جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

جـامـعة عبد الرحـمان ميـرة- بجاية
كلية الحقوق والعلوم السيـاسية
قـسم القانون الخاص

جـريـمـة الإرهــاب الإلــكـتـرونــي: دراســة تحلـيـليـة في ضوء القانـون الجـزائـري

مذكرة لنيل شهادة الـماستر في القـانون الخـاص
التخصص: القانون الجنائي والعلوم الجنائية

. من إعداد الطالبة:
بوقاسم سالـمه

. تحت إشراف الأستاذة، الدكتورة:
هارون نورة

أعضاء لجنة المناقشة

الأستاذ: خلفي أمين.....رئيسا

الأستاذة. الدكتورة: هارون نورة .....مشرفا ومقررا

الأستاذ: فريحة كمال.....ممتحنا

السنة الجامعية: 2025/2024.

بِـسْمِ اللهِ الـرَّحـمَـانْ الـرَّحْـيـمِ

شُكر وتقدير

تقديرًا للعطاء، واعترافًا بالجميل، أفتتح هذه الصفحة بكلمات امتنان صادقة، تعبّر عن عرفان راسخ لكل من كان سندًا حقيقيًا في رحاب هذا العمل العلمي.

أعبر عن خالص امتناني للأستاذة المشرفة الدكتورة **هارون نورة**، التي كانت بنهجها الحكيم ونصائحها الثمينة نبراسًا لهذا البحث. كما أشكر وأثمن عاليًا جهود **أعضاء لجنة المناقشة** الكرام، الذين بعطائهم العلمي وملاحظاتهم البناءة أضافوا للبحث عمقًا ورصانة.

وأخص بالشكر **رئيس الأمن الوطني** لولاية بجاية، على كرم استقباله وطيب تجاوبه مع طلبي، ومساهمته القيمة بإثراء هذا البحث بمعلومات ثمينة.

أتقدم بأسمى آيات الشكر والامتنان لضابط الشرطة الرئيسي **طورشيات غيلاس**، رئيس فرقة مكافحة الجريمة السيبرانية، الذي لم يدخر جهدًا في دعم هذا البحث بمعلوماته الدقيقة وكرمه العلمي، إن التزامه المهني وحرصه الدؤوب كانا من الركائز الأساسية التي ارتكز عليها هذا العمل، ولسيادته مني فائق الشكر والامتنان على ما أبداه من حرص ودعم.

أكنّ بالغ التقدير والامتنان للأستاذ القدير **بوبعاية عبد الغاني**، على ما تفضل به من معلومات قيّمة، وحرصٍ صادق، ودعم متواصل، وتشجيع صادق كان له بالغ الأثر في مسيرة هذا البحث. لقد شكّلت توجيهاته النابعة من خبرة رصينة منارةً حقيقية سارت على نهجها خطوات هذا العمل.

أتوجّه بشكر خاص للمحامي القدير والأخ الفاضل **بوشربة سعيد**، على ما قدّمه من دعم راسخ وسند صادق طيلة مراحل هذا البحث العلمي. لقد كان دعمه موضع تقدير عميق لما تركه من أثر بالغ في دفع هذا العمل نحو الاكتمال، فمني له فائق الشكر والامتنان.

تقدير خاص لرائد القوات البرية العسكرية الأخ **فعودي عزالدين**، على ما قدمه من دعم وافر ومعلومات رصينة، كانت رافدًا أساسيًا في هذا البحث.

أتقدّم بجزيل الشكر والامتنان للأستاذ **تواتي مهني** على ما قدّمه من معلومات قيّمة ساهمت في إثراء هذا العمل.

سالمه.

الإهـداء

إلى من تجلّت في عطائهم معاني العظمة، وأضاءوا دروب الحياة بنور لا يزول، أُهدي هذا العمل بكل فخر وامتنان. إلى **جدي** الغالي والسند، أطال الله في عمره وحفظه، أُهدي هذا العمل تكريمًا لمكانته العـظيمة ودعمه المتواصل، فكان مصدر قوتي ونبض فخري.

إلى **أمي** الغالية، منبع الحنان الذي لا ينضب، وسر القوة التي لا تخبو، التي كانت دوماً ملاذي الآمن، ورفيقة صبري في مسيرة التعلم والبحث. لقد شكّلت بحنانها ودعائها المستمرين دعامة أساسية صقلت روحي وألهمتني الاستمرار رغم كل الصعاب. لهذا أُهدي لها هذا العمل تعبيرًا عن عميق امتناني وتقديري لكل ما قدمته لي من حب ودعم لا حدود له.

إلى **أبي** الغـالي، الذي علمني أن الجد والاجتهاد هما مفتاحا الارتقاء، وإلى من زرع في نفسي روح المثابرة والسعي الدؤوب نحو أعلى المراتب، أُهدي هذا العمل تعبيرًا عن فخري وامتناني.

إلى أخواتي السند: **أحلام**، **نيسة**، **ويسام**، **وريمة** اللواتي كنّ لي معينًا صادقًا في مسيرتي، ورفيقات قلبٍ لا يعوّضن. وإلى **نيسة**، الأخت التي كانت عقلًا إذا التبس الدرب، وصوتًا إذا سكن التعب، أخصّك بإهداء من طِراز الامتنان العالي، يليق بما كنتِ عليه دومًا: مرشدتي النبيلة في مسيرة العلم والحياة.

إلى صغري العائلة، ونبضي النقيّ: **لِيَا** و**محمد**، أنتما البهجة التي تملأ القلب، حضوركما البريء كان لي دفئًا في عزّ التعب، وفرحًا لا يُوصف. أُهديكما هذا العمل بكل حب.

إلى **ليندا**، أختي التي اختارتها الحياة بغير دم، صادقة في دعمها، وفية في وجودها، الداعمة التي لم تكلّ يومًا عن الوقوف بجانبي، ورفيقة الصدق التي كانت لي مرسى الأمان في كل مراحل هذه الرحلة، أهدي لها هذا العمل عرفانًا بجميلها ودعمها المستمر.

إلى **مريم**، التي كانت لي صديقة وأختًا، رفيقة الدرب والدعم، أُهدي لها هذا العمل عرفانًا بمكانتها وقيمتها في حياتي.

سالمه.

قـائمة المختـصرات

أولا: باللغة العربية

- ج.ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية.

-ص: صفحة.

-ص. ص: من الصفحة إلى الصفحة.

- ق.إ.ج: قانون الإجراءات الجزائية.

ثانيا: باللغة الأجنبية

- **P: P**age.

- P. P : De la **P**age à la **P**age.

- Op. Cit : Ouvrage **P**récédemment **C**itée.

- Ibid : Ibidem.

مقـــدمـــة

مقـــــدمـــــــة

شَكَّلت الحقبة الممتدة من 1991-2002 محطة تاريخية دموية عاشتها الجزائر، عُرفت بمرحلة "العُشرية السَّوداء"، حيث شهدت بداية ظهور الإرهاب، وهي ظاهرة إجرامية ارتبطت أساسا بمجموعة من الأسباب السياسية، إضافة إلى ظروف اقتصادية واجتماعية قاسية عاشتها البلاد في تلك الفترة الصعبة.

فنظرًا لتصاعد وتيرة التهديدات الإرهابية في تلك الفترة، خطا المشرع الجزائري خطوة نحو تجريم هذه الظاهرة الإجرامية في القانون الجزائري، وقدم تعريفًا لهذا النشاط الإجرامي، على أنه مجموعة من الأفعال التخريبية التي تستهدف أمن الدولة الجزائرية وسلامتها الترابية. وتنفذ التنظيمات الإرهابية مجموعة من الهجمات والأفعال الإرهابية التي تهدف خلالها إلى خلق جوّ من الرعب واللا أمن في المجتمع، وزعزعة ثقة المواطنين في مؤسسات الدولة، والقيام بأعمال تخريبية واعتداءات وعرقلة تطبيق القوانيـن.

فبهذه الخطوة، جسّد المشرع الجزائري إرادةً حازمة في مجابهة الأعمال الإرهابية والتخريبية، مُعتمِدًا في ذلك على قانون العقوبات الجزائري، كسندٍ تشريعيٍّ شاملٍ يُرسّخ قواعد رَّدع النشاطات الإرهابية الإجرامية. وفي هذا الإطار، خضع قانون العقوبات الجزائري، لسلسلة من التعديلات والتتميمات المتتابعة منذ صدوره وأسفرت عن تطوير وتعميق تنظيم جريمة الإرهاب، من خلال تبني سياسة جنائية صارمة وتوسيع نطاق التجريم وتحديد البنيان القانوني والجزاءات الرَّدعية الصارمة المقررة لمرتبكي جرائم الإرهاب.

تبعا لذلك، فإن جوهر الإرهاب يبقى ثابتًا من حيث أهدافه في إثارة الخوف والهلع داخل المجتمع، وتهديد أمن الدولة الجزائرية، إلا أن أشكاله ووسائله وأساليبه قد تطوّرت، لاسيما مع التحولات الرقمية التي شهدها ميدان الإعلام والاتصال، والتنامي الهائل في بنية التواصل الرقمي، مما أدى إلى تجاوز الحدود الجغرافية التقليدية بين الدول، وفتح فضاء رقمي خصب أمام الجماعات الإرهابية، لشنّ عملياتها وإطلاق تهديداتها بأساليب مستحدثة يصعب ضبطها ومراقبتها، وهو ما فرض تحديات معقدة وطنيًـــا ودوليًـــا.

إذْ يُعتبر الإرهاب الإلكتروني امتدادًا عصريًا للإرهاب التقليدي، وقد أصبح يُشكّل هاجسًا للدولة الحديثة، نظرا لارتباطه بتكنولوجيا الإعلام والإتصال، وهو ما دفع المشرّع الجزائري إلى سنّ نصوص قانونية دقيقة في قانون العقوبات، تتناول أحكام جريمة الإرهاب الإلكتروني، إضافة إلى القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والمرسوم الرئاسي المُلحق به.

كما برزت جهود المشرّع الجزائري في التصدّي لجريمة الإرهاب الإلكتروني من خلال استحداث آليات بحث وتحري وتحقيق، تتلاءم مع طبيعة هذه الجريمة الإلكترونية، ونظرًا لخطورتها والتهديدات التي تنطوي عليها عمل على توسيع دائرة الوقاية بإنشاء مؤسسات وقائية، إلى جانب قطب جزائي وطني قضائي مختص.

تكْمُن أهمية دراسة جريمة الإرهاب الإلكتروني في القانون الجزائري، بإعتباره من بين أخطر وأحدث صور الجريمة المعاصرة المنتشرة حاليا، وواحدًا من المواضيع القانونية التي تستحق الدراسة والبحث المعمّق، نظرًا لما يطرحه من إشكالات قانونية وعملية بالغة التعقيد، كونه يتصل بفضاء افتراضي مفتوح يتجاوز كلّ الحدود التقليدية، ويُستغلّ بشكل متزايد من قبل الجماعات الإرهابية في ظل الثـورة الرقميـة.

فجاء اختيارنا لموضوع الإرهاب الإلكتروني، انطلاقًا من قناعة شخصية بأن جريمة الإرهاب، على خلاف ما يعتقده البعض، لم تختفِ من الواقع المعاصر، بل تطوّرت واتخذت أشكالًا مستحدثة أكثر تقنية احترافية بفضل التطور التكنولوجي، خاصة في ظل توسع استخدام شبـكة الاتصـال والإعلام الحديثـة.

ففي الوقت الذي يرى فيه كثير من الناس أن الإرهاب هو ظاهرة قديمة، تراجعت بسبب الاستقرار الأمني الذي تعرفه الدولة الجزائرية، يُغفل جانب مهم يتمثل في انتقاله إلى الفضاء الرقمي، الأمر الذي يجعل من الضروري تسليط الضوء على هذا النمط الجديد من الجريمة، وكشف مخاطره القـانونية والأمنيـة.

أما الأسباب الموضوعية التي دفعتنا إلى اختيار هذا الموضوع، هو التزايد اللافت في معدلات جريمة الإرهاب الإلكتروني، وما يشكّله ذلك من تهديد متصاعد للأمن الوطني. هذا التنامي فرض الحاجة إلى فهم أعمق لطبيعة هذه الجريمة، وآليات مواجهتها قانونيًا، وفهم الجهود المبذولة في إطار التصدي لهذه الجريمة.

نظرًا لحداثة جريمة الإرهاب الإلكتروني، واجهنا خلال إعداد هذا البحث جملة من التحديات التي حاولنا تجاوزها بعون الله وتوفيقه، وتمثلت أساسًا في الندرة الكبيرة للكتب الجزائرية المتخصصة التي تناولت جريمة الإرهاب الإلكتروني، خصوصًا ما يتعلق بـتحليل أركانها القانونية، وهو ما اضطرّنا إلى الاعتماد بشكل أساسي على المقالات العلمية المحكمة وتحليل النصوص القانونية ذات الصلة لتعويض هذا النقص.

كما مثّل عامل الوقت تحديًا إضافيًا، حيث تطلّب منا الموضوع مجهودًا بحثيًا ظل فترة زمنية ضيقة، ما شكّل ضغطًا خلال مختلف مراحل الإنجاز، دون أن يحول ذلك السعي لتقديم دراسة علمية متكاملـة.

تهدف هذه الدراسة إلى التعمق وفهم خصوصيات جريمة الإرهاب الإلكتروني، سواء من حيث أركانها القانونية، أو خصائصها التقنية، أو دوافعها العامة والخاصة، كما تبرز أهمية البحث في تتبّع موقف الاتفاقيات الدولية والتشريع الجزائري منها، والوقوف على مختلف الآليات القانونية والمؤسساتية التي استُحدثت لمواجهتها، بما يعكس جدية الدولة الجزائرية في التصدي لتهـديدات الإرهـابية الإلكترونيـة.

انطلاقًا من هذا العرض، لتطور جريمة الإرهاب، وتحولها إلى الفضاء الرقمي، تثور الإشكالية التالية:

فيما تتمثل أبعاد السياسة الجنائية المنتهجة من طرف المشرع الجزائري لمجابهة الإرهاب الإلكتروني؟

للإجابة على هذه الإشكالية إعتمدنا التقسيم الثنائي للخطة مستندين على المنهج التحليلي والاستقرائي لنصوص القانونية التي عالجت جريمة الإرهاب الإلكتروني، فيما اقتصر اعتمادنا على المنهج الوصفي على بعض أجزاء الدراسة، وكذلك المنهج النقدي لتقديم البعض من الانتقادات التي تشوب التشريعات المتعلقة بالإرهاب الإلكتروني في الجزائر، وفي ضوء ما سبق، يمكن لنا تقسيم الخطة كالتـالـي:

حيث خصصنا الفصل الأول لدراسة الإطار الموضوعي لجريمة الإرهاب الإلكتروني، والذي ينقسم بدوره إلى مبحثين: يتناول المبحث الأول نطاق تجريم الإرهاب الإلكتروني، بينما يُعالج المبحث الثاني البنيان القانوني لجريمة الإرهاب الإلكتروني في القانون الجزائري.

أما الفصل الثاني بعنوان الآليات الإجرائية لمجابهة الإرهاب الإلكتروني في القانون الجزائري، فقد خصصنا المبحث الأول لدراسة آليات المتابعة الجزائية في جريمة الإرهاب الإلكتروني، في حين تطرقنا في المبحث الثاني إلى الآليات المؤسساتية المستحدثة لتصدي لجريمة الإرهاب الإلكتروني.

الفصل الأول

الأحكام الموضوعية لجريمة الإرهاب الإلكتروني

الفصل الأول: الأحكام الموضوعية لجريمة الإرهاب الإلكتروني

أدت ثورة المعلومات وما رافقها من تطور علمي وتقني في الحقبة الأخيرة، خاصة مع بروز الفضاء الرقمي وتزايد استغلال التقنيات المعلوماتية في مختلف مجالات الحياة، إلى تغيير نمط الحياة في العالم بأسره. ورغم الأثار الإيجابية التي تحملها هذه التقنيات في المساهمة في التطور والرُّقي في المجتمعات، إلا أنه كان لها أثر سلبي، في بروز أشكال جديدة من الجرائم التي تستغل تكنولوجيا الإعلام والاتصال، وتستخدمها وسيلة لارتكاب جرائم تهدد أمن الدول والأفراد على حد سواء، ومن أبرزها جريمة الإرهـــاب الإلكترونـــي.[1]

باعتبار جريمة الإرهاب الإلكتروني[2] من الجرائم العصرية والعابرة للحدود الوطنية، خاصة مع التهديدات الخطيرة التي توعدت بها، وما ترتب عليها من نشر الذعر وإخلال الأمن في العالم، ظهرت حاجة القوانين والاتفاقيات الدولية العالمية والإقليمية، لتعزيز الجهود الدولية والعربية للتصدي لها، كما تم تنظيمها في القانون الجزائري، وذلك بتحديد إطارها القانوني لرّدع الإرهاب الإلكتروني. فهي جريمة تتفق مع الإرهاب التقليدي من حيث الأفعال الإرهابية والأهداف والدوافع، لكن ما يبرز خصوصية الإرهاب الإلكتروني هي وسيلة تنفيذ الجريمة، والمتمثلة في تكنولوجيا الإعلام والاتصال، وكذا الفضاء الرقمي الذي يتم اتخاذه كبيئـة، ومسرح لتخطيط وتنفيذ الهجمات والعمليات الإرهابيـة الإلكترونيـة **(المبحث الأول)**.

كما أن الإرهاب الإلكتروني يُعد من الجرائم الخطيرة والمعقدة التي تستهدف زعزعة الأمن، وتهدد استقرار أمن الدولة الجزائرية، عبر استخدام وسائل التكنولوجيا الحديثة، فقد كان من الضروري وضع إطار قانوني يُحدد الأركان القانونية التي تقوم عليها هذه الجريمة. فحتى يُعترف بالفعل كجريمة إرهاب إلكتروني، لا بد من توفر مجموعة من الأركان القانونية (الركن الشرعي، الركن المادي، وأخيرًا الركن المعنوي) كما أن القانون الجزائري، لم يكتفِ فقط بتحديد العناصر القانونية لها، بل وَضع أيضًا عقوبات صارمة لتكون رادعًا فعالًا، في مواجهة التهديدات والهجمات الإرهابيـة الإلكترونية المعاصـرة **(المبحـث الثاني)**.

---

[1] جدي وفاء،" الإرهاب الإلكتروني أسبابه بين النص والتطبيق"، **مجلة مقاربات**، المجلد03، العدد 05، جامعة الجلفة، الجزائر،2015، ص.30.

[2] يُقصد بالإرهاب الإلكتروني أو ما يُعرف كذلك بالإرهاب السيبراني :" عبارة عن هجومات وتهديدات مع سبق الإصرار، تقوم بها الجماعات الإرهابية، مستعينة في ذلك بتكنولوجيا الإعلام والإتصال، وذلك لبلوغ مجموعة من الأهداف ذات الطابع السياسي، وشن هجومات على الأنظمة المعلوماتية التابعة للدولة، أو لشراء الأسلحة، أو في سبيل التخطيط مع الغير لتنفيذ عمليات إرهابية" نقلا عن: دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة لنيل شهادة الماجستير، شعبة: القانون الجنائي، كلية الحقوق، جامعة منتوري-قسنطينة، الجزائر، 2013، ص.149.

المبحث الأول: نطاق تجريم الإرهاب الإلكتروني

أصبح الإرهاب الإلكتروني واقعًا يفرض نفسه على الدول في العالم، خاصة مع التحولات التي يشهدها القطاع الرقمي والتي تُعد من العوامل الرئيسية، التي أسفرت عن بلورة نوع من الجرائم المستحدثة الفريدة في طبيعتها، كما أثمرت تطورات التكنولوجيا بروز الخوارزميات الذكية، التي تستغلها جماعات الإرهاب الإلكتروني في التخطيط والتحضير، وتنفيذ الاستراتيجيات والهجمات الإرهابية في الفضاء الرقمي.[1]

فنظرًا لتزايد والتفاقم المستمر للإرهاب الإلكتروني، وما يحمله من انعكاسات سلبية على استقرار الأمن المعلوماتي[2] لدول، برزت الحاجة لتوحيد الجهود الدولية العالمية والإقليمية للحد من هذه الجريمة، وذلك من خلال الاتفاقيات الدولية التي سعت إلى وضع قواعد قانونية مشتركة، تُجرّم هذه الأفعال وتعزز التعاون في مكافحتها. وفي المقابل، لم تكن المنظومة القانونية الجزائرية بمنأى عن هذه التطورات، بل سعت بدورها إلى وضع قوانين تعالج جريمة الإرهاب الإلكتروني، وكذا تكييف النصوص القانونية العقابية مع التهديدات الجديدة، من خلال إدراج أحكام واضحة تُجرّم الإرهاب الإلكتروني وتحدد أسسه القانونية بدقة.

انطلاقًا من هذا المعطى، سيتم دراسة المبحث الأول وفق لتقسيم التالي، من خلال التطرق لدراسة مجال تجريم الإرهاب الإلكتروني **(المطلب الأول)**، بهدف فهم الأساس القانوني المعتمد على المستوى الدولي والإقليمي والوطني في مواجهة هذه الجريمة الخطيرة، ثم الانتقال إلى خصوصية جريمة الإرهاب الإلكتروني **(المطلب الثاني)**، من أجل التعرف على طبيعته المتميزة وكذا الدوافع العامة والخاصة التي تُسهم في انتشاره.

المطلب الأول: مجال تجريم الإرهاب الإلكتروني

برزت في السنوات الأخيرة العديد من الاتفاقيات الدولية، سواء على المستوى العالمي أو الإقليمي تهدف إلى دعم التعاون بين الدول، وتعزيز الجهود المشتركة في مواجهة الجرائم، التي تُرتكب باستخدام

---

[1] سحر جمال عبد السلام زهران، "الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني"، **مجلة كلية السياسة والاقتصاد**، المجلد05، العدد04، كلية السياسة والاقتصاد، جامعة بني سويف، مصر، 2019، ص.61.

[2] يُقصد بأمن المعلومات:" العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية، والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام" نقلا عن: الشوابكة عواد عدنان، "دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلوماتي في جامعة الطائف"، **مجلة دراسات و ابحاث**، المجلد 11، العدد04، جامعة زيان عاشور-الجلفة، الجزائر، 2019، ص. 168.

وسائل تكنولوجيا الإعلام والاتصال، أو ما يصطلح بالجرائم المعلوماتية. وهذه الاتفاقيات جاءت كرّد فعل على تنامي هذه الجرائم، خاصة الإرهاب الإلكتروني، الذي أصبح يشكل تهديدًا لأمن الدول واستقرارها.

في هذا الإطار، صادقت الدولة الجزائرية على عدد من هذه الاتفاقيات الدولية، بموجب مراسيم رئاسية، ما يعكس التزامها بالمشاركة في الجهود الدولية لمكافحة هذا النوع من الجرائم. كما عملت على إدراج أحكام قانونية، سواء موضوعية أو إجرائية، ضمن قوانينها الوطنية، بهدف التصدي للإرهاب الإلكتروني.

بناءً على ذلك، سيتم التطرق في هذا المطلب إلى تجريم الإرهاب الإلكتروني في نطاق الاتفاقيات الدولية- العالمية والإقليمية- **(الفرع الأول)**، ثم التطرق إلى تجريم الإرهاب الإلكتروني في القانون الجزائري **(الفرع الثاني)**، بهدف فهم كيفية تعامل كل من المنظور الدولي والقانون الجزائري مع الإرهاب الإلكتروني.

الفرع الأول: تجريم الإرهاب الإلكتروني في نطاق الاتفاقيات الدولية

مع تزايد استخدام تكنولوجيا الإعلام والإتصال في تنفيذ الأعمال الإجرامية بصفة عامة، والأعمال الإرهابية الإجرامية بصفة خاصة، أصبح من الضروري على المجتمع الدولي وضع آليات قانونية موحدة للتصدي لهذه الظاهرة الإجرامية[1]، كما أن اختلاف مستوى تطور البنية الرقمية[2] من دولة لأخرى، فرض نوعًا من التنوع في النصوص القانونية، الأمر الذي جعل التعاون الدولي أمرًا ضروريا لا غنى عنه، لمجابهة ووضع حد لتهديدات الإرهابية الإلكترونية المتنامية، ومن أجل فهم كيفية تناول الاتفاقيات الدولية لموضوع تجريم الإرهاب الإلكتروني، تم تقسيم هذه الاتفاقيات إلى قسمين رئيسيين: الاتفاقيات الدولية ذات الطابع العالمي **(أولًا)**، ثم الاتفاقيات الدولية ذات الطابع الإقليمي **(ثانيًا)**، وذلك بهدف توضيح الجهود الدولية العالمية والعربية الإقليمية المبذولة في سبيل مواجهة هذه الظاهرة الإجرامية.

[1] معمري خديجة، خلفاوي خليفة،" إشكالية تعارض مكافحة الإرهاب الإلكتروني بأهمية حماية حقوق الإنسان"، **الأكاديمية للدراسات الاجتماعية والإنسانية**، المجلد13، العدد02، كلية العلوم الاقتصادية والقانونية، جامعة حسيبة بن بوعلي- الشلف، الجزائر،2021، ص.349.

[2] يُقصد بالبنية الرقمية أو ما يُعرف بالفضاء السيبراني: "هو الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني وبمفهوم أشمل يعرف بأنه مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي أجهزة الكمبيوتر، أنظمة الشبكات وبرمجيات حوسبة المعلومات، نقل وتخزين البيانات ومستخدمي كل هذه العناصر" نقلا عن: نجاري بن حاج علي فايزة، مكافحة الإرهاب الإلكتروني في القانون الدولي، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: قانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2023، ص .15.

أولا: الاتفاقيات الدولية العالمية المُجرمة للإرهاب الإلكتروني

مع تنامي التهديدات المرتبطة باستخدام التكنولوجيا في تنفيذ الأعمال الإرهابية في العالم، برزت ضرورة العمل على وضع اتفاقيات دولية عالمية تساعد على التصدي لهذا النوع من الجرائم، خاصة أن أغلبها يتجاوز الحدود الجغرافية، ويصعب تعقبه بوسائل تقليدية، لذلك ظهرت مجموعة من الاتفاقيات الدولية العالمية، التي سعت إلى وضع قواعد قانونية تُجرّم هذه الأفعال، وتُسهل التعاون بين الدول لمتابعتها.

1) اتفاقية بودابست لمكافحة الجرائم المعلوماتية

وُضعت اتفاقية بودابست، أو ما يُعرف أيضًا باتفاقية الجرائم الإلكترونية، من طرف مجلس أوروبا بتاريخ 23نوفمبر2001، والتي دخلت حيز التنفيذ في سنة 2004. وتشمل الاتفاقية 48 مادة، يتمحور مضمونها حول الجرائم الإلكترونية والتدابير الموضوعية والإجرائية الفعالة، الواجب اتخاذها على الصعيدين الوطني والدولي للتصدي للإجرام الإلكتروني، وحماية المجتمع من الجريمة الإلكترونية.

من الجدير بالذكر أنّ جريمة الإرهاب الإلكتروني تندرج ضمن الفصل الأول من الاتفاقية المعنون بـ "**الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر**"، بحيث تنص المادة 2 من اتفاقية بودابست، التي جاءت بعنوان "النفاذ غير المشروع"، على ما يلي: "**تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدًا وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كمبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية بنية الحصول على بيانات الكمبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر**".[1]

انطلاقًا من نص المادة أعلاه، فإن الدخول أو البقاء في جزء أو كل منظومة معلوماتية عن طريق الغش أو الصدفة، بهدف الحصول على البيانات أو سرقتها يُعتبر جريمة معاقب عليها في منظور إتفاقية

[1] أنظر المادة 2 أُنبثقت اتفاقية بودابست عن اجتماع المجلس الأوروبي بتاريخ 23نوفمبر 2001 تحت رقم 185 تحت عنوان "اتفاقية بودابست لمكافحة الجريمة المعلوماتية"، ودخلت حيز التنفيذ بتاريخ 01جويلية 2004، للتفصيل يرجى مراجعة الموقع الإلكتروني الخاص بالمجلس الأوروبي المتوفر على الرابط التالي https://rm.coe.int/budapest-convention-in-arabic/1680739173 ، تم الاطلاع عليه بتاريخ2025/03/23 على الساعة 10:02.

بودابست، وفي حال ما وقع الاعتداء على أنظمة معلوماتية تابعة للدولة والحكومة، فإن ذلك يدخل في نطاق الإرهاب الإلكتروني نظرًا لما يحمله هذا السلوك الإجرامي من تهديد لأمن الدولة.

كما تنص المادة 3 من اتفاقية بودابست، التي جاءت بعنوان "**الاعتراض غير المشروع**"، على ما يلي: "... **تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدًا وبغير حق: الاعتراض باستخدام وسائل فنية للإرسال غير العمومي لبيانات الكمبيوتر إلى أو من أو داخل نظام كمبيوتر، بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كمبيوتر يحمل هذه البيانات. ويجوز للدولة الطرف أن تستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنية غير صادقة أو في ارتباط بنظام كمبيوتر متصل بنظام حاسوبي آخر**".[1]

ما يُلاحظ من نص المادة أعلاه، أنها تجرم فعل الاعتراض العمدي باستخدام تكنولوجيا الإعلام والاتصال للبيانات المحمية المرسلة غير العامة، وهذا دلالة على أن اتفاقية بودابست تحمي حق سرية البيانات والمراسلات. وفي حال ما وقع هذا الشكل من الاعتداء على الدولة من خلال التجسس الإلكتروني مثلا، فسيشكل ذلك جريمة الإرهاب الإلكتروني.

كما أشارت المادتين 4 و5 من اتفاقية بودابست بعنوان "**التدخل في البيانات**" و"**التدخل في النظام**" على ما يلي: "**تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدًا: إتلاف بيانات حاسوبية، حذفها، إفسادها، تعديلها أو تدميرها.**"،

"... **إذا ما ارتكب عمدًا وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكمبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها**...".

بناءً على ما ورد في نصوص المادتين أعلاه، نلاحظ أن اتفاقية بودابست تُجرم فعل الإتلاف العمدي للبيانات، سواء كانت بيانات تابعة للدولة، أو شخصيات من الحكومة، أو تابعة للدفاع الوطني للدولة أو الأمن الوطني. كما جعلت من العرقلة العمدية لسير نظام تشغيل الكمبيوتر جريمة، وهذا ما يشكل تهديدًا للاستقرار الأمني للدولة، بتالي يمكن تكييف ما سبق ذكره في إطار جريمة الإرهاب الإلكتروني.

[1] أنظر المادة 3 من المرجع نفسه.

2) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية

في إطار تجريم الإرهاب الإلكتروني، يُستشف من المادة 5 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، توجه المشرع ضمنيا إلى اعتبار هذه الاخيرة جريمة، نظرا لطابعها الخطير والعابر للحدود الوطنية، والمنظم، بحيث تنص على ما يلي: "... **تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية جنائيًا عندما ترتكب عمدًا:**

أ) - أي من الفعلين التاليين أو كليهما، باعتبارهما فعلين جنائيين متميزين عن الجرائم التي تنطوي على الشروع في النشاط الإجرامي أو إتمامه:

1- الاتفاق مع شخص آخر أو أكثر على ارتكاب جريمة خطيرة لفرض له صلة مباشرة أو غير مباشرة بالحصول على منفعة مالية أو منفعة مادية أخرى، وينطوي، حيثما يشترط القانون الداخلي ذلك، على فعل يقوم به أحد المشاركين يساعد على تنفيذ الاتفاق، أو تكون ضالعة فيه جماعة إجرامية منظمة؛

2- قيام الشخص، عن علم بهدف جماعة إجرامية منظمة ونشاطها الإجرامي العام أو بعزمهما على ارتكاب الجرائم المعنية، بدور فاعل في:

أ- الأنشطة الإجرامية للجماعة الإجرامية المنظمة

ب- أي أنشطة أخرى تتصل بجماعة إجرامية منظمة، مع علمه بأن مشاركته ستسهم في تحقيق الهدف الإجرامي المبين أعلاه؛

ب) - تنظيم ارتكاب جريمة خطيرة تكون ضالعة فيها جماعة إجرامية منظمة، أو الإشراف أو المساعدة أو التحريض عليه أو تيسيره أو إسباغ المشروعية عليه...".[1]

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة، المؤرخ في 15نوفمبر2000، بمدينة باليرمو الإيطالية، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 02-55، المؤرخ في 5فيفري 2000، ج.ر.ج.ج عدد 09، صادر في10فيفري2000.

3) الاتفاقية الدولية لقمع تمويل الإرهاب

عالجت الاتفاقية الدولية لقمع تمويل الإرهاب موضوع جريمة الإرهاب الإلكتروني، في المادة 2 والتي تنص على ما يلي: **"يُرتكب جريمة بمفهوم هذه الاتفاقية، كل شخص يقوم بأية وسيلة كانت، مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادته، بتحويل أو جمع أموال بنية استخدامها، أو هو يعلم أنها ستُستخدم كليًا أو جزئيًا للقيام بـ: ... ب) بأي عمل آخر يهدف إلى التسبب في موت شخص مدني أو أي شخص آخر، أو إصابته بجروح بدنية جسيمة، عندما يكون هذا الشخص غير مشترك في أعمال عدائية في حالة نشوب نزاع مسلح، عندما يكون غرض هذا العمل، بحكم طبيعته أو في سياقه، موجهًا لترويع السكان، أو لإرغام حكومة أو منظمة دولية على القيام بأي عمل أو الامتناع عن القيام به..."**.[1]

يتضح من نص المادة أعلاه أن عبارة "بأية وسيلة كانت" جاءت لتشمل مختلف الطرق الممكنة، بما فيها استخدام التكنولوجيا الحديثة ووسائل الاتصال الرقمية في تمويل الأنشطة الإرهابية الإلكترونية.

ثانيا: الاتفاقيات الدولية الإقليمية المُجرمة للإرهاب الإلكتروني

صادقت الجزائر في إطار مكافحة الجريمة الإلكترونية بصفة عامة، وجريمة الإرهاب الإلكتروني بصفة خاصة، على مجموعة من الاتفاقيات الإقليمية التي تهدف إلى تعزيز التعاون العربي في مجال مكافحة الجريمة المنظمة عبر الحدود الوطنية، وكذلك الجرائم المعلوماتية المعقدة. ومن أبرزها نذكر ما يلي:

1) الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب

في إطار مكافحة جريمة الإرهاب الإلكتروني، جرَّمت المادة 10 من الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، تحت عنوان **"تجريم تمويل الإرهاب"**، السلوك الإجرامي المتمثل في تمويل الإرهاب على النحو التالي: **"تتخذ كل دولة طرف، وفقًا للمبادئ الأساسية لنظامها القانوني، ما يلزم من تدابير تشريعية لتجريم أي فعل من أفعال تمويل الإرهاب الآتية:**

1- تقديم الأموال تحت أي مسمى مع العلم بأنها ستستخدم لتمويل الإرهاب.

[1] الاتفاقية الدولية لقمع تمويل الإرهاب، المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة، المؤرخ في 9ديسمبر 1999، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم2000-445، المؤرخ في 23 ديسمبر2000، ج.ر.ج.ج العدد الأول، الصادرة في 3يناير2001.

2- اكتساب أو جمع الأموال بأي وسيلة كانت، بقصد تمويل الإرهاب.

3- حيازة أو حفظ أو إدارة استثمار الأموال المعدة لتمويل الإرهاب مع العلم بذلك."[1]

ما يُرصد من نص المادة أعلاه، هو أنه باستخدام عبارة "بأية وسيلة كانت" تم التوسيع من نطاق التجريم ليشمل بذلك استخدام تكنولوجيا الإعلام والاتصال، وهذا ما يدخل في نطاق الإرهاب الإلكتروني.

2) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

في إطار تعزيز التعاون بين الدول العربية في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جرّمت المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، التي جاءت تحت عنوان "**الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات**"، جريمة الإرهاب الإلكتروني بشكل صريح، وذلك من خلال تجريم استخدام تكنولوجيا الإعلام والاتصال في الأفعال الإرهابية، حيث جاء النص عليها كالتالي:

1- "نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات".[2]

3) الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية

ضمن جهود تعزيز التعاون العربي لمنع ومكافحة الجريمة المنظمة عبر الحدود الوطنية، جرّمت المادة 6/21 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الاستعمال غير المشروع لتقنية أنظمة المعلومات لارتكاب أي جريمة من الجرائم التقليدية، على النحو التالي: "**أي جريمة من الجرائم**

[1] الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم14-250، المؤرخ في 8سبتمبر2014، ج.ر.ج.ج عدد 55، الصادر في 23سبتمبر2014.

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21ديسمبر2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 8سبتمبر 2014، ج.ر.ج.ج عدد57، الصادر28سبتمبر2014.

التقليدية تُرتكب بإحدى وسائل تقنية أنظمة المعلومات"[1]، وباعتبار جريمة الإرهاب من الجرائم التقليدية، فإن استعمال تكنولوجيا الإعلام والاتصال لارتكابها سيشكل جريمة الإرهاب الإلكتروني، وستُطالها مظلّة التجريم، المحددة في الإتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

الفرع الثاني: تجريم الإرهاب الإلكتروني في القانون الجزائري

مع التطورات السريعة للوسائل التكنولوجية، وتزايد استخدام الفضاء الرقمي في تنفيذ أعمال تهدد أمن واستقرار الدولة الجزائرية، كان لا بدّ من تدخل المشرّع الجزائري لمواكبة هذه التحولات، وسد الفراغ القانوني الذي يمكن أن تستغله الجماعات الإرهابية. فالإرهاب الإلكتروني، بصفته أحد أخطر أشكال الجريمة المستحدثة، فرض على الجزائر، حتمية وضع نصوص قانونية تواكب هذا التحدي، وذلك سواء في نطاق الدستور الجزائري **(أولا)**، أوفي النصوص التشريعية **(ثانيا)** أو في النصوص التنظيمية **(ثالثا)**.

أولا: نطاق تجريم الإرهاب الإلكتروني في الدستور الجزائري

لا توجد إشارة صريحة إلى جريمة الإرهاب الإلكتروني[2]،كظاهرة إجرامية مستقلة في الدستور الجزائري، لكن يمكن فهم كيفية التعامل مع هذه القضية في سياق مكافحة الإرهاب، خاصة بعد تعديل الدستور في عام 2020. حيث ينص على ضرورة حماية الأمن الوطني والمجتمع من مختلف أشكال التهديدات، بما في ذلك الإرهاب، وهو ما يشمل الإرهاب الإلكتروني في سياق مكافحة الجرائم الإلكترونية.

كما يكفل تعديل الدستور2020، الحقوق الأساسية والحريات العامة، وتضمن الدولة الحماية الضرورية للإنسان من أي انتهاكات، بما في ذلك من جرائم الإرهاب الإلكتروني، وذلك من خلال نصوص المواد 1/35 التي تنص على: "**تضمن الدولة الحقوق الأساسية والحريات**"، وكذلك المادة 1/39: "**تضمن الدولة عدم انتهاك حرمة الإنسان**"، والمادة 47: "**لكل شخص الحق في حماية حياته الخاصة وشرفه؛ لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة بأي شكل كانت، لا مساس بالحقوق المذكورة**

---

[1] الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21ديسمبر2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-251، المؤرخ في 8سبتمبر 2014، ج.ر.ج.ج عدد56، الصادر25سبتمبر2014.

[2] يُقصد بجريمة الإرهاب الإلكتروني: "كل جماعة إرهابية تستعمل الوسائل التكنولوجية كالأنترنيت من أجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق وتبادل المهارات والخبرات والأساليب، أو جمع التبرعات من أجل تمويل عملياتهم الإرهابية" نقلا عن: نجاري بن حاج علي فايزة، الآليات الإلكترونية لمكافحة الإرهاب الإلكتروني، رسالة لنيل شهادة الماجستير، التخصص: القانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، الجزائر، 2016، ص.26.

في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطة القضائية؛ حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي؛ ويعاقب القانون على كل انتهاك لهذه الحقوق".[1]

ثانيا: نطاق تجريم الإرهاب الإلكتروني في النصوص التشريعية

تماشياً مع الاتفاقيات الدولية والإقليمية التي صادقت عليها الجزائر، أو التي تأثرت بها مثل اتفاقية بودابست، قام المشرع الجزائري بتجريم الإرهاب الإلكتروني في نصوص قانونية متفرقة ونجد ذلك فيما يلي:

قانون العقوبات في المواد 87 مكرر 4، 87 مكرر 11، 87 مكرر 12 و87 مكرر 15 التي تُجرم استخدام تكنولوجيا الإعلام والاتصال لارتكاب أفعال إرهابية؛ كذلك، المادة 394 مكرر 3 منه، التي تشدد عقوبة جريمة المساس بأنظمة المعالجة الآلية للمعطيات إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وهو الهدف الجوهري للإرهاب الإلكتروني، وكذلك المادة 144 مكرر من القانون ذاته، التي تجرم استغلال تكنولوجيا الإعلام والاتصال للإساءة وإهانة وسب أو قذف رئيس الجمهورية.[2]

كما تم الإشارة إلى الإرهاب الإلكتروني بصيغة ضمنية، في المادة 1/2 من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أشارت إلى مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حيث حددت أنها تشمل: ".. **أي جريمة ترتكب أويسهل ارتكابها عن طريق منظومة معلوماتية**..."[3]، بالتالي يمكن إدراج ضمن هذا التعريف جريمة الإرهاب الإلكتروني، وكذلك المادة 15 من نفس القانون التي تنص على اختصاص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبياً وتستهدف مؤسسات الدولة الجزائرية، أو الدفاع الوطني، أو المصالح الاقتصادية للدولة الجزائرية.

---

[1] أنظر المادتين 35و39 و47 من دستور الجمهورية الجزائرية الديمقراطية الشعبية، المؤرخ في 28 نوفمبر 1996، المعدل والمتمم، بموجب القانون رقم 02-03، المؤرخ في 10 أبريل 2002، المتضمن التعديل الدستوري، ج.ر.ج.ج عدد 25، الصادر في 14 أبريل 2002، و بالقانون رقم 19-08 المؤرخ في 15 نوفمبر 2008، ج.ر.ج.ج عدد 63، الصادر في 16 نوفمبر 2008، وبالقانون رقم 16-01، المؤرخ في 06 مارس 2016، المتضمن التعديل الدستوري، ج.ر.ج.ج عدد الصادر في 07 مارس 2016، وبالمرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في 01 نوفمبر 2020، ج.ر.ج.ج عدد 82، الصادر في 30 ديسمبر 2020.

[2] أمر رقم66-156 مؤرخ في 8يونيو1966، يتضمن قانون العقوبات، ج.ر.ج.ج عدد49، صادرة في 11يونيو1966، معدل ومتمم.

[3] قانون رقم 09-04 مؤرخ في 5غشت2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد47، صادرة في 25أوت2009.

كذلك يتّضح ضمنيًا، في القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية في نص المادة 117 و118 منه[1]، التي تشير إلى الحرص والالتزام بعدم المساس بالنظام العام والدفاع الوطني والأمن العمومي، أثناء استعمال شبكات أو خدمات الاتصالات الإلكترونية. وفي حال تم المساس بالدفاع الوطني وزعزعة الأمن العمومي والنظام العام باستعمال تكنولوجيا الاعلام والاتصال، وهو ما يدخل في نطاق الإرهاب الإلكتروني، يتم إعذار المتعامل من طرف سلطة ضبط البريد والاتصالات الإلكترونية، قصد التدخل الفوري لمنع النفاذ إلى الشبكات أو خدمات الاتصالات الإلكترونية.

في السياق ذاته، نجد القانون رقم 18-07 الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في المادة 44 منه، والتي تُجرم مايلي: "**إرسال وتحويل معطيات ذات طابع شخصي إلى دولة أجنبية عندما قد يؤدي ذلك إلى المساس بالأمن العمومي أو المصالح الحيوية**..."[2].

في الإطار نفسه، تبرز أهمية قانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية[3]، الذي وسَّع من الاختصاص المحلي للجهات القضائية في بعض الجرائم الخطيرة، منها جرائم الإرهاب والجريمة المنظمة عبر الحدود الوطنية. كما استحدث هذا القانون آليات جديدة للبحث والتحري، مثل اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وإجراء التسرب. وفي ذات الاتجاه أيضًا، وضع القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها قواعد إجرائية مُستحدثة، للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ثالثا: نطاق تجريم الإرهاب الإلكتروني في النصوص التنظيمية

صدرت العديد من المراسيم الرئاسية التي تعزز الوقاية والتصدي للإرهاب الإلكتروني، منها المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا

[1] قانون رقم 18-04 مؤرخ في 10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر.ج.ج عدد27، الصادرة في13مايو2018.

[2] قانون رقم 18-07 مؤرخ في 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج عدد 34 الصادرة في 10يونيو2018.

[3] قانون رقم06-22 مؤرخ في20ديسمبر2006، ج.ر.ج.ج عدد84، الصادرة 24ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 مؤرخ في 8يونيو1966، يتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 48، الصادرة في 10يونيو1966.

الإعلام والاتصال ومكافحتها[1]، حيث تُكلف هذه الهيئة بتنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والمراقبة الوقائية للاتصالات الإلكترونية، ومساعدة السلطات الأمنية والقضائية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

إلى جانب ذلك، استحدث المشرع الجزائري بموجب المرسوم الرئاسي رقم 20-05 منظومة وطنية لأمن الأنظمة المعلوماتية[2]، وأُطلق عليها تسمية أداة الدولة في مجال الأمن المعلوماتي، حيث اعتمد المشرّع في تشكيلها على هيكل ثنائي، يتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، ووكالة لأمن الأنظمة المعلوماتية. بحيث يتولى المجلس الوطني إعداد الاستراتيجيات الوطنية والموافقة عليها وتوجيهها في مجال أمن الأنظمة المعلوماتية، ويتشكل من مجموعة من الوزراء يُمثلون مختلف القطاعات في الدولة، إلى جانب مُمثل عن رئاسة الجمهورية وآخر عن الوزير الأول. أما الوكالة - كمؤسسة عمومية ذات طابع إداري-، فقد إعترف لها المشرع بالشخصية المعنوية، وتضم بدورها ممثلين عن عدة وزارات وهيئات وسلطات رسمية.

يُسند إلى المجلس الوطني مهمة البت في عناصر الاستراتيجيات الوطنية لأمن الأنظمة المعلوماتية التي تقترحها الوكالة، ودراسة التقارير المتعلقة بتنفيذها، والموافقة على اتفاقيات التعاون الدولية في مجال أمن الأنظمة المعلوماتية. في المقابل، تتولى الوكالة تحضير هذه العناصر وعرضها على المجلس، إلى جانب تنسيق تنفيذ الاستراتيجيات المحددة، والقيام بالتحقيقات الرقمية عند وقوع هجمات أو حوادث سيبرانية تمس المؤسسات الوطنية كجرائم الإرهاب الإلكتروني، فضلاً عن ضمان اليقظة التكنولوجية.

بذلك، فإن كلا من المجلس الوطني والوكالة يتقاسمان المهام في إطار منظّم، حيث يركّز المجلس على رسم التوجهات العامة، بينما تتولى الوكالة الجوانب الميدانية للحفاظ على الأمن المعلوماتي لدولة الجزائرية.

بناء على ما سبق ذكره في نصوص المواد القانونية أعلاه، يلاحظ أن المشرع الجزائري قد اعتمد أسلوب النصوص القانونية المبعثرة في تجريمه للإرهاب الإلكتروني، وأن المنظومة القانونية الجزائرية تفتقر إلى قانون خاص ومستقل يُجرم الإرهاب الإلكتروني.

[1] مرسوم رئاسي رقم 21-439مؤرخ في 7نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد86، الصادرة 11نوفمبر2021.

[2] مرسوم رئاسي رقم 20-05 مؤرخ في 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر.ج.ج عدد04، الصادرة 26جانفي2020.

المطلب الثاني: خصوصية جريمة الإرهاب الإلكتروني

في ظل التحولات التكنولوجية، أصبح من الضروري فهم طبيعة الجرائم التي تستغل الفضاء السيبراني في تنفيذ مخططاتها الإجرامية، وعلى رأسها جريمة الإرهاب الإلكتروني. هذه الجريمة ليست كغيرها من الجرائم التقليدية، فهي تحمل خصوصية تجعل من مواجهتها أمرًا معقدًا، على المستويين القانوني والتقني. كما أن الشخص الذي يرتكب هذا النوع من الإجرام، لا يكون دائمًا مدفوعًا بدافع واحد فقط، بل غالبًا ما تتعدد الأسباب التي تقف وراءه، سواء كانت شخصية أو فكرية أو حتى سياسية واقتصادية.[1]

انطلاقًا من ذلك، سيتم التطرق إلى مختلف الجوانب التي تميز جريمة الإرهاب الإلكتروني من حيث الخصائص (**الفرع الأول**)، ثم الوقوف عند الدوافع العامة والخاصة التي تكون وراء ارتكابها (**الفرع الثاني**).

الفرع الأول: خصائص جريمة الإرهاب الإلكتروني

تتميز جريمة الإرهاب الإلكتروني بخصائص تفرّقه عن الجرائم التقليدية، لذلك وجب إبراز هذه السمات التي تميز طبيعتها وأسباب تعقيد مواجهتها، ويمكن تلخيص هذه الخصائص فيما يلي: تكنولوجية الوسيلة في جريمة الإرهاب الإلكتروني(**أولا**)، الاستراتيجيات الإلكترونية في دعم وتنفيذ العمليات الإرهابية (**ثانيا**)، الإرهاب الإلكتروني جريمة عابرة للحدود (**ثالثا**)، صعوبة الاثبات في جريمة الإرهاب الإلكتروني (**رابعا**)، الإرهاب الالكتروني جريمة تواطؤيه (**خامسا**)، الإرهاب الإلكتروني جريمة لا تقادميه (**سادسا**).

أولا: تكنولوجية الوسيلة في جريمة الإرهاب الإلكتروني

لا يعتمد الإرهاب الإلكتروني على العنف أو القوة، وإنما يقوم بتنفيذ الهجمات الإلكترونية باستخدام وسائل إلكترونية ورقمية فقط، دون الحاجة إلى استخدام العنف والأسلحة التقليدية[2]، ونذكر على سبيل المثال بعض الهجمات الإلكترونية المنفذة من طرف المنظمات الإرهابية الإلكترونية:

---

[1] عوينات نجيب بن عمر، " الإرهاب الإلكتروني: المفهوم والجهود الدولية والإقليمية لمكافحته"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد02، العدد 02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف-بالمسيلة، الجزائر، 2017، ص.12.

[2] قيراط محمد، "الاعلام الجديد والإرهاب الالكتروني: آليات الاستخدام وتحديات المواجهة"، **مجلة الحكمة لدراسات الإعلامية والاتصالية**، المجلد5، العدد01، مركز الحكمة للبحوث والدراسات، الجزائر،2017، ص.16.

1- تطوير برمجيات خبيثة (Malware): تستخدم الجماعات الإرهابية الإلكترونية، خوارزميات التعلم الآلي لإنشاء برمجيات خبيثة، تتأقلم مع أنظمة الأمن والحماية، واكتشاف الثغرات الأمنية الجديدة، مما يجعلها أكثر قدرة على التهرب من برامج مكافحة الفيروسات[1]؛ ومن بين هذه البرمجيات نجد حصان طروادة(**les chevaux de Troie**), الذي يتيح فتح باب خلفي داخل جهاز الضحية، مما يسمح للمهاجم بالتحكم فيه عن بُعد أو تثبيت برمجيات ضارة أخرى[2]، ويعد حصان طروادة من أكثر الوسائل فعالية في تدمير البرامج وأنظمة الكمبيوتر، وكذلك نقل البيانات الحساسة إلى جماعات الإرهاب الإلكتروني.[3]

2- هجمات التصيد الاحتيالي :(Phishing) يعتمد التصيد الاحتيالي على خداع الضحايا لدفعهم إلى تقديم بياناتهم ومعلوماتهم الشخصية والمالية لغرض سرقتها واستغلالها؛ ويتم ذلك باستخدام تقنيات الذكاء الاصطناعي لإنشاء رسائل وروابط مزيفة تبدو وكأنها أصلية وصادرة عن جهات موثوقة مثل البنوك.[4]

3- تزوير البيانات والمحتوى(Deepfake) : يتيح الذكاء الاصطناعي إنشاء مقاطع فيديو أو تسجيلات صوتية أو صور مزيفة تُعرف بالتزييف العميق، ويتم استغلال هذه التقنية لخداع الرأي العام، ودفعهم لاتخاذ قرارات خاطئة[5]، والإرهاب الإلكتروني يستخدم التكنولوجيا، بما في ذلك الذكاء الاصطناعي، لتأثير على النظام العام، الأمن الوطني، أو الاستقرار السياسي. وفي هذا السياق، يمكن اعتبار استخدام التزييف العميق من قبل جماعات إرهابية متطرفة، كأداة للتلاعب بالعقول وتحقيق أهدافهم السياسية أو الاجتماعية، وهو ما ينسجم مع مفهوم جريمة الإرهاب الإلكتروني.

4- الويب المظلم(Dark Web) : يُعرف أيضًا بـ "أرض الخدمات المخفية"، وهو موقع خطير يستغل من قِبل الجماعات الإرهابية الإلكترونية. هذا الموقع هو جزء غامض من الإنترنت، لا يمكن الوصول إليه عبر محركات البحث العادية، بل فقط من خلال خدمات مثل **تور(TOR)** والتي تتيح تصفح الإنترنت بشكل آمن، ومجهول الهوية من خلال إخفاء عنوان الـ IP وتشفير الاتصال. كما تساعد في تجاوز الرقابة والوصول

[1] ACBM Avocats, **L'IA au service des hackers**, Disponible sur https://www.acbm-avocats.com/lia-au-service-des-hackers/#_ftnref1, consulté le 11février2025 a 23h22min.
[2] **Boos R**omain, La lutte contre la cybercriminalité au regard de l'action des États, Thèse de doctorat en droit, Faculté de droit, Université de Lorraine, 2016, p38.
[3] **MIRZA M**uhammad Nadeem, **SHAHZAD A**kram muhammad, "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare," **Strategic Studies**, Volume 42, Issue 1, Strategic Studies Institute, Pakistan, 2022, P70.
[4] Ibid, p42.
[5] ACBM Avocats, Op. Cit.

إلى المواقع المحجوبة أو المخفية، ويُستغل هذا الفضاء لبيع البيانات المسروقة، وتبادل البرمجيات الخبيثة، وتنسيق هجمات الإرهاب الإلكتروني بسرية تامة.[1]

كما تجدر الإشارة إلى أن لذكاء الإصطناعي[2] دور إزدواجي، فمن جهة يُعزز الهجمات الإرهابية الإلكترونية، ومن جهة أخرى يساهم في الحد والتنبؤ بتهديدات الإرهاب الإلكتروني. إذ تلعب تقنيات الذكاء الإصطناعي دور فعال وإيجابي في معرفة ورصد فئة الأشخاص الذين لديهم ميولات إيديولوجية متطرفة للجماعات الإرهابية، وبناء على ذلك يتم تحديدهم وحصرهم، كما تم تحديث وابتكار آليات تتنبأ ببؤرة الهجمات الإرهابية وتوقيتها،[3]وذلك من خلال تقنيات التعلم الآلي وتحليل البيانات الضخمة.

علاوة على ذلك، تعمل أنظمة الذكاء الإصطناعي على مراقبة التحركات المثيرة للرّيبة للمستخدمين والتي تعكس خرقا ومساسا بالضوابط الأمنية، كما تساعد على كشف هوية الإرهابيين وكذا المصادر المُمَولة للإرهاب الإلكتروني وتعطيلها[4] فضلا عن رصد الثغرات الأمنية وتعزيز الحماية. وأخيرا، تساهم في التصدي للهجمات بشكل آلي وسريع من خلال التحذيرات الاستباقية وحظر الوصول الى البيانات.[5]

ثانيا: الاستراتيجيات الإلكترونية في دعم وتنفيذ العمليات الإرهابية

تستغل التنظيمات الإرهابية الشبكة المعلوماتية للتنقيب عن المعلومات المرتبطة بالدولة، حيث يُعتبر الفضاء السيبراني بمثابة خزان للمعلومات الحساسة، التي تسعى الجماعات الإرهابية للوصول إليها، مثل المعلومات المتعلقة بطرق مكافحة الإرهاب، وكذلك ما يتعلق بالأماكن العسكرية المهمة. وغالبًا ما تكون هذه المعلومات واردة في مواقع إلكترونية متاحة للجميع دون الحاجة لشن أي اختراق للشبكة المعلوماتية.[6]

---

[1] Ibid.

[2] يُقصد بالذكاء الإصطناعي: Intelligence Artificiel " أحد علوم الحاسب الفرعية التي تهتم بإنشاء برمجيات ومكونات مادية قادرة على محاكاة السلوك البشري" نقلا عن: بتشيم بوجمعة، الذكاء الإصطناعي في منظومة العدالة الحديثة على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022، الطبعة الأولى، ألفا للوثائق، عمان- الأردن، 2023، ص.40.

[3] طارق جمعة مهدي، الذكاء الاصطناعي ومكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية،2023، ص.39.

[4] عوض عبد السميع عادل،" دور الذكاء الإصطناعي بالتنبؤ بمكافحة الإرهاب"، **مجلة متون**، المجلد17، العدد01، كلية العلوم الاجتماعية والإنسانية، جامعة مولاي الطاهر-سعيدة، الجزائر، 2024، ص.80.

[5] البدو محمد عبد الله آمل،" دور الذكاء الإصطناعي في تحسين تجربة التعلم الرقمي وتحقيق الأمان الرقمي في العملية التعليمية"، **مجلة بحث وتربية**، المجلد14، العدد01، المعهد الوطني للبحث في التربية، الجزائر،2024، ص. ص.37 -38.

[6] القرعان محمود أحمد محمد، الجرائم الإلكترونية، دار وائل، عمان، 2017، ص. ص.201-202.

كما يلجأ الإرهاب الإلكتروني إلى استغلال الفضاء السيبراني في التنسيق للهجمات الإلكترونية، والاتصال، والتخفي، ووضع استراتيجيات محكمة، نظرًا لقلة تكاليف الاتصال والتواصل بالرسائل المشفرة عبر شبكة الإنترنت، وكذا سهولة إخفاء الهوية أو تزييفها. ويتم ذلك باستغلال البريد الإلكتروني وغرف الحوار الإلكترونية، في عملية التواصل والدردشة حول التخطيط للعمليات الإرهابية والتدريب عليها.[1]

كذلك تقوم باستغلال تكنولوجيا المعلومات والاتصال، في الحصول على التمويل، سواء بطرق مباشرة من خلال طلب تبرعات من متصفحي مواقع الإرهاب الذين يملكون ميولات إرهابية، أو غير مباشرة من خلال التجارة الإلكترونية، أو كذلك من مصادر مشروعة من خلال منظمات وجمعيات تدَّعي أنها خيرية، أو غير مشروعة من خلال مثلًا تزوير بطاقات الائتمان، والمتاجرة بالمخدرات، أو جرائم تبييض الأموال.[2]

فتلجأ هذه التنظيمات الإرهابية للبريد الإلكتروني لنشر وترويج الأفكار المتطرفة، وكسب المتعاطفين معهم من خلال المراسلات الإلكترونية، كما تقوم بنشر بياناتها الإرهابية من خلال تصميم مواقع خاصة بها في الفضاء الرقمي لغرض التدريب وتعليم آليات القرصنة الإلكترونية، تدمير المواقع والبيانات، وكيفية نشر الفيروسات الخبيثة. لذا نذكر بعض المنصات الإلكترونية العربية التي قامت الجماعات الإرهابية بتصميمها، مثل موقع النداء، ذروة السنام، صوت الجهاد، البتار[3]، أما المواقع الغربية، فنجد منصة المقاومة الإيرانية البيضاء التي أسسها الإرهابي المتطرف توم ميتزجر(Tom Metzger) .[4]

كما تقوم تنظيمات الإرهاب الإلكتروني بالتعبئة وتجنيد الإرهابيين، حيث تنتهج أسلوبًا استعطافيًا وتحفيزيًا حماسيًا عبر المنتديات والمواقع الإلكترونية، لجذب فئة الشباب ذوي الميول الإيديولوجية والمُهتمين بالانخراط في التنظيمات الإرهابية. وهذا ما يساعد على استمرارية هذه التنظيمات لأمدٍ طويل.[5]

---

[1] الفيل علي عدنان، الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقي، بيروت،2011، ص.72.

[2]عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي:(الماهية والجزاء)، منشورات الحلبي الحقوقية، لبنان، 2020، ص. ص.91-92.

[3] بشريف وهيبة، "أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي"، **مجلة الحوار الثقافي**، المجلد7، العدد01، كلية العلوم الاجتماعية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018، ص.65.

[4] محمد الطيب عبد الله خالد، "الإرهاب الالكتروني"، **مجلة كلية الشريعة والقانون**، المجلد13، العدد01، جامعة أم درمان الإسلامية، السودان،2020، ص.104.

[5]امير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية،2011، ص.235.

ثالثا: الإرهاب الإلكتروني جريمة عابرة للحدود

تعتبر هذه الخاصية من أهم سمات جريمة الإرهاب الإلكتروني، باعتبارها جريمة ذات طابع دولي، إذ تتعدى الحدود الجغرافية للدولة[1]، ويعود ذلك إلى طبيعة وسيلة ارتكابها، والمتمثلة في تكنولوجيا الإعلام والاتصال، بحيث تصبح الحدود الإقليمية للجريمة غير مرئية كما هو الحال في الجرائم الإرهابية التقليدية.

لكن هذه الخاصية تثير إشكالية في تحديد القانون الواجب التطبيق، وكذلك الدولة المختصة بالمتابعة القضائية، مما يؤدي إلى تنازع الاختصاص في المتابعة والتحقيق، كما تثير مشكلة احترام سيادة الدولة عند اللجوء إلى استخدام أساليب التحري الخاصة عن الجريمة الإلكترونية.[2]

بالرجوع لنص المادة 3 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، نجد تعريف مصطلح الجريمة العابرة للحدود الوطنية، والتي حددتها في أربع حالات وهي:" **إذا ارتُكبت في أكثر من دولة واحدة - ارتُكب في دولة واحدة ولكن جرى جانب كبير من الإعداد أو التخطيط له أو توجيهه أو الإشراف عليه في دولة أخرى- ارتُكب في دولة واحدة، ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة - ارتُكب في دولة واحدة، ولكن له آثارا شديدة في دولة أخرى.**"

رابعا: صعوبة الإثبات في جريمة الإرهاب الإلكتروني

تختلف جريمة الإرهاب الإلكتروني عن الجرائم التقليدية التي يترك فيها الجاني أدلة وآثارًا مادية في مسرح الجريمة، ويعود ذلك إلى الطبيعة الافتراضية والرقمية لمسرح الجريمة، التي تتيح للمجرمين استخدام تقنيات التشفير والتمويه للهروب من الملاحقة القانونية، كما أن الفضاء المعلوماتي يتيح للجناة استخدام هويات مزيفة أو تقنيات إخفاء الهوية، مما يجعل تعقبهم أمرًا بالغ التعقيد[3]، بالإضافة إلى أن أساليب البحث والتحقيق المتخذة في إطار الجريمة الإلكترونية تختلف عن تلك المتخذة في الجرائم التقليدية.

---

[1] قيراط محمد، مرجع سابق، ص .17.

[2] بن فرحات نور الدين، عمري عبد القادر، " الطابع العابر لمحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي"، **مجلة أبحاث قانونية وسياسية**، المجلد09، العدد01، كلية الحقوق والعلوم السياسية، جامعة الصديق بن يحيى-جيجل، الجزائر،2024، ص.662.

[3] محمد طاهر أحمد رانية، "أثر الذكاء الاصطناعي على الامن الدولي"، **مجلة البحوث المالية والتجارية**، المجلد23، العدد03، كلية التجارة، جامعة بورسعيد، مصر،2022، ص.246.

خامسا: الإرهاب الإلكتروني جريمة تواطؤيه

جريمة الإرهاب الإلكتروني تتم بتعاون أكثر من شخص، سواء من خلال القيام بسلوكيات إيجابية وتقديم تسهيلات في الجانب التقني والمادي، أو من خلال السلوكيات السلبية عبر الالتزام بالصمت لتسهيل إتمام العملية[1] ؛ ويعرف ذلك بمصطلح **"الجماعة الإجرامية المنظمة"**، والتي عرّفتها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية بـ**"جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال الإجرامية وفقًا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى"**.[2]

سادسا: الإرهاب الإلكتروني جريمة لا تقادميه

تُعَدُّ جريمة الإرهاب الإلكتروني نظرا لخصوصيته وتهديده للأمن المعلوماتي للدولة الجزائرية، من الجرائم التي استثناها المشرع الجزائري من قواعد التقادم، إذ ينصّ قانون الإجراءات الجزائية صراحةً على عدم خضوع الدعوى العمومية والدعوى المدنية المترتبة عليها، فضلاً عن العقوبات المقررة في جرائم الإرهاب التقليدية والإلكترونية، لأحكام التقادم.[3]

الفرع الثاني: دو افع جريمة الإرهاب الإلكتروني

لا ترتكب جريمة الإرهاب الإلكتروني من العدم، بل تقف وراءها مجموعة من الدوافع، التي تتنوع بين ما هو شخصي وفكري، وما هو سياسي أو اقتصادي أو حتى اجتماعي. وفهم هذه الدوافع يُعدّ أمرًا ضروريًا، لأنه يساعد على التنبؤ بمخاطر هذا النوع من الجرائم، ويدعم الجهود الوقائية والتشريعية لمواجهتها. فالجناة لا يلجؤون إلى الفضاء الإلكتروني عشوائيًا، بل غالبًا ما يكون ذلك نتيجة ظروف تدفعهم

[1] عبد القادر المومني نهلة، الجرائم المعلوماتية، دار الثقافة، عمان، 2008، ص.58.

[2] المادة 2 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، مرجع سابق.

[3] أنظر المادة 8مكرر والمادة612مكرر من الأمر رقم 66-155 مؤرخ في 8يونيو1966، يتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 48، الصادرة في 10يونيو1966، معدل ومتمم.

لهذا الطريق، معتمدين على البيئة الرقمية التي تسهّل لهم التخفي والتنفيذ دون قيود جغرافية.[1] لذا سيتم التطرق في هذا الفرع لاستعراض الدوافع العامة **(أولا)**، ثم ننتقل إلى الدوافع الخاصة لارتكابها **(ثانيا)**.

أولا: الدو افع العامة لارتكاب جريمة الإرهاب الإلكتروني

تتحدد الدوافع العامة لارتكاب جريمة الإرهاب الإلكتروني في مجموعة من الدوافع الشخصية والفكرية **(1)** بالإضافة إلى الدوافع السياسية، الاقتصادية والاجتماعية **(2)**.

1) الدو افع الشخصية والفكرية لارتكاب جريمة الإرهاب الإلكتروني

غالبًا ما ترتبط الدوافع الشخصية والفكرية لارتكاب جريمة الإرهاب الإلكتروني، بشخصية الجاني أو بعقده النفسية وحالته العائلية، ومن أبرزها الطموح إلى الشهرة والسعي لجذب الأضواء، إلى جانب الفشل والإخفاق في تحقيق أهداف الحياة والفشل العاطفي وعدم الاستقرار العائلي؛ فضلاً عن العُقد النفسية المتمثلة في الشعور بالنقص والظلم والأنانية وانعدام الثقة بالنفس[2]، إضافةً إلى الجهل والخواء الذهني والتفسير الخاطئ للدين والجهل بمقاصد الشريعة الإسلامية، قبل أن يمتد أثرها إلى التطرف الفكري ونقص التأهيل العلمي.[3]

2) الدو افع السياسية والاقتصادية والاجتماعية لارتكاب جريمة الإرهاب الالكتروني

من الدوافع الموضوعية لارتكاب جريمة الإرهاب الإلكتروني نجد الأوضاع السياسية والاقتصادية والاجتماعية، بحيث تتجلّى في الطغيان السياسي والديكتاتورية وكبت الحريات وإسكات الأصوات المعارضة، إضافة إلى الاستبداد بالحكم والتهميش الشعبي وهيمنة السلطة التنفيذية وعجز السلطتين القضائية

[1] حفظاوي سعيد، "ظاهرة الإرهاب:(تعريفها، دوافعها، أشكالها، وأساليبها)"، **مجلة الحقوق والعلوم السياسية**، المجلد09، العد01، جامعة عباس لغرور -خنشلة، الجزائر،2022. ص.547.

[2] كافي مصطفى يوسف، جرائم:(الفساد-غسيل الأموال-السياحة-الإرهاب الإلكتروني-المعلوماتية)، مكتبة المجتمع العربي، عمان، 2013، ص.114.

[3] طارق جواد كاظم الجابري إرساء، جريمة الإرهاب الإلكتروني:(دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، بغداد، 2012، ص.31.

والتشريعية عن أداء مهامهما[1]؛ فضلاً عن الركود الاقتصادي والأزمات المالية التي تعانيها الدولة، وانتشار البطالة والفقر وتفشّي الفساد، ونهب الأموال العامة والتعرض للإذلال الأسري والمجتمعي.[2]

ثانيا: الدو افع الخاصة لارتكاب جريمة الإرهاب الإلكتروني

يلجأ مجرمو الإرهاب الإلكتروني إلى استغلال الفضاء السيبراني لتحقيق أهداف مادية ومعنوية، فضلاً عن التخطيط الدقيق لاستراتيجياتهم الإرهابية وشن الهجمات، وتتجلى دوافعهم لإرتكاب الأفعال الإرهابية في عدة عوامل جوهرية، أولها هشاشة بنية الشبكات المعلوماتية التي تتيح اختراقها بسهولة، ثم انعدام القيود الجغرافية في الفضاء الرقمي، مما يعزز التهديدات الأمنية ويسهل التمويه عن هوية المجرمين، كما تصعب القدرة على رصد وتحديد هوية الفاعل في البيئة الرقمية.

إضافةً إلى ذلك، تمثل سهولة استخدام التكنولوجيا الرقمية وانخفاض تكاليفها المالية عامل جذاب وقوي، يجعل من الفضاء الإلكتروني منصة خصبة وآمنة للتنفيذ الأعمال الإرهابية، خاصة في ظل قصور القوانين الرادعة في معظم دول العالم، وهو ما يفسر تنامي الهجمات الإلكترونية الإرهابية تدريجيا.[3]

بينما تستند هذه العوامل التحفيزية إلى الظروف التقنية والتشريعية، فإن مجرمي الإرهاب الإلكتروني يسعون، في المقابل، إلى تحقيق جملة من الأهداف الإجرامية، من أبرزها: إثارة الرعب وزعزعة الاستقرار ونشر الهلع داخل المجتمع[4]؛ تهديد الهيئات الحكومية والكيانات الدولية[5]؛ وإرباك النظام العام وعرقلة سير الحياة وشلّ المرافق العامة[6]؛ بالإضافة إلى تدمير البنى التحتية وزعزعة الأمن السيبراني، وشنّ هجماتٍ إلكترونية للعبث بالبيانات والمعلومات؛ والحصول على أسرار الدولة عبر التجسس الإلكتروني[7]

---

[1] حفظاوي سعيد، مرجع سابق، ص.546.

[2] سليمي فاطمة الزهراء،" الأسباب الاجتماعية لانتشار ظاهرة الإرهاب:(دراسة سوسيو-تاريخية لبعض العمليات الإرهابية)، **مجلة آفاق لانتشار ظاهرة الإرهاب**، المجلد12، العدد01، دار جامعة نايف، جامعة نايف العربية للعلوم الأمنية،2020، ص. ص.259-261.

[3] طارق جمعة مهدي، مرجع سابق، ص. ص. 73-74.

[4] خالد حسن، أحمد لطفي، الإرهاب الإلكتروني:(آفة العصر الحديث والآليات القانونية للمواجهة)، دار الفكر الجامعي، الإسكندرية، 2018، ص.53.

[5] امير فرج يوسف، مرجع سابق، ص.218.

[6] العبيدي عمر عباس خضير، الإرهاب الإلكتروني في نطاق القانون الدولي، المركز العربي، القاهرة،2021، ص.27.

[7] مشتاق طلب فاضل، استبرق فاضل شعير،" مواقع التواصل والإرهاب في العصر الرقمي (الإرهاب الالكتروني)"، **مجلة القانون والعلوم السياسية**، المجلد13، العدد1، كلية العلوم السياسية، جامعة النهرين، بغداد، 2024، ص.217.

فضلاً عن التحريض على التمرد والعصيان، وتحقيق مكاسب مالية ضخمة غير مشروعة، بل وارتكاب جرائم قتل والاغتيال ضد كبار شخصيات الدولة ورعاياه.[1]

كما يسعى الإرهاب الإلكتروني إلى استهداف المنشآت العسكرية للدولة من خلال إختراق المنظومة الدفاعية العسكرية الإلكترونية، والوحدات الصاروخية النووية والقيام بتحطيم الشفرات السرية، والعبث بأنظمة تشغيلها؛ كما يقوم الإرهاب الإلكتروني بشّن هجومات إلكترونية على محطات توليد المياه والطاقة، لإرباك مجريات الحياة وتجميد الحركة وإيقاظ الفوضى؛ بالإضافة إلى ضرب الشبكات السيبرانية للمواصلات والاتصالات وتعطيل محطات توزيع الاتصالات الهاتفية، والاستحواذ على التحكم بمسارات الملاحة الجوية والبرية والبحرية من خلال تعطيل محطات توزيع الاتصالات الهاتفية والتحكم بمساراتهـا.[2]

المبحث الثاني: البنيان القانوني لجريمة الإرهاب الإلكتروني في القانون الجزائري

تعتبر جريمة الإرهاب الإلكتروني من الجرائم العصرية التي عرفت انتشارًا في العصر الحالي، بفعل الثورة الرقمية وتوسع استخدام وسائل الاتصال الحديثة، ونظرًا لاستغلال الشبكة المعلوماتية كأداة لتنفيذ جرائم الإرهاب من طرف المنظمات الإرهابية، لترويج للأفكار المتطرفة، وارتكاب الأفعال الإرهابية، برزت حاجة الدولة الجزائرية إلى التدخل لوضع حد لهذه الممارسات[3]، وردع كل من يستهدف الإخلال بأمنها.

من هذا المنطلق، تدخل المشرّع الجزائري ليُدرج جريمة الإرهاب الإلكتروني ضمن نصوص قانون العقوبات، ليس فقط من خلال تحديد أركانها وطبيعتها، وإنما أيضًا بوضع عقوبات صارمة تتماشى مع تعقيدها وتعدد أشكالها، وسعيًا لفهم النموذج القانوني الذي اعتمده المشرّع الجزائري في التعامل معهـا.

سنتطرق في هذا المبحث الثاني إلى جانبين أساسيين وفقا لتقسيم المنهجي التالي: أركان جريمة الإرهاب الإلكتروني **(المطلب الأول)**، بحيث سنحدد الأركان القانونية التالية-الركن الشرعي، والمادي،

[1] سليماني مباركة، "الإرهاب الالكتروني وطرق مكافحته"، **مجلة الحقوق والعلوم السياسية**، المجلد04، العدد08، جامعة عباس لغرور - خنشلة، الجزائر،2017، ص.345.

[2] شعنبي صابرة، الجهود الدولية في مكافحة الإرهاب الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي-تبسة، الجزائر، 2019، ص. ص. 60-61.

[3] مشتاق طلب فاضل، استبرق فاضل شعير، مرجع سابق، ص.202.

والمعنوي-، ثم الأحكام الجزائية لجريمة الإرهاب الإلكتروني **(المطلب الثاني)**، مع بيان أنواع العقوبات، ومسألة الشروع والمساهمة فيها، وكذا الأعذار القانونية والظروف التي تؤثر في تشديد وتخفيف العقوبة.

المطلب الأول: أركان جريمة الإرهاب الإلكتروني

جريمة الإرهاب الإلكتروني، وإن كانت حديثة من حيث الوسائل والأدوات المستخدمة في الإعداد والتخطيط لها وارتكابها، إلا أنها تخضع لنفس القواعد العامة التي يقوم عليها التجريم في القانون الجنائي. وهذا يعني أن المشرّع الجزائري لا يكتفي بوصف الفعل على أنه خطير، بل يشترط أن تتوفر فيه مجموعة من الأركان القانونية المحددة، حتى يُعتبر الإرهاب الإلكتروني جريمة يعاقب عليها قانون العقوبات الجزائري.

تُعد هذه الأركان الثلاثة بمثابة الركيزة الأساسية التي يبني عليه المشرّع الجزائري تجريمه للسلوك الإجرامي، وتتمثل في: الركن الشرعي **(الفرع الأول)** أي النص القانوني الذي يُجرّم الفعل، والركن المادي **(الفرع الثاني)**، الذي يشمل السلوك المجرّم والنتائج المترتبة عليه والعلاقة بينهما، والركن المعنوي **(الفرع الثالث)** الذي يتعلق بنية الفاعل ووعيه أثناء ارتكاب الجريمة، ويشمل القصد الجنائي العام والخاص.

الفرع الأول: الركن الشرعي لجريمة الإرهاب الإلكتروني

يعرف الركن الشرعي بأنه " **التكييف القانوني الذي يُلحق بالسلوك ويصفه بعدم المشروعية**"[1]، وتنص المادة الأولى من قانون العقوبات على: **"لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"**، باعتبار جريمة الإرهاب الإلكتروني من الجرائم، أو الجنايات ضد أمن الدولة، نجد أن المشرع الجزائري تطرق لأحكامها بموجب القانون رقم 16-02 المعدل للأمر 66-156 المتضمن قانون العقوبات، وذلك في القسم الرابع مكرر من الفصل الأول من الباب الأول من الكتاب الثالث بعنوان **"الجرائم الموصوفة بأفعال إرهابية وتخريبية"**.

بحيث يضمن قانون العقوبات أحكامًا جديدة تناولت جريمة الإرهاب الإلكتروني، والذي حدد الأفعال المجرمة والجزاءات المقررة لهذه الظاهرة الإجرامية، ويظهر ذلك في مجموعة من النصوص القانونية والمتمثلة في: نص المادة 87مكرر4 من قانون العقوبات، التي تنص على مايلي:**" يعاقب بالسجن المؤقت من**

[1] بوعلي سعيد، شرح قانون العقوبات الجزائري: (القسم العام)، الطبعة الرابعة، دار بلقيس، الجزائر، 2021، ص.63.

خمس (5) سنوات إلى عشر (10) سنوات وبغرامة مالية من 100.000دج إلى 500.000دج، كل من يشيد بالأفعال المذكورة في المادة 87مكرر أعلاه أو يشجعها أو يمولها بأية وسيلة كانت".

المادة 87 مكرر 11 من قانون العقوبات، التي تنص على ما يلي:**"يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر سنوات (10) سنوات وبغرامة من 100.000دج إلى 500.000دج، كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها. يعاقب بنفس العقوبة كل من:**

- يوفر أو يجمع عمدا أموالا بأي وسيلة وبصورة مباشرة أو غير مباشرة، بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض ارتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة،

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

- يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة".

تنص المادة 87مكرر12 من قانون العقوبات على ما يلي:**" يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000دج إلى500.000دج، كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هذا القسم، أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة".**[1]

كما تمم المشرع الجزائري قانون العقوبات بالمادة 87مكرر15 بموجب القـــانون رقم 24-06 التي تنص على ما يلي: "**يعاقب بالسجن المؤقت من عشر (10) سنوات إلى (20) سنة وبغرامة من 1.000.000دج إلى 2.000.000دج، كل من يمول انتشار أسلحة الدمار الشامل. يقصد بتمويل أسلحة**

[1] قانون رقم 16-02 مؤرخ في 19يونيو2016، ج.ر.ج.ج عدد37، صادرة في 22يونيو2016، المعدل والمتمم للأمر رقم66-156 مؤرخ في 8يونيو1966، يتضمن قانون العقوبات، ج.ر.ج.ج عدد49، صادرة في 11جوان1966.

الدمار الشامل، أي عمل يقوم به أشخاص طبيعيون أو كيانات من خلال توفير أو جمع الأموال بقصد استخدامها، كليا أو جزئيا، في حمل أي شخص أو تشجيعه أو حثه، بأي وسيلة كانت، بصورة مباشرة أو غير مباشرة، غير مشروعة أو عن قصد، على ارتكاب أفعال انتشار أسلحة الدمار الشامل".[1]

في نفس السياق، نجد أيضا نص المادة 1/2 من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، قد أشارت إلى مفهوم الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، حيث حددت أنها تشمل **"... أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية..."**، وبتالي يمكن إدراج ضمن هذا التعريف جريمة الإرهاب الإلكتروني.

من خلال استقراء نصوص المواد أعلاه، يتضح أن المشرع الجزائري قد اعتبر استغلال تكنولوجيا الإعلام والاتصال في ارتكاب الأعمال الإرهابية الواردة في هذه المواد، وفي تلك الواردة في المادة 87مكرر من قانون العقوبات، جريمة معاقبًا عليها قانونًا بنص صريح، وذلك تطبيقًا لمبدأ شرعية الجرائم والعقوبات.

الفرع الثاني: الركن المادي لجريمة الإرهاب الإلكتروني

يتكون الركن المادي لجريمة الإرهاب الالكتروني من ثلاث عناصر أساسية، أولها السلوك الإجرامي وهو إما أن يكون سلوك إيجابي أو سلبي يقوم به الجاني في الجريمة **(أولا)**، النتيجة الإجرامية الناتجة عن سلوك الإجرامي للجاني **(ثانيا)**، والعلاقة السببية التي تربط بين سلوك الجاني والنتيجة الإجرامية**(ثالثا)**.

أولا: السلوك الإجرامي في جريمة الإرهاب الالكتروني

السلوك الإجرامي هو النشاط المادي الخارجي للجريمة، وقد يكون في صورة إيجابية في شكل حركة إرادية حرة يأتيها الفاعل باستخدام أعضاء جسده، وقد تكون سلبية في صورة الامتناع عن القيام بعمل يفرضه القانون[2]؛ وفي سياق جريمة الإرهاب الإلكتروني، يتجسد السلوك الإجرامي في مجموعة من الأفعال الإيجابية المتعددة التي حددها المشرع الجزائري، في نصوص المواد 87مكرر4، 87 مكرر 11 ،87 مكر12و 87مكرر15من قانون العقوبات، وتتمثل هذه الأفعال فيما يلي:

[1] قانون رقم 24-06 مؤرخ في 28أبريل 2024، ج.ر.ج.ج عدد30، صادرة في30أبريل2024، المعدل والمتمم للأمر رقم66-156 مؤرخ في 8يونيو1966، يتضمن قانون العقوبات، ج.ر.ج.ج عدد49، صادرة في 11جوان1966.

[2] بوعلي سعيد، مرجع سابق، ص.135.

1) السفر: هو السلوك الإجرامي المحدد في المادة 87 مكرر 11 من قانون العقوبات على النحو التالي: "...**كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى...**". ويُفهم من نص المادة أعلاه، أن المشرع الجزائري قد وسّع من نطاق تجريم الإرهاب الإلكتروني ليشمل كل شخص، سواء كان مواطنًا جزائريًا، يحمل الجنسية الجزائرية، أو كان شخصًا أجنبيًا، وسواء كان مقيمًا بطريقة شرعية أو غير شرعية في الإقليم الجزائري، والذي يقوم بالسفر -أي يغادر الإقليم الجمركي للدولة أو يدخل إليه- بغرض ارتكاب الأفعال الإرهابية، أو التحضير لها، أو التدبير لها، أو المشاركة فيها، أو حتى مجرد تلقي تدريب شخصي حول كيفية ارتكابها، أو تدريب الغير على إرتكاب هذه الأفعال.

كما أن المشرع الجزائري جرم أيضًا كل من **يُحاول** السفر شخصيا لإرتكاب الأفعال الإرهابية، ويقصد بالمحاولة هنا بالشروع، الذي عرفته المادة 30من قانون العقوبات، كما يشمل التجريم أيضًا كل شخص يقوم بتنظيم سفر أشخاص أخرين أو يوفر تسهيلات لسفرهم، وهي أفعال تدخل في نطاق الأعمال التحضيرية للجريمة، والتي في الأصل لا يعاقب عليها القانون، إلا أن خصوصية جريمة الإرهاب الإلكتروني باعتبارها جريمة تمس بأمن الدولة، دفعت المشرع الجزائري إلى توسيع نطاق التجريم، ليشمل جميع الأفعال السابقة لارتكاب السلوك الإجرامي، حتى وإن لم يُستنفذ هذا السلوك بشكل كامل.

يُستفاد كذلك من نص المادة 87 مكرر 11 من قانون العقوبات، أن المشرع الجزائري لم يُجرّم السفر لمجرد كونه فعلًا قائمًا بذاته، وإنما باعتباره نشاطًا يستهدف تحقيق غاية إجرامية، وهي: "...**لغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها**".

كما تجدر الإشارة إلى أن المشرع الجزائري ذكر في الفقرة الأخيرة من نص المادة 87 مكرر 11 من قانون العقوبات، الوسيلة المستخدمة في ارتكاب السلوك الإجرامي؛ وهذه الوسيلة ليست مجرد أداة لتنفيذ الجريمة، بل هي العنصر المميز الذي يضفي نوعًا من الخصوصية والتمييز على جريمة الإرهاب الإلكتروني، مما يجعلها تختلف عن الجرائم التقليدية، وتتمثل هذه الوسيلة في تكنولوجيا الإعلام والاتصال، كما هو مبين في النص التالي: "...**يستخدم تكنولوجيا الإعلام والاتصال لارتكاب الأفعال المذكورة في هذه المادة**".[1]

نجد تعريف تكنولوجيا الإعلام والإتصال في القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، أو ما يُصطلح عليه كذلك بالإنترنت، في المادة 10 منه، على النحو

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

التالي: "**شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية و إقليمية وخاصة، موصولة فيما بينها عن طريق برتوكول الاتصال IP وتعمل معا بهدف تقديم واجهة موحدة لمستعمليها**".[1]

2) **التمويل:** وهو النشاط الإجرامي المحدد في نص المادة 87 مكرر 11 من قانون العقوبات، والتي حددته في الأفعال التالية: "**... يوفر أو يجمع عمدًا أموالًا بأي وسيلة وبصورة مباشرة أو غير مباشرة...**". ويقصد بالأموال، وفقًا للتعريف المحدد في نص المادة 4 من القانون المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب، "**أي نوع من الممتلكات أو الأموال من أي طبيعة كانت، بما فيها الموارد الاقتصادية والقيم المالية الافتراضية، المادية أو غير المادية، المنقولة أو غير المنقولة، الملموسة أو غير الملموسة...**".[2]

يمكن تعريف التمويل على أنه عملية جمع الأموال بأي وسيلة كانت، بما في ذلك استخدام تكنولوجيا الإعلام والاتصال، سواء كانت بطريقة مباشرة، مثل طلب الدعم المالي من الفئة الداعمة للجماعات الإرهابية، أو بطريقة غير مباشرة. كما قد تكون هذه الأموال متحصلة من أنشطة مشروعة، مثل الجمعيات الخيرية، أو غير مشروعة، مثل الجرائم، ويتم تخصيصها لفائدة منظمة إرهابية[3]، أو تقديمها لشخص إرهابي بغرض السفر إلى دولة أخرى لارتكاب أفعال إرهابية أو تدبيرها، أو الإعداد لها، أو المشاركة فيها، أو التدريب على ارتكابها، أو لتلقي تدريب عليها، وذلك وفقًا للمادة 87 مكرر 11 /3 من قانون العقوبات.

كذلك أشار المشرع الجزائري في المادة 87 مكرر 15 من قانون العقوبات، إلى تجريم تمويل انتشار أسلحة الدمار الشامل بأي وسيلة كانت. وبناءً على ذلك، يمكن إدراج ضمن هذه الوسائل تكنولوجيا الإعلام والاتصال. ويُقصد بأسلحة الدمار الشامل الأسلحة النووية أو الكيميائية أو التكسينية أو البكتريولوجية....

كما أكدت المادة 87 مكرر 15 من قانون العقوبات، على تجريم، كل شخص سواء طبيعي أو معنوي يقوم بحمل أي شخص أخر أو تحريضه أو حثه بأي وسيلة كانت، بما في ذلك باستعمال تكنولوجيا الإعلام والاتصال، على ارتكاب أفعال تتعلق بنشر أسلحة الدمار الشامل لأغراض إرهابية، وذلك على النحو

[1] قانون رقم 18-04، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، مرجع سابق.

[2] قانون رقم 05-01 مؤرخ في 6فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج.ر.ج.ج عدد11، الصادرة في 9فبراير2005، معدل ومتمم.

[3] سي ناصر مراد، قريبيز محمد، "مكافحة جريمة تمويل الإرهاب في التشريع الجزائري"، **مجلة العلوم الإنسانية**، المجلد31، العدد1، جامعة منتوري -قسنطينة، الجزائر،2020، ص.97.

التالي:"... **حمل أي شخص أو تشجيعه أو حثه، بأي وسيلة كانت، بصورة مباشرة أو غير مباشرة، غير مشروعة أو عن قصد، على ارتكاب أفعال انتشار أسلحة الدمار الشامل**".

3) التجنيد الإلكتروني: وهو النشاط الإجرامي المحدد في نص المادة87مكرر12 من قانون العقوبات على النحو التالي" **كل من يستخدم تكنولوجيا الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة...**".

في ذات السياق، قدمت المادة 4 من القانون المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب تعريفًا لمصطلحي "إرهابي "و"منظمة إرهابية" على النحو التالي:

"**الإرهابي: هو أي شخص: - يرتكب أو يحاول ارتكاب أفعال إرهابية بأي وسيلة كانت، مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادة الفاعل، -يساهم كشريك في أفعال إرهابية، -ينظم أو يأمر أشخاصا آخرين بارتكاب أفعال إرهابية، - يشارك في قيام مجموعة من الأشخاص تعمل بقصد مشترك بارتكاب أفعال إرهابية وتكون هذه المشاركة بهدف تنفيذ نشاط إرهابي مع العلم بنو ايا المجموعة بارتكاب الفعل الإرهابي.**

منظمة إرهابية: كل مجموعة إرهابية: -ترتكب أو تحاول ارتكاب أفعال إرهابية بأي وسائل كانت، مباشرة أو غير مباشرة، وبشكل غير مشروع وبإرادة الفاعلين، -المساهمة كشركاء في أفعال إرهابية، -تنظم أو تأمر أشخاصا آخرين بارتكاب أفعال إرهابية، -تشارك في قيام مجموعة من الأشخاص تعمل بقصد مشترك بارتكاب أفعال إرهابية وتكون هذه المشاركة بهدف تنفيذ نشاط إرهابي مع العلم بنو ايا المجموعة بارتكاب الفعل الإرهابي".[1]

يُقصد بالتجنيد الإلكتروني، العملية التي يتم من خلالها استغلال تكنولوجيا الاعلام والاتصال لانتقاء وتطوير الكوادر، للقيام بالأدوار المحددة في التنظيمات الإرهابية، سواءً كمقاتلين أو فنيين أو تقنيين، وغير ذلك من المناصب.[2]أو بمفهوم آخر، هو استخدام الشبكة المعلوماتية لنشر الإيديولوجية الإرهابية المتطرفة، بهدف تكوين قاعدة من الإرهابيين الجدد، ضمن الفئات التي لديها ميولا ورغبة في

[1] قانون رقم 05-01، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، مرجع سابق.

[2] زاوي رابح، "الإعلام الأمني في مواجهة ظاهرة التجنيد الإلكتروني للتنظيمات المتطرفة"، **مجلة الآفاق للأبحاث السياسية والقانونية**، المجلد2، العدد4، قسم العلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر،2019، ص.39.

الانخراط للمنظمات الإرهابية وتجنيدهم[1]، لغرض ارتكاب الأفعال الإرهابية، أو تنظيم شؤونها أو دعم أعمالها، والإشادة بأنشطتها الإجرامية، أو نشر أفكارها بصورة مباشرة أو غير مباشرة لتعميم التطرف.

4) **الإشادة:** جرَّم المشرع الجزائري في نص المادة 87مكرر4 من قانون العقوبات، كل شخص يقوم بالإشادة والتعظيم أو التشجيع بالاستعمال تكنولوجيا الاعلام والاتصال الأفعال الإرهابية، على النحو التالي:"**... كل من يشيد بالأفعال المذكورة في المادة 87مكرر أعلاه أو يشجعها أو يمولها بأية وسيلة كانت**".

إذ حرص المشرع الجزائري على تحديد مفهوم الأفعال الإرهابية بدقة في نص المادة 87مكرر من قانون العقوبات، والتي تشمل الأفعال التالية: "**يعتبر فعلا إرهابيا أو تخريبا، كل من يستهدف أمن الدولة والوحدة الوطنية واستقرار المؤسسات وسيرها العادي، عن طريق أي عمل غرضه ما يأتي: - بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي أو الجسدي على الأشخاص أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو المس بممتلكاتهم، - عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية، - الاعتداء على رموز الأمة والجمهورية ونبش أو تدنيس القبور، - الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني، - الاعتداء على المحيط أو إدخال مادة سامة أو تسريبها في الجو أو في باطن الأرض أو إلقائها عليها أو في المياه الإقليمية من شأنها جعل صحة الإنسان أو الحيوان أو البيئة الطبيعية في خطر، - عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام، - عرقلة سير المؤسسات العمومية أو الاعتداء على حياة أعوانها أو ممتلكاتهم أو عرقلة تطبيق القوانين والتنظيمات، - تحويل الطائرات أو السفن أو أي وسيلة أخرى من وسائل النقل، - إتلاف منشآت الملاحة الجوية أو البحرية أو البرية، - تخريب أو إتلاف وسائل الاتصال، - احتجاز الرهائن، - الاعتداءات باستعمال المتفجرات أو المواد البيولوجية أو الكيميائية أو النووية أو المشعة أو غيرها من أسلحة الدمار الشامل، - تمويل إرهابي أو منظمة إرهابية، - السعي بأي وسيلة للوصول إلى السلطة أو تغيير نظام الحكم بغير الطرق الدستورية، أو التحريض على ذلك، - المساس بأي وسيلة بالسلامة الترابية أو التحريض على ذلك**".[2]

[1] عبد الجليل إسماعيل حسن الشيخ زيني، مرجع سابق، ص.111.

[2] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

ثانيا: النتيجة الإجرامية في جريمة الإرهاب الإلكتروني

النتيجة الإجرامية هي الأثر المترتب على السلوك الإجرامي للجاني، ومن خلال تحليل نصوص المواد87مكرر4، 87مكرر11و87مكرر12 و87مكرر15 من قانون العقوبات، يُلاحظ أن المشرع الجزائري انتهج سياسة جنائية معاصرة تركز على التجريم الوقائي لجريمة الإرهاب الإلكتروني.

فقد اعتبر المشرع مجرد استخدام تكنولوجيا الاعلام والاتصال لأغراض إرهابية، جريمة معاقب عليها، باعتبارها من جرائم الخطر التي يكفي فيها احتمال وقوع ضرر يهدد المصالح المحمية قانونا، حتى وإن لم يتحقق هذا الضرر فعليًا.[1] بناءَ على ذلك، فإن جريمة الإرهاب الإلكتروني نظرًا لتهديدها ومساسها بأمن الدولة، تُعد جريمة شكلية، بحيث يكفي لقيامها إتيان السلوك الإجرامي من سفر أو تمويل أو تجنيد أو إشادة باستخدام تكنولوجيا الإعلام والاتصال لأغراض إرهابية، دون شرط تحقق أي نتيجة إجرامية.[2]

ثالثا: العلاقة السببية في جريمة الإرهاب الإلكتروني

يقصد بالعلاقة السببية الرابطة الموجودة بين السلوك الإجرامي والنتيجة الإجرامية، وبعبارة أخرى يشترط توفر العلاقة السببية بين النشاط الإجرامي للجاني والنتيجة الإجرامية، بحيث إذا تم رَّد هذه الأخيرة إلى عامل أخر من غير سلوك الجاني تنعدم العلاقة السببية[3]، لكن، نظرًا لكون جريمة الإرهاب الإلكتروني من الجرائم الشكلية التي لا تتطلب تحقق نتيجة إجرامية، فإنه لا محل للبحث عن العلاقة السببية فيها.

الفرع الثالث: الركن المعنوي في جريمة الإرهاب الإلكتروني

لا يكتمل البنيان القانوني لجريمة الإرهاب الإلكتروني، إلا بوجود الركن المعنوي إلى جانب الركن المادي. وما يُلاحظ من خلال نصوص المواد87مكرر4، و87 مكرر 11، و87 مكرر 12 و87 مكرر 15 من قانون العقوبات، أن جريمة الإرهاب الإلكتروني هي جريمة عمدية، حيث أكد المشرع الجزائري صراحةً على عنصر العمد من خلال استخدامه لمصطلح "عمدًا" في نص المادة 87 مكرر 11 على النحو التالي: "**يوفر أو يجمع**

---

[1] سوماتي شريفة،" التجريم الوقائي في السياسة الجزائية المعاصرة"، **مجلة صوت القانون**، المجلد6، العدد02، مخبر نظام الحالة المدنية، جامعة خميس مليانة، الجزائر،2019، ص.1207.

[2] مزياني عمار،" الجرائم المادية والمسؤولية الجنائية"، **المجلة الجزائرية للحقوق والعلوم السياسية**، المجلد07، العدد02، كلية الحقوق، جامعة أحمد بن يحي الونشريسي-تسمسيلت، الجزائر،2022، ص.20.

[3] خلفي عبد الرحمان، محاضرات في القانون الجنائي العام، دار الهدى، عين مليلة-الجزائر،2012، ص. ص. 105- 106.

عمدًا أموالًا..."، وكذلك **"قام عمدًا بتمويل أو تنظيم سفر..."**، ولقيام هذه الجريمة يشترط توفر القصد الجنائي العام**(أولا)** إلى جانب القصد الجنائي الخاص**(ثانيا)** لاكتمال قيام أركان جريمة الإرهاب الإلكتروني.

أولا: القصد الجنائي العام في جريمة الإرهاب الإلكتروني

يقوم القصد الجنائي العام بتوفر عنصرين، وهما العلم والإرادة، فقد عرفه الفقه على أنه:" **العلم بعناصر الجريمة وإرادة ارتكابها**"[1]، والعلم هو علم الجاني بالقانون حيث لا يعذر بجهل القانون، وكذا العلم بالوقائع المكونة للجريمة، أما الإرادة هي سلوك يتم عن قصد وإدراك بهدف تحقيق غاية محددة.[2] فلقيام جريمة الإرهاب الإلكتروني، استوجب المشرع الجزائري أن يكون الجاني على علم بأن استخدام تكنولوجيا الإعلام والاتصال في السفر أو التمويل أو الإشادة أو التجنيد لأغراض إرهابية يعتبر جريمة معاقب عليها قانونًا، مع اتجاه إرادته إلى ارتكاب هذا السلوك الإجرامي.

ثانيا: القصد الجنائي الخاص في جريمة الإرهاب الإلكتروني

القصد الجنائي الخاص هو تلك الغاية التي يسعى الجاني لتحقيقها من خلال ارتكابه للسلوك الإجرامي[3]، وقد أشار المشرع الجزائري إلى هذا القصد الخاص في نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات، حيث يتمثل في استخدام تكنولوجيا الإعلام والاتصال لغرض ارتكاب أو تدبير أو الإعداد أو المشاركة أو التدريب أو دعم أو تنظيم الأفعال الإرهابية، التي تم تحديدها بدقة في نص المادة 87 مكرر من قانون العقوبات.

المطلب الثاني: الأحكام الجزائية لجريمة الإرهاب الإلكتروني

تعرف العقوبة على أنها "**أي رد فعل من القانون على انتهاك سيادة القانون**" [4]، أو "**الجزاء الذي يُقرره القانون ويُوقعه القاضي على من ثبتت مسؤوليته عن فعل يُعتبر جريمة في القانون**"[5]، وجريمة

---

[1] المرجع نفسه، ص.151.

[2] بوعلي سعيد، مرجع سابق، ص.181.

[3] المرجع نفسه، ص.183.

[4] **HOUNHAGI B**EL Dora Carrol, Sanction pénale et sanctions ayant le caractère d'une punition, Thèse pour l'obtention du titre de Docteur en droit, droit, Ecole Doctorale des Sciences Economiques, Juridiques, Politiques et de Gestion Centre Michel de L'Hospital, Université Clermont Auvergne, France, 2022, p.3.

[5] بودور رضوان، الجزاء الجنائي، مذكرة لنيل شهادة الماجستير، تخصص: القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر، الجزائر، 2001، ص.31.

الإرهاب الإلكتروني، لما لها من خطورة وتهديد لدولة الجزائرية، لم يغفل عليها التشريع الجزائري، بل تم التعامل معها بصرامة من خلال وضع نظام عقابي خاص، يتماشى مع طبيعتها كجريمة إلكترونية متطورة تتجاوز الحدود الإقليمية، وتستهدف زعزعة الأمن العام والوحدة الوطنية واستقرار مؤسسات الدولة.

كما خصصّ المشرّع الجزائري، مجموعة من القواعد القانونية التي تحدد العقوبات المناسبة لكل من يقوم بارتكاب هذه الجريمة، سواء كان شخصًا طبيعيًا أو معنويًا، كما لم يغفل المشرع عن حالات الشروع والمساهمة، وكذلك الظروف التي قد تؤثر في تخفيف أو تشديد العقوبة، أو حتى الإعفاء منها في بعض الحالات. وسيتم دراسة هذا المطلب وفق التقسيم المنهجي التالي: العقوبات المقررة لجريمة الإرهاب الإلكتروني **(الفرع الأول)** ثم ننتقل لنظرية الظروف في جريمة الإرهاب الإلكتروني **(الفرع الثاني).**

الفرع الأول: العقوبات المقررة لجريمة الإرهاب الإلكتروني

إعتمد المشرع الجزائري سياسة جنائية حديثة، تعتمد على إقرار مبدأ مساءلة كل شخص يقوم باستخدام تكنولوجيا الإعلام والاتصال لارتكاب الأفعال الإرهابية، سواء كان شخصًا طبيعيًا أو معنويًا على حد السواء. وقد أكد المشرع الجزائري هذا المبدأ، بحيث يُعاقب مرتكب جريمة الإرهاب الإلكتروني بغض النظر عن كونه شخصًا طبيعيًا **(أولًا)** أو معنويًا **(ثانيًا)** أو مساهماً في جريمة الإرهاب الإلكتروني**(ثالثا)**.

أولا: العقوبات المقررة للشخص الطبيعي في جريمة الإرهاب الإلكتروني

تلحق بالشخص الطبيعي المتورط في ارتكاب جريمة الإرهاب الإلكتروني عقوبات ردعية صارمة، وتشمل هذه العقوبات كل من: العقوبات السالبة للحرية وكذا الغرامات المالية وهذا ما يصطلح بالعقوبات الأصلية **(1)** كما قد تُفرض إلى جانبها عقوبات تكميلية **(2)** والتي تهدف إلى تعزيز الردع العام والخاص.

1) العقوبات الأصلية المقررة للشخص الطبيعي في جريمة الإرهاب الإلكتروني

تعرف العقوبات الأصلية، على أنها العقوبات التي يجوز الحكم بها على نحو منفرد دون إرفاقها بعقوبات أخرى، ومن خلال استقراء نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 من قانون العقوبات، نجد أن المشرع الجزائري قد فرض عقوبة السجن المؤقت من خمس (5) سنوات إلى عشر (10)

سنوات، وبغرامة تتراوح بين 100.000 دج و500.000 دج على النشاط الإجرامي المتمثل في السفر، التمويل، الإشادة والتجنيد لأغراض إرهابية باستخدام تكنولوجيا الإعلام والاتصال.

كما أقر المشرع الجزائري في نص المادة 87 مكرر 15 من قانون العقوبات عقوبة السجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة، وبغرامة تتراوح بين 1.000.000 دج و2.000.000 دج، على من يقوم باستخدام تكنولوجيا الإعلام والاتصال لتمويل أسلحة الدمار الشامل[1].

2) العقوبات التكميلية المقررة للشخص الطبيعي في جريمة الإرهاب الإلكتروني

العقوبات التكميلية، هي تلك العقوبات التي لا يجوز الحكم بها بصورة مستقلة عن العقوبة الأصلية، فيما عدا الحالات التي ينص عليها القانون صراحة. وهي إما أن تكون ملزمة للقاضي أو إختيارية.

لا توجد إشارة للعقوبات التكميلية في نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات، حيث اقتصرت هذه النصوص على ذكر العقوبات الأصلية دون التكميلية؛ في المقابل، نجد أن نص المادة 87 مكرر 17 من قانون العقوبات قد أشار إلى عقوبة مصادرة الأموال والعائدات كعقوبة تكميلية إجبارية، حيث جاء النص كتالي: **"تأمر الجهة القضائية المختصة بمصادرة الأموال والعائدات الناتجة عن الجرائم المنصوص عليها في هذا القسم..."**.

كما أشار المشرع الجزائري في المادة 394 مكرر 6 من قانون العقوبات، إلى عقوبات تكميلية في حال المساس بأنظمة المعالجة الآلية للمعطيات التابعة للدولة، على النحو التالي: **"...يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة، مع إغلاق المواقع التي تكون محلاً للجريمة من الجرائم المعاقب عليها وفقاً لهذا القسم. علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه"**.[2] لكن هذا لا يمنع القاضي من الحكم بالعقوبات التكميلية الأخرى المقررة في المادة 9 وما يليها من قانون العقوبات نظرا لكونها اختيارية وتخضع لسلطته التقديرية.

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

[2] أمر رقم66-156، يتضمن قانون العقوبات، المرجع نفسه.

كما أشار المشرع الجزائري في نص المادة 87مكرر9 من قانون العقوبات إلى أن الجرائم الموصوفة بأفعال إرهابية وتخريبية، وهي تلك المنصوص عليها من المادة87مكرر إلى غاية المادة 87مكرر18من قانون العقوبات، تطبق عليها أحكام المادة 60مكرر من قانون العقوبات، حيث تنص المادة 60مكرر على ما يلي:

"يقصد بالفترة الأمنية، حرمان المحكوم عليه من تدابير التوقيف المؤقت لتطبيق العقوبة، والوضع في الورشات الخارجية أو البيئة المفتوحة، وإجازات الخروج، والحرية النصفية والإفراج المشروط للمدة المعينة في هذه المادة أو للفترة التي تحددها الجهة القضائية. وتطبق في حالة الحكم بعقوبة سالبة للحرية مدتها تساوي عشر (10) سنوات أو تزيد عنها بالنسبة للجرائم التي ورد فيها نص صراحة على الفترة الأمنية. تساوي مدة الفترة الأمنية نصف (2/1) مدة العقوبة المحكوم بها...".[1]

بالتالي، يمكن القول إن الفترة الأمنية هي بمثابة فترة اختبار تُقدر مدتها بنصف مدة العقوبة المحكوم بها، والتي تفرض على المحكوم عليه بعقوبة سالبة للحرية تساوي أو تزيد مدتها عن عشر (10) سنوات. وتتمثل هذه الفترة في حرمان المحكوم عليه من مجموعة من التدابير المنصوص عليها في قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين.

ثانيا: العقوبات المقررة لشخص المعنوي في جريمة الإرهاب الإلكتروني

يُعرف الشخص المعنوي، بالكيان الذي يتكون من مجموعة من الأشخاص والأموال ويسعى لتحقيق هدف معين، ويتميز بالذمة المالية المستقلة والأهلية القانونية، ومعترف له بالشخصية القانونية.[2] **وقد** اعترفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بالمسؤولية الجنائية للأشخاص الطبيعية والمعنوية الذين يرتكبون جريمة الإرهاب الالكتروني، في المادة20 منها: " **تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لمصلحتها، دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيًا**".[3]

---

[1] أنظر المادة 9 والمادة 60مكرر والمادة 87مكرر9 من الأمر رقم66-156، يتضمن قانون العقوبات، المرجع نفسه.

[2] بن عابد بشير، "الشخصية المعنوية"، **مجلة القانون والعلوم السياسية**، المجلد08، العدد02، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحي أحمد- النعامة-، الجزائر،2022، ص. ص.347 -348.

[3] المادة 20 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق.

في ذات السياق، إعترف المشرع الجزائري في المادة 51 مكرر من قانون العقوبات، بالمسؤولية الجزائية للأشخاص المعنوية، مستثنيا بذلك طبعًا كل من الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام.

في إطار جريمة الإرهاب الإلكتروني، يُستشف في نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات، أن المشرع الجزائري قد عمّم التجريم باستخدامه لكلمة "**كل**"، ليشمل الشخص المعنوي أيضًا، كما هو وارد في العبارات التالية: "**...كل جزائري...**" و "**...كل من يستخدم تكنولوجيا الإعلام والاتصال...**" و "**...كل من يمول انتشار أسلحة الدمار الشامل... أي عمل يقوم به شخص طبيعي أو كيانات...**".

لكن لا توجد إشارة إلى العقوبة المقررة للشخص المعنوي في حالة استخدامه لتكنولوجيا الإعلام والاتصال لأغراض إرهابية في نصوص المواد المشار إليها. وبالتالي، يتم تطبيق العقوبات المقررة في نص المادة 18 مكرر من قانون العقوبات، التي تنص على ما يلي:" **العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي: 1) - الغرامة تساوي مرة (1) إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.**

2)- واحدة أو أكثر من العقوبات التكميلية الأتية: - 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 أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات، - مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها، - نشر وتعليق حكم الإدانة، - الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى على الجريمة أو الذي ارتكبت الجريمة بمناسبته."[1]

ثالثا: أحكام المساهمة الجنائية في جريمة الإرهاب الإلكتروني

أشارت المادة 19 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الى تجريم الشروع والاشتراك في جريمة الإرهاب الالكتروني على النحو التالي: " **1- الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص**

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف. 2- الشروع في ارتكاب الجر ائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية." [1]

في ذات السياق، أولى المشرّع الجزائري أهمية خاصة لمسألة الشروع والمساهمة في جريمة الإرهاب الإلكتروني، نظرًا لخطورتها وامتدادها، فلا يكفي معاقبة من يرتكب الجريمة بنفسه فقط، بل يجب شمل أيضًا كل شخص يشرع فيها **(1)** أو يساهم بوسائل مختلفة في تنفيذها **(2)**.

1) الشروع في جريمة الإرهاب الإلكتروني

يعاقب على الشروع في جريمة الإرهاب الإلكتروني برغم من كونها جريمة شكلية، ويصعب في الأصل تصور الشروع فيها. ويعود ذلك إلى السياسة الجنائية الوقائية الصارمة التي ينتهجها المشرع الجزائري في الجرائم الموصوفة بالأفعال الإرهابية والتخريبية، نظرًا لمساسها بأمن الدولة الجزائرية.

استنادا إلى ما تقدم، نصت المادة 87 مكرر 16 من قانون العقوبات على ما يلي: "**يعاقب على الشروع في الجر ائم المنصوص عليها في هذا القسم بالعقوبات المقررة للجريمة التامة**"[2]، بالتالي، يعاقب على الشروع في جريمة الإرهاب الإلكتروني بنفس العقوبة المقررة للجريمة التامة، كما هو منصوص عليه في المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات.

2) المساهمة الجنائية في جريمة الإرهاب الإلكتروني

تعتبر جريمة الإرهاب الإلكتروني من الجرائم التواطؤيه، بحيث تختلف أدوارهم في الجريمة، بين من يقوم بالدور الرئيسي، ويعتبر فاعلاً أصليًا، وبين من يقوم بدور ثانوي ويأخذ حكم الشريك في الجريمة.[3]

أ) المساهمة الجنائية الأصلية في جريمة الإرهاب الإلكتروني

يُعد فاعلاً طبقا لأحكام المادة 41 من قانون العقوبات، كل من شارك مباشرة في تنفيذ الجريمة، أو حرّض على ارتكابها باستخدام طرق معينة كالتحريض مثلا، وفي سياق جريمة الإرهاب الإلكتروني، قد يقوم

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سابق.

[2] أمر رقم66-156، يتضمن قانون العقوبات، معدل ومتمم، مرجع سابق.

[3] فلاك مراد، "المسؤولية الجنائية للشريك في القانون الجزائري"، **مجلة النوازل الفقهية والقانونية**، المجلد02، العدد1، مركز البحث في العلوم الإسلامية والحضارة-الأغواط، الجزائر، 2018، ص.201.

الفاعل الأصلي بدور المساهمة المباشرة في تنفيذ السلوك الإجرامي للجريمة كما بينا سابقًا في عنصر الركن المادي، كما قد يقوم الفاعل الأصلي بدور التحريض على ارتكاب هذه الجريمة، وهو ما يظهر بوضوح في نص المادة 87 مكرر 15 من قانون العقوبات. وتكمن عقوبة الفاعل الأصلي في نفس العقوبة المقررة للجريمة، والمشار إليها في نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات.

ب) المساهمة الجنائية التبعية في جريمة الإرهاب الإلكتروني

يأخذ حكم الشريك كل شخص طبيعي أو معنوي، يقوم بمساعدة الفاعل في إرتكاب الجريمة أو عاونه في التحضير لها أو تسهيلها أو تنفيذها، وهو على علم بذلك، دون أن يشارك مباشرة في ارتكابها.

في جريمة الإرهاب الإلكتروني، نجد أن المشرع الجزائري قد وسّع من دائرة الشركاء من خلال المادة 2/91 من قانون العقوبات، حيث أدرج فئات جديدة تُعتبر شركاء، وهذا يُعد دليلاً على توسيع دائرة التجريم من طرف المشرع، من خلال اعتبار أفعال إضافية صادرة عن أشخاص غير فاعلين أو مساهمين مباشرين بمثابة شراكة في الجريمة، مما يعكس تشددًا في مكافحة جرائم الإرهاب الإلكتروني، وجاء النص كتالي:" **علاوة على الأشخاص المبينين في المادة 42 يعاقب باعتباره شريكا من يرتكب دون أن يكون فاعلا أو شريكا أحد الأفعال التالية: - تزويد مرتكبي الجنايات والجنح ضد أمن الدولة بالمؤن أو وسائل المعيشة وتهيئة مساكن لهم أو أماكن لاختفائهم أو لتجمعهم وذلك دون أن يكون قد وقع عليه إكراه ومع علمه بنو اياهم. - حمل مراسلات مرتكبي هذه الجنايات تلك الجنح وتسهيل الوصول إلى موضوع الجناية أو الجنحة أو اخفائه أو نقله أو توصيله وذلك بأي طريقة كانت مع علمه بذلك.**"

كما تنص المادة 43 من قانون العقوبات على ما يلي:" **يأخذ حكم الشريك، من يقدم مسكنا أو ملجأ أو مكانا للاجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة أو الأمن العام أو ضد الأشخاص أو الأموال مع علمه بسلوكهم الإجرامي**".[1]

وفي سياق جريمة الإرهاب الإلكتروني، نجد أن المشرع الجزائري أدرج في نصوص المواد87 مكرر 4 و87مكرر11 و87مكرر12 و87مكرر15من قانون العقوبات، مجموعة من الأفعال التي تحمل دلالة على المساهمة التبعية مثل:"**... تنظيم سفر أشخاص إلى دولة أخرى...أو تسهيل ذلك السفر**".

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

يُقصد بتنظيم سفر شخص آخر، كأن يقوم الجاني بحجز تذكرة سفر أو يوفّر تسهيلات للحصول على التأشيرة، مما يجعله في حكم الشريك في الجريمة. وتُعد هذه الأفعال من قبيل المساهمة التبعية، ويترتب عنها طبقا لأحكام المادة44 من قانون العقوبات، تطبيق العقوبة ذاتها المقررة للجناية على الشريك في جريمة الإرهاب الإلكتروني، وهذا ما يعكس السياسة الجزائية الصارمة المنتهجة من طرف المشرع الجزائري.

الفرع الثاني: أحكام نظرية الظروف في جريمة الإرهاب الإلكتروني

لا يمكن الحديث عن العقوبة في جريمة الإرهاب الإلكتروني دون الوقوف عند بعض الحالات الخاصة التي قد تُغير من شدتها. ومن هنا تبرز أهمية دراسة الأعذار القانونية لجريمة الإرهاب الإلكتروني**(أولا)**، كذلك سيتم إبراز الظروف المخففة والمشددة لجريمة الإرهاب الإلكتروني**(ثانيا)**.

أولا: الأعذار القانونية المقررة في جريمة الإرهاب الإلكتروني

الأعذار القانونية هي تلك الحالات المحصورة قانونا والتي عند توفرها مع قيام الجريمة والمسؤولية، تؤدي إما إلى إعفاء المتهم من العقوبة **(1)** أو إلى تخفيفها **(2)** ومع ذلك، يحق للقاضي في حالات الإعفاء أن يقرر تطبيق تدابير أمنية على الشخص المعفى عنه.

1) الأعذار المعفية من العقاب في جريمة الإرهاب الإلكتروني

يقصد بنظام الإعفاء من العقاب وجود نص قانوني يمنح للجاني إعفاءً من العقوبة، بالرغم من ارتكابه للجريمة وقيام مسؤوليته الجزائية.

باعتبار جريمة الإرهاب الإلكتروني من الجرائم المكيفة كجناية ضد أمن الدولة، أدرج المشرع الجزائري عذرًا يُعفي من العقاب، والمتمثل في عذر التبليغ عن جريمة الإرهاب الإلكتروني قبل البدء في تنفيذها، وذلك في المادة 1/92 من قانون العقوبات، والتي تنص على مايلي:" **يُعفى من العقوبة المقررة كل من يبلغ السلطات الإدارية أو القضائية عن جناية أو جنحة ضد أمن الدولة قبل البدء في تنفيذها أو الشروع فيها**".[1] تبعا لذلك، فعلى جهة الحكم في حالة الإعفاء أن تُسقط العقوبة، مع جوازية تطبيق تدابير الأمن على المعفى عنه، وكذلك يجوز الحكم عليه بالمنع من الإقامة وبالحرمان من الحقوق الوطنية.

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

2) الأعذار المخففة للعقاب في جريمة الإرهاب الإلكتروني

الأعذار المخففة، هي تلك الحالات المحددة على سبيل الحصر في القانون، ويترتب عليها إلزام القاضي في تخفيف العقوبة المقررة للجريمة وفقا للقواعد المحددة قانونًا.[1]

في سياق جريمة الإرهاب الإلكتروني باعتبارها جريمة ضد أمن الدولة، حرص المشرع الجزائري من خلال أحكام المادة 2/92و3 من قانون العقوبات، على تشجيع الجناة على التعاون مع الجهات القضائية أو الأمنية من خلال الإبلاغ عن الجريمة قبل فتح المتابعة، أو المبادرة في المساعدة على القبض على الفاعلين والشركاء بعد فتح المتابعة الجزائية، مقابل تخفيف العقوبة بدرجة واحدة.

ثانيا: الظروف المخففة والمشددة في جريمة الإرهاب الإلكتروني

يقصد بالظروف المخففة والمشددة، منح السلطة التقديرية للقاضي في تقدير أسباب تخفيف أو تشديد العقوبة انطلاقا من ظروف ارتكاب الجريمة.[2] ومن خلال إستقراء نصوص المواد 87 مكرر 4 و87 مكرر 11 و87 مكرر 12 و87 مكرر 15 من قانون العقوبات، لا نجد إشارة مباشرة لهذه الظروف، بتالي نطبق القواعد العامة المنصوص عليها في قانون العقوبات، ولدراسة ذلك، سيتم تقسيم الفرع كتالي: الظروف المخففة في جريمة الإرهاب الإلكتروني **(1)**، الظروف المشددة في جريمة الإرهاب الإلكتروني **(2)**.

1) الظروف المخففة في جريمة الإرهاب الإلكتروني

أكد المشرع الجزائري في نص المادة 53من قانون العقوبات على جواز تخفيض العقوبة المقررة بالنسبة لشخص الطبيعي المدان بجناية معاقب عليها بالسجن المؤقت، وذلك وفقا لما يلي:

* تخفض العقوبة إلى ثلاث (3) سنوات حبس، إذا كانت العقوبة المقررة هي السجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة، وذلك بالنسبة للحالة الواردة في المادة 87مكرر15 من قانون العقوبات.

[1] بن تركي ليلى،" تأثير الأعذار القانونية على الجزاء الجنائي في التشريع الجزائري"، **مجلة الشريعة والقانون**، المجلد7، العدد2، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر،2018، ص. ص.74-75.

[2] مقدم مبروك،" الظروف المخففة وحالة العود على ضوء القانون رقم: 23/06المؤرخ في 20/12/06المعدل والمتمم لقانون العقوبات"، **مجلة البحوث والدراسات الإنسانية**، المجلد2، العدد1، جامعة20أوت1955 سكيكدة، الجزائر، 2008، ص.263.

* تخفض العقوبة إلى سنة (1) حبس، إذا كانت العقوبة المقررة هي السجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات، وذلك بالنسبة للحالات الواردة في المواد 87مكرر4و 87مكرر11 و87مكرر12 من قانون العقوبات.

لكن بالرجوع إلى نص المادة87مكرر8 من قانون العقوبات، يُلاحظ نوع من التناقض الذي وقع فيه المشرع الجزائري، وذلك بإقراره بعدم إمكانية خفض العقوبة إلى أقل من النصف، عندما تكون العقوبة الصادرة، عقوبة السجن المؤقت، بحيث تنص:" **لا يمكن في كل الحالات أن تكون عقوبات السجن المؤقت الصادرة، تطبيقا لأحكام هذا الأمر، أقل من: عشرين (20) سنة سجنا مؤقتا عندا تكون العقوبة الصادرة، عقوبة السجن المؤبد، -النصف عندا تكون العقوبة الصادرة، عقوبة السجن المؤقت**".[1]

أما بالنسبة للشخص المعنوي فإن استفادته من الظروف المخففة، تختلف بحسب ما إذا كان مبتدئًا أو مسبوق قضائيا، بمعنى إذا كان مبتدئاً يجوز خفض مبلغ الغرامة إلى الحد الأدنى للغرامة المقررة لشخص الطبيعي المرتكب لجريمة الإرهاب الإلكتروني، والمقدرة بـ 100.000دج وذلك بالنسبة للحالات الواردة في المواد87مكرر4 و87مكرر11 و87مكرر12 من قانون العقوبات، أما إذا كان مرتكبا للأفعال الواردة في المادة 87مكرر15من قانون العقوبات، فمبلغ الغرامة سيقدر بـ 1.000.000دج، بتالي القاعدة المطبقة على الشخص المعنوي المبتدئ هي الغرامة تساوي مرة (1) إلى خمس (5) مرات الحد الأدنى للغرامة المقررة للشخص الطبيعي.

لكن إذا كان الشخص المعنوي مسبوقا قضائيا، بمفهوم المادة 53مكرر8 من قانون العقوبات، أي لارتكابه جريمة من جرائم القانون العام، وباعتبار جريمة الإرهاب الإلكتروني جريمة من جرائم القانون العام فلا يجوز إفادته بالظروف المخففة.

[1] أمر رقم66-156، يتضمن قانون العقوبات، مرجع سابق.

2) الظروف المشددة في جريمة الإرهاب الإلكتروني

الظروف المشددة هي مجموعة من الظروف المحددة قانونًا، من شأنها أن تغير من وصف الجريمة إلى وصف أشد أو تزيد من مقدار العقوبة.[1]

من خلال استقراء المواد87مكرر4 و87مكرر11 و87مكرر12 و87مكرر15 من قانون العقوبات، لا نجد نصًا صريحًا يُشير إلى الظروف المشددة لجريمة الإرهاب الإلكتروني، لكن هذا لا يمنع من تطبيق أحكام المادة 54مكرر من قانون العقوبات، المتعلقة بالعود باعتباره ظرفًا مشددًا عامًا يشمل جميع الجرائم.

يعرف العود العام، بأنه العود الذي لم يُحدد له المشرع مدة معينة لارتكاب الجريمة الجديدة، ولم يشترط كذلك أن تكون الجريمة الجديدة تحمل نفس الوصف أو مماثلة للجريمة التي أدين بها سابقا.[2]

في سياق جريمة الإرهاب الإلكتروني باعتبارها جناية معاقب عليها بالسجن المؤقت والغرامة، فأحكام العود بالنسبة للشخص الطبيعي تُطبق على النحو المحدد في المادة 54مكرر الفقرة الثانية والثالثة من قانون العقوبات.

بتالي، فبالنسبة لمرتكب الأفعال الواردة في المادة 87مكرر15 من قانون العقوبات يخضع لرفع الحد الأقصى للعقوبة السجن المؤقت إلى ثلاثين (30) سنة.

أما بالنسبة لمرتكب السلوكيات الإجرامية الواردة في المواد87مكرر4 و87مكرر11 و87مكرر12 من قانون العقوبات، فيرفع الحد الأقصى للعقوبة السالبة للحرية إلى الضعف، كذلك يضاعف الحد الأقصى لعقوبة الغرامة في كل الحالات المذكورة أعلاه.

أما بالنسبة للشخص المعنوي في حالة العود، وتطبيقا لأحكام نص المادة 54مكرر1/5من قانون العقوبات، فإذا سبق الحكم على الشخص المعنوي من أجل جناية، وقامت مسؤوليته جراء ارتكاب جناية جديدة، فإن مبلغ الغرامة يساوي عشر (10) مرات الحد الأقصى لعقوبة الغرامة للجناية الجديدة.

[1] زمورة داود،" الجمع بين تخفيف وتشديد العقوبة في التشريع الجزائري"، **مجلة الحقوق والعلوم السياسية**، المجلد10، العدد1، جامعة عباس لغرور خنشلة، الجزائر، 2023، ص.957.

[2] مقدم مبروك، مرجع سابق، ص.267.

الفصل الثاني
الآليات الإجرائية لمجابهة الإرهاب الإلكتروني في القانون الجزائري

الفصل الثاني: الآليات الإجرائية لمجابهة الإرهاب الإلكتروني في القانون الجزائري

أمام تصاعد وتيرة التهديدات والتحديات التي تفرضها جريمة الإرهاب الإلكتروني، لم تعد الاستجابة القانونية وحدها كافية لمجابهة هذا النوع من الجرائم المعقدة العابرة للحدود الوطنية؛ فالإرهاب الإلكتروني لا يشكّل مجرد اعتداء على الأفراد أو الممتلكات، بل يمتد أثره ليطال السيادة الوطنية، وسلامته الترابية، ويزعزع الأمن العام، والأمن المعلوماتي للدولة، وما يزيد من تعقيد هذا النوع من الجرائم هو طبيعته غير المرئية، واعتماده على تكنولوجيا الإعلام والاتصال، ما يصعّب أحيانًا تتبعه بالأساليب التقليدية المعهودة.

أفرزت هذه التحولات التكنولوجية واقعًا قانونيًا جديدًا، يتطلب تطويرًا للمنظومة التشريعية الجزائرية، بما يتلاءم مع التهديدات السيبرانية المعاصرة، خاصة مع التزايد المستمر لمعدلات الجريمة الإلكترونية[1] عامةً، وجريمة الإرهاب الإلكتروني خاصةً[2]؛ وهو الأمر الذي جعل الدولة الجزائرية تجد نفسها مجبرة، على إعادة النظر في أساليب مكافحة هذه الجريمة المعلوماتية؛ وأصبحت الشرطة القضائية، وعلى رأسها فرقة مكافحة الجريمة السيبرانية، مطالبة باستخدام أساليب تحرٍّ خاصة متقدمة، مثل المراقبة الإلكترونية والتسرب والتسليم المراقب، وهي إجراءات تستوجب تأطيرًا قانونيًا دقيقًا وتدريبًا متخصصًا.

بالإضافة إلى ذلك، يُعدّ التفتيش الإلكتروني أحد أهم آليات التحقيق المستحدثة بموجب القانون رقم09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث يساعد على الوصول إلى أدلة رقمية تساعد في إثبات الجريمة أو تحديد هوية الفاعل، مع ضرورة احترام الضوابط القانونية التي تحمي الحقوق والحريات، ويشمل هذا الإطار القانوني أيضًا ضمان

[1] يُقصد بالجريمة الإلكترونية:" أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون" نقلا عن: زامل صهيب سهيل غازي، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية: (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة وهران-2، الجزائر، 2022، ص.49.

[2] خلال السنوات الثلاث الماضية (2022–2024)، شهدت ولاية بجاية ارتفاعاً في عدد قضايا الجرائم الإلكترونية، حيث ارتفع الرقم من 229 قضية في 2022 إلى 335قضية في 2023 وصولاً إلى 416قضية في 2024، في حين بلغ عدد الأشخاص المتورطين ذروةً في 2023 بواقع 350 شخصاً، (بعد أن كان 224شخص متورط في 2022)، قبل أن يتراجع إلى 228شخصاً في 2024؛ ويُلاحَظ أن عدد الموقوفين ظل منخفضاً نسبياً في 2022 و2023 (7 و 8 أشخاص على التوالي) لكنه سجّل قفزة إلى 20 موقوفاً في 2024، مما يعكس فعالية أكبر في جهود الضبط والتحقيق خلال العام الأخير. أما فيما يتعلق بجريمة الإرهاب الإلكتروني، فقد ارتفع عدد القضايا من 42حالة في 2022 إلى 76حالة في 2023 ثم انخفض إلى 54حالة في 2024، دالّاً على تذبذب في نشاط جريمة الإرهاب الإلكتروني، واستجابة الأجهزة الأمنية خلال الثلاثية المذكورة. المصدر: فرقة مكافحة الجريمة السيبرانية، أمن ولاية بجاية، مراسلة رسمية بتاريخ 25 مارس 2025.

الحماية الجزائية للشهود والخبراء والضحايا في جرائم الإرهاب الإلكتروني، بما يكفل سلامتهم وأمنهم، وأمن عائلتهم طوال مراحل الدعوى العمومية في جريمة الإرهاب الإلكتروني **(المبحث الأول)**.

كما لا يقتصر التصدي للإرهاب الإلكتروني على الإجراءات الأمنية فحسب، بل يشمل أيضًا الأبعاد المؤسسية، ففي هذا الإطار، أنشأت الجزائر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كهيئة وقائية تتولى صياغة الخطط الوطنية لمكافحة الجرائم الإلكترونية، وجرائم الإرهاب على وجه الخصوص، وتفعيل التعاون مع السلطات القضائية الوطنية والمنظمات الدولية، وذلك لمواكبة التطورات التقنية، وضمان تفعيل الإجراءات الوقائية والرقابية لتصدي لهذا النوع من الجرائم الخطيرة.

بينما يلعب القطب الجزائي الوطني للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، دورًا كذلك في التصدي لهذه الجريمة، كهيئة قضائية جزائية وطنية متخصصة في متابعة القضايا الإلكتروني، وعلى رأسها جريمة الإرهاب الإلكتروني، إذ يسهم هذا التمازج بين الدور الوقائي والقضائي في تعزيز الاستجابة المتكاملة للتهديدات الرقمية **(المبحث الثاني)**.

المبحث الأول: آليات المتابعة الجزائية في جريمة الإرهاب الإلكتروني

تتطلب جريمة الإرهاب الإلكتروني، باعتبارها من الجرائم ذات الطابع السيبراني، أساليب تحرٍّ وتحقيق تتلاءم مع طبيعتها الإلكترونية، نظرًا لكون إجراءات البحث والتحري والتحقيق التقليدية، لم تعد قادرة وحدها على التصدي لهذا النوع من الإجرام، لا سيما في ظل اتساع نطاقها، وتطوّر أساليب تنفيذها، واعتمادها على تكنولوجيا الإعلام والاتصال؛ وهذا ما دفع المشرّع الجزائري إلى تبنّي أساليب تحرٍّ خاصة، على غرار المراقبة الإلكترونية، والتسرّب، والتسليم المراقب، للكشف عن النشاطات الإرهابية الإلكترونية.

كما تم تنظيم إجراءات التفتيش الإلكتروني بما يضمن فعالية التحري، مع الحفاظ على الحقوق المكفولة دستوريًا، لما لهذا الإجراء من مساس مباشر بسرية الاتصالات والمراسلات الخاصة، والتي تُعدّ من ركائز الحياة الخاصة للأفراد[1]، ويُعزّز هذا الإطار القانوني كذلك؛ بالتزامه بالحماية الجزائية للشهود

[1] حفصاوي كمال، مخلوف عمر،" التفتيش الإلكتروني بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات"، **مجلة الباحث للدراسات الأكاديمية**، المجلد 11، العدد01، كلية الحقوق والعلوم السياسية، جامعة باتنة1- لحاج لخضر، الجزائر،2024، ص.327.

والخبراء والضحايا في جرائم الإرهاب الإلكتروني، عبر تدابير إجرائية وغير إجرائية لحماية هويتهم، والسماح لهم بالإدلاء بشهادات مكتوبة أو مسجلة تحت إشراف قضائي، بما يضمن سلامتهم خلال مراحل الدعوى.

بناءً على ما تقدّم، سيتم دراسة المبحث الأول وفق التقسيم المنهجي التالي: آليات التحري في جريمة الإرهاب الإلكتروني **(المطلب الأول)**، لما لها من دور محوري في تتبّع النشاطات الإرهابية في الفضاء السيبراني، ثم الحماية الجزائية للشهود والخبراء والضحايا في جريمة الإرهاب الإلكتروني **(المطلب الثاني)**.

المطلب الأول: آليات التحري في جريمة الإرهاب الإلكتروني

تضطلع الشرطة القضائية-فرقة مكافحة الجريمة السيبرانية- بمرحلة شبه قضائية، فبعد أن يتم رَصد محتوى هدام من شأنه المساس بسلامة ووحدة التراب الوطني، والأمن المعلوماتي، تقوم مباشرةَ بإجراء معاينة تقنية للمحتويات الهدامة، بالإنتقال إلى مسرح الجريمة الذي يحمل الطبيعة الافتراضية- البيئة الرقمية للأجهزة الإلكترونية والشبكات- في جريمة الإرهاب الإلكتروني.

بحيث يتم ذلك بعد إخطار وكيل الجمهورية المختص إقليميا (المادة 42 ق.إ.ج)، مع إمكانية الاستعانة بأشخاص مؤهلين ومتخصصين في المجال التقني والمعلوماتي(المادة49 ق.إ.ج)، وفتح تحقيق بالتنسيق مع النيابة العامة (المواد 18 ،32، 40مكرر1، 40مكرر2 ،40مكرر3 ق.إ.ج)، ومباشرة التحريات التقنية بهدف تحديد الهوية التقنية للحسابات المجرمة، ومباشرة عملية جمع الاستدلالات، وتوقيف الأشخاص[1] الذين توجد ضدهم دلائل قوية لارتكابهم لجريمة الإرهاب الإلكتروني، مستعينين في ذلك بأساليب تحرّ خاصة **(الفرع الأول)** و القيام بعمليات التفتيش الإلكتروني **(الفرع الثاني)** للمعدات الإلكترونية وكذا المعطيات المخزنة في المنظومات المعلوماتية لضبط الأدلة الرقمية التي لها علاقة بالجريمة.

[1] "تعتبر جرائم الإرهاب من الجرائم الخطيرة، التي أجاز فيها المشرع تمديد آجال التوقيف للنظر المحددة بـ(48) ساعة إلى (5) خمس مرات" لتفصيل أكثر أنظر المادة 51 والمادة65 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

الفرع الأول: أساليب التحري الخاصة عن جريمة الإرهاب الإلكتروني

في سبيل الكشف عن جريمة الإرهاب الإلكتروني، قدم المشرع الجزائري لضبطية القضائية بموجب القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، صلاحية اللجوء إلى إستعمال أساليب تحرٍّ خاصة والمتمثلة: المراقبة الإلكترونية**(أولا)**، التسرب **(ثانيا)**، التسليم المراقب **(ثالثا)** للكشف عن الجريمة.

في ذات السياق، وضع المشرع الجزائري القانون رقم 16-03[1]،الذي أجاز لضبطية القضائية طلب أخذ عينات بيولوجية وإجراء تحاليل وراثية عليها- مراعين في ذلك كرامة الإنسان وحرمة حياتهم الخاصة ومعطياتهم الشخصية-، للأشخاص المشتبه في ارتكابهم جنايات أو جنح ضد أمن الدولة أو جرائم الإرهاب قصد التعرف على هويتهم أو لمقتضيات التحريات والتحقيق، وذلك بإذن مسبق من السلطات المختصة.

يُباشر هذه العملية ضابط أو عون شرطة قضائية مختص. وقد أقر هذا القانون عقوبات صارمة على من يرفض الخضوع لهذه التحاليل، وكذا لكل من يستعمل العينات لأغراض أخرى غير تلك المنصوص عليها قانونا، وكذا لكل من يقوم بإفشاء المعطيات المسجلة في القاعدة الوطنية للبصمات الوراثية.

أولا: آليات المراقبة الإلكترونية

يضمن الدستور الجزائري حماية حرمة الحياة الخاصة، وكذا الحق في سرية المواصلات الخاصة، وهذا ما نصت عليه المادة 47 منه:" **لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق**".[2]

[1] للاستزادة أنظر القانون رقم 16-03 المؤرخ في 19 يونيو2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، ج.ر.ج.ج عدد37، الصادرة في 22يونيو2016.

[2]مرسوم رئاسي رقم 20 -442، مؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر 2020، ج. ر.ج.ج عدد 82، الصادرة في 30 ديسمبر 2020.

أقام المشرع الجزائري إستثناء على هذه القاعدة، بحيث سمح لضبطية القضائية في إطار البحث والتحري والتحقيق عن الجرائم الخطيرة، والمحصورة في المادة 65مكرر5 ق.إ.ج، اللجوء إلى إجراء المراقبة الإلكترونية، ولتحديد مفهوم هذا الإجراء لابد من التطرق إلى تعريفه **(1)**، ثم تحديد شروطه **(2)**.

1) تعريف آليات المراقبة الإلكترونية

يطلق مصطلح المراقبة الإلكترونية على إجراء إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، والذي يعتبر من الإجراءات الذي يتم إعتماده في سبيل الكشف عن جريمة الإرهاب الإلكتروني.

يُقصد بإعتراض المراسلات بأنها "**عملية مراقبة سرية للمراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة**".[1] كما عرفته المادة 65مكرر5 ق.إ.ج في الفقرة الثانية كتالي: " **إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية**".[2]

أما تسجيل الأصوات، فهي عملية تقنية يتم من خلالها تسجيل المحادثات الخاصة والسرية، المتفوه بها من طرف شخص أو عدة أشخاص في مكان خاص أو عام[3]، أما إلتقاط الصور فهو إجراء تباشره الضبطية القضائية من خلال إلتقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، وهذا طبقًا لما ورد في الفقرة الثالثة من نص المادة 65مكرر5 ق.إ.ج.

2)شروط تطبيق المراقبة الإلكترونية

نظرًا لما يمثّله إجراء المراقبة الإلكترونية من خطورة على الحقوق والحريات الفردية، واعتباره انتهاكًا صارخًا للمادة 1/35 من الدستور الجزائري، التي تنصّ: **"تضمن الدولة الحقوق الأساسية والحريات"**[4]، فقد خصّه المشرّع الجزائري بجملة من الأحكام الخاصة، والتي تمتد من المادة 65 مكرر 5 ق.إ.ج إلى غاية المادة 65 مكرر 10 ق.إ.ج ، سواء في إطار التحريات الأولية المتعلقة بجريمة متلبّس بها، أو في مرحلة التحقيق

[1] خلفي عبد الرحمان، الإجراءات الجزائية في القانون الجزائري المقارن، الطبعة السابعة، دار بلقيس، الجزائر، 2024، ص.103.

[2] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[3]عبد الحميد سفيان،" أساليب التحري الخاصة ي قانون الإجراءات الجزائية الجزائري"، **مجلة صوت القانون**، المجلد9، العدد3، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة خميس مليانة، الجزائر،2023، ص.210.

[4] مرسوم رئاسي رقم 20- 442، يتعلق بإصدار التعديل الدستوري، مرجع سابق.

القضائي؛ وتُحدّد هذه المواد شروط المراقبة الإلكترونية من خلال مجموعة من الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية، بما فيها الشروط الموضوعية **(أ)** والشروط الإجرائية **(ب)**.

أ) الشروط الموضوعية لتطبيق المراقبة الإلكترونية

اشترط المشرع الجزائري لصحة إجراء إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، ألا يتم اللجوء لاستعماله إلاّ في حال ما اقتضت ضرورات التحري، والبحث في الجريمة المتلبس بها، أو في حال ما اقتضت ضرورة التحقيق الابتدائي، في مجموعة من الجرائم المذكورة على سبيل الحصر وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهـــاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفسـاد.

ب) الشروط الإجرائية لتطبيق المراقبة الإلكترونية

اشترط المشرع الجزائري، لضمان صحة إجراء المراقبة الإلكترونية في جريمة الإرهاب الإلكتروني، الحصول على **إذن** مُسبق من السلطات المختصة، سواء من طرف وكيل الجمهورية بمناسبة البحث والتحري في الجريمة المتلبس بها، وكذا للقيام بمجموع الترتيبات التقنية لإجراء المراقبة الإلكترونية، وذلك بالدخول للمحلات السكنية بغير علم أو رضا الأشخاص الذين لهم الحق على تلك الأماكن.

أما في حالة فتح تحقيق قضائي فتتم عمليات المراقبة الإلكترونية بناءًا على إذن من قاضي التحقيق وتحت مراقبته المباشرة؛ لكن بإستقراء نص المادة 1/67من ق.إ.ج التي تنص**" لا يجوزلقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولوكان ذلك بصدد جناية أو جنحة متلبس بها"**[1]، وهذا ما يدل على أن المبادرة لإجراء المراقبة الإلكترونية تبقى بيد وكيل الجمهورية.

في السياق ذاته، يُشترط في الإذن أن يكون مكتوبا، مسبباً ومبررًا، ومحدد المدة، أقصاها أربعة (4) أشهر قابلة لتجديد وذلك حسب مقتضيات التحري والتحقيق، والمشرع ترك المجال مفتوح لتجديد الإذن دون تحديد عدد المرات المسموح بها، كما يُشترط أن يكون شامل لمجموعة من للعناصر التالية (نوع الجريمة، الاتصالات المطلوب إلتقاطها، الأماكن المقصودة سكنية أو غيرها، المدة...).

[1] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

إشترط المشرع الجزائري في القائم بعملية المراقبة الإلكترونية أن يتمتع بصفة ضابط شرطة قضائية، والذي يجوز له تسخير أي عون مؤهل لدى مصلحة، أو وحدة، أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، للتكفل بالجوانب التقنية لعملية المراقبة الإلكترونية.

كما يلتزم مقدمي الخدمة بمساعدة السلطات القضائية المختصة، من خلال وضع جميع المعطيات المتعلقة بمحتوى الاتصالات تحت تصرفها، بما في ذلك ما يُتيح التعرف على هوية مستعملي الخدمة، وهوية المرسل والمرسل إليه، والعناوين الإلكترونية للمواقع التي تم الاطلاع عليها، وكذا المعطيات التي تسمح بتحديد مصدر الاتصال ومكانه، وهذا تطبيقا للمادة 10و 1/11و2 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.[1]

لضمان سلامة الإجراءات، يلتزم ضباط الشرطة القضائية أثناء القيام بعملية المراقبة الإلكترونية لشخص ملزم قانونا بكتمان السر المهني، بإتخاذ جميع التدابير اللازمة لضمان إحترام ذلك السر، والقيام بتحرير محضر استدلالي عن كل عملية اعتراض مراسلات وتسجيل الأصوات وإلتقاط الصور، وكذا عن عمليات وضع الترتيبات التقنية، ولصحة المحضر يجب أن يشمل تاريخ وساعة بداية ونهاية العمليات.

يُلزم كذلك ضابط الشرطة القضائية، وصف ونسخ كل المراسلات والصور والمحادثات ضمن محضر يُرفق بملف القضية، مع إمكانية الاستعانة بمترجم لترجمة المكالمات الأجنبية، وذلك لضمان حماية حقوق الدفاع بتوثيق كل الأدلة المفيدة لإظهار الحقيقة، ما يسمح للمتهم ومحاميه مراجعتها.

ثانيا: آلية التسرب في جريمة الإرهاب الإلكتروني

اعترف المشرع الجزائري بآلية التسرب، كأحد أساليب التحري الخاصة في جريمة الإرهـاب الإلكـتروني، باعتبارها جريمة خطيرة ومنظمة عبر الوطنية، وذلك بموجب إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية المصادق عليها، حيث تنص المادة 1/20منها على مايلي:" **يتعين على كل دولة طرف... باتخاذ ما يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسباً من استخدام أساليب تحرٍّ خاص أخرى، مثل المراقبة الإلكترونية أو غيرها من**

[1] أنظر المادة10 والمادة1/11و2 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

أشكال المراقبة، والعمليات المستترة، من جانب سلطاتها المختصة داخل إقليمها لغرض مكافحة الجريمة المنظمة مكافحة فعّالة".[1]

إنطلاقا من نص المادة أعلاه، يتضح أن مصطلح العمليات المستترة يشير إلى إجراء التسرب الذي يعتبر مصطلح حديث، والذي جاء به القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

كما يعرف كذلك التسرب بمصطلح الإختراق الذي ورد في قانون الوقاية من الفساد ومكافحته في المادة 56 منه التي تنص:" **من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو اتباع أساليب تحر خاصة كالترصد الإلكتروني والإختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة. تكون الأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول بهما".**[2] وفي سبيل ذلك، سيتم التطرق لتعريف آلية التسرب **(1)**، ثم تحديد الضوابط الموضوعية والإجرائية **(2)** لضمان شرعيتها وصحتها.

1) تعريف آلية التسرب في جريمة الإرهاب الإلكتروني

نظم المشرع الجزائري أحكام إجراء التسرب من المادة 65مكرر11 إلى 65مكرر18 من ق.إ.ج، إذ يُعتبر التسرب أحد أساليب التحري الخاصة، الذي يباشره ضابط الشرطة أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بالتنسيق العملية، بمراقبة شخص أو مجموعة من الأشخاص، المشتبه في إرتكابهم لجريمة من الجرائم المحددة على سبيل الحصر في المادة 65مكرر5 ق.إ.ج، وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهـــاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.

تتم عملية التسرب من خلال قيام ضابط الشرط القضائية بإيهام هؤلاء الأشخاص بأنه فاعل معهم أو شريك لهم أو خاف، لغرض الحصول على الأدلة وكشف حقيقة الجريمة، وذلك تطبيقا للمادة 65مكرر12 /1ق.إ. ج التي تنص:" **يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت**

[1] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، مرجع سابق.

[2] قانون رقم06-01 مؤرخ في 20فبراير سنة 2006، يتعلق بالوقاية من الفساد ومكافحته، ج.ر.ج.ج عدد14، الصادرة في 8مارس2006، معدل ومتمم.

مسؤولية ضابط الشرطة القضائية المكلف بالتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

أما بخصوص التسرب الإلكتروني فهي عملية تقنية إلكترونية، تتم في الفضاء الرقمي من خلال قيام ضابط الشرطة القضائية بالتسرب إلى منظومة معلوماتية أو نظام للإتصالات الإلكترونية، بهدف مراقبة أشخاص وإيهامهم بأنه شريك معهم، لغرض الحصول على الأدلة بشأن الجريمة، وذلك تطبيقا لأحكام القانون المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.[1]

ما يُلاحظ عليه، أن إجراء التسرب الوارد في قانون الإجراءات الجزائية، هو نفسه التسرب الإلكتروني الوارد في القانون المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، فكلاهما يعتمدان على قيام ضابط الشرطة القضائية، بإيهام أشخاص مشتبه فيهم في ارتكابهم لجريمة، على أنه فاعل معهم أو شريك لهم، بُغية الحصول على الأدلة، لكن الفرق الوحيد الموجود بينهم، أن التسرب الوارد في قانون الإجراءات الجزائية هو عملية ميدانية، أما التسرب الإلكتروني يكون إلكترونيا باستغلال شبكة الإتصال المعلوماتية أو عبر منظومة معلوماتية، وهي التقنية الأكثر إستعمالاً في سبيل الكشف عن جريمة الإرهاب الإلكتروني، بإعتبار أن جُل التخطيطات والمراسلات بين أعضاء المنظمات الإرهابية تكون إلكترونيا.

إضافة إلى ذلك، خصَّ المشرع الجزائري إجراء التسرب بأحكام خاصة، نظرا لما يُشكله من خطر وتهديد على حياة ضابط الشرطة أو عون الشرطة القضائية القائم بالعملية، وذلك من خلال إمكانية إستعانة هذا الأخير بهوية مستعارة حفاظا على أمنه وسلامة حياته، وهذا ما أكدته الفقرة الثانية من المادة 65مكرر12 ق.إ.ج التي تنص:" **يسمح لضابط الشرطة أو عون الشرطة القضائية أن يستعمل، لهذا الغرض، هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة65مكرر14 أدناه، ولا يجوز، تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم".**[2]

[1] أنظر المادة 26 من القانون 20-05 مؤرخ في 28 أبريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج.ر.ج.ج عدد 25، الصادرة في 29أبريل 2020.

[2] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

وقد ذهب المشرع الجزائري إلى أبعد من ذلك، حيث نص صراحة على عدم جواز كشف الهوية الحقيقة لضابط أو عون الشرطة القضائية القائم بعملية التسرب، ورتب عقوبات صارمة على كل من يخالف ذلك ويتعمد كشف هوية هذا الأخير إضرارًا به.[1]

كما تجدر الإشارة، أن قانون الإجراءات الجزائية أجاز لضابط الشرطة أو عون الشرطة القضائية، الذي يباشر عملية التسرب أن يقوم ببعض الأعمال الإرهابية الإجرامية، دون أن يترتب على ذلك قيام مسؤوليتهم الجزائية، لكن شرط ألا تشكل تلك الأفعال تحريضا على إرتكاب جريمة الإرهاب الإلكتروني، وذلك من خلال المشاركة في الدردشات مع التنظيمات الإرهابية وحلقات النقاش والتخطيط لهذه الجريمة.[2]

2) شروط تطبيق آلية التسرب في جريمة الإرهاب الإلكتروني

حدد المشرع الجزائري في قانون الإجراءات الجزائية جملة من الشروط الموضوعية والإجرائية، لإعمال إجراء التسرب بإعتباره تقنية حديثة في مجال التحري والتحقيق، وذلك نظرا لما يشكله من خطر على حريات وحقوق الإنسان، وعلى أمن ضباط وأعوان الشرطة القضائية، بتالي سيتم التطرق والتفصيل فيها وفق التقسيم التالي: الشروط الموضوعية لإجراء التسرب **(1)**، الشروط الشكلية لإجراء التسرب **(2)**.

أ) الشروط الموضوعية لتطبيق آلية التسرب في جريمة الإرهاب الإلكتروني

بإعتبار التسرب عملية سرية وخطيرة، وجب مراعاة الشروط الموضوعية، وذلك لضمان الشرعية الإجرائية من جهة، ولتسهيل مهام الضبطية القضائية من جهة أخرى لبلوغ أهدافهم والحصول على الأدلة، حيث أكدت المادة 65 مكرر 11 ق.إ.ج، على عدم إمكانية اللجوء إلى عملية التسرب إلا إذا كانت هناك ضرورة قصوى لتحري أو التحقيق في الجرائم المحصورة والمذكورة سالفا في إجراء المراقبة الإلكترونية، ومن بينها جرائم الإرهاب سواء أكانت تقليدية أو في صورتها الحديثة أي الإرهاب الإلكتروني.

[1] أنظر المادة 65مكرر16من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع نفسه.

[2] عبد الرحمان خلفي، الإجراءات الجزائية في القانون الجزائري المقارن، مرجع سابق، ص .109.

يُستفاد من ذلك، أن وجود أدلة كافية تعزز الشبهات أو تدعم الاتهامات يُعد شرطًا جوهريًا قبل اللجوء إلى إجراء التسرب، إذ لا يجوز المجازفة دون توفر مؤشرات قوية. وبالتالي، لا يُعتمد هذا الأسلوب إلا في الظروف الاستثنائية التي يتعذر فيها الحصول على أدلة كافية لإثبات جريمة الإرهاب الإلكتروني.

ب) الشروط الإجرائية لتطبيق آلية التسرب في جريمة الإرهاب الإلكتروني

حرص المشرّع الجزائري على تنظيم تقنية التسرب بضوابط إجرائية دقيقة، من المادة 65مكرر 13 ق.إ.ج إلى غاية المادة 65مكرر18 ق.إ.ج، ورتّب على مخالفتها جزاء البطلان، تأكيدًا لأهمية ضمان مشروعية الدليل المستمد من عملية التسرب، بحيث إشترط المشرع الجزائري حصول ضابط الشرطة القضائية، أو عون الشرطة القضائية المتسرب، على **إذن** مسبق من السلطات المختصة، سواء من طرف وكيل الجمهورية إن كانت القضية في مرحلة البحث والتحري، أو من طرف قاضي التحقيق في مرحلة التحقيق القضائي، وذلك بعد إخطار وكيل الجمهورية، ويُشترط في الإذن أن يكون مكتوبا، مسببا ومبررا، تحت طائلة البطلان.

كذلك من الشروط الجوهرية للإذن، أن يتضمن هوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، وكذا مدة العملية التي حُددت بأربعة (4) أشهر قابلة لتمديد، مع جوازية توقيف عملية التسرب قبل نفاذ المدة المحددة، بمعنى ليس شرط أن يتم إستنفاذ مدة أربعة (4) أشهر كاملة، لكن لضمان أمن حياة وسلامة ضابط أو عون الشرطة القضائية المتسرب، أن يواصل بعض النشاطات المحددة في المادة 65مكرر14 ق.إ.ج[1]، لمدة أربعة (4) أشهر على الأكثر، وذلك في حال ما تقرر توقيف عملية التسرب، أو في حال ما إنقضت مدة الإذن دون الحاجة لتمديده، وذلك لضمان إنسحابه التدريجي الأمن من المجرمين.

عند إتمام عملية التسرب، يقوم ضابط الشرطة المكلف بالتنسيق عملية التسرب، بتحرير تقرير يتضمن العناصر الضرورية لمعاينة جريمة الإرهاب الإلكتروني، ويتم إيداع الرخصة المتضمنة توقيف عملية التسرب قبل إنقضاء المدة المحددة ضمن ملف الإجراءات، ويجوز أن يتم الاستعانة بضابط الشرطة القضائية المتسرب، كشاهد عن العملية أمام القضاء.

[1] أنظر المادة 65مكرر14 من أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

ثالثا: التسليم المراقب كآلية إجرائية لمكافحة جريمة الإرهاب الإلكتروني

في ظل تنامي تهديدات الإرهاب الإلكتروني، الذي يتخذ من الفضاء الرقمي بيئة ملائمة لتخطيط وشن الهجمات وارتكاب الأفعال الإرهابية، أصبحت الأساليب التقليدية عاجزة عن التصدي لهذا النوع من الجرائم؛ وقد أفرز هذا التحدي أساليب تحرٍّ متقدمة تواكب خصوصية هذا الصنف من الإجرام، ويُعدّ إجراء التسليم المراقب أحد أساليب التحري الخاصة، المعترف بها على الصعيدين الوطني والدولي؛ وسنتطرق فيما يلي لتعريف آلية التسليم المراقب **(1)** ثم تبيان شروط العمل به **(2)**.

1) تعريف التسليم المراقب كآلية إجرائية لمكافحة جريمة الإرهاب الإلكتروني

يعتبر إجراء التسليم المراقب أحد أساليب التحري الخاصة، لما له من دور فعّال في الكشف عن الإرهاب الإلكتروني، وقد جاء تعريفه في المادة 2من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، حيث عرفته كتالي:" **يُقصد بتعبير التسليم المراقب الأسلوب الذي يسمح لشحنات غير المشروعة أو مشبوهة بالخروج من إقليم دولة أو أكثر أو المرور عبره أو دخوله، بمعرفة سلطاته المختصة وتحت مراقبتها، بغية التحري عن جرم ما وكشف هوية الأشخاص الضالعين في ارتكابه**".[1]

كما نص القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته على إجراء التسليم المراقب في المادة56 واعتبره أحد أساليب التحري الخاصة، والتي تنص:"**...يمكن اللجوء إلى التسليم المراقب أو إتباع أساليب تحر خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة، تكون للأدلة المتوصل إليها بهذه الأساليب حجيتها وفقا للتشريع والتنظيم المعمول بهما**".[2]

كما تم الإشارة إلى إجراء التسليم المراقب بصورة ضمنية في المادة 16مكرر ق.إ.ج، التي تنص على مايلي:" **يمكن ضباط الشرطة القضائية، وتحت سلطتهم أعوان الشرطة القضائية، ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره، أن يمددوا عبر كامل الإقليم الوطني عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه فيهم بارتكاب الجرائم المبينة في**

[1] أنظر المادة 2 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، مرجع سابق.

[2] قانون رقم 06-01، يتعلق بالوقاية من الفساد مكافحته، مرجع سابق.

المادة16 أعلاه أو مراقبة وجهة أو نقل أشياء أو أموال أو متحصلات من ارتكاب هذه الجرائم أو قد تستعمل في ارتكابها".[1]

يُعرف إجراء التسليم المراقب بأنه أحد التقنيات المستحدثة للكشف عن الجرائم الخطيرة، ويُعد من أساليب البحث والتحري والمراقبة، والتي تهدف إلى الوصول إلى الرؤوس المدبرة للأنشطة الإرهابية الإجرامية. ومن خلال استقراء نصوص المواد ذات الصلة المذكورة أعلاه، يتضح أن آلية التسليم المراقب لا تقتصر فقط على تتبع وجهة نقل الشحنات غير المشروعة، بل يشمل أيضًا مراقبة الأشخاص، وكذا وجهات نقل الأموال والأشياء، سواءً داخل الإقليم الوطني للدولة أو خارجها.

يُعد إجراء التسليم المراقب من الأساليب الأكثر استخدامًا في إطار التحري عن جرائم الإرهاب الإلكتروني، لاسيما فيما يتعلق بمسائل سفر الأشخاص بغرض تقديم أو تلقي تدريبات حول آليات ارتكاب أفعال إرهابية إلكترونية، أو تتبع الأموال الموجهة لتمويل الجماعات الإرهابية، بالإضافة إلى مراقبة الشحنات غير المشروعة، مثل الأسلحة التي غالبًا ما تُرسل مجزأة إلى قطع، وموجهة إلى المنظمات الإرهابية.

2) شروط تطبيق آلية التسليم المراقب

حدد قانون الإجراءات الجزائية جملة من الضوابط الموضوعية والإجرائية الواجب مراعاتها لضمان شرعية الإجراء، ونجاح العملية، ونظرا لخطورة إجراء التسليم المراقب، قام المشرع الجزائري بحصر الجرائم التي يسمح فيها اللجوء إلى إستعمال هذه العملية، في المادة 7/16ق.إ. ج، والمتمثلة في: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد.

كما إشترط المشرع الجزائري على ضابط الشرطة القضائية، وتحت سلطتهم أعوان الشرطة القضائية، الذين يتمتعون باختصاص إقليمي موسع بخصوص التحري عن جريمة الإرهاب الإلكتروني، الحصول على **إذن** وموافقة السلطات المختصة، والمتمثلة في وكيل الجمهورية، كما يشترط في الإذن أن يكون مكتوبا، مسببا ومبررا، ويتضمن مجموعة من العناصر كنوع الجريمة ومبررات اللجوء إلى هذه العملية.

[1] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

أما في حال ما كانت عملية التسليم المراقب على المستوى الدولي وتتعدى الحدود الإقليمية لدولة، يشترط التأكد من وجود إتفاقية دولية بين الدولتين، وهذا ما أكدته المادة 20من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، التي تنص على ما يلي:"**... اتخاذ مل يلزم من تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب، وكذلك ما تراه مناسبا من استخدام أساليب تحرّخاصة أخرى، مثل المراقبة الإلكترونية أوغيرها من أشكال المراقبة، والعمليات المستترة...**".[1]

الفرع الثاني: آلية التفتيش الإلكتروني عن جريمة الإرهاب الإلكتروني

يعتبر التفتيش أبرز إجراءات التحقيق، التي تهدف إلى جمع الأدلة للوصول إلى الحقيقة، وهو الإجراء المعتمد للكشف عن الجرائم التقليدية، حيث بمجرد وصول خبر وقوع جريمة معينة يقوم ضابط الشرطة القضائية بالإنتقال إلى مكان وقوعها، لممارسة صلاحيته المتعلقة بالجريمة المخولة له قانونا.

لكن نظرا للتحولات الحاصلة في مجال الجريمة، أين أصبح يتم الإعتماد على تكنولوجيا الإعلام والإتصال، كوسيلة لتخطيط والتحضير وتنفيذ الجرائم الإلكترونية، وأبرزها جريمة الإرهاب الإلكتروني، ظهرت الحاجة إلى إستحداث إجراءات تحقيق تواكب هذا التطور نظراً لارتباطه ببيانات ومعلومات قد تكون مخزنة في بيئة افتراضية، وتخضع لحماية قانونية خاصة، لذا سنبرز في هذا الفرع أهم إجراء مستحدث والمتمثل في آلية التفتيش الإلكتروني من خلال تحديد مفهومه **(أولا)** ضوابطه **(ثانيا)** ثم آثاره **(ثالثا)**.

أولا: مفهوم التفتيش الإلكتروني

نظرا لطبيعة جريمة الإرهاب الإلكتروني، التي تستغل الفضاء الرقمي كبيئة للإجرام، قام المشرع الجزائري بموجب القانون رقم 09-04 الذي يهدف إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، باستحداث وسيلة جوهرية لجمع الأدلة الرقمية في الفصل الثالث منه، تحت عنوان القواعد الإجرائية، تفتيش المنظومات المعلوماتية.

لم يُعرف المشرع الجزائري إجراء تفتيش المنظومة المعلوماتية في القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، لكن تم تحديد

[1] أنظر المادة 20 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، مرجع سابق.

مفهوم المنظومة المعلوماتية في المادة 2 منه التي تنص:" **أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين**".[1]

إذْ تبرز خصوصية التفتيش الإلكتروني الذي يختلف عن التفتيش التقليدي في المحل الذي ينصب عليه التفتيش، كون أن هذا الأخير ينصب على المنازل وعلى الأشخاص، بينما التفتيش الإلكتروني ينصب على الحاسب الآلي، الذي يتكون من عناصر مادية من (وحدات الإدخال، وحدات الإخراج)، ومن عناصر معنوية (برامج وتطبيقات وأنظمة التشغيل...)، بتالي فالمنظومة المعلوماتية هي البيئة الكاملة التي تحتوي على الأجهزة، والبرمجيات والبيانات والتي تعمل معا لتحقيق معالجة آلية للمعطيات.

بتالي يمكن تعريف التفتيش الإلكتروني على أنه إجراء من إجراءات التحقيق المستحدثة، للكشف عن الجرائم المحددة في المادة 4 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، والذي يخضع في ضوابطه لقانون الإجراءات الجزائية، حيث تباشره السلطة القضائية المختصة وكذا ضباط الشرطة القضائية، من خلال الدخول إلى نظام المعالجة الآلية للمعطيات لغرض تفتيشها ولو عن بعد، وذلك تطبيقا للمادة 1/5 من القانون 09-04 التي تنص على جواز تفتيش المنظومات المعلوماتية كلها أو جزء منها، وكذا منظومات تخزين المعلوماتية.[2]

ثانيا: ضوابط التفتيش الإلكتروني

نظرا للتطور الذي آلت إليه جرائم الإرهاب، والتي أصبحت تستخدم تكنولوجيا الإعلام والإتصال كأداة لتخطيط وتنفيذ الأفعال الإرهابية، بات من الضروري تكييف إجراءات التفتيش التقليدية بما يتمشى مع النسخة المستحدثة لهذه الأخيرة، وقد استجاب المشرع الجزائري لذلك، من خلال وضع قواعد إجرائية تتلاءم مع طبيعة جريمة الإرهاب الإلكتروني، والمتمثلة في إجراء تفتيش المنظومة المعلوماتية، وقد أحاطها المشرع بجملة من الضوابط، منها الموضوعية **(1)** ومنها الإجرائية **(2)**.

[1] قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] أنظر المادة 1/5 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

1) الشروط الموضوعية لإجراء التفتيش الإلكتروني

نظم المشرع الجزائري الشروط الموضوعية لإجراء التفتيش الإلكتروني، في القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ونظرا لحساسية هذا الإجراء وما ينطوي عليه من مساس بخصوصية الأفراد، حصرت المادة3و 4من ذات القانون مبررات اللجوء إليه، والمتمثلة في حماية النظام العام، وكذا لمقتضيات التحريات أو التحقيقات القضائية في الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذا في حال وجود احتمال وقوع اعتداء على منظومة معلوماتية، تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وفي إطار تنفيذ طلبات المساعدة القضائية الدولية في الجرائم المعلوماتية بصفة عامة.

ما يُلاحظ من المادة 4من القانون 09-04[1]، أن التفتيش الإلكتروني موجه في المرتبة الأولى لتحقيق في الجرائم الإرهابية، سواء التقليدية، وهي الأفعال الواردة في المادة 87مكرر من قانون العقوبات، أو في صورته المستحدثة أي الإرهاب الإلكتروني وكذا أفعال التخريب أو الجرائم الماسة بأمن الدولة بصفة عامة.

2) الشروط الإجرائية لإجراء التفتيش الإلكتروني

لضمان صحة إجراء التفتيش الإلكتروني، حرص المشرع الجزائري على تحديد مجموعة من الضوابط الإجرائية الواجب إتباعها، وذلك في قانون الإجراءات الجزائية، وكذا في القانون الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته.

إذ يختص بإجراء التفتيش الإلكتروني تطبيقا للمادة 5 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، كل من السلطات القضائية المختصة، والمتمثلة في قاضي التحقيق بإعتباره صاحب الاختصاص الأصيل، وكذا وكيل الجمهورية، وكذلك يجوز لجهة التحقيق ندب ضابط شرطة قضائية، للقيام بإجراء تفتيش المنظومة المعلوماتية.

[1] " ...أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني..." أنظر المادة 4 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

كما يمكن لسلطات القضائية المكلفة بالتفتيش -وهم ضباط الشرطة القضائية-، بإذن من السلطات القضائية المختصة، تسخير كل شخص ذو كفاءة في مجال تكنولوجيا الإعلام والإتصال له دراية بعمل المنظومة المعلوماتية محل التفتيش، أو بالتقنيات نظام الحماية للمعطيات المعلوماتية التي تتضمنها، وذلك بهدف مساعدة وتزويد ضباط الشرطة القضائية بكل المعلومات الضرورية للوصول إلى الدليل.

كما تستعين السلطات المكلفة بالتحري والتحقيق بمقدمي الخدمة[1]، خصوصًا فيما يتعلق بالمعطيات المرتبطة بالتجهيزات الطرفية المستعملة للاتصال، والتي تُمكّن السلطات المختصة من تحديد نوع الجهاز، ورقم التعريف الفريد له، ونظام التشغيل، وإعدادات الاتصال، والمتصفح المستخدم، وغيرها من المعلومات التقنية ذات الصلة، وهذا عملا بالمادة 11من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.[2]

كما يُشترط من أجل إضفاء الصفة القانونية والإجرائية، على عمليات التحري والتفتيش الإلكتروني الحصول على إذن مسبق وصريح، من طرف وكيل الجمهورية أو قاضي التحقيق لمباشرة تفتيش المنظومة المعلوماتية، ويجب أن يتضمن الإذن على مجموعة من العناصر، التي تبين وصف الجرم موضوع البحث عن الدليل، وعنوان الأماكن التي ستتم وتفتيشها وإجراء الحجز فيها.

باعتبار أن التفتيش الإلكتروني ينصب على منظومة معلوماتية، فإن ذلك يفترض وجود جهاز إلكتروني (سواء كان حاسوبًا آليًا، هاتفًا ذكيًا، أو أي جهاز آخر يُستخدم في المعالجة الآلية للمعطيات). وبناءً عليه، فإن شروط تفتيش المنظومة المعلوماتية قد تختلف باختلاف مكان تواجد هذا الجهاز الإلكتروني.

كما خص المشرع الجزائري جريمة الإرهاب الإلكتروني بأحكام خاصة في مرحلة التحقيق، حيث نص على أنه بمجرد وصول خبر وقوع الجناية، تقوم الضبطية القضائية بالإنتقال إلى مكان وقوعها لإجراء المعاينة التقليدية وذلك تطبيقا لأحكام المواد 42 و63ق.إ.ج.

[1] يُقصد بمقدمي الخدمة: " أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها" المادة 2 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

[2] للاستزادة أنظر المادتين 5 و11 من لمادة 11من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

كما أتاح القانون إمكانية الدخول إلى مسكن الشخص المشتبه فيه بارتكابه جريمة إرهاب إلكترونية، أو مسكن شخص أخر يشتبه في حيازته لأشياء لها علاقة بالجريمة، أو الدخول إلى أماكن عامة، وذلك لغرض البحث عن الأجهزة الإلكترونية المستعملة في إرتكاب جريمة الإرهاب الإلكتروني، لإجراء تفتيش في المنظومة المعلوماتية، في كل ساعة من ساعات النهار والليل، ودون شرط حضور صاحب المسكن، أو حضور الشهود، غير أنه إذا وقع التفتيش في مسكن شخص ملزم قانونا بكتمان السر المهني، يجب مراعاة ذلك، وإتخاذ التدابير اللازمة للحفاظ على ذلك السر المهني.[1]

أما المعاينة الإلكترونية، فلم يتطرق المشرع الجزائري لأحكامها في قانون الإجراءات الجزائية، ويقصد بالمعاينة الإلكترونية انتقال ضابط الشرطة القضائية إلى البيئة الرقمية للجريمة، لمعاينة الآثار الرقمية التي يتركها الإرهابي أثناء استخدامه للشبكة المعلوماتية؛ فتشمل هذه الآثار جميع الرسائل والاتصالات وسجلات التصفُّح، وأرشيف البحث عبر الجهاز الإلكتروني، وتتم هذه العملية عن بُعد، أي يمكن في مكتب ضابط الشرطة القضائية دون الحاجة إلى تنقل ميداني.

ولضمان فاعلية المعاينة الإلكترونية ونجاحها، يتعين على ضابط الشرطة القضائية الإنتقال سريعًا وبمرونة إلى المسرح الافتراضي للجريمة فور ورود البلاغ بوقوع جريمة الإرهاب الإلكتروني، ثم السيطرة الكاملة عليه عبر استخدام التقنيات الرقمية، وذلك لضمان عدم إتلاف الأدلة وكذا لعدم مبارحة الموقع.

في السياق ذاته، وبنظر لخصوصية جريمة الإرهاب الإلكتروني من جهة، وطبيعة الدليل الرقمي من جهة أخرى، أجاز المشرع الجزائري في المادة 2/5و3من القانون 09-04، بعد إبلاغ السلطات القضائية المختصة، أي وكيل الجمهورية وقاضي التحقيق، تمديد التفتيش في حدود الإقليم الوطني للدولة إلى منظومة معلوماتية أخرى موجودة في جهاز آخر، وذلك في حال وجود دلائل توحي بأن المعطيات المتعلقة بالإرهاب الإلكتروني المبحوث عنها موجودة في المنظومة الثانية، وأن الوصول إليها مرتبط بالمنظومة الأولى.

لكن إذا كانت المنظومة المعلوماتية خارج الإقليم الوطني للدولة، فإن تمديد التفتيش إلى المنظومة الثانية، يكون بمساعدة السلطات الأجنبية المختصة، تطبيقا لمبدأ المعاملة بالمثل وللاتفاقيات الدولية، وهذا ما أكدته26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.[2]

[1] أنظر المادتان 45 و47 من الأمر 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] أنظر المادة 26 من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، مرجع سابق.

عند استكمال عملية التفتيش الإلكتروني، يتعين على ضابط الشرطة القضائية تحرير محضر عن عملية التفتيش الإلكتروني، وذلك طبقا لأحكام المادة 18 ق.إ.ج التي تنص:" **يتعين على ضباط الشرطة القضائية أن يحرروا محاضر بأعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات والجنح التي تصل إلى علمهم. وعليهم بمجرد إنجاز أعمالهم أن يو افوه مباشرة بأصول المحاضر...** ".[1]

ثالثا: آثار التفتيش الإلكتروني عن جريمة الإرهاب الإلكتروني

بعد إتمام السلطات القضائية المختصة عملية التفتيش، تقوم بضبط كل ما يمكن أن يؤدي لإظهار الحقيقة، ويُعدّ الضبط الوسيلة القانونية التي تُمكّن السلطات المكلفة بالتحقيق من وضع يدها على الأدلة[2]، وبهذا المعنى، يُتصوَّر الضبط في إطار الأدلة المادية، والتي يمكن أن تشمل الأجهزة الإلكترونية المستعملة في إرتكاب الجريمة، دون أن يشمل الأدلة المعنوية، أو ما يسمى بالأدلة الإلكترونية،

من أجل تكييف الإجراءات مع خصوصية الجريمة الإلكترونية، إستحدث قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، أحكام تتماشى مع طبيعة الجريمة الإلكترونية، والمتمثلة في الحجز على المعطيات المعلوماتية.

إذْ يُعرف الدليل الإلكتروني بأنه: " **الدليل المأخوذ من أجهزة الكمبيوترويكون في شكل ذبذبات أو نبضات مغناطسية أوكهربائية يمكن تجميعها باستخدام برامج تطبيقات وتكنولوجيا، وهي مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم**".[3] بعد التعريف بالدليل الإلكتروني، يثور التساؤل حول مدى حجيته أمام القضاء، ومدى اقتناع القاضي به كوسيلة لإثبات جريمة الإرهاب الإلكتروني، وفي هذا السياق، أجازت المادة 212 ق.إ.ج. إثبات الجرائم بأي طريق من طرق الإثبات، مما يفسح المجال للاعتراف بالدليل الإلكتروني كوسيلة للإثبات.

كما أكدت هذه المادة حرية القاضي في إصدار أحكامه تبعًا لاقتناعه الشخصي، وهو ما يعزز مبدأ السماح بالاستعانة بأي دليل أو وسيلة إثبات، طالما أنها تساهم في تكوين اقتناع القاضي. ويؤكد نص المادة

[1] أنظر المادة 18 من الأمر 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] عالية سمير، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت-لبنان، 2020، ص .488.

[3] طاهري حسين، الجرائم الإلكترونية:(ماهيتها وخصائصها وتصنيفها وأنواعها والوقاية منها، أركانها، الاختصاص القضائي بالجرائم المعلوماتية، المسؤولية الجزائية الناشئة عن الجرائم المعلوماتية، في اثباتها الدليل الإلكتروني، في مكافحتها وطنيا ودوليا مرفقة بالاجتهاد القضائي المقارن والتشريعات المقارنة والمعاهدات الدولية)، منشورات دار الخلدونية، الجزائر،2022، ص.265.

307 من ق.إ.ج أن القانون لا يطلب من القاضي أن يقدم الوسائل التي وصل بها إلى تكوين اقتناعه في القضية، مما يدل على أن القاضي له الحرية المطلقة في بناء اقتناعه على أي دليل، شرط أن يكون مشروعًا.

إنطلاقا من التحليل السابق، يُقصد بالمشروعية، أن يكون الحصول على الدليل الإلكتروني قد تمّ عبر عمليات بحث وتحري وتحقيق خاضعة للضوابط القانونية؛ فإذا حصل عبر عملية تفتيش إلكتروني باطل ينتهك القواعد القانونية، فلا يقبل كدليل. وكذا يجب أن يكون الدليل يقيني، ويجب مناقشة الدليل الإلكتروني في معرض المرافعات شفاهة، ولا يكتفي القاضي بما هو مدون في المحاضر فقط.

بناءً على ذلك، فإن عملية الحجز على المعطيات المعلوماتية تُعدّ مرحلة أساسية، في إطار التفتيش الإلكتروني في جرائم الإرهاب الإلكتروني، وتتطلب احترامًا صارمًا لإجراءات وذلك لضمان الحفاظ على سلامة المعطيات وصحتها. وتنطلق هذه الإجراءات عادة بعد أن تكتشف السلطات المكلفة بتفتيش المنظومة المعلوماتية، معلومات ومعطيات مخزنة في هذه المنظومة المعلوماتية.

تقوم السلطات المكلفة بالتفتيش بعملية نسخ هذه الأدلة الرقمية، في دعامة تخزين إلكترونية كـ(الأقراص الصلبHard Disk، أقراص الحالة الصلبةSSD، مفاتيحUSB ، بطاقات الذاكرةSD cards، الأقراص المضغوطة أو الرقميCD/DVD)، وذلك حتى تكون هذه الأدلة قابل للحجز والوضع في أحراز مختومة، وذلك عملا بأحكام المادة 2/84و3 ق.إ.ج التي تنص على ما يلي:**"يجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة..."**.[1]

كما أجاز القانون للسلطات المختصة بالتفتيش، إستعمال كافة الوسائل التقنية لتشكيل أو إعادة تشكيل المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط ألا يؤدي ذلك إلى المساس بسلامة المعطيات أو تغيير محتوها، كما أشار المشرع الجزائري إلى إجراء الحجز عن طريق منع الوصول إلى المعطيات، الموضوعة تحت تصرف الأشخاص المرخص لهم إستعمال المنظومة، وذلك في حال ما استحال على السلطات المكلفة بالتفتيش توقيع الحجز لأسباب تقنية.[2]

[1] أنظر المادة 2/84و3 الأمر 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] أنظر المادتين 6 و7 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

أما في حال ما كانت المعطيات المحجوزة تحمل محتوىً ذا طابع إجرامي، فإن السلطات المكلفة بالتفتيش تتخذ التدابير اللازمة لمنع الاطلاع عليها، سواء من خلال تكليف شخص ذو كفاءة في المجال التقني لتولي هذه المهمة، أو من خلال التعاون مع مقدمي خدمات الإنترنت الذين يتدخلون، في إطار التزاماتهم، لسحب المحتويات المخالفة للقانون، أو عبر إعاقة أو حظر الوصول إليها من خلال وضع ترتيبات تقنية تحدّ من إمكانية الدخول إليها، وهذا عملا بأحكام المواد8 و11 و12 من القانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.[1]

المطلب الثاني: تدابير الحماية الجزائية المستحدثة في جريمة الإرهاب الإلكتروني

أولى المشرع الجزائري أهمية بالغة لمسألة توفير حماية قانونية فعّالة، للشهود والخبراء والضحايا المبلغين والمساهمين في تقديم معلومات حول مرتكبي جريمة الإرهاب الإلكتروني، من خلال إقراره لمجموعة من التدابير الحمائية الإجرائية وغير الإجرائية.

إذْ يعود سبب هذه الحماية إلى الطبيعة الخاصة لهذه الجريمة، وما يحيط بها من مخاطر أمنية على سلامة حياتهم، وحياة عائلتهم وضغوط نفسية واجتماعية، وهذا ما أكدته المادة 65مكرر19 ق.إ.ج التي تنص:" **يمكن إفادة الشهود والخبراء من تدبير أو أكثر من تدابير الحماية غير الإجرائية و/أو الإجرائية المنصوص عليها في هذا الفصل إذا كانت حياتهم أو سلامتهم الجسدية أو حياة أو سلامة أفراد عائلاتهم أو أقاربهم أو مصالحهم الأساسية معرضة لتهديد خطير، بسبب المعلومات التي يمكنهم تقديمها للقضاء والتي تكون ضرورية لإظهار الحقيقة في قضايا الجريمة المنظمة أو الإرهاب أو الفساد**" .

لكن قبل التطرق لهذه التدابير، يجدر أن نقدم تعريفا لهذه الفئات الثلاث، فالشاهد هو شخص طبيعي يدلي بأقوال تتعلق بالواقعة الإجرامية محل النظر، وما عاينه بنفسه، على أن يكون إدراكه دقيقاً وصادراً عن إرادة حرة، وألا يكون محكوماً عليه بعقوبة جناية، وألا تربطه بالمتهم صلة قرابة، وألا يكون قانوناً ممنوعاً من أداء الشهادة. أما الخبير هو شخص ذو معارف وكفاءة علمية أو فنية، تستعين بها

[1] لتفصيل أكثر أنظر المواد 8 و11 و12 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

المحكمة، عند الإقتضاء من أجل إدراك أو إثبات وقائع، متعلقة بمسائل فنية أو علمية، خارجة عن نطاق معارف القاضي القانونية [1]، أما الضحية هو الشخص المتضرر من الجريمة.

إنطلاقا مما سبق، سيتم دراسة هذا المطلب كالتالي: التدابير غير الإجرائية **(الفرع الأول)**، والتدابير الإجرائية **(الفرع الثاني)** المقررة للحماية الجزائية للشهود والخبراء والضحايا في جريمة الإرهاب الإلكتروني.

الفرع الأول: التدابير غير الإجرائية لحماية الشهود والخبراء والضحايا في جريمة الإرهاب الإلكتروني

نظراً للطابع التهديدي الذي تكتنف به جريمة الإرهاب الإلكتروني، حرص المشرع الجزائري على توفير حماية خاصة للشهود والخبراء، وللضحايا -عند تواجدهم كشهود - فسّن مجموعة من التدابير غير الإجرائية، والتي يمكن تفعيلها تلقائيا من السلطات المختصة، أو بطلب من ضباط الشرطة القضائية أو من الشخص المعني، سواء قبل مباشرة المتابعة الجزائية أو في أي مرحلة من الاجراءات القضائية.

باعتبار ان هذه الحماية تقرر قبل المتابعة الجزائية، فيناط بوكيل الجمهورية سلطة إقرارها وذلك بعد التشاور مع السلطات المختصة، ويختص بتنفيذها ومتابعتها إلى غاية فتح تحقيق قضائي، حيث ينتقل بعدها الاختصاص إلى قاضي التحقيق، وتظل هذه التدابير سارية المفعول الى حين زوال الخطر، أو تعديلها.

كما حصرت المادة65مكرر20 ق.إ.ج مجموع هذه التدابير غير الاجرائية والتي يمكن عرضها كتالي: **" تتمثل التدابير غير الإجرائية لحماية الشاهد والخبير، على الخصوص، فيما يأتي: إخفاء المعلومات المتعلقة بهويته،- وضع رقم هاتفي خاص تحت تصرفه،- تمكينه من نقطة اتصال لدى مصالح الأمن،- ضمان حماية جسدية مقربة له مع إمكانية توسيعها لأفراد عائلته و أقاربه،- وضع أجهزة تقنية وقائية بمسكنه،- تسجيل المكالمات الهاتفية التي يتلقاها أو يجريها بشرط مو افقته الصريحة،- تغيير مكان إقامته،- منحه مساعدة اجتماعية أو مالية،- وضعة إن تعلق الأمر بسجين، في جناح يتوفر على حماية**

[1] ركاب أمينة، حماية الشهود والخبراء والضحايا في القانون الجزائي الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: القانون العام المعمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد -تلمسان-، الجزائر، 2020، ص.31.

خاصة،- يستفيد الضحايا أيضا من هذه التدابير في حالة ما إذا كانوا شهودا.- تحدد كيفيات تطبيق هذه المادة، عند الاقتضاء عن طرق التنظيم".[1]

يُستخلص من نص المادة أعلاه، أن المشرع الجزائري قصر الحماية على الضحايا بصفة الشهود فقط، دون أن يقرّ لهم أي حماية بوصفهم ضحايا إرهاب إلكتروني مستقلين، الأمر الذي يفضي إلى استبعادهم من الاستفادة من التدابير الحمائية المقررة خارج نطاق الشهادة، كما أن المشرع الجزائري لم يبيّن صراحة استمرارية سريان التدابير الحمائية غير إجرائية عقب مرحلة المحاكمة، وغياب أي تحديد في النصّ حول مدة الحماية أو شروط استمرارها، مما يطرح إشكالية قانونية تتعلّق بمدة النفاذ وآلية إنهائها.[2]

الفرع الثاني: التدابير الإجرائية لحماية الشهود والخبراء والضحايا في جريمة الإرهاب الإلكتروني

نصّ المشرع الجزائري على مجموعة من التدابير الإجرائية الخاصة بحماية الشهود والخبراء والضحايا أثناء مجريات الدعوى العمومية، وذلك لضمان سلامتهم وتسهيل مساهمتهم الفعّالة في الكشف عن جريمة الإرهاب الإلكتروني دون تأثرهم بالضغوط أو التهديدات.

حصرت المادة 65 مكرر 23 ق.إ. ج مجموعة من التدابير الإجرائية الحمائية، معتمدًا مبدأ تدرج هذه التدابير وفقًا لجسامة كل حالة، والتي نص عليها كما يلي:" **تتمثل التدابير الإجرائية لحماية الشاهد والخبير فيما يلي: عدم الإشارة لهويته أو ذكر هوية مستعارة في أوراق الإجراءات، - عدم الإشارة لعنوانه الصحيح في أوراق الإجراءات، - الإشارة، بدلا من عنوانه الحقيقي، إلى مقر الشرطة القضائية أين تم سماعه أو إلى الجهة القضائية التي سيؤول إليها النظر في القضية...".**[3]

يتبيّن من نص المادة أعلاه، استبعاد المشرع الجزائري لضحايا الإرهاب الإلكتروني تمامًا من دائرة الحماية الإجرائية، إذ يُعدّ إقصاء الضحايا من نطاق الحماية الإجرائية إخلالًا بجوهر العدالة الإجرائية، مما يفرض الاقتصار في عنوان الفصل السادس على "حماية الشهود والخبراء" وحذف "الضحايا" تناغمًا مع مضمون النصوص القانونية.

---

[1] للاستزادة أنظر المواد من65مكرر20إلى 65مكرر22 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] لوكال مريم،" الآليات القانونية المستحدثة لحماية الشهود والخبراء والضحايا بموجب الأمر15-02 المعدل لقانون الإجراءات الجزائية: دراسة مقارنة"، **حوليات جامعة الجزائر-1-**، المجلد31، العدد2، جامعة الجزائر-1-، الجزائر، 2017، ص. ص .115 -118.

[3] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

تبعا لذلك، فعلى الرغم من إقرار أحكام خاصة لحماية هوية كل من الشاهد والخبير في جريمة الإرهاب الإلكتروني خلال مراحل الدعوى العمومية، فقد أولى المشرع عناية أكبر بهوية الشاهد، وهذا ما يظهر جليًا من المادة65 مكرر 23 إلى غاية 65مكرر25ق.إ. ج، التي ألزمت وكيل الجمهورية بالاحتفاظ بسرية الملف الخاص بهوية وعنوان الشاهد والخبير ويمنع الاطلاع عليه دون إذنه، فيما تعود للنيابة العامة وحدها صلاحية تكليف المعنيين بالحضور عند الاقتضاء.

كما يتولى قاضي التحقيق إخفاء هويتهم في محاضر السماع، عبر الامتناع عن ذكر أسمائهم أو بياناتهم الشخصية مع الإشارة إلى الأسباب الأمنية المبررة لذلك، ويحفظ جميع المعلومات المتعلقة بهويتهم في ملف سري خاص، يحتفظ به قاضي التحقيق ويمنع الاطلاع عليه دون إذنه، ولضمان عدم تعريضهم للخطر، يعرض قاضي التحقيق مسبقاً على ذاته كافة الأسئلة التي تعتزم أطراف الدعوى توجيهها إليهم، ويستثني أو يعدل أي سؤال قد يؤدي إلى كشف هويتهم. كما يتخذ كل الاحتياطات الإجرائية اللازمة بما يضمن سلامتهم واستمرار تعاونهم دون مخاوف أمنية.

في إطار عصرنة قطاع العدالة، حرص المشرع الجزائري على توفير حماية إضافية لشهود في جريمة الإرهاب الإلكتروني، وذلك من خلال إستحداث تقنية المحادثة المرئية عن بُعد والتي يتم اللجوء إليها، لمقتضيات حسن سير العدالة أو الحفاظ على الأمن أو لدواعي احترام مبدأ الآجال المعقولة، استعمال هذه التقنية في الإجراءات القضائية، لسماع الشاهد وهذا ما يصطلح عليه بالشهادة الإلكترونية.

لذا ولضمان صحة الشهادة الإلكترونية، يجب أن تُقدَّم في إطار الخصومة القضائية، ولا يُعتد بأي شهادة تُؤدى خارج هذا الإطار. ويتم سماع الشهادة الإلكترونية أمام قاضي الحكم عن طريق تقنية المحادثة المرئية عن بعد، وذلك وفقاً لأحكام المادة 65 مكرر 27 من ق.إ. ج.[1]

كما يشترط أن تُؤدى الشهادة شفاهةً أمام المحكمة، وأن تخضع للمناقشة الشفهية من قبل الخصوم. ولا يُلجأ إلى الشهادة الإلكترونية إلا لإثبات الوقائع المادية أو لإثبات الحق المتنازع عليه، خاصة في قضايا الإرهاب. ورغم أن المشرع الجزائري لم ينص صراحة على مصطلح "الشهادة الإلكترونية" في ق.إ.ج،

[1] أنظر المادة 65مكر27 والمادة 441مكرر من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

إلا أنها تُعد من وسائل الإثبات، تطبيقاً لأحكام المادة 212 من ق.إ.ج، ويمكن للقاضي أن يستند إليها لإثبات الوقائع المعروضة عليه، وتقدير مدى حجيتها بناءً على قناعته الشخصية في قضايا الإرهاب.[1]

كما منح المشرع الجزائري السلطة التقديرية لجهة الحكم في الفصل، فيما إذا كانت معرفة هوية الشاهد عن جريمة الإرهاب الإلكتروني ضرورية، لممارسة حقوق الدفاع، وإلا وجب إبقاؤها سرية، مع فتح استثناء ضيق يتمثل في حال كانت أقواله الدافعة الوحيدة للإدانة، إذ يُسمح عندئذ بالكشف عن هويته شريطة موافقته، واتخاذ تدابير حماية إضافية، وتظلّ شهادته مجرد استدلال لا يكفي وحده للإدانة.

كما كرّس المشرع الجزائري حماية فعّالة ومتقدمة، لهوية الشاهد والخبير في جريمة الإرهاب الإلكتروني، عبر تجريم كشفها وفرض عقوبات صارمة، بالحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50.000دج إلى 500.000دج، وهذه خطوة تعكس حرصًا تشريعيًا على ضمان أمنهم وسلامتهم.

المبحث الثاني: الآليات المؤسساتية المستحدثة لتصدي لجريمة الإرهاب الإلكتروني

تُعدّ المواجهة المؤسساتية لجريمة الإرهاب الإلكتروني من أبرز المداخل الفعّالة للتصدي لهذا التهديد المتنامي، وهو ما أدركته السلطات الجزائرية من خلال إستحداث مؤسسات وقائية وقضائية. ففي الجانب الوقائي، تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الجرائم المعلوماتية)، كجهاز وطني متخصص يهدف وضع الاستراتيجيات الوطنية المناسبة للوقاية من الجرائم.

في هذا السياق، يبرز الدور العملي الذي تضطلع به الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، في تجسيد الاستراتيجية الوطنية للوقاية من جرائم الإرهاب الإلكتروني، من خلال وضع آليات للوقاية والتدخل، ومواكبة التطورات التقنية المتسارعة. كما تعمل الهيئة على دعم التعاون القضائي، داخليًا وخارجيًا، لمواجهة هذا النوع من الجرائم ذات الطابع العابر للحدود، وهو ما يعكس أهمية تقييم فعالية أدائها ومساهمتها في التصدي للتهديدات الإلكترونية المتزايدة[2] **(المطلب الأول).**

[1] قادري نور الهدى، "الشهادة الإلكترونية وحجيتها في الإثبات"، **مجلة الفكر القانوني والسياسي**، المجلد 7، العدد01، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي-الأغواط، الجزائر، 2023، ص.1600.

[2] قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

أما في الجانب القضائي، فقد تم استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الذي أُنيط به اختصاص إقليمي ونوعي ذو طابع خاص، و ذلك لضمان التحقيق والمتابعة في الجرائم المعلوماتية، والجرائم المعقدة، وفي مقدّمتها جريمة الإرهاب الإلكتروني، وذلك بالنظر لطبيعتها العابرة للحدود، ويمثل القطب الجزائي دعامة أساسية لتفعيل أدوات العدالة الجزائية المتخصصة، من خلال إجراءات اتصال دقيقة بملف الدعوى، واعتماد آليات متقدمة في التحقيق، فضلًا عن التنسيق مع الجهات الأمنية والقضائية لملاحقة الجناة وضمان فعالية الردع **(المطلب الثاني)**.

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كآلية لمواجهة الإرهاب الإلكتروني

برز المشرع الجزائري في المادة 14من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المهام الجوهرية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنبع أهمية هذه المهام من الطبيعة القانونية للهيئة **(الفرع الأول)** كسلطة إدارية مستقلة.

كما تُوضح هذه المادة الدور الفعّال للهيئة للوقاية والتصدي لتهديدات الإرهاب الإلكتروني، وذلك من خلال تنفيذ استراتيجية الوقاية من جرائم الإرهاب الالكتروني، من خلال تنسيق عمليات المراقبة الوقائية للإتصالات الإلكتروني، كما أن دورها لا ينحصر فقط في الوقاية فحسب، بل يمتد ليشمل تنفيذ المساعدة القضائية الوطنية والدولية **(الفرع الثاني)**، وذلك بهدف حماية المجال الرقمي لدولة الجزائرية.

الفرع الأول: الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم المعلوماتية

تلا صدور القانون رقم 09-04 الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، العديد من المراسيم الرئاسية لتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تباينت في تحديد الطبيعة القانونية للهيئة، وهذا يعكس تطورًا تدريجيًا في تصور الدولة الجزائرية، لأهمية هذا الجهاز في مواجهة تهديدات الإرهاب الإلكتروني. وبناءً على ذلك، سيُعتمد في هذه الدراسة على المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

تبعا لذلك، اعترف المشرع الجزائري في المادة 2 منه، بالطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، بأنّها **"سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى رئيس الجمهورية"**[1]، وتأكيداً لاستقلاليتها، تخضع مهامها لرقابة السلطة القضائية فقط، كما تملك صلاحية إصدار القرارات وفرض العقوبات. وباعتبارها ذات شخصية معنوية، فهي المسؤولة عن تسيير مواردها المالية والبشرية، وينتج عن ذلك ذمة مالية مستقلة وأهلية قانونية في حدود القانون، ومقر بمدينة الجزائر مع إمكانية نقله بمرسوم رئاسي، كما لها حق التقاضي بصفتها مدعية أو مدعى عليها، وتتحمل وحدها مسؤولية التعويض عن الأضرار المادية والمعنوية الناجمة عن نشاطها.[2]

كما حرص المشرع الجزائري، لضمان حسن سير عمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أن يتم تنظيمها ضمن هيكل ثنائي يشمل مجلس توجيه ومديرية عامة. إذ يتشكل مجلس التوجيه، برئاسة الأمين العام لرئاسة الجمهورية، وعضوية أمناء عامين من الوزارات وقادة الأجهزة الأمنية، وممثّل عن رئاسة الجمهورية، ومكلف بوضع السياسات العامة والمداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية، وتقييم التهديدات السيبرانية لتحديد عملية التصدي لها.

أما المديرية العامة-بإشراف المدير العام المعين بمرسوم رئاسي، تختص بالتنفيذ الميداني للقرارات عبر مديريات متخصصة (المراقبة الوقائية واليقظة الإلكترونية، الإدارة والوسائل، الدراسات والتلخيص، التعاون واليقظة التكنولوجيا، والملحقات الجهوية)، واقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والسهر على تنفيذها، مع الحرص على حماية سرية العمل وضمان الحماية القانونية لموظفيها ضد أي ضغوط أو تهديدات ناشئة عن ممارستهم للمهام.[3]

كما حرص المشرّع الجزائري على ضبط سير عمل الهيئة وضمان انسجامها وفعاليتها، من خلال العمل على تكوين مواردها البشرية التي تضم قضاةً وفق الضوابط التشريعية، وضباطاً وأعواناً للشرطة القضائية من الأمن الوطني والدرك الوطني يُحدَّد عددهم بقرارات مشتركة، بالإضافة إلى مستخدمي الدعم

[1] أنظر المادة 02 المرسوم رئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] لتفصيل أكثر أنظر المواد2 و3 و29 من المرسوم رئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[3] للاستزادة أكثر أنظر المواد من 6إلى 12 والمادة 39من المرسوم رئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

التقني والإداري للمصالح العسكرية، مع إتاحة إمكانية توظيف فئات أخرى والاستعانة بالخبراء عند الحاجة. وأكّد المرسوم في المادة 22 على أن حماية المعلومات السرية تمثل أولوية، إذ يُلزم كل من يُسمح له بالاطلاع عليها بأداء اليمين القانونية أمام المجلس القضائي يتعهّد فيه بالإخلاص والتصرّف الشريف.

كما فرض واجب التحفّظ والسّر المهني على مستخدمي الهيئة الوطنية للوقاية من الجرائم المعلوماتية، ومقدمي خدماتها، مع إخضاع المطلعين على المعلومات السرية لإجراءات التأهيل اللازمة.[1]

الفرع الثاني: تنفيذ إستراتيجية الوقاية من جرائم الإرهاب الالكتروني

أولى المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، اهتمامًا خاصاً بجريمة الإرهاب، وذلك من خلال تعزيز الدور الوقائي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتمكينها من المراقبة الوقائية للإتصالات الإلكترونية**(أولا)**، وتنفيذ طلبات المساعدة القضائية الوطنية والدولية لتصدي لجريمة الإرهاب الإلكتروني **(ثانيا)**.

أولا: مفهوم المراقبة الوقائية للاتصالات الإلكترونية

تعتبر المراقبة الوقائية للإتصالات الإلكترونية من المهام الجوهرية المناطة بالهيئة الوطنية للوقاية من الجرائم المعلوماتية، وهذا ما جاء في المادة 5/4 من المرسوم الرئاسي رقم 21-439، التي تنص:"**...ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة...**".

لم يقم المشرع الجزائري بتعريف إجراء المراقبة الوقائية للإتصالات الإلكترونية، واكتفى بتعريف الاتصالات الإلكترونية في المادة 2من قانون 09-04، على النحو التالي:" **أي تراسل أو إرسال أو استقبال علامات أو إشارات أوكتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية**".[2]

[1] أنظر المواد من 20 إلى23 والمادة32 من مرسوم رئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[2] قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحها، مرجع سابق.

إنطلاقا من ذلك، يمكن تعريف المراقبة الوقائية للإتصالات الإلكترونية بأنه، إجراء وقائي وسري يسبق مرحلة البحث والتحري، تختص به الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويقوم على مراقبة الاتصالات الإلكترونية، بالمنعى الموضح في نص المادة أعلاه، وذلك لغرض الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

1) ضوابط المراقبة الوقائية للإتصالات الإلكترونية

نظرا لما يشكله إجراء المراقبة الوقائية للإتصالات الإلكترونية من مساس بحرمة الحياة الخاصة، حرص المشرع الجزائري على وضع مجموعة من الضوابط الموضوعية **(1)**، وأخرى إجرائية **(2)**، لضمان مشروعية الإجراء، وحماية الحق في سرية المراسلات والاتصالات الخاصة المكرسة في الدستور الجزائري.

أ) الضوابط الموضوعية لإجراء المراقبة الوقائية للإتصالات الإلكترونية

تُعد المراقبة الوقائية للاتصالات الإلكترونية أحد الأساليب الحساسة، التي تلجأ إليها الدولة في إطار حماية أمنها المعلوماتي الوطني، غير أن ممارستها تستوجب توافر شروط موضوعية، تضمن التوازن بين متطلبات الوقاية واحترام الحقوق الأساسية، ويمكن حصرها فيما يلي:

نظرا لخطورة إجراء المراقبة الوقائية للاتصالات الإلكترونية، حصر المشرع الجزائري في المادة 1/4من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الحالات التي يُسمح فيها اللجوء لإجراء المراقبة الوقائية للإتصالات الإلكترونية، وهي كتالي: " **يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3أعلاه في الحالات الآتية:**

أ) - للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ب) - في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ج) - لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، د) - في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة..."[1]

[1] قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، المرجع نفسه.

انطلاقًا من نص المادة أعلاه، يتبيّن أن المشرّع الجزائري قد حصر اللجوء إلى إجراء المراقبة الوقائية للاتصالات الإلكترونية في الجرائم التي تُشكّل تهديدًا صريحًا لأمن الدولة، وعلى رأسها جريمة الإرهاب. وبناءً على ذلك، فإن الحق في الخصوصية، رغم أهميته، لا يُمكن التمسّك به متى تعلّق الأمر بجرائم من هذا النوع، باعتبار أن حماية كيان الدولة واستقرارها تتقدّم في سلم الأولويات على الحريات الفردية، وهذا ما أكدته المادة2/79 من الدستور الجزائري، التي تنص:**" يعاقب القانون بكل صرامة على الخيانة والتجسس والولاء للعدو، وعلى الجرائم المرتكبة ضدّ أمن الدولة"**.[1]

كما حددت المادة 3من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، دواعي اللجوء لإجراء المراقبة الوقائية للإتصالات الإلكترونية، وحصرتها في مقتضيات حماية النظام العام، وكذا لمستلزمات التحريات والتحقيقات القضائية.

ب) الضوابط الإجرائية لإجراء المراقبة الوقائية للإتصالات الإلكترونية

وضع المشرّع الجزائري مجموعة من الضوابط الإجرائية الدقيقة، لتنظيم استخدام إجراء المراقبة الوقائية للإتصالات الإلكترونية، بهدف منع التعسف وضمان احترام القانون، ويمكن تحديدها فيما يلي:

أشارت المادة4من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، على شرط جوهري لمباشرة إجراء المراقبة الوقائية للإتصالات الإلكترونية، والمتمثل في الحصول على **إذن** من السلطات القضائية المختصة، ويُعتبر النائب العام لدى مجلس قضاء الجزائر هو المختص بمراقبة وتقديم الإذن لمباشرة إجراء المراقبة الوقائية للإتصالات الإلكترونية[2]، و يُشترط في الإذن أن يكون مكتوبا، مبررًا ومحدد المدة، وقد حُددت مدة الإذن لمباشرة إجراء المراقبة الوقائية للإتصالات الإلكترونية في جرائم الإرهاب،(6) أشهر قابلة للتجديد، عملا بالمادة 4من قانون 09-04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[1] مرسوم رئاسي رقم 20 -442، يتعلق بإصدار التعديل الدستوري، مرجع سابق.

[2]" لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الامر بالحالة المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13أدناه، إذنا لمدة ستة (6) أشهر قابلة لتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها". المادة 2/4و3 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحها، مرجع سابق.

أما الجهة المختصة حصريًا بمباشرة إجراءات المراقبة الوقائية للاتصالات الإلكترونية، هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ما أشارت إليه كل من الموادة4[1] و25من من المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال[2].

على أن يُمارس إختصاص المراقبة الوقائية للاتصالات الإلكترونية عبر الأجهزة المركزية للهيئة (مديرية المراقبة الوقائية واليقظة الإلكترونية) وهذا ما أكدته المادة 1/14 التي تنص على ما يلي:" **تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية بما يأتي: أ- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول**".

تساعدها في ذلك أجهزتها المساعدة (مصلحة التعاون واليقظة التكنولوجية)، طبقا للمادة 18 من المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، التي تنص على مايلي:" **تكلف مصلحة التعاون واليقظة التكنولوجيا، على الخصوص، بما يأتي: أ) - التعاون مع الشركاء فيما يخص تنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ب) - اليقظة الدائمة في متابعة تكنولوجيا الإعلام والاتصال المتعلقة بنشاطات الهيئة**".

كذلك الملحقة الجهوية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا تطبيقا للمادة 19 من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، التي تنص:" **تُكلف الملحقة الجهوية بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيا**

[1] " ضمان المراقبة الوقائية للإتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة." المادة5/4 من المرسوم الرئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] "قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها، تكلف الهيئة حصريا، في مجال اختصاصها، بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة، وفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، على أن تخضع لإجراءات التفتيش والحجز لأحكام قانون الإجراءات الجزائية". المادة 25 من المرسوم الرئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

الاعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا...".[1]كما يمكن للهيئة القيام بوضع وحدات مراقبة مجهزة بالتجهيزات التقنية، لغرض مراقبة الاتصالات الإلكترونية.

يُكلف بتنفيذ إجراء المراقبة الوقائية للإتصالات الإلكترونية، ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ويقوم الأعوان المنتمين للهيئة بمساعدتهم في المسائل التقنية المرتبطة بإجراء المراقبة الوقائية للإتصالات الإلكترونية، كما يمكن أن تستعين الهيئة بالخبراء والموظفين المختصين في مجال تكنولوجيا الإعلام والإتصال.

ففي ذات السياق، تتمتع الهيئة دون سواها بصلاحية استيراد وحيازة واقتناء واستعمال، كل الوسائل والتجهيزات التقنية للقيام بعملية المراقبة الوقائية للإتصالات الإلكترونية.[2]

في هذا السياق، تنص المادة 30 من المرسوم الرئاسي رقم 21-439، على تمكين القضاة وضباط الشرطة القضائية التابعين للهيئة، أثناء ممارسة وظائفهم ووفق الشروط القانونية، من القيام بإجراءات تفتيشية في الأماكن أو الهياكل أو الأجهزة، عند توفر معلومات أو شبهات تفيد بوجود وسائل أو تجهيزات موجهة لمراقبة الاتصالات الإلكترونية، دون ترخيص، وهذا ما يؤكد احتكار الهيئة لهذه الوسائل وعدم جواز امتلاكها أو استعمالها من طرف جهات أخرى، باستثناء المنشآت التابعة لوزارة الدفاع الوطني.[3]

كما أجاز المشرع الجزائري للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، وضع ترتيبات تقنية تمس نوعا ما بالحياة الخاصة للغير، وذلك لغرض جمع وتسجيل المعطيات ذات صلة للوقاية من جرائم الإرهاب، ويجب تحرير تقرير يبين طبيعة هذه الترتيبات والغرض منها.

تلتزم السلطات المختصة عند الانتهاء من عملية المراقبة الوقائية للإتصالات الإلكترونية، بحفظ المعطيات المستخرجة أو المسجلة من العملية، وفقًا للكيفيات والشروط المحددة في المواد 27 و28 و29من

[1] مرسوم رئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع نفسه.

[2]"تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير". المادة 8/4 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحها، مرجع سابق.

[3] أنظر المادة 30 من المرسوم الرئاسي رقم 21-439، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، وتسلّيمها إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحتفظ السلطات القضائية، دون سواها بهذه المعطيات أثناء المدة القانونية المحددة، ومنع توظيفها لأي أغراض أخرى غير تلك المنصوص عليها قانونًا.

ثانيا: تنفيذ المساعدة القضائية الوطنية والدولية لتصدي لجريمة الإرهاب الإلكتروني

نظرًا للتهديد الأمني الوطني والدولي الذي تسببه جريمة الإرهاب الإلكتروني، التي تستغل الفضاء الرقمي في الترويج للفكر المتطرف وتنفيذ العمليات الإرهابية، أصبحت الحاجة مُلحة إلى آليات فعالة لمكافحته. وتضطلع الهيئة الوطنية للوقاية من الجرائم المعلوماتية بدور محوري في هذا المجال، من خلال دعم السلطات القضائية والأمنية، وتبادل المعلومات على المستوى الوطني **(1)**، وعلى المستوى الدولي **(2)**.

1) تنفيذ المساعدة القضائية الوطنية لتصدي لجريمة الإرهاب الإلكتروني

تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال مهمة جوهرية، في سبيل التصدي لجريمة الإرهاب الإلكتروني وهي" **مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية**".[1]

لم يتم التفصيل في الإجراءات الواجب اتباعها عند تدخل الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال لمساعدة السلطات القضائية، لكن وبالرجوع إلى المادة 3 من القانون رقم09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، فإنه يتم تطبيق القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية وكذا في القانون رقم 09-04، وعليه نُخلص إلى مايلي:

[1] أنظر المادة 14 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحها، مرجع سابق.

تتدخل الهيئة الوطنية لمساعدة السلطات القضائية وتزويدها بالمعلومات والمعطيات المتعلقة بجريمة الإرهاب الإلكتروني، إما بطريقة تلقائية أي بمبادرتها دون طلب مسبق، أو بناء على طلب رسمي من طرف السلطات القضائية أو مصالح الشرطة القضائية، وهذا طبقا لما ورد في المادة 5/14 من المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، وهذا ما يعكس الدور التنسيقي الاستشاري للهيئة اتجاه السلطات القضائية.

أما في الحالة التي تستدعي اتخاذ الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، إجراءات تمس بسرية المراسلات والاتصالات، وبحرمة الحياة الخاصة للغير لمساعدة السلطات القضائية ومصالح الشرطة القضائية، فذلك يستدعي حصول الهيئة[1] وكذا مصالح الشرطة القضائية على إذن قضائي مسبق، ويكون مكتوبا، مسببا ومبررا، ومحدد المدة.

يلتزم القائمين بهذا الإجراء عند إتمام العملية بـ: **"تحرير محضر أشغال وفقا لأحكام القانون، الاحتفاظ بالمعلومات المستقاة أثناء عمليات المراقبة، تسجيل الاتصالات الالكترونية التي تكون موضوع مراقبة وتحرر وفقا للشروط والأشكال المنصوص عليها في القانون، تسليم التسجيلات والمحررات إلى السلطات القضائية المختصة، الالتزام بالسر المهني".**[2]

2) تنفيذ المساعدة القضائية الدولية لتصدي لجريمة الإرهاب الإلكتروني

في إطار التعاون الدولي لمواجهة التهديدات العابرة للحدود، يبرز دور الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، في تنفيذ المساعدة القضائية الأجنبية كآلية أساسية لتعزيز جهود التصدي لجريمة الإرهاب الإلكتروني، من خلال تبادل المعلومات، وتنسيق التحقيقات، ودعم

[1] " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة ". المادة6/4 قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

[2] حابت أمال،" دورالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، **المجلة الدولية للبحوث القانونية والسياسية**، المجلد05، العدد03، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمّه لخضر- الوادي، الجزائر، 2021، ص .475.

ملاحقة المتورطين وفقًا للمعايير القانونية الدولية، وهذا عملا بالمادة 4/14من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.[1]

نتيجة لما تم بيانه، فالمساعدة القضائية الأجنبية تتخذ عدة أشكال، يأتي في مقدمتها تبادل المعلومات، وذلك تطبيقا للمادة 12/4من المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، التي تنص على ما يلي:" **السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها ...**".

في هذا السياق، تبرز أهمية تبادل المعطيات والمعلومات المفيدة، التي من شأنها المساعدة على التعرف على مرتكبي جريمة الإرهاب الإلكتروني، وذلك وفقًا لما ورد في المادة 3/14 من المرسوم الرئاسي رقم 21-439الذي يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المعلوماتية، التي تنص على مايلي:" **تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتعرف عليهم.**"

كما يشمل تنفيذ المساعدة القضائية الأجنبية أيضًا طلب اتخاذ إجراءات تحفظية، وهو إجراء قانوني تتقدم به الدولة الطالبة إلى دولة أخرى، تطلب فيه اتخاذ تدبير قضائي مؤقت أو عاجل، يكون لازماً للمساعدة في الفصل في قضية جنائية منظورة أمام القضاء،[2] وهو ما يُعرف بإجراء تبادل الإنابة القضائية الدولية، وهذا عملا بالمادة17 من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، التي تنص على مايلي:" **تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل**".[3]

[1] " تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم ". المادة4/14 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

[2] حابت أمال، مرجع سابق، ص.476.

[3]قانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، مرجع سابق.

تبعا لذلك، فقد حصر المشرع الجزائري في قانون الإجراءات الجزائية، وكذا في القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، جملة من الضوابط الواجب مراعاتها لقبول المساعدة القضائية الدولية، والتي يمكن حصر أهمها في شكلية إرسال طلبات المساعدة القضائية في قضايا الإرهاب الإلكتروني، والتي تكون في الأصل بالطريق الدبلوماسي، أو بواسطة وسائل وتقنيات الإتصال السريعة كالفاكس أو البريد الإلكتروني.[1]

كما تُنفذ المساعدة القضائية الدولية في إطار قانوني منظم، حيث تقوم أساسًا على وجود اتفاقيات دولية ثنائية أو متعددة الأطراف تُبرم بين الدول المعنية، أو في حال عدم وجودها، على مبدأ المعاملة بالمثل، الذي يتيح التعاون القضائي استنادًا إلى التزام متبادل، بتقديم المساعدة وفق ما تمنحه الدولة الطالبة في حالات مماثلة[2]، إذ يُعد تجريم الإرهاب الإلكتروني في كلتا الدولتين، من الشروط الجوهرية للمساعدة القضائية الدولية، إذ لا يمكن تنفيذ طلب المساعدة ما لم يكن الإرهاب الإلكتروني يُشكل جريمة وفقًا للتشريع المعمول به، في كل من الدولة الطالبة والدولة المطلوب منها.

ضف إلى أن الاستجابة لطلب المساعدة القضائية الدولية تخضع لسلطة التقديرية لدولة المطلوب منها، حيث يمكن أن تكون بالقبول الكامل، أو الرفض وذلك في حال المساس بالسيادة الوطنية أو النظام العام، أو يمكن أن تكون الإجابة بالقبول المقيد بشروط أو قيود معينة، تراها الدولة ضرورية لحماية نظامها العام أو مصالحها الأساسية، كشرط المحافظة على سرية المعلومات المبلغة، وكذا بشرط عدم استعمالها في غير ما هو موضح في الطلب، وهذا عملا بأحكام المواد16و18 من قانون 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[1] "في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني. يمكن، في حال الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها". المادة 16 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، المرجع نفسه.

[2] حابت أمال، مرجع سابق، ص.477.

المطلب الثاني: القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كآلية لمواجهة جريمة الإرهاب الإلكتروني

شهدت المنظومة القضائية الجزائرية سنة 2021 تحولات عميقة، خاصةً مع تعديل قانون الإجراءات الجزائية بموجب الأمر رقم 21-11[1]، بحيث استدعت التحديات المتزايدة التي فرضتها ظواهر الجريمة المعقدة، لاسيما تلك التي تستغل تكنولوجيا الإعلام والإتصال كأداة لتنفيذ الجريمة، وعلى رأسها جريمة الإرهاب الإلكتروني، ضرورة إستحداث جهة قضائية مختصة في هذا النوع من الإجرام العصري.

في هذا السياق، تم استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، أو ما يصطلح عليه كذلك بالقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية، إذْ يتميز بهيكل تنظيمي واختصاص قضائي ذو طابع خاص **(الفرع الأول)** قادرة على مجابهة هذا النوع من الإجرام بفعالية، ويهدف إلى تحقيق نوع من النجاعة القضائية، في متابعة جرائم الإرهاب الإلكتروني **(الفرع الثاني)**.

الفرع الأول: الاختصاص القضائي للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

يعتبر القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إحدى أهم الهيئات القضائية المتخصصة، التي اعتمدها المشرع الجزائري في مواجهة جريمة الإرهاب الإلكتروني.

يستمد هذا القطب فعاليته من طبيعته المتخصصة، سواء من حيث هيكله التنظيمي من جهة، والذي يتشكل من وكيل جمهورية، والذي يعمل تحت السلطة السلمية للنائب العام لدى مجلس قضاء الجزائر، ويمارس هذا الأخير صلاحية النيابة العامة في القضايا التي تدخل ضمن اختصاصه، وكذا من قاضي تحقيق، ورئيس القطب اللذان يخضعان إداريا لسلطة رئيس مجلس قضاء الجزائر[2]، أو من حيث اختصاصه القضائي من جهة أخرى، والذي يتيح له معالجة القضايا الخطيرة والمعقدة والعابرة للحدود.

[1] أمر رقم 21-11 مؤرخ في 25غشت 2021، ج.ر.ج.ج عدد 65، الصادرة في 26غشت 2021، المعدل والمتمم للأمر رقم 66-155 مؤرخ في 8يونيو1966، يتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 48، الصادرة في 10يونيو1966

[2] أنظر المادة 211مكرر4 والمادة 211مكرر5 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، مرجع سابق.

يتجلى الاختصاص القضائي للقطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من خلال عدة أوجه، تشمل الاختصاص الإقليمي(**أولا**)، والنوعي (**ثانيا**)مما يستدعي الوقوف عند كل منهما.

أولا: الاختصاص الإقليمي للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

تُعدّ جرائم الإرهاب من الجرائم التي تتميّز بخصوصية معينة فيما يتعلّق بالاختصاص القضائي الإقليمي، إذ ينعقد الاختصاص لثلاث جهات قضائية مختلفة، وذلك باختلاف طبيعة جريمة الإرهـــاب.

إذ تعتبر محكمة مقر مجلس قضاء الجزائر، الجهة القضائية المختصة في المتابعة والتحقيق في الجرائم المحددة على سبيل الحصر في المادة 211مكرر18 ق.إ.ج والمتمثلة في **"عرقلة عمل السلطات العمومية أو حرية ممارسة العبادة والحريات العامة وسير المؤسسات المساعدة للمرفق العام، إتلاف منشآت الملاحة الجوية أو البحرية أو البرية، تخريب إتلاف وسائل الإتصال، الاعتداءات باستعمال المتفجرات أو المواد البيولوجية أو الكيميائية أو النووية أو المشعة أو غيرها من أسلحة الدمار الشامل، تمويل إرهابي أو منظمة إرهابية، كل جزائري ينشط أو ينخرط في الخارج في جمعية أو جماعة أو منظمة إرهابية أو تخريبية مهما كان شكلها أو تسميتها وكانت أفعالها موجهة للإضرار بمصالح الجزائر"**. ويمارس وكيل الجمهورية وقاضي التحقيق بمحكمة مقر مجلس قضاء الجزائر صلاحيتهما في كامل الإقليم الوطني.

أما الجهة الثانية تتمثل في المحكمة المختصة إقليميًا بالنظر في باقي جرائم الإرهاب التقليدية، باستثناء تلك المحصورة في المادة211مكرر18ق.إ. ج أعلاه، وهذا عملا بالنصوص المواد 211مكرر20 و211مكرر21 ق.إ.ج.[1] أما بالنسبة لجريمة الإرهاب الإلكتروني، وباعتبارها من الجرائم المستحدثة ذات الطابع الإلكتروني، فقد أسند المشرع الاختصاص فيها حصريًا للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ويمارس وكيل الجمهورية وقاضي التحقيق وكذا رئيس القطب، صلاحيتهم في كامل الإقليم الوطني، بمعنى يتمتعون باختصاص إقليمي موسع، (المادة 211مكرر27 ق.إ.ج).[2]

[1] لتفصيل أكثر أنظر المواد 211مكرر20 و211مكرر21 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

[2] "دون الإخلال بأحكام المادتين 211مكرر24و211مكرر25أعلاه، يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37و40و329من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها." المادة 211مكرر1/27 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

ضف إلى ذلك، فقد ذهب المشرع الجزائري إلى أبعد من ذلك، وقام بتمديد إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إلى خارج الإقليم الوطني، وجعله مختص بالنظر في الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، المرتكبة خارج الإقليم الوطني الجزائري وهذا تطبيقا للمادة15 من القانون رقم 09-04 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، التي تنص على مايلي:" **زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني**".

كما أشارت المادة 211 مكرر 22 ق.إ.ج، إلى نقطة جوهرية، حيث تنص على مايلي:" **ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها...**".[1]

من خلال إستقراء نص المادة أعلاه، يتضح أن المشرع الجزائري قد أسند للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مهمة المتابعة والتحقيق في جريمة الإرهاب الإلكتروني، دون أن يمنحه صراحةً صلاحية البحث والتحري.

ما يفتح المجال أمام قراءة تفسيرية، مفادها أن المشرع احتفظ بمهمة البحث والتحري في قضايا الإرهاب الإلكتروني لجهات أمنية متخصصة، والمتمثلة في الجهات القضائية المختصة وكذا مصالح الشرطة القضائية، والتي تملك إختصاص إقليمي موسع، يمتد إلى كامل الإقليم الوطني في إطار البحث والتحري في جرائم الإرهاب الإلكتروني، وهذا ما أكدته المادة 7/16 ق.إ. ج[2]، والجهة الثانية المتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[1] أمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

[2] " غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني." المادة7/16 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

ثانيا: الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

يتميّز الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بطابع خاص، ويعود ذلك لطبيعة الجرائم التي يعالجها، ويُلاحظ من خلال النصوص القانونية المنظمة لهذا القطب أن اختصاصه النوعي، يتوزع بين اختصاص خاص **(1)**، وحصري **(2)**، ومشترك **(3)**.

1) الاختصاص الخاص للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

تنص المادة 211مكرر22 ق.إ.ج على مايلي:" **ينشأ على مستوى مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها...**".[1]

إنطلاقا من نص المادة أعلاه، يتحدد الاختصاص الخاص للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، وكذا بالجرائم المرتبطة بالجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، والتي يمكن أن تكون جرائم تقليدية أو جريمة ذات طابع إلكتروني.

كما حدد المشرع الجزائري في نص المادة أعلاه، مفهوم الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال، وما يلاحظ عليه، أن هذا التعريف كرّس نهجًا توسعيًا في التجريم، وأناط بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مهمة التصدي لكل جريمة ترتكب باستعمال تكنولوجيا الإعلام والاتصال، كما طالت مظلة التجريم حتى الاستخدام غير المباشر، لتكنولوجيا الإعلام والاتصال لتيسير وتسهيل ارتكاب الجريمة، ليشمل بذلك أكبر قدر ممكن من الجرائم.

ما يُلاحظ كذلك في نص المادة أعلاه، أن المشرع الجزائري وسّع من نطاق الوسائل المستعملة في ارتكاب الجريمة، بحيث لم يحصرها في وسائط محددة، بل شمل كل وسيلة أو آلية لها صلة بتكنولوجيا الإعلام والاتصال، تاركًا المجال مفتوحًا أمام التطورات المستقبلية في هذا المجال، وهو ما يُضفي على النص طابعًا مرنًا ويمنحه قابلية للاستمرار والصلاحية على المدى البعيد، دون الحاجة لتعديلات متكررة.

[1] الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

يُستفاد من نص المادة أعلاه كذلك، وبإعتبار أن جريمة الإرهاب الإلكتروني تحمل وصف جناية، فالمشرع الجزائري قد خول للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، صلاحية مباشرة إجراءات المتابعة والتحقيق دون الامتداد إلى إصدار الأحكام، وهذا أكدته الفقرة الثانية من نص المادة أعلاه، أن القطب يختص فقط في الحكم في الجرائم التي تحمل وصف جنحة.

إذ تُسند مهمة الحكم والفصل في قضايا الإرهاب الإلكتروني، إلى محكمة الجنايات باعتبارها الجهة القضائية المختصة نوعيًا، وفقًا لطبيعة الجريمة كوصف جنائي، وذلك بتشكيلة خاصة، تضم قضاة فقط دون هيئة محلفين، بحيث تتشكل محكمة الجنايات الابتدائية من رئيس برتبة مستشار على الأقل في المجلس القضائي، بالإضافة إلى قاضيين مساعدين، أما محكمة الجنايات الاستئنافية تتشكل من قاض برتبة رئيس غرفة بالمجلس القضائي على الأقل، رئيسا، ومن قاضيين مساعدين.[1]

2) الاختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

في إطار تحديد الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، نصّ المشرع في المادة 211مكرر 24ق.إ.ج، على اختصاص حصري لهذا القطب، يتعلّق بفئات محددة من الجرائم[2]، مؤكدا بذلك وجوب مراعاة أحكام الفقرة الثانية من المادة211مكرر22 ق إ ج التي تنص:**" كما يختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحة".**

كما نصّت المادة 211مكرر 25ق.إ.ج على أن القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، يختص بالمتابعة والتحقيق والحكم في نوع معيّن من الجرائم، وهي الجرائم المتصلة بالتكنولوجيا التي تتسم بدرجة عالية من التعقيد، بالإضافة إلى الجرائم المرتبطة بها .غير أن المشرع الجزائري يُشدد ويؤكد على أن اختصاص هذا القطب في الحكم يظل محصورًا في الجنح فقط، دون أن يمتد إلى الجرائم التي تحمل وصف جناية.

يقصد بالجرائم المتصلة بالتكنولوجيا الإعلام والاتصال الأكثر تعقيدًا، بمفهوم المادة 211مكرر2/25 ق.إ.ج،**" الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع**

[1] "تتشكل محكمة الجنايات الابتدائية ومحكمة الجنايات الاستئنافية، عند الفصل في الجنايات المتعلقة بالإرهاب والمخدرات والتهريب، من قضاة فقط..." المادة 3/258من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، معدل ومتمم، المرجع نفسه.

[2] لتفصيل في الجرائم أنظر المادة 211مكرر24 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي".

انطلاقًا من المواصفات التي وضعها المشرع للجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدًا، يتبيّن بوضوح أن جريمة الإرهاب الإلكتروني تندرج ضمن هذا التصنيف، باعتبارها غالبًا ما تتسم بتعدد الفاعلين، واتساع النطاق الجغرافي لارتكابها، فضلًا عن جسامة آثارها وطابعها العابر للحدود، مما يستوجب بالضرورة استعمال وسائل تحرٍ خاصة، وأحيانًا اللجوء إلى آليات التعاون القضائي الدولي، بتالي تدخل ضمن إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

3) الاختصاص المشترك للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية

نظم المشرع الجزائري في المادة 211مكرر27ق.إ.ج، حالة من التداخل في الاختصاص بين القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والأقطاب الجزائية المتخصصة، وذلك في إطار ما يُعرف بالاختصاص المشترك، ويكون في الجرائم المحددة على سبيل الحصر والمتمثلة: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد، شرط أن تكون هذه الجرائم قد ارتُكبت أو تم تسهيل ارتكابها بواسطة تكنولوجيات الإعلام والاتصال.[1]

من ثم، يتضح جليًا أن جريمة الإرهاب الإلكتروني، تندرج بطبيعتها ضمن هذا النطاق، مما يُخول للقطب الجزائي الوطني لمكافحة الجرائم المعلوماتية، المتابعة والتحقيق فيها في إطار اختصاصه المشترك.

الفرع الثاني: إجراءات اتصال القطب الجزائي الوطني المعلوماتي بدعاوى الإرهاب الإلكتروني

في ظل التحديات التي تفرضها جريمة الإرهاب الإلكتروني، يبرز دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك من خلال الإجراءات التي يباشرها، للاتصال بملف الدعوى العمومية، وتفعيل وسائل تقنية حديثة خلال مراحل الدعوى تتلاءم مع طبيعة هذه الجريمة.

[1] أنظر المادة 211مكرر1/27 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

إذْ تُحدد الإجراءات الخاصة باتصال القطب بملف جريمة الإرهاب الإلكتروني، في الأحكام المنصوص عليها في المادة 211 مكرر 26 ق.إ.ج[1]، والتي تُحيل بدورها إلى مجموعة من النصوص القانونية التي توضح الإجراءات الواجب اتباعها، وذلك في حال ما كانت جريمة الإرهاب الإلكتروني، تدخل ضمن الاختصاص الحصري للقطب**(أولاً)**، أما المادة 211 مكرر 27 ق.إ.ج[2]، فهي تُحيل إلى مجموعة من النصوص القانونية التي تبيّن الإجراءات الواجب اتباعها للاتصال بملف الدعوى، إذا اعتُبرت الجريمة تدخل ضمن اختصاص المشترك للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال**(ثانيا)**.

أولا: الإجراءات الخاصة في إطار الاختصاص الحصري

بإعتبار جريمة الإرهاب الإلكتروني من الجرائم المعقدة، فيختص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالمتابعة والتحقيق فيها، ويتصل وكيل الجمهورية لدى القطب بملف جريمة الإرهاب الإلكتروني، من خلال مبادرة مصالح الضبطية القضائية، بإرسال كل التقارير الإخبارية وإجراءات التحقيق له، حيث يتلقى ضباط الشرطة القضائية التعليمات منه مباشرة. وفي حال ما تبيّن أن القضية تدخل ضمن اختصاص القطب، يتم فتح تحقيق قضائي، ويتلقى ضباط الشرطة الإنابات القضائية مباشرة من قاضي التحقيق لدى القطب.

أما إذا رأى وكيل الجمهورية أن القضية لا تدخل ضمن اختصاصه، فيصدر قرارًا بالتخلي عنها لفائدة وكيل الجمهورية المختص إقليميًا.؛ حيث يتلقى ضباط الشرطة القضائية التعليمات منه مباشرة. في ذات السياق، إذا تبين لقاضي التحقيق أن القضية لا تدخل ضمن اختصاصه، يصدر أمرًا بعدم الاختصاص، سواء من تلقاء نفسه أو بناءً على طلب وكيل الجمهورية، وتُحال الإجراءات إلى النيابة العامة المختصة إقليميًا. وتظل الأوامر التي سبق أن أصدرها قاضي التحقيق، نافذة إلى حين صدور أوامر جديدة من الجهة القضائية المختصة، على أن تُعاد كل إجراءات التحقيق والمتابعة بعد قرار عدم الاختصاص. [3]

---

[1] " تطبق على الاختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، المنصوص عليه في المادتين 211مكرر24 و211مكرر25 أعلاه، الإجراءات المنصوص في المواد 211مكرر19 إلى 211مكرر21 من هذا القانون". المادة211مكرر26 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

[2] "...تطبق، في هذه الحالة، الإجراءات المنصوص عليها في المواد 211مكرر4 إلى 211مكرر15من هذا القانون، أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال." المادة 211مكرر1/27 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، معدل ومتمم، المرجع نفسه.

[3] أنظر المادة 211مكرر21 من الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، المرجع نفسه.

ثانيا: الإجراءات الخاصة في إطار الاختصاص المشترك

وضع المشرع الجزائري إجراءات خاصة لتنظيم اتصال القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بملف الدعوى في جريمة الإرهاب الإلكتروني، وذلك في إطار ما يُعرف بالاختصاص المشترك، مع الجهات القضائية ذات الاختصاص الإقليمي الموسع، بما يضمن التنسيق وتفادي تداخل الصلاحيات القضائية. فيتصل وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بملف جريمة الإرهاب الإلكتروني تلقائيا، من خلال قيام وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع، بإرسال كل محاضر الضبطية القضائية، وكل إجراءات البحث والتحري المنجزة من طرفها.

كما يمكن أن يقوم وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالمطالبة بملف الإجراءات في أي مرحلة كانت عليها الدعوى، بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر، بحيث إذا كانت في مرحلة التحريات الأولية والمتابعة، يقوم وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع، بإصدار مقررا بالتخلي بعد تلقيه للالتماسات وكيل الجمهورية لدى القطب.

أما إذا كانت في مرحلة التحقيق تحال التماسات وكيل الجمهورية لدى القطب، من قبل وكيل الجمهورية لدى الجهات القضائية ذات الاختصاص الإقليمي الموسع، على قاضي التحقيق لدى هذه الجهة الاخيرة، والذي يصدر أمر بالتخلي لصالح قاضي التحقيق لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

يتم إرسال ملف الإجراءات مرفقا بجميع الأوراق والمستندات والأدلة، بمعرفة وكيل الجمهورية لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع، إلى وكيل الجمهورية لدى القطب، وتبقى كل الأوامر الصادرة من قاضي التحقيق لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع، سارية إلى غاية صدور أوامر مخالفة من طرف قاضي التحقيق لدى القطب، مع الحرص على تجديد كل الإجراءات المتخذة، ويتلقى ضباط الشرطة القضائية التعليمات والإنابات القضائية، مباشرة من وكيل الجمهورية وقاضي التحقيق لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

خـاتـمة

خـــاتمـــــة

في ختام دراستنا لموضوع جريمة الإرهاب الإلكتروني على ضوء القانون الجزائري، والتي حاولنا من خلالها التطرق لمختلف الجوانب القانونية المرتبطة بهذه الجريمة، سواء من حيث الأساس الموضوعي، أين استعرضنا مختلف النقاط، التي تبرز خصوصية هذه الظاهرة الإجرامية المعقدة والعابرة للحدود الوطنية، وكذا موقف الاتفاقيات الدولية المصادق عليها من طرف الجزائر، والتي أولت اهتماما بتجريم الإرهاب الإلكتروني، فضلا عن تحليل البنيان القانوني، من خلال تسليط الضوء على مختلف الأركان القانونية التي يقوم عليها التجريم في القانون الجزائري، وكذا الجزاءات الصارمة المفروضة لرّدع كل من المرتكبين والمساهمين في هذه الجريمة.

كما أن دراستنا لم تقتصر على الجانب الموضوعي فقط، بل تطرقنا أيضا إلى الجانب الإجرائي المرتبط بها، حيث ركزنا على مختلف أساليب التحري الخاصة المعتمدة من طرف مصالح الضبطية القضائية، وفرقة مكافحة الجريمة السيبرانية، في سبيل البحث والتحري والتحقيق عن هذه الجريمة، بما يتلاءم مع طابعها المعلوماتي والتقني. ونظرا لما ينطوي عليه الإرهاب الإلكتروني من تهديد على سلامة حياة الأشخاص وأمنهم، بادر المشرع الجزائري، على إقرار جملة من التدابير الحمائية القانونية، بما يكفل حماية أطراف الدعوى العمومية، إذ من شأنها أن تعزز تفاعل هؤلاء الأطراف مع أجهزة العدالة في سبيل تسهيل عملية ملاحقة الجناة في هذه الجريمة.

علاوة على ذاك، وفي سبيل الكشف عن جريمة الإرهاب الإلكتروني، تبنت الجزائر سياسة وقائية، تجسدت في إستحداث هيئة وطنية تهدف إلى الوقاية من الجرائم المعلوماتية بصفة عامة، ومن الإرهاب الإلكتروني على وجه الخصوص، كما تم تدعيم هذه السياسة، من خلال إستحداث قطب قضائي متخصص في المتابعة والتحقيق والحكم في الجرائم المعلوماتية.

بناءا على ما تقدم، يُمكن القول أن المشرع الجزائري وُفق إلى حد معين في وضع سياسة جنائية ناجعة لتصدي لجريمة الإرهاب الإلكتروني، سواء من حيث الجانب الموضوعي، أو من حيث الإجراءات المُسطرة للوقاية منها ولمواجهتها، إلا أن هذا التوفيق يبقى نسبيًا، ويستدعي مواصلة الجهود التشريعية لمواكبة التطور التكنولوجي، الذي تستغله الجماعات الإرهابية للتخطيط، والتنظيم، وتنفيذ الهجمات الإرهابية ونشر الفكر المتطرف.

في ضوء ما تم عرضه، تتجلى أبرز النتائج التي انتهت إليها هذه الدراسة التحليلية فيما يلي:

- من خلال تحليل النصوص القانونية ذات الصلة، سواء في قانون العقوبات أو القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، يتّضح أن المشرع الجزائري، لم يُدرج مصطلح الإرهاب الإلكتروني، واكتفى فقط بالإشارة إلى الأفعال الإرهابية التقليدية المرتكبة باستعمال تكنولوجيا الإعلام والإتصال، دون تخصيص تعريف صريح لها.
- جاء تجريم الإرهاب الإلكتروني في المنظومة القانونية الجزائرية، استجابةً للاتفاقيات الدولية العالمية والإقليمية، وسعيا لحمايةً أمن الدولة الجزائرية من التهديدات السيبرانية.
- تبنى المشرع الجزائري من خلال معالجته لجريمة الإرهاب الإلكتروني، سياسة تجريمية وقائية، أين قام بتوسيع نطاق التجريم ليشمل كل من ساهم، بشكل مباشر أو غير مباشر، في ارتكاب هذه الجريمة، كما أبقى مجال الوسائل التكنولوجية المستعملة في إرتكاب الأفعال الإرهابية مفتوحا، بما يسمح بتجريم مختلف الوسائل الحديثة والمستقبلية، ما يجعل من النصوص القانونية مرنة وصالحة في المدى البعيد، كما تجلّت هذه السياسة التجريمية الوقائية في العقوبات الصارمة، حتى وإن لم يفضي السلوك الإجرامي إلى أي نتيجة إجرامية، وهذا ما يعكس توجها ردعيًا صارما وواضحًا.
- تُعد السياسة المنتهجة من طرف المشرع الجزائري في القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، خُطوة إيجابية، إذ مكّنه هذا الإطار القانوني في شمل وتجريم عدد واسع من الجرائم المعلوماتية، وعلى رأسها جريمة الإرهاب الإلكتروني، من خلال إقراره بتجريم كل جريمة ترتكب أو يسهل إرتكابها باستعمال التكنولوجيا الحديثة.
- إن إستحداث منظومة وطنية لأمن الأنظمة المعلوماتية إلى جانب هيئة وطنية للوقاية من الجرائم المعلوماتية، يُعد بمثابة خطوة فعّالة تُعبر عن وعي الدولة الجزائرية بأهمية الوقاية وحماية الفضاء السيبراني، وتعزيز الأمن المعلوماتي الوطني، والحفاظ على الحقوق والحريات وأمن واستقرار الممتلكات العمومية الإلكترونية.
- وجود فرقة متخصصة لمكافحة الجريمة السيبرانية لدى مصالح الشرطة القضائية، يُعد مؤشرا نحو توجه المشرع الجزائري، إلى دعم التخصص في مجال مكافحة الجريمة، وهو ما يعكس إدراكًا لمدى أهمية الاستعانة بضباط وأعوان شرطة قضائية، متخصصين وذوي خبرة وكفاءة في المجال التقني والمعلوماتي.

- استحداث المشرع لقطب جزائي وطني مختص في المتابعة والتحقيق في الجرائم المعلوماتية، وعلى رأسها جريمة الإرهاب الإلكتروني، يعكس توجه المشرع الجزائري إلى دعم التخصص القضائي، بما يتلاءم مع الطبيعة المعقدة لهذه الجريمة، ويضمن فعالية من طرف قضاة مُلمين بالجانب التقني والمعلوماتي.

انطلاقا من النتائج المتوصل إليها، نقدم مجموعة من الاقتراحات لتعزيز الإطار القانوني لمكافحة جريمة الإرهاب الإلكتروني:

- باعتبار أن الإرهاب ليس بظاهرة حديثة على الدولة الجزائرية، وهي جريمة معروفة منذ القدم، لكن ببروز صورتها الحديثة المرتبطة باستعمال تكنولوجيا الإعلام والاتصال كأداة لإرتكاب الأفعال الإرهابية، نقترح تخصيص قانون مستقل لمكافحة جرائم الإرهاب، ليشمل الأشكال التقليدية والحديثة لهذه الجريمة.
- في إطار تجريم الإرهاب الإلكتروني، نقترح على المشرع الجزائري إعادة النظر في نظرية الظروف القانونية المرتبطة بهذه الجريمة، من خلال وضع نصوص قانونية مفصلة تنظم الظروف المخففة والمشددة بدقة.
- نقترح على المشرع الجزائري إعادة النظر في قانون الإجراءات الجزائية، وتكييفه أكثر مع خصوصية الجرائم المعلوماتية، بما في ذلك جريمة الإرهاب الإلكتروني، خصوصا أن الإجراءات المعمول بها حاليا أعدت أساسا للتعامل مع الجرائم التقليدية.
- يختص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المتابعة والتحقيق في جريمة الإرهاب الإلكتروني، أما الفصل وإصدار الأحكام يكون أمام محكمة الجنايات، بتالي حبذا لو يتم إستحداث جهة قضائية متخصصة في الفصل في الجنايات المعلوماتية، نظرا لما تتطلبه من إلمام دقيق بالجوانب التقنية، وهو ما قد تفتقر إليه المحاكم العادية بسبب عدم تخصص القضاة في المجال المعلوماتي.
- نقترح تعزيز التعاون الدولي، بين الجزائر والدول ذات الخبرة المتقدمة في المجال التكنولوجي، بهدف تبادل المعارف والخبرات حول أساليب إرتكاب الجرائم الإرهابية الإلكترونية، أو الجريمة المعلوماتية بوجه عام، وكذا لدعم قدرات وجهود الدولة الجزائرية على التصدي لهذا النوع من الإجـــرام.

قـائمة المصـادر والمراجـع

قائمة المصادروالمراجع

I. باللغة العربية

أولا: الكتب

1. العبيدي عمر عباس خضير، الإرهاب الإلكتروني في نطاق القانون الدولي، المركز العربي، القاهرة،2021.

2. الفيل علي عدنان، الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقي، بيروت،2011.

3. القرعان محمود أحمد محمد، الجرائم الإلكترونية، دار وائل، عمان، 2017.

4. أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر الانترنت، مكتبة الوفاء القانونية، الإسكندرية،2011.

5. بتشيم بوجمعة، الذكاء الإصطناعي في منظومة العدالة الحديثة على ضوء أحدث أحكام التشريع والقضاء المقارن إلى غاية سنة 2022، الطبعة الأولى، ألفا للوثائق، عمان- الأردن، 2023.

6. بوعلي سعيد، شرح قانون العقوبات الجزائري: (القسم العام)، الطبعة الرابعة، دار بلقيس، الجزائر، 2021.

7. خالد حسن أحمد لطفي، الإرهاب الإلكتروني:(آفة العصر الحديث والآليات القانونية للمواجهة)، دار الفكر الجامعي، الإسكندرية، 2018.

8. خلفي عبد الرحمان، محاضرات في القانون الجنائي العام، دار الهدى، عين مليلة-الجزائر،2012.

9. _____، الإجراءات الجزائية في القانون الجزائري المقارن، الطبعة السابعة، دار بلقيس للنشر، الجزائر، 2024.

10. طارق جمعة مهدي، الذكاء الاصطناعي ومكافحة الإرهاب، دار الفكر الجامعي، الإسكندرية،2023.

11. طاهري حسين، الجرائم الإلكترونية:(ماهيتها وخصائصها وتصنيفها وأنواعها والوقاية منها، أركانها، الاختصاص القضائي بالجرائم المعلوماتية، المسؤولية الجزائية الناشئة عن الجرائم المعلوماتية، في اثباتها الدليل الإلكتروني، في مكافحتها وطنيا ودوليا مرفقة بالاجتهاد القضائي المقارن والتشريعات المقارنة والمعاهدات الدولية)، منشورات دار الخلدونية، الجزائر،2022.

12. عالية سمير، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت-لبنان، 2020.

13. عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي:(الماهية والجزاء)، منشورات الحلبي الحقوقية، لبنان، 2020.

14. عبد القادر المومني نهلة، الجرائم المعلوماتية، دار الثقافة، عمان، 2008.

15. كافي مصطفى يوسف، جرائم:(الفساد-غسيل الأموال-السياحة-الإرهاب الإلكتروني-المعلوماتية)، مكتبة المجتمع العربي، عمان، 2013.

ثانيا: الأطروحات والرسائل الجامعية

1) أطروحات الدكتوراه

1. ركاب أمينة، حماية الشهود والخبراء والضحايا في القانون الجزائي الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: القانون العام المعمق، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد - تلمسان-، الجزائر، 2020.

2. زامل صهيب سهيل غازي، البحث والتحري عن الدليل الإلكتروني في المسائل الجزائية: (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة وهران-2، الجزائر، 2022.

3. شعنبي صابرة، الجهود الدولية في مكافحة الإرهاب الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي-تبسة، الجزائر، 2019.

4. نجاري بن حاج علي فايزة، مكافحة الإرهاب الإلكتروني في القانون الدولي، أطروحة مقدمة لنيل شهادة الدكتوراه، التخصص: قانون، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2023.

2) رسائل الماجستير

1. بودور رضوان، الجزاء الجنائي، رسالة لنيل شهادة الماجستير، تخصص : القانون الجنائي والعلوم الجنائية، كلية الحقوق بن عكنون، جامعة الجزائر، الجزائر، 2001.

2. دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة لنيل شهادة الماجستير، شعبة: القانون الجنائي، كلية الحقوق، جامعة منتوري- قسنطينة، الجزائر، 2013.

3. طارق جواد كاظم الجابري إرساء، جريمة الإرهاب الإلكتروني: (دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، بغداد، 2012.

4. نجاري بن حاج علي فايزة، الآليات الإلكترونية لمكافحة الإرهاب الإلكتروني، رسالة لنيل شهادة الماجستير، التخصص: القانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري- تيزي وزو، الجزائر، 2016.

ثالثا: المقالات العلمية

1. البدو محمد عبد الله آمل،" دور الذكاء الإصطناعي في تحسين تجربة التعلم الرقمي وتحقيق الأمان الرقمي في العملية التعليمية"، **مجلة بحث وتربية،** المجلد14، العدد01، المعهد الوطني للبحث في التربية، الجزائر،2024، ص. ص 30 -51.

2. الشوابكة عواد عدنان، "دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلوماتي في جامعة الطائف"، **مجلة دراسات و ابحاث،** المجلد 11، العدد04، جامعة زيان عاشور-الجلفة، الجزائر، 2019، ص. ص 164-187.

3. بشريف وهيبة، "أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي"، **مجلة الحوار الثقافي**، المجلد7، العدد01، كلية العلوم الاجتماعية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2018، ص. ص 54-65.

4. بن تركي ليلى،" تأثير الأعذار القانونية على الجزاء الجنائي في التشريع الجزائري"، **مجلة الشريعة والقانون**، المجلد7، العدد2، كلية الشريعة والاقتصاد، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر،2018، ص. ص 51 -92.

5. بن عابد بشير، "الشخصية المعنوية"، **مجلة القانون والعلوم السياسية**، المجلد08، العدد02، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحي أحمد- النعامة، الجزائر،2022، ص. ص 346- 358.

6. بن فرحات نور الدين، عمري عبد القادر، " الطابع العابر لمحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي"، **مجلة أبحاث قانونية وسياسية**، المجلد09، العدد01، كلية الحقوق والعلوم السياسية، جامعة الصديق بن يحيى-جيجل، الجزائر،2024، ص. ص 660- 673.

7. جدي وفاء،" الإرهاب الإلكتروني أسبابه بين النص والتطبيق"، **مجلة مقاربات**، المجلد03، العدد 05، جامعة الجلفة، الجزائر،2015، ص. ص 33- 43.

8. حابت أمال،" دورالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، **المجلة الدولية للبحوث القانونية والسياسية**، المجلد05، العدد03، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمَّه لخضر- الوادي، الجزائر، 2021، ص. ص 465-483.

9. حفصاوي كمال، مخلوف عمر،" التفتيش الإلكتروني بين ضرورة التحقيق والحق في سرية المراسلات والاتصالات"، **مجلة الباحث للدراسات الأكاديمية**، المجلد 11، العدد01، كلية الحقوق والعلوم السياسية، جامعة باتنة1- لحاج لخضر، الجزائر،2024، ص. ص 326-345.

10. حفظاوي سعيد، "ظاهرة الإرهاب: (تعريفها، دوافعها، أشكالها، وأساليبها)"، **مجلة الحقوق والعلوم السياسية**، المجلد09، العدد1، جامعة عباس لغرور-خنشلة، الجزائر،2022، ص. ص 543-555.

11. زاوي رابح، "الإعلام الأمني في مواجهة ظاهرة التجنيد الإلكتروني للتنظيمات المتطرفة"، **مجلة الآفاق للأبحاث السياسية والقانونية**، المجلد2، العدد4، قسم العلوم السياسية، جامعة عمار ثليجي-الأغواط، الجزائر،2019، ص. ص 38-55.

12. زمورة داود،" الجمع بين تخفيف وتشديد العقوبة في التشريع الجزائري"، **مجلة الحقوق والعلوم السياسية**، المجلد10، العدد1، جامعة عباس لغرور-خنشلة، الجزائر، 2023، ص. ص 956 -975.

13. سحر جمال عبد السلام زهران، "الجوانب القانونية الدولية لجريمة الإرهاب الإلكتروني"، **مجلة كلية السياسة والاقتصاد**، المجلد05، العدد04، كلية السياسة والاقتصاد، جامعة بني سويف، مصر، 2019، ص. ص 61- 87.

14. سليماني مباركة، "الإرهاب الالكتروني وطرق مكافحته"، مجلة الحقوق والعلوم السياسية، المجلد04، العدد08، جامعة عباس لغرور-خنشلة، الجزائر،2017، ص. ص 340-355.

15. سليمي فاطمة الزهراء،" الأسباب الاجتماعية لانتشار ظاهرة الإرهاب : (دراسة سوسيو-تاريخية لبعض العمليات الإرهابية) ، **مجلة آفاق لانتشارظاهرة الإرهاب**، المجلد12، العدد01، دار جامعة نايف للنشر، جامعة نايف العربية للعلوم الأمنية، السعودية،2020، ص. ص 254 -265.

16. سوماتي شريفة،" التجريم الوقائي في السياسة الجزائية المعاصرة"، **مجلة صوت القانون**، المجلد6، العدد02، مخبر نظام الحالة المدنية، جامعة خميس مليانة، الجزائر،2019، ص. ص. 1198- 1223.

17. سي ناصر مراد، قريبيز محمد، "مكافحة جريمة تمويل الإرهاب في التشريع الجزائري"، **مجلة العلوم الإنسانية**، المجلد31، العدد1، جامعة منتوري -قسنطينة، الجزائر،2020، ص. ص91-106.

18. عبد الحميد سفيان،" أساليب التحري الخاصة ي قانون الإجراءات الجزائية الجزائري"، **مجلة صوت القانون**، المجلد9، العدد03، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة خميس مليانة، الجزائر،2023، ص. ص 206 -225.

19. عوض عبد السميع عادل،" دور الذكاء الإصطناعي بالتنبؤ بمكافحة الإرهاب"، مجلة متون، المجلد17، العدد01، كلية العلوم الاجتماعية والإنسانية، جامعة مولاي الطاهر-سعيدة، الجزائر، 2024، ص. ص 72- 108.

20. عوينات نجيب بن عمر، " الإرهاب الإلكتروني: المفهوم والجهود الدولية والإقليمية لمكافحته"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد02، العدد 02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف-بالمسيلة-، الجزائر، 2017، ص.ص 9 -26.

21. فلاك مراد، "المسؤولية الجنائية للشريك في القانون الجزائري"، **مجلة النوازل الفقهية والقانونية**، المجلد02، العدد1، مركز البحث في العلوم الإسلامية والحضارة-الأغواط، الجزائر، 2018، ص. ص 199 - 224.

22. قادري نور الهدى، "الشهادة الإلكترونية وحجيتها في الإثبات"، **مجلة الفكر القانوني والسياسي**، المجلد 07، العدد01، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي-الأغواط، الجزائر، 2023، ص. ص 1592-1604.

23. قيراط محمد، "الاعلام الجديد والإرهاب الالكتروني: آليات الاستخدام وتحديات المواجهة"، **مجلة الحكمة لدراسات الإعلامية والاتصالية**، المجلد05، العدد01، مركز الحكمة للبحوث والدراسات، الجزائر،2017، ص. ص 10 -36.

24. لوكال مريم،" الآليات القانونية المستحدثة لحماية الشهود والخبراء والضحايا بموجب الأمر15-02 المعدل لقانون الإجراءات الجزائية: دراسة مقارنة"، **حوليات جامعة الجزائر-1-**، المجلد31، العدد2، جامعة الجزائر-1-، الجزائر، 2017، ص.ص 98 -124.

25. محمد الطيب عبد الله خالد، "الإرهاب الالكتروني"، **مجلة كلية الشريعة والقانون**، المجلد13، العدد01، جامعة أم درمان الإسلامية، السودان،2020، ص. ص95 -114.

26. محمد طاهر أحمد رانية، "أثر الذكاء الاصطناعي على الامن الدولي"، **مجلة البحوث المالية والتجارية**، المجلد 23، العدد03، كلية التجارة، جامعة بورسعيد، مصر،2022، ص. ص 228-276.

27. مزياني عمار،" الجرائم المادية والمسؤولية الجنائية"، **المجلة الجزائرية للحقوق والعلوم السياسية،** المجلد07، العدد02، كلية الحقوق، جامعة أحمد بن يحي الونشريسي تسمسيلت، الجزائر،2022، ص. ص 18 -34.

28. مشتاق طلب فاضل، استبرق فاضل شعير،" مواقع التواصل والإرهاب في العصر الرقمي (الإرهاب الالكتروني)"، **مجلة القانون والعلوم السياسية،** المجلد13، العدد1، كلية العلوم السياسية، جامعة النهرين، بغداد، 2024، ص. ص201-226.

29. معمري خديجة، خلفاوي خليفة،" إشكالية تعارض مكافحة الإرهاب الإلكتروني بأهمية حماية حقوق الإنسان"، **الأكاديمية للدراسات الاجتماعية والإنسانية**، المجلد13، العدد02، كلية العلوم الاقتصادية والقانونية، جامعة حسيبة بن بوعلي- الشلف-، الجزائر،2021، ص. ص 349 -358.

30. مقدم مبروك،" الظروف المخففة وحالة العود على ضوء القانون رقم: 23/06المؤرخ في 20/12/06المعدل والمتمم لقانون العقوبات"، **مجلة البحوث والدراسات الإنسانية**، المجلد2، العدد1، جامعة20أوت1955 سكيكدة، الجزائر، 2008، ص. ص260 - 292.

رابعا: النصوص القانونية

1) الدستور

1. دستور الجمهورية الجزائرية الديمقراطية الشعبية، المؤرخ في 28 نوفمبر 1996، المعدل والمتمم، بموجب القانون رقم 02-03، المؤرخ في 10 أبريل 2002، المتضمن التعديل الدستوري، ج.ر.ج.ج. العدد 25، الصادر في 14 أبريل 2002، و بالقانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، ج.ر.ج.ج. العدد 63، الصادر في 16 نوفمبر 2008، وبالقانون رقم 16-01، المؤرخ في 06 مارس 2016، المتضمن التعديل الدستوري، ج.ر.ج.ج. العدد الصادر في 07 مارس 2016، وبالمرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في 01 نوفمبر 2020، ج.ر.ج.ج. العدد 82، الصادر في 30 ديسمبر 2020.

2) الاتفاقيات الدولية

1. الاتفاقية الدولية لقمع تمويل الإرهاب، المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة، المؤرخ في 9ديسمبر 1999، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم2000-445، المؤرخ في23 ديسمبر2000، ج.ر.ج.ج العدد الأول، الصادرة في 3يناير2001.

2. اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المعتمدة بموجب قرار الجمعية العامة للأمم المتحدة، المؤرخ في 15نوفمبر2000، بمدينة باليرمو الإيطالية، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 02-55، المؤرخ في 5فيفري2002الجريدة الرسمية الجمهورية الجزائرية عدد 09، الصادرة في10فيفري2002.

3. اتفاقية بودابست، المعتمدة من طرف المجلس الأوروبي، المؤرخ في 23نوفمبر2001، تحت رقم 185، تحت عنوان "اتفاقية بودابست لمكافحة الجريمة المعلوماتية"، ودخلت حيز التنفيذ بتاريخ 01جويلية2004. (غير مصادق عليها)

4. الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم14-250، المؤرخ في 8سبتمبر2014، ج.ر.ج.ج عدد 55، الصادر في 23سبتمبر2014.

5. الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21ديسمبر2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-251، المؤرخ في 8سبتمبر 2014، ج.ر.ج.ج عدد56، الصادر25سبتمبر2014.

6. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المعتمدة من طرف وزراء الداخلية والعدل العرب والمحررة بالقاهرة، المؤرخ في 21ديسمبر2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 8سبتمبر 2014، ج.ر.ج.ج عدد57، الصادر28سبتمبر2014.

3) النصوص التشريعية

1. أمر رقم 66-155 مؤرخ في 8يونيو1966، يتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 48، الصادرة في 10يونيو1966، معدل ومتمم لاسيما بالقانون رقم06-22 مؤرخ في 20ديسمبر2006، ج.ر.ج.ج عدد84، الصادرة 24ديسمبر2006. وكذا بالأمر رقم 21-11 مؤرخ في 25غشت 2021، ج.ر.ج.ج عدد 65، الصادرة في 26غشت 2021.

2. أمر رقم66-156 مؤرخ في 8يونيو1966، المعدل والمتمم لقانون العقوبات، ج.ر.ج.ج عدد49، صادرة في 11يونيو1966، معدل ومتمم لاسيما بالقانون رقم 16-02 مؤرخ في 19يونيو2016، ج.ر.ج.ج عدد37، صادرة في 22يونيو2016. وكذا بالقانون رقم 24- 06 مؤرخ في 28أبريل 2024، ج.ر.ج.ج عدد30، صادرة في30أبريل2024.

3. قانون رقم 05-01 مؤرخ في 6فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، ج.ر.ج.ج عدد11، الصادرة في 9فبراير2005، معدل ومتمم.

4. قانون رقم06-01 مؤرخ في 20فبراير سنة 2006، يتعلق بالوقاية من الفساد ومكافحته، ج.ر.ج.ج عدد14، الصادرة 8مارس2006، معدل ومتمم.

5.قانون رقم 09-04 مؤرخ في 5غشت2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد47، صادرة في 25أوت2009.

6. قانون رقم 16-03 مؤرخ في 19 يونيو2016، يتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، ج.ر.ج.ج عدد37، الصادرة في 22يونيو2016.

7. قانون رقم 18-04 مؤرخ في10 مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر.ج.ج عدد27، الصادرة في13مايو2018.

8. قانون رقم 18-07مؤرخ في 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج عدد 34 الصادرة قي 10يونيو2018.

9. قانون 20-05 مؤرخ في 28 أبريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج.ر.ج.ج عدد 25، الصادرة في 29أبريل 2020.

4) النصوص التنظيمية

1. مرسوم رئاسي رقم 20-05 مؤرخ في 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر.ج.ج عدد04، الصادرة 26جانفي2020.

2. مرسوم رئاسي رقم 21-439مؤرخ في7نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج عدد86، الصادرة 11نوفمبر2021.

خامسا: مصادر الأنترنت

1. الموقع الإلكتروني الخاص بالمجلس الأوروبي، المتوفر على الرابط التالي: https://rm.coe.int/budapest-convention-in-arabic/1680739173 .

2. الموقع الخاص بوزارة العدل، المتوفر على الرابط التالي: https://droit.mjustice.dz/ar .

3.الموقع الرسمي للأمانة العامة للحكومة، المتوفر على الرابط التالي: https://www.joradp.dz/HAR/Index.htm

II. باللغة الأجنبية

1) The Scientific articles

1. **MIRZA** Muhammad Nadeem, **SHAHZAD** Akram Muhammad, "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare," Strategic Studies, Volume 42, Issue 1, Strategic Studies Institute, Pakistan, 2022, P.P80-62.

2) Les Thèses de Doctorat

1. **Boos R**omain, La lutte contre la cybercriminalité au regard de l'action des États, Thèse de Doctorat en droit, Faculté de droit, Université de Lorraine, 2016.

2**. HOUNHAGI B**EL Dora Carrol, Sanction pénale et sanctions ayant le caractère d'une punition, Thèse pour l'obtention du titre de Docteur en droit, droit, Ecole Doctorale des Sciences Economiques, Juridiques, Politiques et de Gestion Centre Michel de L'Hospital, Université Clermont Auvergne, France, 2022.

3) Les Sites internet

1. ACBM Avocats, **L'IA au service des hackers**, Disponible sur https://www.acbm-avocats.com/lia-au-service-des-hackers/#_ftnref1 , consulté le 11février2025, a 23h22min.

الفهـرس

The Crime of Cyberterrorism: An Analytical Study in Algerian Law

Abstract :

Since Algeria has faced terrorist acts since its independence, such offences are deeply rooted in its history of security challenges rather than being a recent development. The rapid progress of technology and the information revolution, accompanied by evolving crime-commission methods, has added a new dimension to terrorism: the use of Information and Communication Technologies (ICT) to plan, threaten, and carry out attacks. This evolution has given rise to what is known as cyberterrorism.

To address this threat, the Algerian legislature amended the Penal Code by introducing provisions that clearly define the constitutive elements of cyberterrorism and impose harsh penalties on those responsible. In addition to these amendments, lawmakers have enacted other statutes targeting cyberterrorism and established both preventive and judicial mechanisms aimed at the early identification and effective management of such threats. All these measures form part of a balanced criminal policy that combines criminalization with prevention, with the ultimate goal of protecting national cybersecurity.

Keywords : Cyberterrorism, Cybersecurity, Digital Environment, Information and Communication Technology (ICT), Cybercrime, Criminal Policy.

جريمة الإرهاب الإلكتروني: دراسة تحليلية في ضوء القانون الجزائري

ملخص:

تُعد الجرائم الإرهابية من الظواهر الإجرامية التي عرفتها الدولة الجزائرية منذ الاستقلال، مما يجعلها من الجرائم الراسخة في سجل التحديات الأمنية وليست بظاهرة حديثة النشأة. ومع التطور المتسارع في مجال التكنولوجيا والثورة المعلوماتية، وما رافقه من تحول وتطور في أنماط ارتكاب الجرائم، اكتسب الإرهاب بُعداً جديداً تمثل في استغلال تكنولوجيا الإعلام والاتصال في التخطيط والتهديد وتنفيذ العمليات الإرهابية، مما أدى إلى بروز ما يُعرف بجريمة الإرهاب الإلكتروني. وفي هذا السياق، برزت جهود المشرع الجزائري في التصدي لهذه الجريمة من خلال تعديل قانون العقوبات وإدراج نصوص قانونية تُحدد أركان هذه الجريمة وتُقرّ عقوبات صارمة في حق مرتكبيها. وإلى جانب قانون العقوبات، عمل المشرع الجزائري على وضع قوانين أخرى تعالج جريمة الإرهاب الإلكتروني، كما تم اعتماد أسس وقائية وأخرى قضائية تهدف إلى الكشف والتصدي لهذه التهديدات والتعامل معها بفعالية، في إطار سياسة جنائية متوازنة تمزج بين التجريم والوقاية، سعياً لحماية الأمن السيبراني الوطني.

الكلمات المفتاحية: الإرهاب الإلكتروني، الأمن السيبراني، الفضاء الرقمي، تكنولوجيا الإعلام والإتصال، الجريمة المعلوماتية، السياسة الجنائية.