدايات ميلاد هذه الخدمة المصغرة **تويتر** أوائل عام 2006، عندما أقدمت شركة Obvious الأمريكية على إجراء بحث تطويري لخدمة التدوين المصغرة، ثم أتاحت الشركة المعنية ذاتها استخدام هذه الخدمة لعامة الناس في أكتوبر من نفس العام، ومن ثم أخذ هذا الموقع بالانتشار، باعتباره خدمة حديثة في مجال التدوينات المصغرة، بعد ذلك أقدمت الشركة ذاتها بفصل هذه الخدمة المصغرة عن الشركة الأم، واستحدثت لها أسما خاصة يطلق عليه تويتر وذلك في أبريل عام 2007[1].

[1] أماني إبراهيم: شعوب أون لاين، مقال منشور بتاريخ 2010/12/26 ، وكالة انباء ONA.

إن **تويتر** هو موقع تواصل اجتماعي لا يقل أهمية عن **الفيس بوك** ويعتبر المنافس الأكبر له، ويقدم خدمة مصغرة لمستخدميه من المغردين، تمكنهم من إرسال تحديثاتهم برسالة لا تزيد على 140 حرفا للرسالة الواحدة إلى صفحاتهم الخاصة، ويمكن للزوار قراءتها وكتابة الردود عليها، ويتميز تويتر بسرعة إيصال المعلومات خصوصا الإخبارية"[2].

3- اليوتيوب:

هو أحد المواقع الإجتماعية الشهيرة، والذي استطاع بفترة زمنية قصيرة الحصول على مكانة متقدمة ضمن مواقع التواصل الإجتماعي، وخصوصا في دوره المتميز في الأحداث الأخيرة التي جرت ووقعت في أنحاء مختلفة من العالم منها: الكوارث الطبيعية والتحركات والانتفاضات الجماهيرية والثورات الشعبية. **اليوتيوب** هو: موقع لمقاطع الفيديو متفرع من غوغل، يتيح إمكانية التحميل عليه أو منه لعدد هائل من مقاطع الفيديو، وهناك أعداد كبيرة للمشتركين فيه ويزوره الملايين يومية، وتستفيد منها وسائل الإعلام بعرض مقاطع الفيديو، التي لم تتمكن شبكات مراسيلها من الحصول عليها، كما يستفيد مرتادي **الفيس بوك** من مقاطع الفيديو التي تتعلق بالانتفاضات الجماهيرية في كل البلدان العربية والشرق الأوسط وعرضها على صفحات **الفيس بوك**، ويعتبر **اليوتيوب** من شبكات التواصل الاجتماعية الهامة .

تأسس **اليوتيوب** من قبل ثلاثة موظفين كانوا يعملون في شركة باي بال "**PayPal**" عام 2005 في ولاية كاليفورنيا في الولايات المتحدة الأمريكية، ويعتمد اليوتيوب في عرض المقاطع المتحركة على تقنية **أدوب فلاش**، ويشتمل الموقع على مقاطع متنوعة من أفلام السينما والتليفزيون والفيديو والموسيقى. وقامت **غوغل** عام 2009 بشراء الموقع مقابل

---

[1] .www.marefa.org visite le 08/05/2019 à14h

[2] ويكيبيديا الموسوعة الحرة

1ر65[1] مليار دولار أمريكي،ويعتبر **اليوتيوب** من الجيل الثاني ، وأصبح **اليوتيوب** عام 2009 شبكة التواصل الأولى حسب اختيار مجلة **تايم** الأمريكية[2]

وحول تاريخ الموقع تقول موسوعة ويكيبيديا العالمية أنه: "تأسس موقع **يوتيوب** عن طريق **تشاد هرلي، وستيف تشن، وجواد كريم**، وهم موظفون سابقون في شركة **PayPal**. قبل ذلك درس **هرلي** التصميم في جامعة إنديانا بولاية **بنسيلفينيا**، بينما درس **تشن وكريم** علوم الحاسوب في جامعة **إيلينوي**. أصبح النطاق YouTube.com نشطة في 15 فبراير 2005 ، ومن ثم تم العمل على تصميم الموقع لبضع أشهر. أفتتح الموقع كتجربة في مايو 2005، وافتتح رسمية بعد ستة أشهر".

يشهد موقع **اليوتيوب** إقبالا كبيرا من الشباب والمراهقين خصوصا ومن الجنسين، ويعتبر موقع **اليوتيوب** موقعة غير ربحية لخلوه تقريبا من الإعلانات، إلا أن الشهرة التي وصل إليها الموقع تعد مكسب كبيرة لهؤلاء الثلاثة الذين قاموا بإنشائه وتأسيسه، بحيث أصبح **اليوتيوب** أكبر مستضيف لأفلام الفيديو، إن كانت على الصعيد الشخصي أو شركات الإنتاج، وأصبح يتردد أسم **اليوتيوب** عندما تذكر أسماء الشركات التكنولوجية الكبرى الفاعلة على الصعيد العالمي، والتي تحتل موقعا مهمة على شبكة الإنترنت. إن موقع **اليوتيوب** واسع الانتشار، لم يعد حكرا على مؤسسات إعلامية أو قنوات تليفزيونية فضائية، أو أشخاص مهتمين من الصحفيين وغيرهم، بل أصبح متاحة لكل من يرغب بالحصول على موقع خاص به، ابتداء من كبار القادة والمسؤولين في العالم، إلى عامة الناس بمختلف فئاتهم العمرية وخصوصا الشباب منهم، لما يقوم به هذا الموقع من خدمات مميزة خصوصا دوره البارز في أحداث العالم الأخيرة. لقد أصبح **اليوتيوب** جزء لا يتجزأ من اهتمامات

[1] www.marefa.org visite le 08/05/2019 à14h.

[2] موقع الاتحاد بتاريخ22/05/2019 www.alithad.com visite le

الملايين من الناس على اختلاف أعمارهم وبمختلف اهتماماتهم، كما وأنه أضاف خدمة كبيرة وفاعلة لوسائل الإعلام والاتصال الجماهيري الحديثة.

المطلب الثاني: التجنيد عبر شبكات التواصل.

درس الخبير في قضايا الإرهاب الرقمي **جيف باردين** [1]أنشطة مجموعات جهادية على مختلف مواقع ومنتديات التواصل الاجتماعي طيلة السنوات الثماني الماضية، وخلص إلى أن **داعش** يجند شهريا أكثر من 3400 عنصر عبر حملات الكترونية غاية في التنسيق. هؤلاء المجندون حسب باردين هم مقاتلون قادرون على القيام بأي أنشطة مسلحة دون أن تتمكن دول غربية من تتبع تحركاتهم لانشغالها بإعداد خطط ميدانية قد تمهد لهجوم بري محتمل. تتكب مخابرات دول غربية على تحليل المعطيات الخاصة بأعضاء مجموعات جهادية وفك خيوط عملياتها والاندساس داخلها بشكل يسمح بتفكيك مكوناتها..

وفي آخر بحث منشور له في مجلة "**بيزنيسانيسايدر**[2]" الأسترالية، برر باردين عدم تحرك أجهزة استخبارات العديد من الدول لتطويق الشبكات المتشددة النشيطة على مواقع التواصل الاجتماعي بتركيزها على جمع أكبر قدر من المعلومات للوصول إلى رؤوس تلك التنظيمات: إنها تتكب على تحليل المعطيات الخاصة بأعضاء مجموعات جهادية وفك خيوط عملياتها والاندساس داخلها بشكل يسمح بتفكيك مكوناتها ليسهل التعرف على هويات من يقف وراء تلك التنظيمات السرية."

[1] جيف باردين: انظم إلى المجموعة الاستراتيجية وريادة الأعمال في كلية ادارة الأعمال في سبتمبر عام 2013، حصل على شهادة البكالوريوس اقتصاد من جامعة نورث كارولينا في تشابل هابل، وحصل على شهادة الماجستير في إدارة الأعمال في نظم المعلومات والأعمال التجارية الدولية مدرسة كيلي لإدارة الأعمال جامعة انديان ، وحاز على الدكتوراه في الادارة من كلية فوكو للأعمال في جامعة ديوك . ينظر: www.business.org

[2] www.businessinsider.com

لكن الخبير الأمني حث دول التحالف التي تحارب **داعش** على التمييز بين التجنيد عبر مواقع التواصل الاجتماعي وجمع التبرعات المالية وتنسيق التحركات العسكرية التي تستطيع استخبارات دول معينة تتبعها، وبين الأنشطة التي تسعى إلى نشر أيديوليجية التنظيم المتشددة بين زوار الشبكات الاجتماعية من أي مكان في العالم، والتي تحتاج، حسب باردين، إلى تحرك سريع للتصدي لها بإغلاق حسابات من يقف خلفها وتعطيل خوادم تلك المنتديات بشكل نهائي[1].

وتسير المعالجة القانونية للأنشطة المحرضة على العنف على الإنترنت بشكل متواز مع إغلاق تلك الفظاءات الافتراضية حسب رئيس المركز المغربي للدراسات في الإعلام وحقوق الإنسان علي كريمي، الذي يعتبر اتفاقية بودابست الخاصة بالجريمة عبر الانترنت الموقعة سنة 2001 إطارا يدعم التشريعات الدولية لمعاقبة المحرضين على العنف. ويتابع في تصريح لموقع "الحرة": عندما تشعر أي دولة أن هناك أطرافا تهدد سيادتها ومصالحها القومية فستسعى إلى اعتقال من يدير تلك التنظيمات رغم إدراكها لصعوبة ذلك لأن هذه الحركات ألغت مفهوم السيادة لكونها تتحرك عبر نواة عابرة للقارات تستطيع التخفي وتخطط في منطقة على أن يتم التنفيذ في نقطة جغرافية أخرى[2]."

[1] www.csoonline.com visite le 10/04/2019 à14h30

[2] http://www.alhurra.com visite le 10/05/2019 à 15h30

الفرع الأول: مدلول عملية تجنيد الشباب عبر الانترنت:

أولا: عملية التجنيد: يقصد بمصطلح التجنيد (اسم) والذي مصدره جند ، أي أعلن عن تجنيد الجنود الاحتياطيين ، أي جمعهم لمواجهة حرب أو كارثة ، وجند (فعل)،يجند ، تجنيدا، فهو مجند ، والمفعول مجند. جند الجنود أي صيرهم جنودا وهيأهم لذلك [1].

وللتجنيد" مفهوم أوسع يستمد إطاره من الواقع التطبيقي والفعلي في اغلب دول العالم ، والتي عانت من ويلات ظاهرة التجنيد وتتمثل هذه العملية في جمع وحشد الأشخاص واستقطابهم بمعنى أخر استخدمهم قصرا أو طواعية ، بغرض الإنظمام والالتحاق بالجماعات الإرهابية ومهما كان غرضها ، عن طريق إعدادهم ماديا ومعنويا لخدمة هذه الجماعات محلية كانت او دولية [2].

وتتم عملية تجنيد الشباب بطريقة ممنهجة لإعادة تكوين التنشئة ، عن طريق استعمال أساليب قهرية وقصريه للإقناع وذلك بإتباع مراحل أو شروط لاقتناص الشباب ليجد نفسه عضوا في الجماعات الإرهابية [3].

فبالإضافة الى الترويج والدعاية نجد ان تجنيد الشباب من اهم خصائص الإرهاب الرقمي ، حيث تلجا الجماعات الإرهابية الى شبكة الانترنت كوسيلة لتجنيد عناصر إرهابية جديدة لتساهم في تنفيذ مشاريعهم الإرهابية [4].

---

[1] **معجم المعاني: الجامع الإلكتروني، أظر الرابط: جند**/www.almaany.com/ar/dict/ar-ar

[2] نورة بنداري عبد الحميد فايد **:** دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية "**دراسة حالة داعش**"، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية ، تاريخ الإطلاع 2019/04/21 بتوقيت 20:12 .

[3] لطيفة الشملان **:**تدابير منع الشباب من قبل الجماعات الإرهابية العالمية ، تقرير مقدم للجنة الإقليمية الخاصة بمنطقة الشرق الأوسط وشمال إفريقيا تاريخ الاطلاع 2019/04/21 .بتوقيت 22:45 .

الفرع الثاني:الانترنت كبيئة لتجنيد الشباب:

شبكة الانترنت عبارة عن ارتباط جهاز الحاسوب بجهاز أخر عن طريق كوابل أو عن طريق خيوط الهاتف الثابتة العادية ، وفي حالة ما إذا كانت الحواسيب متواجدة في أماكن مختلفة ترتبط فيما بينها عن طريق الأقمار الصناعية [1] .

فانتقال الإرهاب من البيئة المادية الطبيعية إلى البيئة الافتراضية الإلكترونية، يكسبه خصائص جديدة سوء من حيث وسائله أو من حيث طرق ارتكابه لجرائم تقليدية، الشيء الذي جعل الإرهاب ينتشر بسرعة الضوء في كامل بقاع العالم فأصبح من الصعب القضاء عليه [2].

فتحولت شبكة الانترنت إلى أداة فعالة في تجنيد الإرهابيين حيث أصبحت تغني عن معسكرات التدريب والتي كانت موجودة سابقا [3] في أفغانستان، ونتيجة للرقابة الأمنية الإلكترونية التي فرضت مؤخرا على شبكة الانترنت السطحية (surface web) ويقصد بها الشبكة الرسمية العادية والمتاحة لعموم الناس [4]، والتي لا تمنحنا سوى نسبة 16 بالمائة من المعلومات، أما باقي المعلومات فلا نجدها سوى على الانترانت الخفي أو المظلم [5]، هذا ما

---

[1] عبد الرحمان بيومي حجازي : الجريمة في عصر العولمة ، دار الفكر الجامعي ، ط1، الإسكندرية 2008 ، ص 14

[2] وليد محمد ابو رية:**التعرف على** الإرهاب الإلكتروني ، جامعة نايف العربية للعلوم الأمنية ، مركز الدراسات والبحوث ،ط1 ، المملكة العربية السعودية 2012، ص 52،51.

[3] وليد محمد ابو رية : المرجع نفسه.

[4] نورة بنداري عبد الحميد فايد : **المرجع السابق**

[5] **خالد عباس طلشكندي : الشبكة المظلمة** DEPP WEP ، المقال المتاح على موقع السكينة الالكتروني ، تاريخ الاطلاع 2019/05/21 بتوقيت 09:15

دفع بالجماعات الإرهابية (**داعش**) التوجه نحو استخدام شبكة الانترانت الخفية غير الرسمية [1]ويطلق عليه اسم "الشبكة المظلمة او الانترنت الخفي الأسود "(deep web) ، والتي تستعمل من طرف المافيا والمنظمات الإجرامي والجماعات الإرهابية من اجل التواصل بين أعضائها وترويج أفكارها الخبيثة ، وكذا استقطاب وتجنيد الشباب من خلال غرف الدردشة المنتشرة بكثرة على الشبكة المظلمة ،كما تعتمد على استعمال بعض التطبيقات والبرامج الالكترونية كتطبيق (المحفظة المظلمة)،" darkwallet" وهو عبارة عن تطبيق الكتروني مهمته إخفاء المعاملات المالية الخاصة والقائمة باستخدام وسيلة دفع افتراضية تدعى " عملة البيت كوين" ، كما أطلقت **داعش** في منصف شهر يناير في عام 2015 تطبيق عالي التشفير يدعى " **الراوي arawi**" والذي من المستحيل تحميله لان ذلك يقتضي الولوج إلى شبكة الانترنت المظلم بواسطة روابط سرية ، لا يتداولها إلا أفراد تنظيم **داعش** ، باستخدام برنامج " التيلغرام " المشفر ، وانطلاقا من الشبكة الخفية فإن الجماعات الإرهابية تعتمد على البريد الالكتروني المشفر ، وكذا مواقع " **Gps**" الوهمية وهذا كله من اجل عرقلة مهمة تتبعهم من طرف اجهزت الأمن والمخابرات أو التجسس عليهم من طرف القراصنة المحترفين "**هاكرز**[2] "، وبما أن أسلوب التخفي من ابرز أساليب الإرهاب الالكتروني فإن الدراسات الحديثة والتي أجريت مؤخرا بريادة "**ليث الخوري**" و " **اليكس كاسيرير** " الباحثين على مستوى مركز "**فلاش بونيت** " الأمريكي والمتخصص في رصد المحتوى الالكتروني على الشبكة العميقة "**deep wep** " ، أظهرت العديد من المنتجات والمنصات الرقمية التي يعتمد عليها تنظيم **داعش** للتخفي من بينها .

[1] خالد عباس طلشكندي : الشبكة المظلمة DEPP WEP ، المقال المتاح على موقع السكينة الالكتروني ، تاريخ الاطلاع 2019/05/21 بتوقيت 09:15 : انظر الرابط

[2] خالد عباس طلشكندي : المرجع نفسه.

أ –المتصفحات الآمنة : بينت الدراسة أن تنظيم **داعش** لا يستخدم المتصفحات العادية كالتي نستخدمها نحن مثل " كروم وسفاري" وذلك لإمكانية الكشف عن عنوان "IP " الخاص بهم بل تعتمد على متصفح TOR .

ب– الشبكات الخاصة الافتراضية وخادم " البر وكسي : والتي تساهم بتامين طبقة إضافية من التشفير وتوفير الخصوصية للمستخدم .

ج– خدمات البريد الالكتروني المحمية: التي توفر ميزات الآمان والتشفير " **END TO END**" بحيث تعرقل القدرة على المراقبة والتتبع.

د– تطبيقات التراسل المشفرة : نتيجة للقرارات الصادرة عن شركات " **تويتر و فايس بوك**" والمتعلقة بالتصدي للخطابات الإرهابية التي ينشرها تنظيم **داعش** ، لجا هاذ الأخير إلى استخدام تطبيقات مشفرة يصعب الوصول إليها ومن أبرزها " **تطبيق تليغرام** [1] ."

الفرع الثالث: فئة الشباب المستهدف بالتجنيد:

يجمع المختصين النفسانيين والقانونيين والتربويين وكذا المثقفين على ان الفئات المستهدفة من طرف الجماعات الإرهابية للتجنيد هم فئة الشباب البطالين ومدمنين المخدرات والمتشددين في الدين ، بحيث تستهدف هذه الجماعات بشكل خاص الأطفال والشباب المحطمين نفسيا وتعدهم بالشهرة والفردوس ، وتتراوح الفئة العمرية المستهدفة ما بين 15 و25 سنة كونها الأكثر تأثرا في ظل غياب الرقابة من طرف الأولياء وكذا العيش في فراغ بلا دراسة او عمل [2].

[1] أدوات التخفي الرقمية حياة لداعش ، مقال متاح على موقع " جريدة المدن " الإلكتروني ، تاريخ الاطلاع 2019/04/30 بتوقيت 12:54 WWW.ALMODON .COM/MEDIA

[2] التنظيمات الإرهابية تصطاد المراهقين والمحطمين نفسيا ، مقال متاح على موقع " صحيفة المدينة " **الالكتروني** ، بتاريخ 2017/10/24 تاريخ الاطلاع 2019/04/30 بتوقيت 01:20 WWW.AL MADN.COM /ARTICLE

ومن جهة اخرى أوضح الكاتب " **روبرت إيفانزر**" في مقاله " **7 أشياء تعلمتها من قراءتي لكل أعداد مجلة داعش الدابقية** " ، وهو نفس الأمر الذي صرح به البرلمان الأوروبي عقب هجمات باريس والتي اقر فيها بان **داعش** استطاعت في الآونة الأخيرة تجنيد خبراء في الكيمياء والفيزياء وكذا علوم الحاسوب ، كما أكد الدكتور " **كمال حبيب** " الخبير في شؤون الحركات الإسلامية ، أن الفئات المستهدفة في الآونة الأخيرة من قبل تنظيم "**داعش**" هي فئة طلاب الجامعات ذوي الاختصاصات الجيدة والذين يعيشون حياة الرفاهية العالية والارتياح المادي الاجتماعي [1] .

[1] زينب **القرشي :** تجنيد داعش للمثقفين والعلماء كارثة تهدد بقاء البشرية ، مقال متاح على موقع **"الوفد" الالكتروني** ، القاهرة ، تاريخ الاطلاع :2019/04/30 بتوقيت 14:30.

الفصل الثاني: آليات مكافحة الإرهاب الالكتروني في التشريع الجزائري:

لقد تم تقسيم الفصل إلى ثلاثة مباحث رئيسية من خلال التطرق إلى الآليات الموضوعية لمكافحة الإرهاب الالكتروني في المبحث الأول يليه المبحث الثاني: الآليات الإجرائية لمكافحة الإرهاب الالكتروني ليختتم الفصل بمبحث ثالث تناول الآليات الإجرائية في ظل القانون 04/09.

المبحث الأول: الآليات الموضوعية لمكافحة الإرهاب الالكتروني.

لقد تضمن المبحث مطلبين أساسين فيما يخص الآليات الموضوعية **ولقد** تم تفريد المطلب الأول لمسالة التجريم فيما ارتكز المطلب الثاني على العقوبات المقررة لجرائم الإرهاب الالكتروني

المطلب الأول: التجريم.

لقد تنوعت النصوص التجريمية التي تناولها المشرع الجزائري لمكافحة ظاهرة الإرهاب الالكتروني بين النصوص التقليدية التي جاء بها **قانون العقوبات على غرار المواد من 87** مكرر إلى غاية المادة 87 **مكرر** 10 وبين النصوص المستحدثة كما هو الحال بالنسبة **للمواد** 87 مكرر 11 و87 **مكرر** 12 .

الفرع الأول:أركان جريمة الإرهاب الالكتروني.

تتمثل **أركان** الجريمة مثل الجريمة العادية في الركن الشرعي والمادي والمعنوي :

اولا : الركن الشرعي :

معناه اعتراف المشرع والنص على تجريم الفعل المرتكب" لا جريمة ولا عقوبة إلا بنص "بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من **الفصل** الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات [1].

ثانيا: الركن المادي :

يتكون الركن المادي لجريمة الإرهاب الالكتروني من السلوك الإجرامي والنتيجة والعلاقة السببية ، علما انه يمكن تحقق الركن المادي دون تحقق النتيجة ، كالتبليغ عن الجريمة قبل تحقيق نتيجتها ويتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي **مرتكب** .

[1] أحسن بوسقيعة :الوجيز في القانون الجزائي العام ،الطبعة الأولى 2002 ،الديوان الوطني للأشغال التربوية

ثالثا : الركن المعنوي :

يتكون الركن المعنوي لجريمة الإرهاب الالكتروني من عنصرين أي العلم **والإرادة** .

1- العلم: هو إدراك الفاعل **للأمور**.

2- الإرادة: هي اتجاه السلوك الإجرامي لتحقيق النتيجة طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا فالقصد الجنائي العام هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود ارتكاب الفعل.أما القصد الجنائي الخاص فهو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بإرتكاب الجريمة بل يذهب للتأكد من تحقيق النتيجة وعليه ماهو القصد الجنائي الذي يجب توافره في جريمة الإرهاب الالكتروني . الاصل ان الفاعل في الجريمة يوجه سلوكه الجرامي نحو ارتكاب فعل غير مشروع **أو** غير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي .

الفرع الثاني : النصوص التقليدية والمستحدثة لتجريم الارهاب الالكتروني .

وجاءت هذه النصوص لتوقيع العقاب بعد تجريم الفعل وهنا نميز بين العقوبات الأصلية والتكميلية .

أولا: العقوبات الأصلية.

"هي تلك العقوبات التي تكتفي بذاتها للحكم بها بصفة أصلية وأساسية كجزاء للجريمة **وتوقع منفردة دون أن** يكون الحكم بها معلقا على الحكم بعقوبة أخرى "[1] **وتقسم العقوبات** الأصلية **إلى** عقوبات بدنية تتمثل في عقوبة الإعدام وعقوبات ماسة بالحرية والمتمثلة في **السجن والحبس** ، **وعقوبات** مالية تتمثل في الغرامة .

1- العقوبات البدنية والعقوبات الماسة بالحرية :

أ – عقوبة الإعدام: تهدف **إلى الاستئصال** والقضاء على المجرمين الخطيرين فهي تمس بحياة **الجاني، وتنفذ بكثرة في جرائم القتل مع سبق الإصرار والترصد والجرائم الماسة بأمن الدولة** [2].

ب- عقوبة السجن:" هي العقوبة **الأشد وتقرر عادة للجرائم الموصوفة** بأنها جناية، وقد تكون مؤبدة أي مدى الحياة كما قد تكون مؤقتة وذلك لمدة معينة ".

---

[1] سامي عبد الكريم محمود: الجزاء الجنائي، منشورات الحلبي الحقوقية، الطبعة الأولى، لبنان 2010، ص124.

[2] لحسين بن شيخ : **مباديء القانون الجزائي العام** (النظرية العامة للجريمة) ،دار هومة للطباعة والنشر والتوزيع ،الجزائر 2004،ص 175

ج- عقوبة الحبس:"هي العقوبة المقررة بالنسبة للوقائع التي توصف على أنها جنحة، والحبس يكون دوما لمدة محددة من الزمان **"[1].**

2- العقوبات المالية :

"يتمثل الإيلام فيها إلزام المحكوم عليه بدفع مبلغ من النقود يقدره حكم الإدانة إلى خزينة الدولة ،وهي عقوبة أصلية في مواد الجنح والمخالفات في قانون العقوبات الجزائري"

وقد ينص عليها المشرع كعقوبة أصلية منفردة في بعض الجرائم ،كما قد يضاف إليها عقوبة الحبس وقد ينص القانون على تطبيق الحبس والغرامة معا او التخيير بين إحدى العقوبتين ، في حين تكون عقوبة الغرامة هي الأصل في مواد المخالفات البسيطة من الفئة الثانية كما يجوز أن تضاف إليها عقوبة الحبس قصير المدة [2].

وتجدر الإشارة إلى أن عقوبة الغرامة في مواد الجنايات تعتبر عقوبة تكميلية بحيث تضاف إلى العقوبة الأصلية السالبة للحرية كما هو الحال بالنسبة للجرائم الماسة بأمن الدولة، كما قد تكون عقوبة في مواد الجنح والمخالفات.[3]

وبالتالي فإن المشرع الجزائري سابقا لم ينص على عقوبة الغرامة في الجرائم الإرهابية ولكنه تدارك الأمر بموجب نص المادة (87 مكرر 4 ق ع).

فقد نص المشرع عليها بالإضافة إلى عقوبة الحبس بصفة وجوبية كما هو الحال بالنسبة لنص المادة (87 مكرر6 ق ع) ، كما قد تكون عقوبة جوازية تخضع لسلطة قاضي الموضوع التقديرية كما هو الشأن بالنسبة لعقوبة القذف الموجه للأفراد المادة (298ف1ق ع)[4]

وتنص المادة (10) من القانون 05-04 المؤرخ في 6 فبراير سنة 2005 المتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين: تختص النيابة العامة، دون سواها، بمتابعة تنفيذ الأحكام الجزائية.

غير انه، تقوم مصالح الضرائب أو إدارة الأملاك الوطنية، بناء على طلب النائب العام أو وكيل الجمهورية، بتحصيل الغرامات، ومصادرة الأموال، وملاحقة المحكوم عليهم بها.."[1].

---

[1] لخميسي عثمانية،: السياسة العقابية في الجزائر على ضوء المواثيق الدولية لحقوق الإنسان،دار هومة للطباعة والنشر والتوزيع الجزائر 2012، ص 140

[2] - لمقدم حمر العين:الدور الإصلاحي للجزاء الجنائي ، رسالة دكتوراه في القانون الخاص،كلية الحقوق والعلوم السياسية ،جامعة ابو بكر بلقايد ،تلمسان ،2014،2015،ص143.

[3] علي عبد القادر القهوجي: المرجع السابق، ص203، 204.

[4] انظر المادة : (87 مكرر12)ق،ع.

وبالرجوع إلى نص المادة (87 مكرر12ق ع) من القانون 16-02 المتمم لقانون العقوبات نجد أن المشرع الجزائري قد قرر عقوبات أصلية لقمع جريمة التجنيد الإلكتروني للإرهاب دون النص على العقوبات التكميلية والتي يقتضي منها الرجوع إلى النصوص العامة المتعلقة بالعقوبات التكميلية المقررة للجرائم الإرهابية .

وتمثل العقوبات الأصلية لجناية التجنيد الالكتروني للإرهاب في :

- عقوبة سالبة للحرية تتراوح مدتها ما بين خمس (5)سنوات إلى عشر (10)سنوات سجن مؤقت.
- عقوبة مالية تتمثل في الغرامة المقدرة بـ:100000دج إلى 500.000دج[2].

ثانيا:العقوبات التكميلية.

" هي عقوبات قررها المشرع الجزائري من اجل إلحاقها بالعقوبة الأصلية ، والأصل أن تكون العقوبات التكميلية جوازية ولكن هناك بعض الحالات نص المشرع على إلزامية الحكم بها"

وبالرجوع إلى نص المادة (87 مكرر 12 ق ع) المتعلقة بتجريم فعل التجنيد الالكتروني للإرهاب نجد أن المشرع الجزائري لم ينص على العقوبة التكميلية فقد اكتفى بالعقوبات الأصلية فقط السالبة للحرية والغرامة.

ونستشف من ذلك أن المشرع قد أحالنا ضمنيا إلى نص المادة (87 مكرر9 ق ع) ، والتي تنص على : " يجب النطق بالعقوبات التبعية المنصوص عليها في المادة 6 من قانون العقوبات لمدة سنتين (2) إلى عشر (10) سنوات في حالة الحكم بعقوبة جنائية تطبيقا لأحكام هذا الأمر فضلا على ذلك يمكن مصادرة ممتلكات المحكوم عليه".

وبالرجوع إلى نص المادة (06 ق ع) الملغاة بموجب القانون 06-23 المتضمن قانون العقوبات، نجد أن العقوبات التبعية تتمثل في:

- الحجر القانوني.
- الحرمان من الحقوق الوطنية.

والملاحظ أن المشرع قد احتفظ بمصطلح العقوبات التبعية ضمن المادة (87مكرر9ق ،و،ج،إ،إ)،بالرغم من انه قد الغي نص المادة (06 ق ع) التي كانت تنص عليها ، بحيث قام

---

[1] أحسن بوسقيعة :الوجيز في القانون الجزائي العام ،الطبعة الاولى 2002 ،الديوان الوطني للأشغال التربوية ، ص 325.

[2] أحسن بوسقيعة :الوجيز في القانون الجزائي العام ،مرجع السابق ، ص 325

إدماجها في نص المادة (09 ق ع) بموجب القانون 06-23 فأصبحت تعتبر عقوبات تكميلية وليست تبعية ، والتي كانت تطبق تلقائيا على المحكوم عليه بعقوبة جنائية سواء كان بصدد جريمة عادية أو جريمة إرهابية ، كما أبقى هاتين العقوبتين التكميليتين بموجب التعديل 06-23 إلزامية النطق بهما من طرف القاضي متى كنا بصدد جناية ، أما باقي العقوبات التكميلية الواردة في نص المادة (09ق ع) المعدلة بموجب القانون سالف الذكر فالقاضي ليس مجبر على النطق بها.

والملاحظ أن القاضي عند نطقه بعقوبة تكميلية لجريمة إرهابية يحيل إلى النص العام المتضمن العقوبة التكميلية التي تطبق على مختلف جرائم القانون العام ، بالإضافة إلى النص الخاص المتعلق بالعقوبة الأصلية المقررة للجريمة وبصدور القانون رقم 06-23 المعدل والمتمم لقانون العقوبات تم إلغاء الفقرة المتعلقة بالعقوبة التبعية وكذا المواد من " ...العقوبات التكميلية هي تلك التي لايجوز الحكم بها مستقلة عن عقوبة أصلية ، فيما عدا الحالات التي ينص عليها القانون بصراحة ، وهي إما إجبارية أو اختيارية ...[1]

وتجدر الإشارة إلى ان المادة (87 مكرر9 ق ع) قد حددت مدة تطبيق العقوبة التبعية والتي تتراوح مابين سنتين (2) إلى عشر (10) سنوات في حين المادة (8 ق ع) لم تحدد مدة تطبيق العقوبة[2]

وتتمثل العقوبات التكميلية حسب نص المادة (9 ق ع) فيما يلي:

1- الحجز القانوني.
2- الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية.
3- تحديد الإقامة.
4- المنع من الإقامة.
5- المصادر الجزئية للأموال.
6- المنع المؤقت من ممارسة مهنة او نشاط.
7- إغلاق المؤسسة.
8- الإقصاء من الصفقات العمومية.
9- الحضر من إصدار الشيكات و/أو إلغاؤها مع المنع من استصدار رخصة جديدة.
10- تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة.

[1] مفيدة ضيف: سياسة المشرع في مواجهة ظاهرة الإرهاب ، رسالة ماجستير تخصص قانون العقوبات والعلوم الجنائية ، كلية الحقوق والعلوم السياسية، جامعة الأخوة منتوري ، قسنطينة ، السنة الجامعية 2009-2010، ص140،138

[2] احميدي بوجليطية بوعلي :سياسة مكافحة الإرهاب في الوطن العربي ، دراسة مقارنة بين الجزائر ومصر ، رسالة ماجستير ،كلية العلوم السياسية والإعلام ، جامعة دالي إبراهيم ، الجزائر 2 السنة الجامعية 2009-2010 ،ص160

11-سحب جواز السفر.

12- نشر او تعليق حكم أو إضافة الى العقوبات التكميلية سالف قرار الإدانة[1]

وفي تقديرنا الخاص وبالاستناد إلى نص المادة (394 مكرر 6 ق ع) المتعلقة بجريمة المساس بأنظمة المعالجة الإلية للمعطيات، يجوز للقاضي بالإضافة إلى العقوبات التكميلية سالفة الذكر الحكم بعقوبات تكميلية خاصة تتعلق بالجرائم الواقعة ضمن البيئة الالكترونية شانها شان جريمة التجنيد الإلكتروني شانها شان جريمة التجنيد الإلكتروني للإرهاب والمتمثلة في :

- الحكم بمصادرة الأشياء المستعملة في ارتكاب الجريمة او الناتجة عنها.
- إغلاق المواقع الإلكترونية.
- غلق المحل أو مكان الاستغلال إذا كان صاحب المحل على علم بذلك.

المطلب الثاني: العقوبات المقررة لجرائم الإرهاب الالكتروني.

لقد تم التركيز في هذا المطلب على العقوبات المقررة على الشخص الطبيعي و المعنوي

الفرع الاول: العقوبات المطبقة على الشخص الطبيعي:

وجب التميز بين العقوبات الأصلية والتكميلية

أ- العقوبات الأصلية:

- عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات، حسب الفعل المرتكب والغرامة تتراوح قيمتها من خمسين ألف دج إلي خمسة مائة ألف دج،حسب الفعل المرتكب: الدخول والبقاء بالغش (الجريمة البسيطة)، الدخول والبقاء بالغش (الجريمة المشددة) و تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة الاعتداء ألعمدي على المعطيات.[2]

[1] انظر المادة:(09) ق ع.

[2] أنظر: المواد القانونية، 394 مكرر، 394 مكرر1، 394 مكرر2.

ب- العقوبات التكميلية:

- المصادرة تشمل الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية. و إغلاق المواقع والأمر

يتعلق بالمواقع (les sites) التي تكون محلا الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها

ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها.[1]

ت- عقوبة الشروع في الجريمة : جاءت به المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي واعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية ، بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ، إذ أصبح الشروع معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها.[2]

ج - الظروف المشددة: نص القانون على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، تضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات العامة.[3]

---

[1] أنظر المادة: 394 مكررة " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها."

[2] - أنظر المادة: 394 مكررة " يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها

[3] - أنظر المادة: 394 مكررة " تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات اشد."

الفرع الثاني:العقوبات المقررة على الشخص المعنوي.

إن" الشخص المعنوي هو مجموعة من الأشخاص او الأموال تتحدد من اجل تحقيق غرض معين ومعترف لها بالشخصية القانونية فهو في فقه القانون كيان تثبت له أهلية الوجوب وأهلية الأداء"[1].

أولا: أنواع الأشخاص المعنوية المسؤولة جزائيا:

تقسم الأشخاص المعنوية العامة الى نوعين : أشخاص معنوية عامة وهي تلك التي تخضع لقواعد القانون العام ، وأشخاص معنوية خاصة وهي التي تسري عليها قواعد القانون الخاص "[2].

وبالرجوع إلى نص المادة (51 مكرر ق ع) نجد أن المسؤولية الجزائية قررت للشخص المعنوي التابع للقطاع الخاص دون الأشخاص المعنوية العامة والمتمثلة في المؤسسات العمومية ذات الطابع الإداري أو العلمي أو التكنولوجي أو الثقافي أو المهني ، أو الأشخاص المعنوية التابعة للدولة والجماعات المحلية المتمثلة في الولاية والبلدية ، غير ان المؤسسات ذات الطابع الصناعي والتجاري تسال جزائيا لأنها من جهة تخضع للقانون الإداري فيما يخص علاقتها مع الدولة كما تخضع للقانون الخاص في علاقتها مع الغير [3].

ثانيا : المسؤولية الجزائية للشخص المعنوي.

كرس المشرع الجزائري بموجب القانون رقم 04-15 المؤرخ في : 10-11-2004 المعدل والمتمم لقانون العقوبات المسؤولية الجزائية للشخص المعنوي في نص المادة (51 مكرر) منه والتي تنص على : " باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العم ، ويكون الشخص المعنوي مسؤولا جزئيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته آو ممثليه الشرعيين عندما ينص القانون على ذلك.

---

[1] متعب هلال لعتيبي : المسؤولية الجنائية عن جريمة غسل الأموال الرقمية في المملكة العربية السعودية ، رسالة الماجستير ، كلية الدراسات ، قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الإنسانية الرياض ، ص 2013

[2] عبد الرحمان خلفي : المسؤولية الجزائية للأشخاص المعنوية عن جرائم تبيض الأموال (دراسة في التشريع الجزائري مع الإشارة الى الفقه والتشريع المقارن) مجلة الأكاديمية للبحث القانوني ، عدد2011/02 كلية الحقوق والعلوم السياسية جامعة عبد الرحمان ميرة ، بجاية ، ص ،24.

[3] أحسن بوسقيعة :الوجيز في القانون الجزائي العام ،مرجع سابق ، ص 275،274.

إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي **او** كشريك في نفس الأفعال ".وبالتالي نلاحظ ان المشرع قد عمم المسئولية الجزائية للشخص المعنوي من خلال نصه عليها ضمن تشريع جزائي عام ، أما التعديل الأخير المتضمن **قانون العقوبات رقم** 06-23 **المؤرخ في** 20-12-2006 ، فقد فتح مجال المسؤولية الجزائية أكثر من خلال تعميمها على جميع جرائم الأموال مادامت متطابقة مع نص المادة (51 **مكررق ع**) والتي تنص على شروط المساءلة الجزائية **للشخص المعنوي** [1].

ومن خلال نص المادة السالفة الذكر نلاحظ أن الشخص المعنوي يسال جزائيا مثله مثل الشخص الطبيعي عن الجرائم التامة أو المشروع في تنفيذها كما يكون فاعلا أو شريكا.

ثالثا : الجرائم محل المساءلة الجزائية :

1-**الجرائم المقررة بموجب القانون** 04-15**:**

-**جرائم** تكوين جمعية الأشرار المادة (177 **مكررق ع**).

-جرائم تبيض الأموال المادة (389 **مكرر** 7 **ق ع**).

-الاعتداءات على أنظمة المعالجة الآلية للمعطيات المادة (394 **مكرر** 4 **ق ع**).

الجرائم المقررة بموجب القانون 06-23:

-الجنايات والجنح ضد امن الدولة المواد (61 **إلى** 96 **ق ع**).

-الجنايات والجنح ضد **الدستور** (**من** 175 **مكررق ع**).

- جرائم التزوير المواد (197 **إلى** 253 **ق ع**).

- جرائم الاعتداء على الحريات الفردية والخطف المواد (295 **مكررق ع**).

- الجنايات والجنح ضد الأشخاص المواد (303 **مكرر** 3 **ق ع**).

-الجنايات والجنح التي من شانها الحيلولة دون التحقيق من شخصية طفل المادة (321).

- الجنايات والجنح ضد الأموال المادة (382 **مكرر** 1 **و**417 **مكرر** 3 **ق ع**).

- جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية المادة (435 **مكررق ع**)

[1] عبد الرحمان خلفي،: المرجع السابق ،ص22.

2- الجرائم المقررة بموجب قوانين خاصة :

-المادة (25) من القانون 04-18 المؤرخ في 25-12-2004 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها.

-المادة (25) من الأمر 06-01 المؤرخ في 20-02-2006 المتعلق بمكافحة التهريب.

-المادة (53) من القانون رقم 06-01 المؤرخ في 20-02-2006 المتعلق بالوقاية من الفساد ومكافحته[1].

رابعا :العقوبات المقررة للشخص المعنوي:

خصص المشرع مجموعة من التدابير الاحترازية تتماشى وطبيعة الشخص المعنوي كالمراقبة وحل الشخص المعنوي والغلق وتضييق نطاق عمله والغرامة والمصادرة [2].

أ –العقوبات المطبقة في مواد الجنايات والجنح :

وبالرجوع إلى نص المادة (18 مكرر ق ع) التي تنص على: " العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

- الغرامة التي تساوي من مرة (1) إلى خمس مرات (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب الجريمة .
- واحدة أو أكثر من العقوبات التكميلية الآتية
- حل الشخص المعنوي .
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5)سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5)سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر او غير مباشر ، نهائيا آو لمدة لا تتجاوز خمس (5) سنوات وتنصيب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته[3] .

---

[1] أحسن بوسقيعة : المرجع السابق ،ص 284،282

[2] منصور رحماني: الوجيز في القانون الجنائي العام ، دار العلوم للنشر والتوزيع عنابة ، طبعة 2006ص 211.

[3] انظر المادة : (18 مكرر)ق ع.

ب- العقوبات المطبقة في مواد المخالفات :

تنص المادة (18 مكرر 1ق ع) على "العقوبات التي تطبق على الشخص المعنوي في المخالفات هي:

الغرامة التي تساوي مرة (1) إلى خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة كما يمكن الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة او نتج عنها " وتجدر الإشارة إلى انه في حالة عدم النص على عقوبة الغرامة المقررة للأشخاص الطبيعية سواء في مواد الجنايات أو الجنح وقامت المسؤولية الجزائية للشخص المعنوي طبقا للمادة 51 مكرر من القانون نفسه ، فإن الحد الأقصى للغرامة المحتسب لتطبيق النسبة القانونية المقررة للعقوبة فيما يخص الشخص المعنوي تكون كالأتي:

1-2.000.000 عندما تكون الجناية معاقبا عليها بالإعدام أو السجن المؤبد.

2- 1.000.000دج عندما تكون الجناية معاقبا عليها بالسجن المؤقت.

3- 5.000.000دج بالنسبة للجنح [1]

خامسا :صور الأشخاص المعنوية القائمة بالتجنيد الالكتروني:

من ابرز الصور للأشخاص المعنوية التابعة للجماعات الإرهابية والقائمة بعملية تجنيد الإرهاب تتمثل في:

وسائل الإعلام والإذاعات ووكالات الأنباء والمجلات الإلكترونية الإرهابية والتي تظم مختلف القنوات التلفزيونية التابعة لتنظيم الدولة الإسلامية ، كالمؤسسات الإعلامية : مؤسسة الفرقان، مؤسسة الصقيل ، مؤسسة الحياة، مؤسسة أعماق ، مجلة دابق ...إلخ.

كما قد تكون في شكل جمعيات خيرية أو جمعيات إغاثة أو مراكز تعليمية مهما كان نشاطها أو الهدف الذي نشأت من اجله.

سادسا :العقوبات المقررة للشخص المعنوي القائم بالتجنيد الالكتروني للإرهاب :

استنادا إلى نص المادة (87 مكرر 12 ق ع) نجد أن المشرع لم يقر صراحة بمسؤولية الشخص المعنوي ولكنه عمم الحكم من خلال استعماله للفظ "كل من" وبالتالي تكون

[1] انظر المواد: (18مكرر 1)، (18 مكرر2)، ق ع.

عقوبة الشخص المعنوي القائم بعملية التجنيد الإلكتروني للإرهاب في هذه الحالة وفقا للقواعد العامة المنصوص عليها ف قانون العقوبات ، وذلك بالاستناد إلى النصوص القانونية التي تقر بالمسؤولية الجزائية للشخص المعنوي في مادة الجنايات الواردة في نص المادة (18 مكررق ع)وتتمثل في العقوبات التالية :

- عقوبة أصلية تتمثل في الغرامة التي تساوي من مرة إلى خمس مرات للغرامة المقررة للشخص الطبيعي.
- عقوبات تكميلية الواردة في نص المادة (18 مكرر 1)سالفة الذكر [1].

المبحث الثاني : الآليات الإجرائية لمكافحة الإرهاب الالكتروني.

وتم تقسيم المبحث إلى ثلاثة مطالب تناولت على التوالي مرحلة البحث والتحري ، أساليب التحري الخاصة وتم اختتام المبحث بالتطرق إلى الإجراءات الخاصة بالبحث والتحري الالكتروني .

المطلب الأول:مرحلة البحث والتحري.

تعد المتابعة الجزائية سلسلة من الإجراءات القانونية التي تنطلق بمجرد وقوع الجريمة إبتداءا بمرحلة البحث والتحري الذي تقوم بها الضبطية القضائية ، مرورا بمرحلة التحقيق القضائي وتنتهي بمرحلة المحاكمة .
وبما أن جريمة التجنيد الالكتروني للإرهاب جريمة ذات أبعاد قانونية متنوعة فإن إجراءات المتابعة فيها تمتاز بنوع من الخصوصية كونها تأخذ الطابع الإلكتروني الافتراضي من جهة والطابع المادي من جهة أخرى ، ما نتج عنه تنوع في الإجراءات الجزائية المتبعة لقمع هذه الجريمة الأمر الذي طرح تحديات صعبة في الواقع العملي بشأنها.

-كما تعد مرحلة البحث والتحري على الجرائم أهم مرحلة تقوم بها الضبطية القضائية في إطار الكشف عن الجريمة الإلكترونية ومرتكبيها ، كما عرفها "محمد محدة " على أنها " تتبع وسائل الإثبات من ظروف مادية وأقوال ونصوص ومعاينة والإحاطة بكل ماله من صلة بأحداث الجريمة وتعيين المجرم "[2].

---

[1] انظر المادة: (87 مكرر 12) ق ع.

[2] - عبد الواحد إلهام مرسي: الموسوعة الذهبية في التحريات ، دار المعارف والمكاتب الكبرى ، د ط ، ص 66.

فإذا اخذنا جريمة التجنيد الالكتروني للإرهاب فإنها جريمة إرهابية ذات طابع رقمي أخضعها المشرع الجزائري إلى خليط من إجراءات البحث والتحري منها ما هو منصوص عليه في قانون الإجراءات الجزائية ومنها ما ورد في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الأول: الإجراءات العادية (الأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية)

ويمكن أن نعدد هذه الإجراءات فيما يلي:

- تلقي البلاغات والشكاوى: حسب نص المادة (17 ق إ ج) يباشر ضباط الشرطة القضائية السلطات الواردة في نص المواد (12و13 ق إ ج)، ويتلقون الشكاوى والبلاغات غير انه فيما يخص الجرائم الإرهابية لا يشترط وجود بلاغ أو شكوى.
- جميع الاستدلالات: تخول المادة (17 ق إ ج) سالفة الذكر لضباط الشرطة القضائية صلاحية جمع الاستدلالات.
- طلب المساعدة للبحث عن الأشخاص المشتبه في ارتكابهم جرائم إرهابية
- تنفيذ الإنابة القضائية.
- إجراء التحقيقات التمهيدية: تخول المادة (17) من نفس القانون للضبطية القضائية سلطة إجراء التحقيقات الابتدائية.
- القيام بعملية التفتيش .
- التوقيف للنظر.
- إخطار وكيل الجمهورية بغير تمهل بالجنايات والجنح ذات تكييف إرهابي: ألزمت المادة (18 ق إ ج) بإخطار وكيل الجمهورية بالجنايات والجنح فور علمهم بها.
- طلب مساعدة القوة العمومية في تنفيذ مهام ضباط الشرطة القضائية.
- تحرير محاضر بأعمال ضباط الشرطة القضائية: ألزمت المادة (18) من نفس القانون الضبطية القضائية بتحرير محاضر أعمالهم.
- إرسال المحاضر إلى وكيل الجمهورية [1].

الفرع الثاني: الإجراءات الاستثنائية(التلبس بالجريمة الإرهابية أو التخريبية):

ويمكن أن نعدد هذه الإجراءات فيما يلي :

[1] - عبد الرحمان خلفي : الإجراءات الجزائية في التشريع الجزائري والمقارن ، دار بلقيس للنشر ، الجزائر 2015، ص 71، 72.

- إخطار وكيل الجمهورية بوقوع جرائم ذات وصف إرهابي للتكفل بنفسه بمعاينة حالة التلبس طبقا للمادة (42ف 1ق إ ج).
- معاينة مسرح الجريمة مع ضرورة المحافظة على الآثار .
- ضبط المشتبه فيه واقتياده لأقرب مركز للشرطة طبقا للمواد (41 و55ق إ ج).
- إلقاء القبض على المتهم الذي تقوم بحقه دلائل قوية ومتماسكة بارتكابه أفعال إرهابية او تخريبية .
- التحقق من هوية الأشخاص المتواجدين في مسرح الجريمة وأمرهم بعدم مبارحة الأمكنة طبقا للمادة (50ق إ ج).
- لضابط الشرطة القضائية الاستعانة بتقارير الخبراء مع وجوب أدائهم لليمين وكتمان السر المهني حسب المادة (49ق إ ج).
- توقيف المشتبه فيه بارتكابه أفعال إرهابية أو تخريبية تحت النظر وهو إجراء يقوم به ضابط الشرطة القضائية طبقا للمادة (51ق إ ج) ، مع جواز تمديد أجال التوقيف خمس مرات بإذن مكتوب من وكيل الجمهورية.

المطلب الثاني: أساليب التحري الخاصة:

وللوقوف على هذه الأساليب وجب تعريفها وكذا تبيان الأجهزة المختصة بالبحث والتحري

الفرع الاول: تعريفها:

استحدث المشرع الجزائري بموجب الأمر رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية أساليب وآليات حديثة تدخل ضمن اختصاص الضبطية القضائية في إطار إجراءات التحري والتحقيق في بعض الجرائم الواردة على سبيل الحصر في نص المواد (65 مكرر وما بعدها)من نفس القانون [1].
وسميت بأساليب التحري الخاصة لان القيام بها يتطلب خبرة ودراية في مجال التكنولوجيا كونها تشكل مساسا خطيرا بحق الأفراد في حرمة حياتهم الخاصة ولا يتم اللجوء إلى مثل هكذا أساليب في حالة ما إذا كانت الإجراءات الأخرى العادية لا تفي بإظهار الحقيقة [2].

---

[1] - عبد الرحمان خلفي : الإجراءات الجزائية في التشريع الجزائري والمقارن ، دار بلقيس للنشر ، الجزائر 2015 ، ص 71-72.

[2] - الداودي مجرب :الأساليب الخاصة للبحث والتحري في الجريمة المنظمة ، رسالة دكتوراه ، كلية الحقوق ، جامعة الجزائر 1بن يوسف بن خدة ،2016/2015،ص192.

وعرفها الفقه على أنها "تلك العمليات أو الإجراءات أو التقنيات التي تستخدمها الضبطية القضائية تحت المراقبة وإشراف السلطة القضائية ،بغية البحث والتحري عن الجرائم

الخطيرة المقررة في قانون العقوبات ،وجمع الأدلة عنها والكشف عن مرتكبيها ، وذلك دون علم ورضا الأشخاص المعنيين".

أ- مجال تطبيقها:

حصر المشرع الجزائري اللجوء إلى أساليب التحري الخاصة في إطار سبعة انواع من الجرائم هي :

1- جرائم المخدرات
2- جرائم تبيض الأموال
3- الجرائم الإرهابية والأعمال التخريبية.
4- الجرائم الماسة بالأنظمة العابرة للحدود الوطنية
5- جرائم الصرف.
6- جرائم الفساد.

ب - صورها:

1- المراقبة: نصت المادة (16 مكرر ق إ ج) على ان "الرقابة عملية أمنية يقوم بها ضباط وأعوان الضبطية القضائية عبر كامل التراب الوطني بهدف البحث والتحري المباشر على الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه في ارتكاب احد الجرائم الخطيرة أو نقل الأشياء أو الأموال أو متحصلات من ارتكاب احد الجرائم الخطيرة او نقل الأشياء أو الأموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها " .

2- اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

يقصد بعملية اعتراض المراسلات القيام بمراقبتها سواء كانت سلكية او لا سلكية او عن طريق الاعتراض أو التسجيل أو النسخ ،بغرض الوصول إلى الحقيقة في إطار عمليات البحث والتحري عن الجرائم وجمع الأدلة أما تسجيل الأصوات والتقاط الصور تتم عن طريق "تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية او خاصة وفي مكان علم او خاص وكذلك التقاط صور لشخص او عدة أشخاص يتواجدون في مكان خاص [1].

[1] عبد الرحمان خلفي:المرجع السابق، ص 71-72.

3- التسريب: نص المشرع الجزائري على إجراء التسريب كأسلوب تحري خاص ضمن المادة (65 مكرر 12 ق إ ج) :"يقصد بالتسريب قيام ضابط أو عون الشرطة القضائية تحت طائلة البطلان ، إن تشكل هذه الأفعال تحريضا على ارتكاب جرائم [1].

4- الأحكام الخاصة:

إضافة إلى قواعد البحث والتحري العامة وأساليب التحري الخاصة الواردة في قانون الإجراءات الجزائية ،استحدث المشرع الجزائري قواعد قانونية حديثة تتماشى والإجرام المستحدث من اجل الإحالة الشاملة والفعالة بالأساليب الحديثة في ارتكاب الجرائم ،كون أن القواعد التقليدية لم تعد كافية لملاحقة هذا النوع من الإجرام ، وبالتحديد جريمة التجنيد الإلكتروني للإرهاب التي أخذت أبعاد متعددة الأمر الذي جعلها تخضع لنصوص قانونية مختلفة كونها تحمل أكثر من وصف فبالإضافة إلى أنها جريمة إرهابية وتخريبية فهي جريمة إلكترونية وجريمة في أن واحد ، وانطلاقا من هذا قرر المشرع

قواعد تضمنها القانون رقم 09-04- المؤرخ في 05 غشت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الثاني - الأجهزة المختصة بالبحث والتحري الالكتروني :

1- وطنيا:

- **جهاز الشرطة:** في إطار الوقاية من مكافحة الوقاية من الجريمة الإلكترونية تم إنشاء مخبر رئيسي للشرطة العلمية على مستوى المديرية العامة للأمن الوطني المتواجد "**بالشطاوف**" بالجزائر العاصمة ، ومخبرين جهويين بالشرق الوطني بقسنطينة وفي الغرب الجزائري بوهران ،كما تم تدعيم مراكز **الأمن الولائي بفرق متخصصة في** مجال التحقيق في الجرائم المعلوماتية .
- **جهاز الدرك الوطني :** يتولى مهمة التحقيق الالكتروني **قسم الإ**علام والإلكترونيك المتواجد على مستوى المعهد الوطني للأدلة الجنائية وعلم الإجرام والذي مقره **"بوشاوي"** التابع للقيادة العامة للدرك الوطني إضافة إلى مراكز الوقاية ومكافحة

[1] انظر المادة:65 مكررق، إ.ج

الجرائم المعلوماتية المتواجد مقره" **ببئر مراد رايس**" التابع لمديرية **الأمن العمومي** للدرك الوطني قيد التأسيس [1].

2- دوليا:

المنظمة الدولية للشرطة الجنائية (الانتربول): نصت المادة (16 ق و) على انه :" **في** إطار التحريات **أو** التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها ، يمكن للسلطات المختصة تبادل المساعدات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني "[2].

من اجل تبادل المعلومات بين الدول في الخارج بشان الجريمة والتعرف على الفاعلين وتحديد مكان تواجدهم ، تقوم الهيئة الوطنية الجزائرية بمشاركة الأعمال التحضيرية الضرورية مع الهيئات الدولية المماثلة لها بهدف البحث والتعرف على الجرائم المعلوماتية ومرتكبيها وتحديد مكان تواجدهم [3] .وعليه تعد المنظمة الدولية للشرطة

الجنائية أهم جهاز دولي في مجال مكافحة الإجرام بما فيها **الجرائم** المعلوماتية، **كما** تعمل على تشجيع التعاون الدولي بين أجهزة **الشرطة، من خلال وضع قائمة تضم** ضباط متخصصين في مجال البحث والتحري بشان الإجرام المعلوماتي والذين يمكن الاستعانة بيهم من طرف الدول الأطراف [4] **كما تعمل** على تسيير عملية تبادل المعلومات بين الدول كما تسهل الإجراءات القضائية المتعلقة بتسليم المجرمين وتنفيذ الإنابات القضائية الدولية وكذا نشر **أوامر** القبض الدولية للمبحوث عنهم والمطالب بتسليمهم [5].

المطلب الثالث: الإجراءات الخاصة بالبحث والتحري الالكتروني:

---

[1] - نعيم سعيداني : آليات البحث والتحري عن الجريمة المعلوماتية في **القانون الجزائري** ، **رسالة** ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ،2013/2012،ص103.

[2] - **أنظر المادة** (16) ق ،و،ج،إ،إ.

[3] - احمد مسعود مريم: آليات مكافحة جرائم تكنولوجيا الأعلام والاتصال في ظل القانون 04/09، لرسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، ،ص 46.

[4] - نعيم سعيداني : المرجع نفسه ،ص108 .

[5] - **عبد الرحمان حملاوي: مداخلة بعنوان** "دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية " ،**الملتقى الوطني حول** " الجريمة المعلوماتية " المنعقد بتاريخ :16-17 **نوفمبر** 2015 ، بكلية الحقوق والعلوم السياسية ،جامعة محمد خيضر ، بسكرة ،ص 6،5.

وقد تضمن هذا المبحث إجراء التفتيش وكذا الحجز الالكتروني ليختتم بالاختصاصات الاستثنائية لضباط الشرطة القضائية.

الفرع الأول: التفتيش .

هو " ..البحث عن شيء يتصل بجريمة وقعت ، ويفيد في كشف الحقيقة عنها وعن مرتكبيها ، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة [1].

لم يعرف المشرع الجزائري إجراء التفتيش الواقع على المنظومة المعلوماتية **فاكتفى بالنص** على إجراءات القيام ،لكن يمكنني **أن** اعتبره ذلك الإجراء القانوني الواقع بداخل بيئة افتراضية والمتمثلة في المنظومة المعلوماتية والتي تشكل مسرح الجريمة الإلكترونية ، والذي يهدف إلى البحث عن الحقيقة.

1-القائم به: خول المشرع الجزائري مهمة القيام بالتفتيش عن بعد وذلك حسب نص المادة (05) **من القانون** 09-04 إلى سلطتين هما:

السلطة القضائية المتمثلة في قاضي التحقيق أو وكيل الجمهورية وذلك حسب الحالات **وضباط الشرطة** القضائية.[2]

2-شروطه: نصت المادة (05) من نفس القانون على الحالات التي يجوز فيها اللجوء الى التفتيش وهي :

-**إذا** كانت هناك أسباب تدعو للاعتقاد بان هناك المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وان المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى .

- إذا تبين مسبقا بأن المعطيات محل البحث والتي يمكن الدخول إليها انطلاقا من المنظومة **الأولى، مخزنة في منظومة** معلوماتية تقع خارج الإقليم **الوطني**.

- إعلام السلطة القضائية ، وذلك لان المشرع الجزائري لم يشترط استصدار إذن كما هو الحال بالنسبة للتفتيش المادي بل اكتفى بإعلام السلطات المتمثلة في وكيل الجمهورية او قاضي التحقيق حسب الحالات [3] .

---

[1] - **احمد فتحي سرور :** الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ، 1980، ص 499.

[2] - **انظر المادة**: (5) ق ،و،ج،إ،إ.

[3] -احمد مسعود مريم **:** آليات مكافحة جرائم تكنولوجيا الأعلام والاتصال في ظل القانون 04/09، لرسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، ص 91

3-محل التفتيش عن بعد :

حددت المادة (05) من نفس القانون الأنظمة المعلوماتية محل التفتيش وهي:
منظومة معلوماتية كلها أو جزء منها، وقد عرف المشرع الجزائري المنظومة المعلوماتية في نص المادة (02) من نفس في الفقرة "ب"أي نظام او مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها او أكثر بمعالجة إلية للمعطيات تنفيذا لبرنامج معين ".
المعطيات المعلوماتية المخزنة فيها ، ويقصد بها حسب نص المادة (02) من نفس القانون" أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها [1]. وعليه فان البيانات والمعلومات الالكترونية يمكن أن تكون محلا للتفتيش والاستناد إليها من وسائل الإثبات الجنائي.

4: تنفيذ التفتيش عن بعد :

أ- **داخل الإقليم الوطني** :بالاستناد على نص المادة (50) من القانون 09-04 والتي تنص على " في الحالة المنصوص عليها في الفقرة أ من هذه المادة ، إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية إخرى وان هذه المعطيات يمكن الدخول إليها ، انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة او جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك" [2].

وعليه متى كانت المعطيات محل البحث مخزنة داخل جهاز اخر متصل بالجهاز الأول عن طريق شبكة الاتصالات لكن في أماكن متفرقة داخل الإقليم الوطني ، وكان من الممكن الدخول إليها من خلال الجهاز الثاني يجوز تمديد التفتيش في هذه الحالة ولا يهم إن كان هذا الجهاز مللك للمتهم أو لشخص أخر انه احتوي على المعطيات محل البحث[3].
نلاحظ أن المشرع قد أجاز إمكانية تمديد التفتيش بموجب إشعار مسبق للسلطات القضائية دون الالتزام باستصدار إذن تمديد التفتيش، متى كان التفتيش داخل الإقليم الوطني.

ب-**خارج الإقليم الوطني** :نصت المادة (05) من نفس على " إذا تبين مسبقا بان المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني ، فإن الحصول عليها يكون

[1] - انظر المادة (02) ق، و،ج،إ،إ.

[2] - أسامة بن غانم ألعبيدي: مرجع سابق، ص 90.

[3] - المادة: (05) ق ،و،ج،إ،إ.

بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل[1].

وعليه في حالة ما إذا تم تخزين المعطيات المعلوماتية محل الجريمة ضمن أنظمة معلوماتية خارج الإقليم الوطني عن طريق شبكة الانترنت ، يجوز القيام بإجراء تفتيش نظم الحاسب المرتبطة به الموجودة في دول أخرى ، ولكن للحصول على تلك المعطيات لابد من مساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية وتكريسا لمبدأ المعاملة بالمثل كونها مسالة تتعلق بسيادة الدولة على أراضيها.[2]

كما أجازت المادة (32) من الاتفاقية الأوربية المتعلقة بمكافحة الجرائم المعلوماتية المعدة من طرف المجلس الأوروبي والتي تم التوقيع عليها في بودابست عام 2001 الدخول لأجهزة الحاسب أو الشبكات داخل إقليم دول أخرى للتفتيش عنها أو ضبطها وذلك دون الحاجة للحصول على إذن في حالتين هما:

- تفتيش معلومات أو بيانات عمومية متاحة للجمهور.
- رضا مالك هذه البيانات أو الذي كانت بحوزته.

الفرع الثاني:- الحجز الالكتروني:

لم يتعرض المشرع الجزائري ضمن قانون 09-04 إلى تعريف الحجز الإلكتروني للمعلومات واكتفى بتسميته حجز وليس ضبط كما هو متعارف في قانون الإجراءات الجزائية ، وربما يرجع ذلك إلى أن إجراء الضبط لا يتم إلا على الأشياء المادية الملموسة أما الحجز فهو يشمل الإجراء المادي والإجراء الإلكتروني معا ، ويقصد بحجز المعطيات المعلوماتية اي ضبط الدليل الالكتروني :

ويتمثل الحجز في " وضع اليد على الشيء يتصل بجريمة وقعت ويفيد في كشق الحقيقة عنها ، وعن مرتكبها ".

1محل الحجز : يقع الحجز على أشياء مادية كالأوراق الموجودة في مسرح الجريمة الالكترونية التي تمت طباعتها وأجهزة الحاسب الآلي وجميع لواحقه ، كما يقع على أشياء معنوية أو إلكترونية كالبيانات وغيرها [3].

---

[1] - احمد مسعود مريم: آليات مكافحة جرائم تكنولوجيا الأعلام والاتصال في ظل الفانون 04/09، لرسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، ص 91.

[2] - المادة (05) ف 3 ق ،و،ج،إ،إ.

[3] - سليمان غازي و بخيت المقيطي العتيبي: دور البحث الجنائي في الكشف على الجرائم المعلوماتية (دراسة تطبيقية على شرطة منطقة مكة المكرمة)، رسالة دكتوراه، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الامنية ، الرياض 2016 ، ص 42.

أ- **إجراءات حجز المعطيات المعلوماتية** : نصت المادة (42) من قانون الإجراءات الجزائية على انه " يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس ان يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية ويتخذ جميع جميع التحريات ....وان يضبط كل ما يمكن أن تؤدي إلى إظهار الحقيقة ..[1].

من خلال نص المادة نجد أن المشرع الجزائري ألزم ضباط الشرطة القضائية الانتقال إلى مسرح الجريمة للقيام بعملية للعلم بعملية والتفتيش من اجل حجز الأدلة الرقمية وكل دليل من شانه إظهار الحقيقة.

من خلال نص المادة نجد أن المشرع الجزائري ألزم الشرطة القضائية الانتقال إلى مسرح الجريمة للقيام بعملية المعاينة والتفتيش من اجل حجز الأدلة الرقمية وكل دليل من شانه إظهار الحقيقة.

ب- أساليب حجز المعطيات الالكترونية :

نص المشرع الجزائري في المواد (06-07-08) من القانون رقم 09-04 على أساليب حجز المعطيات في:

1 - حجز المعطيات المعلوماتية ونسخها : نصت المادة (06) من نفس القانون 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 محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير انه يجوز لها **لستعمل** الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات ، قصد جعلها قابلة للاستغلال لأغراض التحقيق ، شرط آلا يؤدي ذلك **إلى** المساس بمحتوى المعطيات [2].

بالاستناد إلى نص المادة نجد أن المشرع قد أجاز للسلطات القضائية المكلفة بمهمة التفتيش عدم القيام بإجراء الحجز الكلي للمنظومة المعلوماتية مدام انه بإمكانهم نسخ المعطيات

[1] - المادة: (42) ق، إ.ج.

[2] - انظر المادة: (07) ق ،و.ج،إ.إ.

محل الجريمة وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في احراز طبقا لقانون الإجراءات الجزائية ، كما ألزم القائمين بالتفتيش أو الحجز المحافظة على الدليل الرقمي المتحصل عليه.

كما أجاز المشرع في نص المادة (06) فقرة 03 من نفس القانون لستعمل الوسائل الضرورية من اجل جعل المعطيات قابلة لان تكون دليل رقمي مقبولا قانونيا وذلك عن طريق تشكيلها أو إعادة تشكيلها لجعلها صالحة.

2-الحجز عن طريق منع الوصول إلى المعطيات :

نصت المادة (07 ق، و) **على** انه: " إذا استحال إجراء الحجز وفقا لما هو منصوص عليه **في المادة** 6 **أعلاه، لأسباب** تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، **أو إلى** نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه **المنظومة**.

نلاحظ من خلال نص المادة أن المشرع ألزم السلطة المخول لها قانونا القيام بإجراء الحجز **أن** تقوم بالإجراءات التقنية اللازمة من اجل منع الإطلاع على المعطيات المخزنة بالمنظومة المعلوماتية أو حتى الوصول إليها أو نسخها في حالة ما إذا تعذر عليها حجز هذه المعطيات نتيجة لأسباب تقنية .

3- منع الإطلاع على المعطيات المحجوزة :

نصت المادة (08) من نفس القانون على انه"يمكن للسلطة **أن** تباشر التفتيش بان **تأمر باتخاذ الإجراءات** اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، **لا** سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك [1].

من خلال نص المادة تبين لنا ان المشرع أجاز للسلطة القائمة بالتفتيش منع الاطلاع **على** المعطيات المخزنة في منظومة معلوماتية آو على جهاز الحاسب متى كان محتواها يشكل جريمة ، كما هو الحال بالنسبة لإجراءات حجب وتدمير المواقع الالكترونية التي تعمل على تجنيد الشباب ضمن الجماعات الإرهابية.

[1] - اظر المادة : (08) ق ،و،ج،إ،إ.

الفرع الثالث:الاختصاصات الاستثنائية لضباط الشرطة القضائية في الجرائم المعلوماتية.

يؤول اختصاص المحاكمة في الجزائر على خلاف النظام القضائي الفرنسي في ما يخص الجرائم المعلوماتية DES POLES SPECIALISE بعدد أربعة على المستوى الوطني (قسنطينة ، الجزائر العاصمة ، سيدي أمحمد ، وهران ، ورقلة) .
كما ان المشرع الجزائري على خلاف سائر الجرائم فإنه وسع من اختصاص ضباط الشرطة القضائية بصفة استثنائية في حالة ما إذا كان التحقيق التمهيدي يخص جرائم معينة أي تلك المتعلقة بـ: المخدرات ، تبيض الأموال أو تلك المتعلقة بالتشريع الخاص بالصرف او الملسة بأظمة المعالجة الآلية للمعطيات والجريمة المنظمة العابرة للحدود الوطنية وكذا جرائم الفساد والمنصوص والمعاقب عليها بموجب القانون رقم 06-01 المؤرخ في 20-02-2006 والمتعلق بالوقاية ومكافحة الفساد فقد أصبح بموجب القانون رقم 06-01 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية يتمتع باختصاصات اوسع في سبيل تسهيل إجراءات البحث والتحري عن تلك الجرائم وكشف مرتكبيها وجمع الاستدلالات عنها بما يمكنه من مواجهة الصعوبات التي قد تعترضه نظرا لخطورة وطبيعة تلك الجرائم ، كما مكن المشرع ضباط الشرطة القضائية بموجب القانون 06-22 من اختصاصات جديدة لم يكن يتمتع بها قبل صدور هذا القانون وهي سلطة مراقبة الأشخاص والأموال والأشياء واعتراض المراسلات وتسجيل الأصوات والصور والقيام لعمليات التسريب [1]

[1] - محمد حزيط :"مذكرات في قانون الإجراءات الجزائية "،دار هومة، الطبعة الثالثة 2008،الجزائر ، صفحة 68.

المبحث الثالث: الآليات الإجرائية في ظل القانون 04/09.

لعل خصوصية الجريمة المعلوماتية كما رأينا سابقا أبرزت مشكلة المكافحة الإجرائية خاصة من ناحية كيفية جمع الأدلة الإلكترونية و مدى حجيتها، و حتى تتوفر في الدليل الإلكتروني المشروعية التي تشترطها القوانين في كافة التشريعات.

و المشرع الجزائري، اقتداء بالمشرعين الذين سبقوه، سارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية، و ذلك بتعديل بعض المواد في قانون الإجراءات الجزائية و إصدار قوانين خاصة و جديدة في مجال الإجراءات و التي سنتناولها بالتوضيح كالتالي :

المطلب الأول: الأحكام الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.نظم المشرع الجزائري في القانون رقم 04/ 09 المؤرخ في 05 أوت 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، أحكاما جديدة و خاصة بمعالجة الجريمة المعلوماتية تتماشى و التطور الذي الحق بهذه الجريمة، من هذه القواعد ما نص عليه في المادة الثالثة منه التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات و التحقيقات القضائية من ترتيبات تقنية الهدف منها هو :

أ- مراقبة الاتصالات الإلكترونية وتجميعها، حيث نجد أن المشرع الجزائري قد تبني هذا الإجراء رغم ضمانه لسرية المراسلات و الاتصالات بكل أشكالها بنص المادة 39[1] من الدستور الجزائري، نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا كما سنرى لاحقا).

ب- تسجيل الاتصالات الإلكترونية في حينها

ج- القيام بإجراءات التفتيش و الحجز للمنظومة المعلوماتية.

[1] - أنظر المادة :39 من القانون الدستوري.

كما بين هذا القانون (قانون09/04) الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها في مادته الرابعة الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية و ذلك على سبيل الحصر و هذه الحالات هي:

1-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2-في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3-المقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية. ، في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، تنص المادة 16 [1]من القانون 04 / 09 على إمكانية تبادل المساعدات القضائية على المستوى الدولي النجاح عمليات التحقيق و التحريات لمكافحة الجرائم المعلوماتية، غير أن هذه المساعدة يجب أن تتم وفق شروط معينة وهي أن تتم وفقا للاتفاقيات الدولية المبرمة في مجال تبادل المعلومات و تسليم المجرمين أو كل ما هو مرتبط بالجريمة المعلوماتية و أن تخضع لمبدأ المعاملة بالمثل.

كما أن المادة 18 من القانون 04 / 09 السابق الإشارة إليه قد بينت الحالات التي لا تجوز فيها عملية المساعدة القضائية الدولية و حددتها بالحالات التالية:

1- إذا كان فيها مساس بالسيادة الوطنية.

2- إذا كان فيها مساس بالنظام العام.

[1] المادة:16 من القانون 09/04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

وكمثال على المساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية، قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية بومرداس بعد تقديم المكتب الفدرالي الأمريكي للتحقيقات شكوى ضده مفادها أن هذا الشاب قد بعث برسالة إلكترونية لهذا المكتب مهددا فيها بوضع قنبلة في أحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم.[1]

أما المادة الخامسة (5) من القانون رقم 09/04 فهي تبين إجراءات التفتيش للمنظومة المعلوماتية، حيث نجدها تنص على أنه : "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة الرابعة أعلاه الدخول بغرض التفتيش ولو عن بعد إلى :

أ- منظومة معلوماتية أو جزء منه وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية.

والمشرع الجزائري في المادة الخامسة من القانون رقم 09/04 يقصد بالتفتيش في مجال الجرائم المعلوماتية التفتيش المنصوص عليه في قانون الإجراءات الجزائية، و حتى وان اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45[2] من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون 09/04 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب،

[1] قضية منشورة بجريدة الخبر الأحد 10/08/2010 .

[2] - انظر المادة: 45 من ق،إ،ج.

للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.

كما نص المشرع الجزائري ودائما في نفس القانون 04/09على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، و هذا الاجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء و التقنيين المختصين في الإعلام الآلي و فن الحاسبات الإجراء عمليات التفتيش على المنظومة المعلوماتية، و جمع المعطيات المتحصل عليها و الحفاظ عليها و تزويد السلطات المكلفة بالتفتيش بهذه المعلومات .

كما ألزمت المادة 10 من نفس القانون 09/04 و المذكور سابقا مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية و التفتيش و حفظ المعلومات طبقا للمادة 11من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب في مادته 12 على مقدمي الخدمات التزامات خاصة هي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية و تقنية
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام و أن يخبروا المشتركين لديهم بوجودها.[1]

[1] ربيحة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى الجزائر ، طبعة 2011 ،ص 155.

الفرع الأول: الإجراءات الجديدة المنصوص عليها في قانون الإجراءات الجزائية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه تطويقها والقضاء عليها، أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث انه بتعديلي 01/09 ، و 04/14 وضع قواعد و أحكام خاصة لسلطة المتابعة و الاختصاص، الغرض منها هو مواجهتها، و هذه الأحكام هي:

1. جواز تمديد الاختصاص المحلي للمحكمة: حيث نصت المادة 329 من ق اج في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محلكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

2.**توسيع مجال اختصاص النيابة العامة** : حيث انه وبموجب المادة 37 من ق آج تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها بها من قبل حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و جرائم تبييض الأموال والإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف.

3. **العمل بنظام المشروعية في تحريك الدعوى العمومية** : حيث سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، حيث يلتزم وكيل الجمهورية[1] بتحريك الدعوى

[1]- المواد: 144 مكرر144 مكرر 1 و 144 مكرر2 من قانون العقوبات المعدل و المتمم بالقانون 01/09 المؤرخ في 26 يونيو 2001.

العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية و عدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر144 مكرر 1 و 144 مكرر2 من قانون العقوبات المعدل و المتمم بالقانون 01/09 المؤرخ في 26 يونيو 2001 .

4. إضافة لما سبق و دائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات و تسجيل الأصوات والتقاط الصور[1] حسب نص المادة 65 مكرر 5 في إطار تعديل ق إج بالقانون 06/22 المؤرخ في 20/12/2006 التي تنص إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية أن يأذن بما يأتي :

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين، من اجل التقاط و تثبيت وبث تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أملكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون و بغير علم أو رضا الأشخاص

[1] -**أنظر المادة: 65 مكرر 05** في إطار تعديل ق إج بالقانون 06/22 المؤرخ في 20/12/2006

الذين لهم حق على تلك الأماكن. تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص".

5. **التسرب** : إضافة لما سبق تجدر الإشارة إلى الإجراء الجديد الخاص بمكافحة الجرائم المعلوماتية والمنصوص عليه في المادة 65 مكرر11 من قإج ج، و هو إجراء التسرب فتنص المادة 65 مكرر 11 على انه "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكررة أعلاه، يجوز لوكيل الجمهورية أو القاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه"، و هي المواد 65 مكرر12 الى 65 مكرر18 من قانون الإجراءات الجزائية.

وقد عرفت المادة 65 مكرر 12 التسرب على انه "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 لهم أو خاف"[1].

كما سمحت الفقرة الثانية من المادة 65 مكرر 12 أن يستعمل لغرض إجراء التسرب هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65 مكرر 14 و هذه الأفعال هي:

أ- اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

ب- و 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.

[1] - **أنظر** المادة: 65 مكرر 12 من ق،إ،ج.

ويمكن للمتسرب بإتيان هذه الأفعال دون أن تترتب عليه المسؤولية الجزائية لأنه مرخص له بهذه الأفعال بهدف الوصول إلى مرتكبي الجريمة.

وقد بينت المادة 65 مكرر 15 الشروط الواجب توفرها في الإذن بالتسرب، وهي أن يكون مكتوبا ومسببا و أن يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته[1].

كما يجب أن يحدد فيه أي الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65 مكرر 15 كإجراء جديد في مكافحة الجريمة المعلوماتية اعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في إجراءات التحقيق فيها.

الفرع الثاني: إستراتيجية الجزائر في التعامل مع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

تقوم هيئات الدولة الجزائرية المختصة تجاه الجرائم الالكترونية باتخاذ مجموعة من الإجراءات بموجب مقتضيات معينة تتمثل أساسا في حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا لقواعد قانون الإجراءات الجزائية مع وضع ترتيبات لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

تمارس عمليات المراقبة من قبل الجهات المختصة في حالات عديدة أهمها الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، إذ يختص

[1] - **أنظر** المادة: 65 مكرر 15 من ق،إ،ج.

النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته إذن لمدة 6

أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها توضع الترتيبات التقنية وتوجه حصريا لتجميع و تسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على امن الدولة ومكافحتها . في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني أو في حال صعب الوصول إلى نتيجة تهم الأبحاث الجارية متعلقة بمقتضيات التحريات والتحقيقات القضائية و في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة حيث يمكن للسلطات المختصة الجزائرية تبادل المساعدة القضائية في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم وكشف مرتكبيها ولجمع الأدلة الخاصة بالجريمة الالكترونية . تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية بناءا على الاتفاقيات الدولية ذات الصلة و الاتفاقيات الثنائية وحسب مبدأ المعاملة بالمثل بينما يتم رفض طلبات المساعدة الدولية إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام .

يطبق إجراء عمليات المراقبة في هذه الحالات حصرا بموجب إذن مكتوب من السلطة القضائية المختصة.[1]

[1] المواد من 03 إلى 15 من القانون رقم 09-04 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، صادر بالجريدة الرسمية للجمهورية الجزائرية، العدد 47، 16 غشت 2009، ص 06-08.

المطلب الثالث: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:

ولقد تضمن المطلب القوانين الخاصة للتصدي للجرائم الالكترونية وكذا الهياكل الخاصة لهذا النوع من الجرائم ويختتم بالنتائج المحققة في اطار مكافحة الإرهاب الالكتروني.

الفرع الأول: القوانين الخاصة للتصدي للجرائم الإلكترونية

هناك العديد من القوانين التي تصدت لجرائم الإرهاب الالكتروني و ذلك من خلال :

أولا: قانون البريد والاتصالات السلكية واللاسلكية:

باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 منه[1]، كما نصت المادة 84/2 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية"[2]. كما نص في المادة 105منه على إحترام المراسلات[3]. بينما أنت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.[4]

---

[1]المادة :87 من قانون البريد والإتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ في 2000/08/05. على أنه يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني"

[2]أنظر المادة: 84/2 من نفس القانون، تطبق أحكام المادة 80 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية.

[3]أنظر المادة :105 من نفس القانون "لا يمكن في أي حال من الأحوال انتهاك حرمة المراسلات"

[4]أنظر المادة: 127 من نفس القانون،" كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم باختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30. 000 دج إلى 500 . 000 دج ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في

ثانيا: قانون التأمينات:

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي[1]، في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع او من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93 مكرر2.[2]

ثالثا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والإتصال وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية[3]. من مراقبة و تفتيش المنظومات المعلوماتية عند الضرورة،

مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها. ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات"

[1]أنظر المادة:6 مكرر1، والمادة 65 مكرر1 من القانون رقم 01/ 08 المؤرخ في 2008/01/23 والمعدل والمتمم القانون 01/ 83 المتعلق بالتأمينات.

[2]أنظر المادة :93 مكرر2و3 من نفس القانون، دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني المهن الصحة

[3]أنظر المواد: من المادة الثانية حتى 14 من قانون رقم 04-09 المؤرخ في 05/ 08 /2009 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

و حجز المعطيات المعلوماتية، و حفظ. المعطيات المتعلقة بحركة السير على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: الهياكل الخاصة للتصدي للجرائم الإلكترونية .

لقد تم ايجاد العديد من الهياكل الخاصة بهدف التصدي لجرائم الإرهاب الالكتروني وذلك من خلال :

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

وأنشئت بموجب القانون رقم 04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية، في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية الاقتصاد الوطني.[1]

أ- تشكيلة وتنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تعتبر الهيئة لبنة جديدة في إطار مسار الإصلاحات التي تنتهجها الجزائر مؤخرا ذات الطابع القانوني والأمني والسياسي لتعزيز دولة القانون والتأكيد على سيادته في كل الأحوال وإصلاح العدالة،[2] تعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي يوجد مقرها بالجزائر وضعت لدى الوزير المكلف

[1] أنظر القانون: رقم 04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها السابق ذكره.

[2] مقال بعنوان" الجرائم الالكترونية تحت مجهر السلطات"، أخبار الأسبوع، 01-02-2017 الموقع الالكتروني:www.akhbarousboue.com.php

بالعدل تم إنشاؤها بموجب المرسوم الرئاسي الموقع من قبل رئيس الجمهورية رقم 15-261.[1]

ب- المهام الموكلة إلى الهيئة تمارس الهيئة العديد من المهام والمسؤوليات في ظل احترام الأحكام التشريعية تتمثل أساسا في:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

- 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.[2]

- العمل على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها قصد جمع المعلومات المفيدة في

---

[1] نادية سليماني: إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال "، يومية الشروق، 08-10-2015، الموقع الالكتروني: www.echoroukonline.com.html

[2] مقال بعنوان" إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، الأربعاء 14 ديسمبر 2016، وكالة الأنباء الجزائرية، على الموقع الالكتروني: www.aps.dz/sante.science

التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[1]

– 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.[2]

ج– تشكيلة الهيئة وتنظيمها:

تضم الهيئة من حيث تشكيلتها لجنة مديرة، مديرية عامة، مديرية للمراقبة الوقائية واليقظة الالكترونية مديرية التنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية.

1– اللجنة المديرة:

يرأس اللجنة الوزير المكلف بالعدل تتشكل من الأعضاء التالية الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا.

[1] انظر المادة 14 من القانون رقم 09–04 المؤرخ في 5 اغسطس 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق، ص 08.

[2] انظر المواد 2 و 3 من 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، ص 16–17.

تمارس اللجنة المديرة وتكلف بالقيام بالمهام التالية توجيه عمل الهيئة والإشراف عليه ومراقبته بالإضافة لدراسة كل مسالة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر اللجوء للمراقبة الوقائية للاتصالات الالكترونية و ضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه. قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة كما تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ناهيك عن دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه دون إغفال دراستها التقرير السنوي لنشاطات الهيئة والمصادقة عليه وإبداء رأيها في كل مسالة تتصل بمهام الهيئة مع تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة.[1]

2- المديرية العامة:

يتولى إدارتها مدير عام يعين بموجب مرسوم رئاسي وتنهي مهامه بنفس الطريقة حيث يمتلك المدير العام العديد من الصلاحيات حتى يتمكن من القيام بمهامه على أكمل وجه تتمثل أهمها في العمل على حسن سير الهيئة الوطنية عن طريق ضمان تنفيذ برنامج عملها وتنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها وقيامه بتحضير اجتماعات اللجنة المديرة، بالإضافة لقيامه بتمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية ولدى القضاء وفي جميع أعمال الحياة المدنية ناهيك عن ممارسة السلطة السلمية على مستخدمي الهيئة والعمل على احترام قواعد حماية السر في الهيئة والقيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة مع إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه كما يعمل على ضمان التسيير الإداري و المالي للهيئة.

[1] انظر المادة :06 من المرسوم الرئاسي رقم 15-261، مرجع سابق، ص 17

3- مديرية المراقبة والوقاية واليقظة الالكترونية:

يتم تعيين مديرها بموجب مرسوم رئاسي موقع من رئيس الجمهورية كما يتم إنهاء مهامه بموجب نفس الطريقة. تتكفل مديرية المراقبة بالقيام بالعديد من المهام لضمان فعالية الهيئة نذكر منها على وجه الخصوص القيام بتنفيذ عمليات المراقبة والوقاية للاتصالات الالكترونية من اجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بناءا على رخصة مكتوبة تمنح من السلطة القضائية وتتم تحت مراقبتها، و إرسال المعلومات المحصل عليها من خلال القيام بالمراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة بالإضافة لتنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخلات الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و التعرف عليهم.

تتولى أيضا مهمة جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والعمل على تنظيم أو المشاركة في عمليات التوعية حول كيفية استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها ناهيك عن تنفيذ التوجيهات المقدمة إليها من قبل اللجنة المديرة وتزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناءا على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيره والحفاظ على الحالة الجيدة لمنشاته وتجهيزاته ووسائله التقنية مع ضرورة تطبيق قواعد الحفاظ على السر في نشاطاتها الممارسة.[1]

[1] أنظر المواد: 9- 18 من المرسوم الرئاسي رقم 15-261، مرجع سابق، ص 17-18.

4- مديرية التنسيق التقني:

يتم تعيين مدير المديرية وإنهاء مهامه بموجب مرسوم رئاسي صادر عن رئيس الجمهورية، تتولى بدورها مهام عديدة لكفالة أداء الهيئة بكافة فروعها وأجهزتها واجباتها وتحقيق الغرض من إنشائها حيث تتولى المديرية ممارسة المهام المتمثلة في انجاز الخبرات القضائية في مجال اختصاص الهيئة وتكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها و إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالإضافة للقيام بمبادرة منها أو بناءا على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها .

5- مركز العمليات التقنية:

يتم تزويده بالمنشآت والتجهيزات والوسائل المادية وبالمستخدمين التقنيين الضروريين لتنفيذ العمليات التقنية لمراقبة الاتصالات الالكترونية يتبع المركز مديرية المراقبة الوقائية واليقظة الإلكترونية حيث يتم تشغيله من طرفها.

6- الملحقات الجهوية يتم تشغيلها من طرف مديرية المراقبة والوقاية واليقظة الالكترونية التي تكون تابعة لها

د - كيفية سير وممارسة الهيئة لمهامها ومساهمتها في تقليص الإجرام الالكتروني عامة والإرهاب الالكتروني بالخصوص:

تجتمع الهيئة بناءا على استدعاء من رئيسها أو بناءا على طلب أحد أعضائها إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه حيث يتم تزويدها بقضاة وضباط وأعوان الشرطة 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.

في إطار الوقاية من الأفعال الموصوفة بجرائم الإرهاب او 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.

يتم 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]

[1] انظر المواد: من 19- 26 من المرسوم الرئاسي 15-261، مرجع سابق، ص 19-20

في 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 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 المراقبة الاتصالات الالكترونية إلا الهيئة أو عند الاقتضاء سلطة ضبط الاتصالات السلكية واللاسلكية أو المؤسسة العمومية المكلفة بشبكات الاتصالات.[1]

ثانيا: الهيئات القضائية الجزائية المتخصصة

أنشئت بموجب القانون 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37،329، و40 من ق. إ. ج. تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذيرقم06/384المؤرخ في 2006/01/05. بحيث تنظر في القضايا المتصلة بتكنولوجيا

[1] انظر المواد :من 30-32 من المرسوم الرئاسي رقم 15-261، مرجع سابق، ص 20.

الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 04/09.[1]

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الجرائم.

يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية،ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.[2]

رابعا: المديرية العامة للأمن الوطني

تتصدى هده المديرية للجريمة الإلكترونية من عدة جوانب أو منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL هاته الأخيرة تتيح مجالات للتبادل ألمعلوماتي الدولي وتسهل الإجراءات

[1] هواري عياش: مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية المعهد الوطني للأدلة الجنائية وعلم الإجرام ، جامعة بسكرة كلية الحقوق،2016، ص3.

[2] حملاوي عبد الرحمان: مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة بسكرة كلية الحقوق، 2016، ص

القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.[1]

في خاتمة هذا العمل المتواضع، والذي لا أعتبره بحثا معمقا، وإنما محاولة للإلمام بالموضوع وما يطرحه من إشكالات عديدة ومبادئ جديدة القد توصلنا إلى نتائج جد هامة كما قدمنا بعض الاقتراحات التي رأيناها مفيدة الموضوع الدراسة.

الفرع الثالث: النتائج المحققة في إطار مكافحة الإرهاب الالكتروني:

تمكنت 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]

هذا 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

---

[1] علي عبد القادر القهوجي:الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية للطباعة والنشر، بيروت، 1999،ص 120 .

[2] مقال بعنوان:" الجزائر تبحث تحصين مؤسساتها من هجمات الإرهاب الإلكتروني"، جريدة البلاد، 2017-01-25، على الموقع: www.elbilad.nd/article65620

[3] مقال بعنوان:" إيداع ملفات 58 شخص لدى العدالة لتورطهم في قضايا الإرهاب الالكتروني"، 2016-24- 07، يومية الفجر، على الموقع: 339439www.alfajr.com/

المتبادلة وما يزيد عن خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة **الفيس بوك والتويتر** لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب اتصالات محلية و دولية.[1]

عدم وجود تعاون دولي، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين ولكن النتيجة تحدث في بلد أخر ليس بالضرورة أن ينتج هذا السلوك أثاره في بلد المجرمين.

[1] مقال بعنوان:" الجيش الالكتروني يوقف 160 داعشيا في الجزائر"، 25-12-2016، أخبار اليوم، على الموقع الالكتروني: www.akhbarelyoum.com

يتجلى لنا من خلال دراستنا للسياسة الجنائية لمكافحة الإرهاب الإلكتروني في التشريع الجزائري إن هذه السياسة تنصب على معالجة أكثر الجرائم التي عرفها العالم الحديث خطورة ، وذلك لما يتسم به هذا الجرم من اختلاف عن الجرائم المعروفة في العالم التقليدي ، فبالإضافة إلى التحديات التي فرضتها على الجهات الخاصة بوضع قوانين و إنفاذها ، وإذا كنا قد تناولنا جريمة الإرهاب الإلكتروني ، فإننا قد تناولنا مشكلة من المشكلات التي أفرزتها ثورة الاتصالات ، فهذه الثورة كما نعلم على قدر ما قدمته من تسهيلات للأفراد والمجتمعات على حد سواء فقد زعزعت سكينتهم بهذا النوع الجديد من الجرائم التي تتميز بطبيعة فنية وعلمية معقدة فقد غير الإرهاب الإلكتروني النظرة التقليدية التي كان ينظر بها إلى الجريمة على العموم فهذا النوع من الإجرام ظهر معه مفهوم جديد لهذه الظاهرة لم يكن يعرفه القانون من قبل ، فإذا كانت الجريمة التقليدية قد حضيت بمختلف الأطر القانونية من اجل تحديد مفهومها وطبيعتها فإن جريمة الإرهاب الالكتروني لم تنل هذا القدر من التقنين ، حيث أن هذه الجريمة اتسمت بخصوصية ميزتها عن الجرائم التقليدية .

ويمكن لنا آن نوجز ما تضمنته الدراسة من نتائج منبثقة عن الإشكاليات المطروحة في تحديد ماهية الإرهاب الالكتروني وكذا آليات مكافحته فيما يلي:

- صعوبة إيجاد تعريف موحد لجريمة الإرهاب الالكتروني فقد تعددت التعريفات واختلفت في وصف الظاهرة الإجرامية المستحدثة فمنها من ارتكز على موضوع الجريمة ومنها من ذهب إلى ضرورة معرفة المجرم بمختلف الطرق التي يتم ارتكاب الجريمة من خلالها أساسا لتعريفها ، في حين ذهب جانب أخر إلى تعريفها على أساس الوسيلة المرتكبة بواسطتها ، غير ان كل هذه التعريفات لم تف بالغرض نظرا لعدم إلمامها بمختلف جوانب الجريمة .
- إن التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب ولايمكن تصور فكرة التخلي عنها ، نظرا لتزايد مجالات استعمالها في كافة المجالات ، وذلك بالرغم من كافة التهديدات التي تشكلها الجريمة الإرهاب الالكتروني على امن وسلامة نظمها ومستعمليها .
- يستحيل القضاء على الظاهرة الإرهابية الالكترونية بشكل نهائي، وذلك لاتصالها المباشر بتقنية المعلوماتية، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة المعلوماتية، وذلك بالرغم من درجة التطور التي ألت إليها المنظومة القانونية العقابية منها والإجرائية في مجال مكافحة الجريمة المعلوماتية .

- تنامي ظاهرة الإرهاب الالكتروني والنشاط الإجرامي المنظم، فقد أصبحت الجماعات الإجرامية والإرهابية تستغل شبكة الانترنت لأجل حصد موارد ونشر أفكارها واستغلال كل ذلك في ترهيب وترويع الشعوب والحكومات.
- تصنيف الجرائم المعلوماتية في صور التجنيد للقتال من بين اخطر الجرائم نظرا لقلة حيلة وضعف الضحايا في هذه الحالة لما قد تتسبب فيه من قيام نزعات بين الشعوب.
- على المستوى القانوني فالمشرع الجزائري يحاول مسايرة التطورات وذلك من خلال تعديل قانون العقوبات سنة 2016 لاسيما النصوص التي استحدثها والتي تتجلى في المواد 87 مكرر 11و87 مكرر12 وكذلك في القانون 09-04 وقانون حماية المعطيات الشخصية سنة 2018 بالإضافة إلى إقامة العديد من الملتقيات حول الأمن ألمعلوماتي وسياسات الدفاع الالكتروني.
- يقترن نجاح إجراءات البحث والتحقيق في الجرائم المعلوماتية بمدى براعة وفعالية وجاهزية الجهات المختصة بمباشرة الإجراءات لتتبع الأدلة الالكترونية ، وتحصيلها وحفظها بغرض عرضها على الجهات المختصة بتقديرها ، ذلل كان الدليل الالكتروني هو دليل جنائي من نوع خاص لا يشترك مع باقي الأدلة الجنائية في أي صفة مميزة ، فهو ذو طبيعة رقمية غير مادية ، كما انه قابل للفقدان من خلال تدميره أو محوه بكل سهولة ومن أي مكان ، من قبل الإرهابي الالكتروني او حتى من قبل المحققين ذاتهم خطا منهم او تقصيرا في التعامل بالقواعد الاحتياطية مع الأدلة الالكترونية .
- ضعف المنظومة التشريعية في مواجهة الجريمة الإرهابية الالكترونية ، م خلال عدم توفر المناخ القانوني الملائم ، سواء من ناحية النص ألتجريمي أو الإجرائي ، وهو ما يتسبب في خلق فجوات قانونية هائلة بين مجالي الجريمة الإرهابية والتشريع ، وهو ما يعرقل خطة مكافحة جريمة الإرهاب الالكتروني بما فيها من خاصة بالبحث والتحقيق في هذا المجال ، نظرا لافتقار الجهات المختصة بالبحث والتحقيق في مجال الجرائم المعلوماتية للسند القانوني .
- ضعف القدرات الأدائية للجهات المختصة بالبحث والتحقيق في الجرائم المعلوماتية ، إما لعدم تخصص أفرادها بمجال المعلوماتية واعتمادهم على الطرق التقليدية لحل القضايا الإجرامية في التعامل مع الجريمة المعلوماتية ، مما يتسبب في فقدان الأدلة الالكترونية والقضاء على معالم الجريمة ، او العكس من ذلك اي تغليبهم للجانب الفني على القانوني ما يجعل من الإجراءات المتخذة والأدلة المحصلة باطلة من الناحية القانونية ، او قد يكون السبب ماديا بحتا من خلال عدم توفر الوسائل المادية الضرورية ممثلة في الحواسيب المتطورة والمزودة بأحدث البرامج في مجال ترصد وتتبع مجرمي الجرائم المعلوماتية .

وعليه وبناءا على كل ما استعرضناه جاز لنا وضع والتنويه بمجموعة **من الاقتراحات** التي تساهم في حل الإشكاليات والعوائق التي صادفتنا في مجال البحث، والتي نوجزها فيما يلي:

- العمل على التحسيس بخطورة الجريمة المعلوماتية على الأمن العام ، وامن الإفراد من خلال إدراج مفهوم الجريمة المعلوماتية الإرهابية ضمن القرارات الدراسية وخصوصا منها الجامعية ، في مجال الحقوق والمعلوماتية ، وكذلك من خلال تنظيم أيام دراسية وتحسيسية لفائدة موظفي الشركات والمؤسسات خصوصا المالية منها ، من اجل وضعهم امام واقع الجريمة الإرهابية الالكترونية ، باعتبارها خطرا يهدد امن وسلامة النظم المعلوماتية لهذا النوع من المؤسسات بالدرجة الأولى ، باعتبار أن الغرض الرئيس لمجرمي المعلوماتية هو الترويع وتدمير البنية التحتية المعلوماتية.
- ضرورة تحسيس ضحايا الجرائم من التجنيد او نشر الفكر المتطرف بضرورة التبليغ عن أي جريمة معلوماتية قد يقعون ضحايا لها ، وذلك من اجل السماح للجهات المكلفة بالبحث والتحقيق بالاطلاع على مدى جسامة وحقيقة الجريمة ، إضافة إلى الإطلاع على كافة الأساليب الإجرامية الحديثة المستعملة في هذا النوع من الجرائم ، والتي يمكن أن تبقى محل عدم تبليغ الضحايا عن الجرائم المعلوماتية التي تستهدفهم .

على المستوى التشريعي :

- دعوة السلطات العليا إلى ضرورة الانضمام إلى المعاهدات الدولية لمكافحة الجرائم المعلوماتية ، وذلك باعتبارها اتفاقيات مفتوحة للتوقيع والتصديق من قبل كافة الدول ، وذلك حتى نستفيد من جملة الجهود التشريعية الدولية في مجال أعمال البحث والتحقيق في الجرائم المعلوماتية الإرهابية .
- يجب على وجه الاستعجال استحداث نصوص قانونية متلائمة ومستوى التطور الذي ألت إليه تقنية المعلوماتية، ودرجة خطورة الجرائم المعلوماتية الإرهابية ، وذلك أولا على مستوى قانون العقوبات الجزائري فالنصوص الواردة فيه غير متكاملة وغير مضبوطة المصطلحات ، فنجد أن الأسلوب الغالب عليها هو أسلوب العمومية وعدم الدقة في تفصيل النص بذاتها وأركانها إضافة إلى تشديد العقوبات في هذا المجال من أجل إحداث الأثر الوقائي والردعي المرجو من إقرار قانون العقوبات .
- تعديل قانون الإجراءات الجزائية على وجه الاستعجال من خلال إدراج قسم خاص بأعمال البحث والتحقيق في الجرائم المعلوماتية وذلك من خلال إفراد نصوص قانونية خاصة بأعمال البحث والتحقيق في الجرائم المعلوماتية ، وذلك من خلال إفراد نصوص قانونية

- خاصة بالإجراءات الجزائية المتبعة خلال مرحلة البحث والتحري وكذلك التحقيق بشكل مفصل وواضح ، بين قواعد الاختصاص النوعي والمحلي بدقة ووضوح ، إضافة إلى طبيعة الإجراءات المتخذة في هذا الشأن ، وذلك للقضاء على كل لبس قد ينشا جراء المزج بين النصوص العامة والخاصة وذلك تجسيدا للطبيعة الخاصة للجريمة الإرهابية الالكترونية بمفهومها الخاص ، ضمن فصول وأحكام القانون الإجرائي .
- تعزيز عمل الجهات الأمنية والقضائية في مجال مكافحة الجرائم المعلوماتية ، وذلك من خلال حسن تدريب الكفاءات العاملة على طبيعة الإجراءات المتخذة في مجال الجرائم الالكترونية الإرهابية ومدى خصوصية هذا النوع من الجرائم والمجرمين في أن واحد ، إضافة إلى تعزيزيهم بأحدث وسائل التكنولوجية في مجال المعلوماتية من حواسيب وبرامج معلوماتية ، تسمح لهم بتأدية مهامهم على أكمل وجه.
- وضع سجل امني إلكتروني يتضمن قائمة بمجرمي المعلوماتية يسمح بوضعهم تحت المراقبة الأمنية ، أي رصد نشاطاتهم المعلوماتية المشبوهة عبر الشبكة ، والتي تنذر بوقوع جريمة إرهابية إلكترونية .

إذن كانت هذه جملة من التوصيات والمقترحات التي يرى الباحث بضرورة تبينيها و تجيدها على ارض الواقع من اجل الوصول إلى ضمان فعالية قصوى في عمل الجهات المختصة بالبحث والتحقيق في الجرائم المعلوماتية ، وبالتالي تجسيد السياسة الحنائية المثلى لمكافحة الإرهاب الالكتروني .

محتويـــات البحث	رقم الصفحة
– مقدمـــــــــــــــة	06-02
- الفصل الأول:الإطار ألمفاهيمي للإرهاب الالكتروني	08
- المبحـــث الأول: تعريف الإرهاب	08
- المطلب الأول: تعريف الإرهاب لغة واصطلاحا.	08
- الفرع الأول:الإرهاب في اللغة.	08
- الفرع الثاني:الإرهاب في الاصطلاح	09-08
- المطلب الثاني: تعريف الإرهـاب الإلكتروني.	12-10
- الفرع الأول: تاريخ الإرهـاب.	14-12
- الفرع الثاني:أنــواع الإرهاب.	14
- المطلب الثالث: وسائل الإرهاب الالكتروني.	15
- الفرع الأول:البريد الإلكتروني.	15
- الفرع الثاني :إنشاء مواقع على الإنترنت.	15
- الفرع الثالث:اختراق المواقع..	16
- المبحث الثاني: الجريمة الالكترونية	17
- المطلب الأول: تعريف الجريمة الإلكترونية	19-17
- الفرع الأول:خصائص الجريمة الالكترونية	19
- الفرع الثاني:مميزات الجريمة الالكترونية	21-20
- الفرع الثالث:أنواع الجريمة الالكترونية.	22-21
- المطلب الثاني:الأسباب الدافعة لارتكاب الجريمة وأهداف المجرم منها...	23
- الفرع الأول: الأسباب الدافعة لارتكاب الجريمة الإلكترونية	23
- الفرع الثاني: أهداف المجرم الالكتروني	24-23
- الفرع الثالث: صعوبة إثبات الجريمة الالكترونية كونها عابرة للحدود	27-24
- المبحث الثالث:الإرهاب وصفحات التواصل الاجتماعي	28
- المطلب الأول:مواقع التواصل الاجتماعية	31-29

- **الفرع الأول**:ميزات الشبكات الاجتماعية	**31**
- **الفرع الثاني**:أنواع شبكات التواصل الاجتماعي	**36-32**
- **المطلب الثاني: التجنيد عبر شبكات التواصل**	**38-36**
- **الفرع الأول**: مدلول عملية تجنيد الشباب عبر الانترنت	**38**
- **الفرع الثاني**:الانترنت كبيئة لتجنيد الشباب	**41-39**
- **الفرع الثالث**: فئة الشباب المستهدف بالتجنيد	**42-41**
- **الفصل الثاني:آليات مكافحة الإرهاب الالكتروني في التشريع الجزائري**	**44**
- **المبحث الأول: الآليات الموضوعية لمكافحة الإرهاب الالكتروني.**	**44**
- **المطلب الأول: التجريم.**	**44**
- **الفرع الأول**:أركان جريمة الإرهاب الالكتروني	**45-44**
- **الفرع الثاني**:النصوص التقليدية والمستحدثة لتجريم الإرهاب الالكتروني.	**49-45**
- **المطلب الثاني: العقوبات المقررة لجرائم الإرهاب الالكتروني.**	**49**
- **الفرع الأول**:العقوبات المقررة على الشخص الطبيعي.	**54-49**
- **الفرع الثاني**: العقوبات المطبقة على الشخص المعنوي.	**55-54**
- **المبحث الثاني: الآليات الإجرائية لمكافحة الإرهاب الالكتروني.**	**55**
- **المطلب الأول:مرحلة البحث والتحري.**	**56-55**
- **الفرع الأول**:الإجراءات العادية	**57-56**
- **الفرع الثاني** :الإجراءات الاستثنائية	**57**
- **المطلب الثاني:أساليب التحري الخاصة**	**57**
- **الفرع الأول**:تعريفها	**58-57**
- **الفرع الثاني**: الأجهزة المختصة بالبحث والتحري الالكتروني	**60-59**
- **المطلب الثالث:الإجراءات الخاصة بالبحث والتحري الالكتروني**	**61**
- **الفرع الأول**:التفتيش	**63-61**
- **الفرع الثاني**: الحجز الالكتروني	**66-63**
- **الفرع الثالث**:الاختصاصات الاستثنائية لضباط الشرطة القضائية	**66**
- **المبحث الثالث: الآليات الإجرائية في ظل القانون 04/09.**	**67**
- **المطلب الأول: الأحكام الخاصة بالوقاية من جرائم الإعلام و الاتصال.**	**71-67**

- **الفرع الأول**: الإجراءات الجديدة في قانون الإجراءات الجزائية	**74-71**
- **الفرع الثاني**: إستراتيجية الجزائر في التعامل مع جرائم الإعلام والاتصال.	**75-74**
- **المطلب الثاني: القوانين والهياكل الخاصة للتصدي للجرائم الإرهاب الإلكترونية**	**76**
- **الفرع الأول**: القوانين الخاصة للتصدي للجرائم الإرهاب الإلكترونية	**78-76**
- **الفرع الثاني**: الهياكل الخاصة للتصدي للجرائم الإرهاب الإلكترونية	**87-78**
- **الفرع الثالث**: النتائج المحققة في إطار مكافحة الإرهاب الالكتروني	**88-87**
- **الخاتمة**	**93-90**
- **قائمة المراجع**	**101-95**
- **الفهرس**	**105-103**

قائمة المراجع.

أولا :النصوص القانونية .

01 – الجـــريدة الرسمية للجمهوريـــة الجزائريـــة، العدد 47 المؤرخ في: 16 غشت 2009.

02- الجريدة الرسميـــة للجمهورية الجزائريـــــة العدد 53 المـــــؤرخ في: 8 أكتوبر 2015.

03- القانون رقم 04-09 المؤرخ في 05/ 08 /2009 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

04- قانـون العقوبات المعدل و المتمم بالقانـــون 01/09 المـــؤرخ في 26 يونيو 2001.

05- قانـون الإجراءات الجزائيـــة المعـــدل بالقانون 06/22 المؤرخ في 20/12/2006 .

06- قانون البريد والاتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ في: 2000/08/05.

07- القانون رقم 01/ 08 المؤرخ في 2008/01/23 والمعدل والمتمم القانون 01/ 83 المتعلق بالتأمينات.

08- 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.

ثانيا:الكتـــب.

01- ابن فارس: مجمل اللغة لابن فارس، مؤسسة الرسالـــــــة، بيروت، الطبعة2، 1989.

02- أحسن بوسقيعة :الوجيز في القانون الجزائي العام ،الطبعة الأولى 2002 ،الديوان الوطني للأشغال التربوية .

03- حسن محمد ربيع : شرح قانون العقوبات القسم العام ، دار النهضة العربية القاهرة 2008 .

04- ربيحة زيدان: الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى الجزائر ، طبعة 2011.

05- رستم، هشام محمد فريد : الجوانب الإجرائية للجرائم المعلوماتية ، دراسة مقارنة ، أسيوط، مصر، مكتبة الآلات الحديثة 1994.
06- سايمو نكولن :التجارة على الإنترنت، ، نقله إلى العربية يحيى مصلح، بيت الأفكار الدولية بأمريكا 1999م.
07- سامي عبد الكريم محمود: الجزاء الجنائي، منشورات الحلبي الحقوقية، الطبعة الأولى، لبنان 2010.
08- علي حسين الخلف و.سلطان عبد القادر الشاوي : المبادئ العامة في قانون العقوبات ،بيروت2012.
09- عبد الفتاح بيومي: مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي.
10- عبد الفتاح بيومي حجازي،: الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر 2002 .
11- عبد الرحمان بيومي حجازي : الجريمة في عصر العولمة ، دار الفكر الجامعي ، الطبعة الأولى، الإسكندرية 2008 .
12- علي عبد القادر القهوجي : قانون العقوبات (القسم العلم)،الكتاب الثاني (المسؤولية الجنائية والجزاء الجزائي) ،دار المطبوعات الجامعية ، الإسكندرية 1998.
13- علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية للطباعة والنشر، 1999، بيروت.
14- عبد الرحمان خلفي : المسؤولية الجزائية للأشخاص المعنوية عن جرائم تبيض الأموال (دراسة في التشريع الجزائري مع الإشارة الى الفقه والتشريع المقارن) عدد2011/02 كلية الحقوق والعلوم السياسية جامعة عبد الرحمان ميرة ، بجاية ، الجزائر.
15- عبد الرحمان خلفي : الإجراءات الجزائية في التشريع الجزائري والمقارن ، دار بلقيس للنشر ، الجزائر 2015.
16-عودة عبد القادر: التشريع الجنائي الإسلامي، مؤسسة الهالة، بيروت.
17- لحسين بن شيخ ، مبادئ القانون الجزائي العلم (النظرية العامة للجريمة) ،دار هومة للطباعة والنشر والتوزيع ،الجزائر 2004.
18- لخميسي عثمانية: السياسة العقابية في الجزائر على ضوء المواثيق الدولية لحقوق الإنسان،دار هومة للطباعة والنشر والتوزيع الجزائر 2012.

19- محمد عبد المطلب: تعريف الإرهاب الدولي بين الاعتبارات السياسية والاعتبارات الموضوعية، دار الجامعة الجديدة، الإسكندرية،طبعة 2007، مصر.

20- محمد السيد اليماني: الجوانب القانونية لدور براءة الاختراع في نقل التكنولوجيا، دون طبعة.

21- محسن شفيق: نقل التكنولوجيا من الناحية القانونية، جامعة القاهرة ،طبعة 1984م .

22- **منصور رحماني:** الوجيز في القانون الجنائي العام ، دار العلوم للنشر والتوزيع عنابة ،**طبعة** .

23- وليد محمد حجاج: شرح قانون العقوبات القسم العام كلية الحقوق جامعة أسيوط 2006.

24- وليد محمد أبو رية:التعرف على الإرهاب الإلكتروني ، جامعة نايف العربية للعلوم الأمنية ، مركز الدراسات والبحوث ، **الطبعة الأولى** 2012، المملكة العربية السعودية .

25- هلال بن محمد: الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دراسة قانونية وفنية مقارنة ،دار النهضة العربية، 2009 مصر.

ثالثا:الرسائل والمذكرات.

أ-رسائل الدكتوراه.

01- **الداودي مجرب:** الأساليب الخاصة للبحث والتحري في الجريمة المنظمة ، رسالة دكتوراه ، كلية الحقوق ، جامعة الجزائر 1بن يوسف بن خدة.

02- سليمان غازي **و** بخيت المقيطي العتيبي :**،دور البحث الجنائي في الكشف على** الجرائم المعلوماتية (دراسة تطبيقية على شرطة منطقة مكة المكرمة)، **رسالة دكتوراه،** كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية ، 2016،الرياض.

03- لمقدم حمر العين:**الدور الإصلاحي للجزاء الجنائي ، رسالة دكتوراه في القانون** الخاص،كلية الحقوق والعلوم السياسية ،جامعة **أبو** بكر بلقايد ، 2014،2015، **تلمســـان.**

ب- رسائل الماجستير.

01- احميدي بوجليطية بوعلي :سياسة مكافحة الإرهاب في الوطن العربي ، دراسة مقارنة بين الجزائر ومصر ، رسالة ماجستير ،كلية العلوم السياسية والإعلام ، جامعة دالي إبراهيم ، الجزائر 2 السنة الجامعية 2009-2010 .

02- احمد مسعود مريم : آليات مكافحة جرائم تكنولوجيا الأعلام والاتصال في ظل القانون 04/09، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، 2009.
03- احمد فتحي سرور :، الوسيط في قانون الإجراءات الجنائية ، دار النهضة العربية ، القاهرة ومتعب هلال لعتيبي ،المسؤولية الجنائية عن جريمة غسل الأموال الرقمية في المملكة العربية السعودية ، رسالة الماجستير ، كلية الدراسات ، قسم العدالة الجنائية ، جامعة نايف العربية للعلوم الإنسانية الرياض 1980.
04- مفيدة ضيف: سياسة المشرع في مواجهة ظاهرة الإرهاب ، رسالة ماجستير تخصص قانون العقوبات والعلوم الجنائية ، كلية الحقوق والعلوم السياسية، جامعة الأخوة منتوري ، قسنطينة ، السنة الجامعية 2009-2010، ص140،138
05- نعيم سعيداني : آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ،2013/2012.

خامسا: المقـــــالات

01- وولترلاكير ، دراسات الإرهاب ،مقال منشور على موقع مرافئ .

www.marafea.org

02- سهير حجازي : التهديدات الإجرامية للتجارة الإلكترونية ، مركز البحوث والدراسات ، شرطة دبي ، دولة الإمارات العربية المتحدة ، العدد91.

03- تعريف خبراء منظمة التعاون الاقتصادي والتنمية وتم مناقشة هذا التعريف في اجتماع المنظمة بباريس عام 1983.

04- نورة بنداري عبد الحميد فايد : دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية "دراسة حالة داعش"، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية ،

05-فهد بن ناصر العبود: الشبكات الاجتماعية على الانترنت، ،مقال منشور في جريدة الرياض بتاريخ 30/يناير 2010 العدد 15195.

06-اماني إبراهيم :شعوب أون لاين، مقال منشور بتاريخ 2010/12/26 ، وكالة أنباء ONA.

07-خالد عباس طلشكندي : الشبكة المظلمة DEPP WEP ، المقال المتاح على موقع السكينة الالكتروني .

08-أدوات التخفي الرقمية حياة لداعش ، مقال متاح على موقع " جريدة المدن " الإلكتروني ، تاريخ الاطلاع 2019/04/30 بتوقيت 12:54 .اظر الرابط : WWW.ALMODON .COM/MEDIA

09-التنظيمات الإرهابية تصطاد المراهقين والمحطمين نفسيا ، مقال متاح على موقع " صحيفة المدينة " الالكتروني ، بتاريخ 2017/10/24 تاريخ الاطلاع 2019/04/30 بتوقيت 01:20 أظر الرابط WWW.AL MADN.COM /ARTICLE /40972

10-زينب القرشي : تجنيد داعش للمثقفين والعلماء كارثة تهدد بقاء البشرية ، مقال متاح على موقع "الوفد" الالكتروني ، القاهرة ، تاريخ الاطلاع :2019/04/30 بتوقيت 14:30.

11-مقال بعنوان" الجرائم الالكترونية تحت مجهر السلطات"، أخبار الأسبوع، 01-02-2017 الموقع الالكتروني:www.akhbarousboue.com.php

12-مقال بعنوان" إبراز دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال في تعزيز دور القانون"، الأربعاء 14 ديسمبر 2016، وكالة الأنباء الجزائرية، على الموقع الالكتروني: www.aps.dz/sante.science

13- مقال بعنوان" الجزائر تبحث تحصين مؤسساتها من هجمات الإرهاب الإلكتروني"، جريدة البلاد، 25-01-2017، على الموقع: www.elbilad.nd/article65620

14-مقال بعنوان" إيداع ملفات 58 شخص لدى العدالة لتورطهم في قضايا الإرهاب الالكتروني"، 07، يومية الفجر، على الموقع: 339439www.alfajr.com/

15- مقال بعنوان" الجيش الالكتروني يوقف 160 داعشي في الجزائر"، 25-12-2016 ، أخبار اليوم، على الموقع الالكتروني: www.akhbarelyoum.com

رابعا: المواقع الالكترونية .

01- الإرهاب الدولي، دراسة فقهية تحليلية، بقلم أ. د. علي محيى الدين القره داغي ، الحلقة 3 تعريف معاهدة منظمة المؤتمر الإسلامي للإرهاب، موقع الاتحاد العام للعلماء المسلمين.

-http://www.mokarabat.com .

02- موقع السياسة الدولية، دور المجتمع الدولي في مكافحة الإرهاب، مفيد شهاب.

-http://www.siyassa.org.eg

03- الاتحاد الدولي في مواجهة الإرهاب -http://arabic. euronews.com

04- الإرهاب الإلكتروني في عصر المعلومات، عبد الله بن عبد العزيز بن فهد العجلان، بحث منشور.

-http://icacc.ccis-imsiu.edu.sa.

05-حنا عيسى، الإرهاب تاريخه وانواعة وأسبابه.

-http://www.abouna.org visite le 04/05/2019

06-وسائل الإرهاب الالكتروني، المكتبة الشاملة.

- http://shamela.ws visite le 04/05/2019

01- التقنيات وأساليب مكافحة الإرهاب ، د .احمد سعد جوهر ، جامعة نايف ، المملكة العربية السعودية ، دورة تدريبية.

- visite le 09/05/2019 à09h :30

- 08 -http://www.mokarabat.com

09- -http://www.assakina.com

10 - -www.marefa.org visite le 08/05/2019 à14h

11- ويكيبيديا الموسوعة الحرة.

12- موقع الاتحاد -www.alithad.com

13 - -www.businessinsider.com

14- -www.csoonline.com

15- -http://www.alhurra.com

16- معجم المعاني الجامع الإلكتروني، أظر الرابط: جند
- www.almaany.com/ar/dict/ar-ar/

17- نادية سليماني، إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال .
- www.echoroukonline.com.html

سادسا:وثائق الأمم المتحدة .

01- لطيفة الشملان :تدابير منع الشباب من قبل الجماعات الإرهابية العالمية ، تقرير مقدم للجنة الإقليمية الخاصة بمنطقة الشرق الأوسط وشمال إفريقيا تاريخ الاطلاع 2019/04/21 .بتوقيت 22:45 .

02- محمد محي الدين عوض: مشكلات السياسة الجنائية المعاصرة جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 1993.

فهرس المحتويات

مبحث تمهيدي

مقدمة

الفصل الأول

الفصل الثاني

ملخص الدراسة

خاتمة

قائمة المصادر والمراجع