جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

وزارة التعليم العالي والبحث العلمي

جامعة عبد الرحمان ميرة – بجاية –

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

عنوان المذكرة

المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية

(دراسة مقارنة)

مذكرة مقدمة لاستكمال شهادة الماستر في الحقوق والعلوم السياسية

تخصص: قانون جنائي وعلوم جنائية

من إعداد الطلبة:

- **مويسي سيلية**
- **نايت إغيل تيزيري**

تحت إشراف الأستاذ(ة):

- **بن سليمان محمد الأمين**

لجنة المناقشة:

الأستاذ(ة) هارون نورة جامعة عبد الرحمان ميرة بجاية..... رئيســــــــا.

الأستاذ(ة) بن سليمان محمد الأمين أستاذ محاضر "أ"..... مشرفا ومقررا.

الأستاذ(ة) فروج سكينة جامعة عبد الرحمان ميرة بجاية..... ممتحنــــــا.

السنة الجامعية 2024/2023


بسم الله الرحمن الرحيم

الشكر والتقدير

أتقدم بجزيل الشكر والامتنان إلى مشرفي الدكتور بن سليمان محمد أمين الذي كان خير أستاذ لي، وقد نهلت من بحر علمه الواسع والذي لم يبخل عليّ بمعلومة ما من علمه الغزير فإني أقف له احتراماً على تفضله بالإشراف على هذه المذكرة، وأسال الله أن يديم عليه صحته وأن يبقيه منارة لكل منأراد طريق العلم.

كما أتقدم بجزيل الشكر إلى أساتذتي أعضاء هيئة المناقشة الكرام الذين طوقوني بتكرمهم بالموافقة على مناقشة مذكرتي، جزاهم الله جميعاً كل خير.

أتقدم بالشكر إلى كل أساتذة كلية الحقوق والعلوم السياسية لجامعة– بجاية-

إهداء

أهدي ثمرة جهدي المتواضع

إلى من وهبوني الحياة والأمل، والنشأة على شغف

الاطلاع والمعرفة، ومن علموني أن أرتقي سلم الحياة بحكمة وصبر،

برّا، وإحسانا، ووفاء لهما: والدي العزيز، ووالدتي العزيزة.

إلى من وهبني الله نعمة وجودهم في حياتي إلى العقد المتين

من كانوا عونا لي في رحلة بحثي: إخواني عماد وياسين وأختي مريسا.

وأخيرا إلى كل من ساعدني، وكان له دور من قريب أو بعيد في إتمام هذه الدراسة،

سائلة المولى أن يجزي الجميع

خير الجزاء في الدنيا والآخرة.

سيلية

إهداء

لا شيء أعز من رب الكون الذي لم يبخل على برحمته ونعمته له

الشكر والحمد حمدّا كثيراً لا نهاية له.

أهدي هذا العمل المتواضع

إلى ينبوع الحنان التي علمتني الصبر والمثابرة إلى التي تعبت من أجلي لتراني في أعلى المراتب أمي الغالية.

إلى من أضاء دروبي وطريقي وقدوتي في كل خطوة أخطوها نحو العلم والمعرفة أبي الغالي.

إلى أغلى ما أملك في هذه الدنيا الذين وقفوا معي في كل خطوة أخطوها من أجل العلم و المعرفة تقاسموا معي مشقة الحياة إخواتي : عبد المؤمن و محند وكهينة، كنزة وحنان

إلى أصدقائي وزملائي اللذين سندوني طوال مشواري الدراسي مريم،ليندة،باية وصوفيان .

إلى من ساعدني لكي أصل إلى ما أنا عليه اليوم "م.ع" الذي كان دائما يوجهني نحو العلم والمعرفة.

إلى الأشخاص اللذين أحمل لهم كل المحبة والتقدير: "أ.م"

إلى كل من ساهم في إنجاز هذا البحث "د/مصطفى خالد رويشدة " والمحامي "محمد رفعت" ساعدوني بنصائحهم بالمعلومات والمراجع وكذلك في إعداد خطة البحث.

وإلى كل من ساعدني من قريب أو بعيد.

تيزيري

قائمة أهم المختصرات:

باللغة العربية:

-ق ع ج: قانون العقوبات الجزائري.

-ق إ ج ج: قانون الإجراءات الجزائية الجزائري.

-ج رج ج: الجريدة الرسمية للجمهورية الجزائرية.

-ط: طبعة.

-ص: صفحة.

-د ط: دون طبعة.

-ج: جزء.

ج إ: جريمة إلكترونية.

باللغة الأجنبية:

-Le web: World Wide Web.

-IP : Internet Protocol.

-TCP : Transmission Control Protocol.

-OIPC : Organisation Internationale De Protection Civile.

-FBI: Federal Bureau of Investigation.

مقدمة

تطورت الجريمة على مر العصور بتطور المجتمعات وتغير الظروف الاجتماعية والاقتصادية والسياسية، حيث كانت الجريمة ترتبط بشكل أساسي بالأعمال العنيفة مثل القتل والسرقة والاعتداء، ومع التطور وظهور المدن الكبيرة وتنوع الأنشطة الاقتصادية، زادت أشكال الجريمة لتشمل الاحتيال التجاري والتزوير والسرقة بطرق متطورة، ما جعل الحكومات تسعى إلى تطبيق نظم قانونية أكثر تنظيمًا لمكافحة جريمة العصر الحديث والعصر الصناعي، وشاهد هذا الأخير زيادة في الجريمة المنظمة بسبب تطور الأنظمة كما بدأت الجرائم ضد الممتلكات تشمل أيضًا السرقة الإلكترونية والاحتيال البنكي، اختلفت التسميات لهذا الشكل المستحدث للجرائم ليطلق عليها بالجريمة الإلكترونية أو الجريمة السيبرانية.

أصبحت البيانات الرقمية هدفا للسرقة والاستغلال، مما أدى إلى تشديد العقوبات وتعزيز الأمن السيبراني، حيث تعرف بأنها نوع من أنواع الجرائم التي تتعلق بالاستخدام الغير القانوني لتكنولوجيا المعلومات والاتصالات،حيث أن التطور السريع لها من أبرز الأسباب التي أدت إلى زيادة حالات الجريمة المعلوماتية.

تعتبر البيانات الرقمية من أهم الأصول التي يمكن استهدافها لتشمل هذه الجرائم كل أنواعا لاختراق وسرقة البيانات والتلاعب بها والاحتيال والتجسس الإلكتروني وانتشار البرامج الخبيثة (المالوير) والتهديد الإلكتروني، حيث تتسبب هذه الجرائم في خسائر كبيرة للأفراد والشركات بالإضافة إلى الآثار السلبية على الاقتصاد والأمن القومي، ولذلك تعمل الحكومات والمؤسسات الخاصة والعامة على تعزيز تشريعاتها وتطوير تقنياتها لمكافحة هذه الظاهرة وتحقيق الردع عبر تشديد عقوباتها.

ما يميز هذه الجرائم عن الجرائم التقليدية هو أن المجرم فيها يتميز بالذكاء والمهارات التقنية العالية في مجال التكنولوجيا والحوسبة، مما يمكنه من اختراق الأنظمة الإلكترونية والتلاعب بها، وغالبا ما يكون لديه معرفة عميقة بالقوانين المتعلقة بالجرائم الإلكترونية، بالإضافة إلى فهم دقيق للتقنيات المستخدمة في ارتكاب هذه الجرائم، ويتمتع بالقدرة على إيجاد ثغرات في الأنظمة والتطبيقات واستغلالها بطرق ذكية وإبداع، من الصعب تعقبه بسبب قدرته على تغيير عناوين الآيبيIP، واستخدام تقنيات التخفي والتمويه، هدفه تحقيق أرباح مالية كبيرة من خلال الاحتيال الإلكتروني وغيرها من الأنشطة الإجرامية عبر الإنترنت.

من الجرائم الإلكترونية الأكثر شيوعا والتي تهدد الأفراد في مالهم ونفسهم جريمة التهديد الإلكتروني والتي يختلف مفهومها عن تلك المنصوص نصوص المواد 284 إلى287 من ق ع ج[1]، حيث

[1]يراجع في ذلك:

المواد من 284 إلى 287من الأمر رقم 66-156 مؤرخ في 18 صفر عام 1336 الموافق 08 يونيو سنة 1966، يتضمن قانون العقوبات، ج ر ج ج عدد 49 صادر في 21 صفر عام 1386 الموافق 11 يونيو سنة 1966، معدل ومتمم.

تعرف جريمة التهديد بمفهومها التقليدي على أنه كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني لجريمة ضد النفس، أو المال أو إفشاء أو نسبة أمور مخلة للشرف، وقد يحمله التهديد تحت تأثير ذلك الخوف إلى إجابة الجاني إلى ما ابتغى متى صاحب التهديد طلب، وغني عن البيان أن التهديد ينطوي على إحداث آثار خطيرة في نفوس الأفراد نظراً لما يوقعه في نفوسهم من خوف واضطراب في حياتهم ما يؤدي إلى تعطيلها وتوقفها لحين انتهاء تلك الفاجعة التي حلت بهم، نظراً لما يمثله فعل من خطورة على الأفراد.

قرر المشرع الجزائري وضع فعل التهديد تحت طائلة التجريم، حيث قرر معاقبة كل شخص يتعمد تهديد غيره أياً كانت صورة التهديد وأيا كان الغرض منه، أما بالنسبة لجريمة التهديد بمفهومها الحديث لم تعرفها التشريعات العقابية محل المقارنة ، وتُرك الأمر لفقهاء القانون الجنائي الذين عرفوا هذا السلوك بتعريفات عديدة تتفق في مضمونها على أن التهديد هو: كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المُهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخدوشة للشرف، وقد يُحمله ذلك الخوف إلى إجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب.

وهناك من عرف التهديد بأنه: الوعيد بشر يصيب المجني عليه مهما كانت الوسيلة التي أحدثت الرعب في نفسية الجاني، سواء كان الشر بالاعتداء على نفسه أو ماله أو عرضه، فكل فعل مادي أو قول يشكل اعتداء على الحرية والأمن للمجني عليه فالتهديد يتمثل في إنذار الشخص والضغط على إرادته بهدف إيقاع ضرر عليه أو شخص أو أشياء لها صلة به.

ومن جماع هذه التعريفات نجد أن التهديد من الجرائم التي من شأنها أن تحدث أثار خطيراً في حياة المجني عليه، ، وذلك بالضغط على إرادته بهدف تحقيق رغبة معينة يرمي إليها الجاني ومرجع التجريم لهذه الجريمة يكمن في كونها تقيداً لحرية المجني عليه، وتكون الخطورة أكبر إذا ما كان من شأن الفعل الذي يأتيه الجاني إخضاع المجني عليه للإكراه المعنوي.

ازدادت خطورة هذه الجريمة مع انتشار استخدام الإنترنت والوسائط الإلكترونية، مما سهل على مرتكبيها ارتكابها دون الكشف عن هوياتهم، ولا تمس فقط الأشخاص الطبيعية بل أصبح فعل التهديد يقع أيضا على الأشخاص المعنوية، ومنه يمكن تعريف التهديد الإلكتروني أنه ذلك الفعل الذي يستهدف الاعتداء على المعطيات الشخصية للأفراد و الأنظمة الإلكترونية والمعلوماتية للمؤسسات والشركات، الذي يشمل مختلف الاختراقات السيبرانية، لذا ظهرت الحاجة إلى دراسة المسؤولية الجنائية عن جريمة التهديد الإلكتروني وذلك لتحديد العناصر المكونة لهذه الجريمة وشروط قيامها وأشخاصها، وصورها ومختلف العقوبات المقررة لها، وبيان التحديات التي تواجه تطبيق المسؤولية الجنائية.

تعد هذه الدراسة مهمة لأسباب عديدة منها الحد من انتشار جريمة التهديد الإلكتروني، وحماية أمن المجتمع واستقراره ضمان تحقيق العدالة ومعاقبة مرتكبي هذه الجريمة وحماية حقوق المجني عليه، وتطوير القوانين المتعلقة بالجرائم الإلكترونية لجعلها أكثر فاعلية في مكافحة هذه الجرائم.

ستركز هذه الدراسة على المقارنة بين مختلف التشريعات حول تجريم ظاهرة التهديد الإلكتروني، وتظهر خصوصية هذه الجريمة في البحث والتحري وطبيعة الدليل المستخلص وتعتبر مسألة حساسة ومعقدة فهي تتضمن توازنًا دقيقًا بين حقوق الأفراد في الخصوصية وضرورة مكافحة الجريمة الإلكترونية وحماية الجمهور، ومن بين أهم أساليب التحري التي تستخدم في جرائم التهديد الإلكتروني والمتمثلة في إجراءات التحري العامة(التقليدية) داخل المنظومة المعلوماتية والتي تشمل كل من إجراءات التفتيش والخبرة والمعاينة، وإجراءات أخرى خاصة مستحدثة تتمثل في اعتراض المراسلات، التسرب وحفظ المعطيات المتعلقة بحركة السير، ومن خلال هذه الإجراءات يتم استخلاص أدلة ذات طابع تقني مع اتخاذ الخبير كشاهد، إلا أنها تتعرض للعديد من العراقيل التي تواجه السلطات القضائية وذلك راجع إلى أنها ترتكب في بيئة افتراضية، ويتحدد الاختصاص القضائي في هذا النوع من الجرائم بناءا على مبادئ.

بما أن جريمة التهديد الإلكتروني من الجرائم العابرة للحدود لذا تستوجب إجراء الإنابة القضائية وتعرف بالتفويض أو تكليف بالمهمة التي تصدرها سلطة مختصة بالتحقيق إلى سلطة أخرى لتنفيذ جزء من إجراءات التحقيق، والتي تستند على مبدأ الملائمة الإجرائية التي تبررها الكفاءة في مباشرتها، إذ نصت عليه المادة 68 فقرة 05 من قانون الإجراءات الجزائية الجزائري[2]

ولمكافحة الجرائم السيبرانية ظهرت العديد من الهيئات والاتفاقيات على المستوى الدولي والإقليمي والمحلي.

***هناك العديد من الدوافع التي دفعتنا لاختيار موضوع المسؤولية الجزائية للتهديد عبر الوسائل الإلكترونية ومن أهمها:**

-الأسباب الموضوعية: كون موضوع البحث له أهمية كبيرة من الناحية الاجتماعية، ويهدف إلى تحليل وفهم الموضوع من أجل التوعية الاجتماعية.

-الأسباب الشخصية: اهتمامنا بهذا الموضوع ورغبتنا في دراسته وفهمه بشكل أعمق واختيارنا له راجع للانتشار الواسع لجريمة التهديد الإلكتروني كونه من المشاكل الحديثة التي تواجه المجتمع، والتي تثير اهتمام الكثير من الأفراد والمؤسسات نظراً لانتشارها الواسع، ونظراً لأهمية الأمن والخصوصية الرقمية

---

[2] راجع في ذلك:

المادة 68 فقرة 05 منالأمر رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج ، عدد 48، الصادر بتاريخ 1966/06/10، معدل ومتمم.

في حياتهم اليومية، ولفهم الموضوع بشكل أفضل والعمل على حماية أنظمته وبياناته، وكون مجال الأمن السيبراني ومكافحة التهديدات الإلكترونية من المجالات الهامة في تأمين البيانات والمعلومات ما يستدعي الدراسة وذلك من الناحية القانونية.

إشكالية الدراسة:

أصبح الفضاء الرقمي الإلكتروني من أهم الفضاءات التي تقوم فيه الجرائم وعلى رأسها جريمة التهديد الإلكتروني، ولمعالجة موضوعنا والإلمام بجوانبه نطرح الإشكالية التالية:

ما مدى فعالية النصوص الجزائية التي كرسها المشرع لمحاربة جريمة التهديد عبر الوسائل الإلكترونية والحد منها؟

المنهج المتبع:

لمعالجة موضوع بحثنا والإلمام بجوانبه والإجابة على الإشكالية المطروحة اعتمدنا المنهج الوصفي لتوضيح المسؤولية الجزائية لجريمة التهديد عبر الوسائل الإلكترونية، وإلى جانبه المنهج الاستقرائي التحليلي وذلك من خلال استقراء النصوص القانونية المتعلقة بها، والمنهج المقارن الذي يقوم على تحليل المضمون والمقارنة بين التشريعات.

خطة البحث:

للإجابة على الإشكالية المطروحة إرتئينا إلى تقسيم موضوع دراستنا إلى فصلين رئيسيين، تناولنا في الفصل الأول القواعد الموضوعية لجريمة التهديد الإلكتروني، والذي ينقسم بدوره إلى مبحثين المبحث الأول البنيان القانوني لجريمة التهديد الإلكتروني، الذي ينقسم إلى مطلبين المطلب الأول تحت عنوان أركان وشروط قيام جريمة التهديد الإلكتروني، والمطلب الثاني تحت عنوان نطاق المسؤولية الجزائية لجريمة التهديد الإلكتروني وشروطها، أما المبحث الثاني مظاهر جريمة التهديد الإلكتروني والبعض من تطبيقاته التشريعية، حيث ينقسم إلى مطلبين نعالج في المطلب الأول مظاهر التهديد الإلكتروني، والمطلب الثاني التطبيقات التشريعية لجريمة التهديد الإلكتروني، وتناولنا في الفصل الثاني القواعد الإجرائية لجريمة التهديد الإلكتروني، والذي ينقسم أيضا إلى مبحثين المبحث الأول التحقيق والإثبات في جريمة التهديد الإلكتروني، الذي ينقسم بدوره إلى مطلبين المطلب الأول إجراءات التحقيق في جريمة التهديد الإلكتروني، وفي المطلب الثاني طرق الإثبات في جريمة التهديد الإلكتروني، أما المبحث الثاني المحاكمة في جريمة التهديد الإلكتروني ومكافحتها، والذي ينقسم إلى مطلبين نتناول في المطلب الأول الاختصاص والإنابة القضائية في جريمة التهديد الإلكتروني، والمطلب الثاني مكافحة جريمة التهديد الإلكتروني.

الفصل الأول

العناصر الموضوعية لقيام المسؤولية الجزائية عن التهديد الإلكتروني

أفرز التطور والتقدم العلمي والتقني في مجال التكنولوجيا الرقمية استحداث العديد من الجرائم التي كانت ترتكب في السابق بطرق بسيطة باستعمال آلات يدوية، فالوسائل المستخدمة الآن في ارتكاب هذه الجرائم لا يتسع المقام لذكرها، وأصبح العالم الافتراضي بيئة لها ووسائل التكنولوجيا الحديثة أساسا لقيامها، وتعتبر جريمة التهديد الإلكتروني وليدة هذا التطور، وهي نوع من أنواع الجرائم الإلكترونية الناعمة التي تخلو من العنف وفي نفس الوقت الأخطر والأكثر انتشارًا في العالم، حيث أن المجرم فيها يختبئ وراء شاشة ويمارس عبرها وبواسطتها عملاً إجراميًا يكون موضوعه الاعتداء على مصلحة يحميها القانون.

يعتمد هذا النوع من الجرائم لتنفيذها على الحاسب الآلي والانترنت بشكل عام، ومواقع التواصل الاجتماعي بشكل خاص، الهدف من القيام بجريمة التهديد الإلكتروني تحقيق غاية مادية أو معنوية يرجوها الجاني من حيث لم يسلم أي فرد كان رجلاً أو امرأة، مؤسسة أو شركة وحتى الدولة من هذه الجريمة.

إن هذه الآفة الاجتماعية (جريمة التهديد الإلكتروني) دفعت مختلف التشريعات للتدخل لإيوائها عبر تغير وتعديل مقتضيات النص القانوني ليتلاءم مع هذه الأوضاع الجديدة، حماية لحقوق وخصوصية الأشخاص الطبيعية أو المعنوية الخاصة أو العامة، والتي تتجسد في هذه الجريمة على شكل معلومات ومعطيات، وأيضا عبر توقيع عقوبات صارمة تحقق الإصلاح والردع.

تجمع جريمة التهديد الإلكتروني صورتين من التهديد أو الجرائم، أولاً جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وثانيًا الجرائم التي تقع عبر الأنترنت.

تمت معالجة جريمة التهديد الإلكتروني بطرق مختلفة في مختلف التشريعات فهناك من وضع نصوص خاصة تجرم هذا الفعل كالتشريع السعودي والأردني والمصري وهناك من عالجه في نصوص متفرقة كالمشرع الجزائري والفرنسي، إلا أن العناصر المكونة لهذه الجريمة والوسائل المستعملة لارتكابها هي نفسها في كل التشريعات وكذلك الشروط الواجبة لقيامها.

فمنه سنحاول من خلال هذا الفصل التطرق إلى البنيان القانوني لجريمة التهديد الإلكتروني والذي يتناول العناصر المكونة لهذه الجريمة من أركان وشروط لقيامها بالإضافة إلى نطاق المسؤولية الجنائية الناشئة عنها كمبحث أول أما في المبحث الثاني فنستعرض مظاهر جريمة التهديد الإلكتروني وخصائصها وبعض من التطبيقات التشريعية التي تتمثل في العقوبات المقررة لها.

المبحث الأول

البنيان القانوني لجريمة التهديد الإلكتروني

ظاهرة التهديد الإلكتروني تتمثل في كل تهديد يأتيه الجاني، ويؤثر في نفسية المجني عليه، ويتم عبر وسيلة إلكترونية ،ومن صور الإيذاء الأخرى المتشابهة معه مثل التسلط الإلكتروني وتعد ظاهرة التهديد الإلكتروني أحد أهم المواضيع الشائكة والتي استفحلت في مجتمعاتنا بشكل رهيب، وخاصة بعد انتشار الوسائل الإلكترونية الحديثة، فباتت أعراض الناس وخصوصياتهم مع هذا التقدم التقني ليست ذات أهمية وعليه يجدر مراجعة القوانين ووضع عقوبات ردعية في حق المجرمين الذين يستغلون هذه الوسائل الإلكترونية في أغراض خسيسة فلا يراعون فيها حرمات الناس .

ولقد انتشرت مؤخراً ظاهرة التهديد الإلكتروني، والتي أثرت على جميع أطياف المجتمع بشكل كبير وسريع نظراً لسهولة ارتكابها وصعوبة الوصول إلى الجاني، إذ أنها ظاهرة إجرامية مستحدثة تتم من خلال استخدام الوسائل الإلكترونية والإنترنت، لهذا فإن هذه الظاهرة لها طبيعة تميزها عن غيرها، إذ أنها تعتمد على الوسائط الإلكترونية المرتبطة بشبكة الإنترنت ما جعلها ذات خطورة ذاتية.

لقيام جريمة التهديد الإلكتروني لا

بد من توافر عناصر لقيامها أو ما يعرف في فقه قانون العقوبات بأركان التجريم، حيث نعتمد في هذا المجال على القواعد العامة التي تقوم عليها أي جريمة فلابد من توفر أركان وشروط خاصة بها، وتتميز جريمة التهديد الإلكتروني بنطاقها الواسع ليمتد ويشمل عددا من الأطراف إضافة إلى الجاني، الذين تقوم مسؤوليتهم بصفة مباشرة أو غير مباشرة عن فعل التهديد.[3]

من خلال هذا المنطلق إرتئينا إلى تقسيم هذا المبحث إلى الأركان والشروط الخاصة لقيام جريمة التهديد الإلكتروني كمطلب أول، أما في المطلب الثاني سوف نتطرق إلى نطاق قيام المسؤولية الجزائية لجريمة التهديد الإلكتروني.

---

(3) يراجع في ذلك:

طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الالكتروني عبر مواقع التواصل الاجتماعي (دراسة مقارنة)، رسالة لنيل شهادة الماجستير في القانون العام، كلية القانون والعلوم السياسية، جامعة كركوك، العراق،2021، ص52.

المطلب الأول

أركان وشروط قيام جريمة التهديد الإلكتروني

إن أغلب القوانين العربية والعالمية تجرم جنح التهديد، كونها من الجرائم الخطيرة التي تلحق الضرر للشخص في سمعته ونفسيته وحياته الخاصة، فمعظم هذه القوانين صنفتها ضمن الجرائم الخطيرة، وحددت لها أركان خاصة بها.

فكل فرد يستخدم الإنترنت معرض لعمليات التهديد والاحتيال وغيرها، فمعظم القوانين تناولت ظاهرة الخصوصية الشخصية للأفراد، ووضعت لها أهمية ومكانة بالغة، حيث تدخل القانون وفرض الحماية الجزائية على الخصوصية الإلكترونية، واعتبر الاعتداء عليها جريمة، فقد تستهدف الجريمة الإلكترونية الجانب الأخلاقي خاصة في المجتمعات العربية التي تعتز بمبادئها وقيمها الفاضلة، فهذه الجريمة تقضي على حياة الأفراد، فمختلف التشريعات سعت لبيان هذه الجريمة وذلك عبر تحديد أركانها والتي تتمثل في الركن الشرعي الركن المادي والركن المعنوي كما سنت قوانين رادعة لها،ولتحقق هذه الجريمة بجميع أركانها وجب توفر جملة من الشروط منها سابقة لارتكاب الجريمة، من خلال مطلعنا هذا سنتطرق في الفرع الأول إلى أركان جريمة التهديد الإلكتروني وخصصنا الفرع الثاني لشروط قيام جريمة التهديد الإلكتروني.[4]

الفرع الأول

أركان جريمة التهديد الإلكتروني

ولقيام جريمة التهديد الإلكتروني لابد من توافر عناصر قيام الجريمة أو ما يعرف في فقه قانون العقوبات بأركان التجريم، ونحن في هذا المجال تعتمد على المبادئ العامة التي تقوم عليها أي جريمة، لأن الجريمة في فقه قانون العقوبات لا تفترض، إذا لا بد من وجود أركان محددة لقيام الجريمة، وفي غيابها تنتفي الجريمة مهما بلغ حجم الضرر منها أو مهما بلغ حد الاستنكار الاجتماعي لها، إذ أن الأعراف والنظرة الاجتماعية لا تخلق الجريمة ولا تكونها، وإنما النص التشريعي، وهذه من المبادئ المستقرة في فقه قانون العقوبات والمستمدة من التشريعات ابتداء من الدستور وحتى النصوص الخاصة بقوانين العقوبات أو القوانين الجنائية،[5]وحتى تقوم جريمة التهديد الإلكتروني يجب توافر أركانها المرتبطة بالجريمة نفسها،

---

(4)يراجع في ذلك:

الحسن بوشعير، شعيب حداد، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مذكرة لنيل شهادة ماستر مهني في القانون العام، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022-2023، ص52.

(5)يراجع في ذلك:

زهراء عادل سلبي، جريمة الابتزاز الالكتروني (دراسة مقارنة)، د ط، شركة دار الأكاديميون للنشر والتوزيع، عمان، الأردن، 2020، ص69

حتى تصبح جريمة معاقب عليها وفق القانون والأنظمة التي تجرمها، متمثلة في الركن الشرعي وهو وجود نص قانوني يحدد الفعل الإجرامي والعقوبة الجنائية وبوجوده ينتقل الفعل من دائرة الإباحة إلى دائرة التجريم.

أما الركن المادي فهو كل ما يدخل في كيان جريمة التهديد الإلكتروني وهو المظهر الخارجي للجريمة حيث يتضمن السلوك الإجرامي والنتيجة والعلاقة السببية ويكون ذو طبيعة مادية ملموسة فالركن المعنوي داخلي كامن في نفسية مرتكب الجريمة،[6]ومن هذا المنطلق يمكن تقسيمه فرعنا هذا إلى 3 عناصر أو ثلاثة أركان:

أولا: الركن الشرعي لجريمة التهديد الإلكتروني

يعتبر الركن الشرعي هو نقطة الانطلاق للبحث في قيام جريمة ما، ويقصد به التكييف القانوني الذي يضعه المشرع على الفعل، وهو الذي يوضح نطاق الصلة التي يتعين تحقيقها بين شخصية الجاني وماديات الجريمة، وفي إطار هذه العلاقة يتم تحديد درجة المسؤولية وجسامتها، وليس هناك أدنى شك في أن مرجع ذلك هو نصوص قانون العقوبات والقوانين المكملة له فلتحقق جريمة التهديد الإلكتروني لا بد من وجود نص في قانون العقوبات يوضح الفعل المكون لهذه الجريمة والعقوبة الواجب توقيعها على مرتكب جريمة التهديد الإلكتروني، وهذا المبدأ هو الذي يعبر عنه بمبدأ الشرعية، على أنه ينبغي ملاحظة أن قيام جريمة التهديد الإلكتروني لا يتوقف على مجرد خضوع الفعل لنص التجريم، بل يتطلب كذلك عدم خضوع الفعل لسبب تبرير أيضا،[7]فالركن الشرعي هو نص التجريم والعقاب فهو النص الذي نعتمد عليه لتجريم فعل معين والعقاب عليه ويكون ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة "لا جريمة ولا عقوبة ولا تدبير أمن بغير قانون". المادة 1 من قانون العقوبات الجزائري،[8] وبناءً على ما سبق سيتم معالجة عنصر الركن الشرعي لجريمة التهديد

---

(6)يراجع في ذلك:

أمال برحال، جريمة الابتزاز الالكتروني عبر الوسائل الالكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، 2020، ص ص 33 34.

(7)يراجع في ذلك:

نظام توفيق المجالي، شرح قانون العقوبات القسم العام: دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية،ط6، دار الثقافة للنشر والتوزيع،عمان،ص102.

(8) يراجع في ذلك:

المادة 1 من قانون العقوبات الجزائري، مرجع سابق.

الإلكتروني في التشريع الجزائري،[9] كما سنتطرق إلى الركن الشرعي لجريمة التهديد الإلكتروني في بعض التشريعات المقارنة أيضا:

1-الركن الشرعي لجريمة التهديد الإلكتروني في التشريع الجزائري

أولى المشرع الجزائري أهمية بالغة للخصوصية الشخصية للأفراد واعتبر الاعتداء عليها جريمة تصيب مركز المجني عليه حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه جريمة التهديد الإلكتروني في المجتمع الجزائري هذه الجريمة كفيلة لهدم حياة المجني عليه لمساسها بحياته الخاصة وشرفه واعتباره في المجتمع.[10]

تناول المشرع الجزائري تلك الحماية في نص المادة 47 من الدستور: " لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلته واتصالاته الخاصة في أي شكل كانت."[11]

يقصد من مفهوم المادة سالفة الذكر أنه لا يجوز انتهاك حرمة الحياة الخاصة للأفراد وحرمة شرفه وحتى المراسلات والاتصالات الخاصة بكل أشكالها مضمونة ومحمية بموجب القانون.

المشرع الجزائري تبنى الشمولية في تجريمه الأفعال التي يكون مسرحها إلكتروني وذلك على غرار باقي التشريعات، من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،[12] منه يتبين أنه جرم بدوره كل الأفعال التي ترتكب باستخدام

---

(9)يراجع في ذلك:

حسن بوشعير شعيب حداد، مرجع سابق، ص52.

(10)يراجع في ذلك:

أمال برحال، مرجع سابق، ص34.

(11)يراجع في ذلك:

المادة 47 من دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996، منشور بموجب المرسوم الرئاسي رقم 96-438، مؤرخ في 07 ديسمبر سنة 1996، ج ر ج ج عدد 76، صادر في 08 ديسمبر سنة 1996، معدل ومتمم بالقانون رقم 02-03، مؤرخ في 10 أفريل سنة 2002، يتضمن التعديل الدستوري، ج ر ج ج عدد 25، صادر في 14 أفريل 2002، معدل ومتمم بالقانون رقم 08-19، مؤرخ في 15 نوفمبر سنة 2008، يتضمن التعديل الدستوري، ج ر ج ج عدد 63، صادر في 16 نوفمبر سنة 2008، معدل ومتمم بالقانون رقم 16-01، مؤرخ في 06 مارس سنة 2016، يتضمن التعديل الدستوري، ج ر ج ج عدد 14، صادر في 07 مارس سنة 2016، معدل بالتعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020 في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، صادر بموجب المرسوم الرئاسي رقم 20-442، مؤرخ في 30 ديسمبر سنة 2020، ج ر ج ج عدد 82، صادر في 30 ديسمبر 2020.

(12)يراجع في ذلك:

القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق ل 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج عدد 47، الصادر بتاريخ 25 شعبان 1430، الموافق ل 16 غشت سنة2009.

تكنولوجيا الإعلام والاتصال، وما التهديد الإلكتروني إلا صورة مستجدة للتهديد التقليدي المنصوص عليه في المادة 284 من قانون العقوبات الجزائري.[13]

2-الركن الشرعي لجريمة التهديد الإلكتروني في التشريع السعودي: حيث أشار إلى تجريم التهديد الإلكتروني ضمن المادة 03 من نظام مكافحة جرائم المعلوماتية السعودي،[14] يندرج تحت شمول النص كل ما شأنه المساس أو في حكمها، إضافة على ذلك كل شخص يرتكب أيا من الجرائم المعلوماتية التالية:

أ-الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بهذا الفعل أو الامتناع عنه مشروعا بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا.

ب-التشهير بالآخرين، وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

ووفقا للنظام السعودي تعد جريمة التهديد الإلكتروني من تلك الجرائم المعلوماتية الخطيرة الموجبة للتوقيف وذلك بنص القرار الوزاري رقم 2000 بتاريخ 1435هـ بشأن الجرائم الموجبة للتوقيف، حيث تضمنت الفقرة الرابعة: أن الجرائم المنصوص عليها في نظام مكافحة الجرائم المعلوماتية تعد من الجرائم الكبيرة الموجبة التوقيف.[15]

فكل النصوص نصت بشكل صريح على تجريم التهديد الإلكتروني بصورة مختلفة، مما جعل تلك النصوص تمثل الركن الشرعي للجريمة والذي من خلاله يتم العقاب عليها.

3-الركن الشرعي لجريمة التهديد الإلكتروني في التشريع الفرنسي: نص المشرع الفرنسي على التهديدات التي يتم إرسالها عبر طرق الاتصال الإلكتروني في قانون العقوبات الخاص به وذلك في نص المادتين 222-17 و222-18 حيث نصت الأولى على:" يعاقب على التهديد بارتكاب جريمة أو جنحة ضد الأشخاص وعلى محاولتهم بالسجن لمدة ستة أشهر وغرامة 7500 يورو، إذا تكررت أو تحققت كتابة أو صورة أو أي شيء آخر"، أما المادة الثانية:" يعاقب على التهديد بارتكاب جريمة أو جنحة ضد الأشخاص بأي وسيلة كانت

---

(13) يراجع في ذلك:

المادة 284 من الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

(14) يراجع في ذلك:

المادة 03 من نظام مكافحة جرائم المعلوماتية السعودي لسنة 1428 الموافق لسنة 2007، مرسوم ملكي رقم 17 بتاريخ 08 ربيع الأول سنة 1428، الموافق ل 27 مارس، آذار سنة 2007، قرار مجلس الوزراء رقم 79 الصادر بتاريخ 07 ربيع الأول سنة 1428، الموافق ل 28 مارس، آذار سنة 2007، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية.

(15) يراجع في ذلك:

الفقرة الرابعة من القرار الوزاري رقم 2000 بتاريخ 1435/06/10، المنشور على موقع مختارات عدلية، المتواجد على الرابط التالي:
https://x.com/Law3li/status/1197221360092745730

الذي تم الاطلاع عليه بتاريخ: 2024/03/10 على الساعة 11:30.

بالسجن لمدة ثلاث سنوات وغرامة قدرها 45000 يورو عندما تتضمن تنفيذ شرط، وتشدد العقوبة إلى السجن لمدة خمس سنوات وغرامة قدرها 75000 يورو إذا كان تهديدا بالقتل."[16]

4-الركن الشرعي لجريمة التهديد الإلكتروني في التشريع الأردني: عاقب المشرع الأردني في قانون الاتصالات الأردني رقم 13 لعام 1995 وتعديلاته على جريمة التهديد بأي وسيلة من وسائل الاتصالات بالمادة 75والتيتنص على أن:

أ-كل من أقدم بأية وسيلة من وسائل الاتصالات على توجيه رسائل تهديد أو إهانة أو رسائل منافية للآداب أو نقل خبراً مختلفاً بقصد إثارة الفزع يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن سنة أو بغرامة لا تقل عن 300 دينار ولا تزيد على2000دينار أو بكلتا هاتين العقوبتين[17]

ب-كل من قام أو ساهم بتقديم خدمات اتصالات مخافة للنظام العام أو الآداب العامة يُعاقب بالعقوبات المنصوص عليها في الفقرة "أ" من هذه المادة، بالإضافة إلى تطبيق الأحكام المنصوص عليها في المادة 40من هذا القانون، وقد جاء في قرار لمحكمة التمييز الأردنية التهديد بواسطة الهاتف تشكل جنحة بمخالفة أحكام المادة 1/75من قانون الاتصالات الأردني، حيث جاء في هذا القرار: "بنتيجة إجراءات المحاكمة توصلت محكمة جنايات بقرارها الصادر بالدعوىرقم1225/2016.بتاريخ 2017/11/29 إلى أن واقعة هذه القضية تتلخص في الآتي: إنه وفي بداية الشهر السادس من عام 2016 تعرف المجني عليه.... إلخ على الجاني عبر الفيس بوك وتم التواصل فيما بينهما وعبر الهاتف حصلت نقاش حاد بينهما قام من خلالها الجاني بتهديد المجني عليه وبعدها طلب الجاني مقابلته في منطقة إقامته.... الخ القرار." ويتعلق نص المادة 75من قانون الاتصالات الأردني بالجرائم التي تقع باستخدام أي وسيلة من وسائل الاتصالات كجريمة التهديد أو الإهانة أو توجيه رسائل منافية للآداب والنظام العام، وتقديم خدمة اتصالات مخالفة النظام العام أو الآداب العامة.[18]

5-الركن الشرعي لجريمة التهديد الإلكتروني في التشريع المصري:

---

(16)يراجع في ذلك:

المادة 222-17 من قانون العقوبات الفرنسي، المنشور على منصةLégifrance ، المتواجد على الرابط التالي:

https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719

الذي تم الإطلاع عليه بتاريخ 2024/04/07 على الساعة 10:08.

(17) يراجع في ذلك :

المادة 75 من قانون الاتصالات الأردني، المنشور على منصة هيئة تنظيم قطاع الاتصالات، المتواجد على الرابط:

https://trc.gov.jo/EchoBusV3.0/SystemAssets

المطلع عليه بتاريخ 2024/05/05 على الساعة 09:33.

(18)يراجع في ذلك:

زهرة عادل سلبي، مرجع سابق، ص 73.

أطلق المشرع المصري تسمية أخرى لجريمة التهديد الإلكتروني وهي الابتزاز الإلكتروني، إلا أنه لم يضع نص خاص يعالج فيه هذه الجريمة، ونص على جريمة التهديد في نص المادة 327 من قانون العقوبات المصري على: " كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المؤبد أو المشدد أو بإفشاء أمور أو نسبة أمور مخدشة بالشرف وكان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن...". [19]

ثانيا: الركن المادي لجريمة التهديد الإلكتروني

هو السلوك المادي الخارجي الذي ينص القانون على تجريمه أي كل ما يدخل في كيان جريمة التهديد الإلكتروني، فهو السلوك الذي يظهر إلى حيز الوجود، حيث يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة التهديد الإلكتروني في أركانها عن جريمة التهديد التقليدية فهي تتطلب سلوك إجرامي يصدر من الجاني سواء بالقول أو الكتابة أو أي فعل أخر يتمثل في القيام بفعل التهديد ينشر البيانات أو الصور أو مقاطع فيديو للضحية ولا يهم من أين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنه عثر عليها في أجهزة مسروقة، كما لا يشترط التهديد الإلكتروني أن يتم بطريقة معينة فيمكن أن يتم عن طريق أو البريد الإلكتروني أو التسجيل الصوتي، كما لا يهم إن كان التهديد لمصلحة الجاني المشروعة أو غير المشروعة فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد إرغام المجني عليه للقيام بذلك الفعل،[20] بالتالي فالركن المادي لأي جريمة يتكون من المحل والفعل.

يقصد بمحل جريمة التهديد الإلكتروني هو أمر أو واقعة تسند إلى المجني عليه وذلك للمساس بشرفه أو شرف غيره ولا يهم من إن كانت الواقعة التي يهدد بها الجاني المجني عليه بأن تكون صحيحة أو غير صحيحة ولا يهم أيضا إن كانت تلك الواقعة تخص المجني عليه أو تمتد إلى شخص أخر، العبرة هنا ما يهتم به القانون من حيث المحل المادي لجريمة التهديد الإلكتروني أن يكون من شأن الواقعة المساس بشرف المجني عليه أو المساس بشرف وكرامة أقاربه، أما من حيث السلوك الجرمي (الفعل) لجريمة التهديد الإلكتروني فإن الفعل الرئيسي هو التهديد بفضح أمر معين حيث يكون هدف الجاني الضغط على المجني عليه من أجل تحقيق غاية معينة، وأهم ضابط لسلوك المادي هو درجة المساس بالمكانة

---

(19) يراجع في ذلك:

المادة 327 من قانون العقوبات المصري رقم 58 لسنة 1937 معدل ومتمم، المتواجد على الرابط التالي:
https://elmo7amy.tv/wp-content/uploads/2023/04/كود-العقوبات-المصرى-pdf.pdf.
الذي تم الإطلاع بتاريخ 2024/06/10 على الساعة 11:45

(20) يراجع في ذلك:

عراب مريم، "جريمة التهديد والابتزاز الإلكتروني"، **مجلة الدراسات القانونية المقارنة**، المجلد 07، العدد 01، 2021، ص1208.

الاجتماعية واعتبار المجني عليه أو شرفه، منه فعناصر الركن المادي لجريمة التهديد الإلكتروني تتمثل في ثلاثة عناصر والمتمثلة في السلوك الإجرامي والنتيجة والعلاقة السببية.[21]

1-السلوك الإجرامي: يعد من أهم عناصر الركن المادي لأي جريمة، لأنه يكشف عن سلوك مخالف لإرادة المشرع، ويبدو بمظاهر مادية ملموسة في العالم الخارجي، ويعني ذلك أن الأفكار التي تكون داخلية لا عقاب عليها، السلوك الإجرامي في الجرائم التقليدية على أنه فعل الجاني الذي يحدث أثر في العالم الخارجي بغير هذا السلوك لا يمكن محاسبة الشخص مهما بلغت خطورة أفكاره وهواجسه الداخلية، فالسلوك هو الذي يخرج النية والتفكير في الإجرام إلى حيز الوجود واعتبار القانون، ولا يكاد يفرق بين السلوك الإجرامي (الفعل) والسلوك السلبي (الامتناع عن فعل) مادام لهما نفس النتيجة.[22]

أ-السلوك الإيجابي: يكون في صورة فعل أو قول يجرمه القانون يصدر عن الجاني ويؤدي إلى إحداث نتيجة في الجرائم التي تشترط تحقق نتيجة لقيامها، وكذلك يعتبر سلوكا إجراميا في ذاته في الجرائم الشكلية، ولا يهتم القانون بالوسيلة سواء كانت مادية أو معنوية، فإذا كان السلوك محظوراً قانوناً فهو يشكل جريمة، ويدخل ضمن السلوك الإيجابي فعل التحريض على الجريمة وغيرها من السلوكيات.

ب-السلوك السلبي: يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه أن يعمل فلا يعمل، ففي هذه الحالة يقوم المكلف بالحيلولة دون جسمه كله أو بعضه ويبين الحركة التي يتطلبها القانون أو يتحرك باتجاه مضاد لما أمره به، يقوم الفعل السلبي على الامتناع أو إجبار شخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، وعليه فلا يجوز للقاضي أن يمتنع عن الحكم بالدعوى ولا الشاهد أن يمتنع عن الإدلاء بشهادته أمام المحكمة بواقعة يعلمها ولا للموظف أن يمتنع عن أداء مهام وظيفته.[23]

2-النتيجة الإجرامية: يقصد بها الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، فالسلوك قد أحدث تغييراً حسيا ملموسا في الواقع الخارجي، ومفهوم النتيجة كعنصر في الركن المادي

---

(21) يراجع في ذلك:

مصطفى خالد الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، د ط، مركز الكتاب الأكاديمي،عمان، الأردن،2020، ص ص 57 58.

(22) يراجع في ذلك:)

برحال أمال، مرجع سابق، ص42

(23) يراجع في ذلك:

تعريف ومفهوم السلوك الإجرامي في القانون، المنشور على منصة محامات نت، المتواجد على الرابط:

https://www.mohamah.net/law

الذي تم الإطلاع عليه بتاريخ 2024/06/01 على الساعة 15:01.

للجريمة يقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج، بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.[24]

3-العلاقة السببية : تمثل هذه العلاقة الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وأهمية العلاقة السببية ترجع إلى إسناد النتيجة إلى الفعل وهو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتتحقق العلاقة السببية تلازما مادياً بين الفعل والنتيجة يؤدي إلى وقف مسؤولية الجاني عند حد الشروع، إذا لا يعد مسئولا عن النتيجة التي تحققت، أما إذا كانت الجريمة غير عمدية، فإن نفي رابطة السببية يؤدي إلى انتفاء المسؤولية عنها، ذلك أنه لا شروع في الجرائم العمدية .[25]

ثالثا: الركن المعنوي لجريمة التهديد الإلكتروني

يعتبر الركن المعنوي هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هو المسلك الذهني أو النفسي للجاني باعتباره محور القانون الجنائي، من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبنى على المقومات هذا على العموم في جميع الجرائم، غير أن التساؤل يثور في مجال الجرائم المرتكبة عبر الإنترنت.

1-عناصر القصد الجنائي:

أ-العلم: لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء تعلق الأمر بسلوكه الإجرامي أم بموضوع الاعتداء، فإذا كان الجاني جاهلا بشيء من ذلك فلا يتحقق القصد الجنائي، وليس في كل جهل ينتفي معه القصد الجنائي، بل هناك وقائع يؤثر الجهل بها في القصد وأخرى لا يتأثر بها القصد.[26]

ب-الإرادة: هي النشاط نفسي يهدف إلى تحقيق غرض معين، فإذا كان غرض الجاني تحقيق نتيجة إجرامية، كانت الإرادة المتجهة إلى الفعل المنطوي على إحداث النتيجة هي القصد الجنائي والغرض هو

---

(24) يراجع في ذلك:

سكينة فروج، عبد الرحمان خلفي، "أثر النتيجة الإجرامية على التفريد العقابي"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد 07، العدد02، ديسمبر 2022، ص 98.

(25) يراجع في ذلك:

صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص ص65 67.

(26) يراجع في ذلك:

طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الالكتروني عبر مواقع التواصل الاجتماعي (دراسة مقارنة)، رسالة لنيل شهادة الماجستير، كلية القانون و العلوم السياسية، جامعة كركوك، العراق، 2021، ص ص 104 106.

الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو الدافع إلى إشباع حاجة معينة، وهذا الدافع له طبيعة نفسية، بخلاف الغاية التي لها طبيعة موضوعية.[27]

2-صور القصد الجنائي:

أ-القصد الجنائي العام: يهدف الجاني عند ارتكابه للواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين بتحقيقه قد تتم الجريمة ويتوافر لها القصد الجنائي العام، وعليه فالقصد العام أمر ضروري ومطلوب في كل الجرائم العمدية.[28]

ب-القصد الجنائي الخاص: يتميز هذا النوع من القصد الجنائي بأن الشخص يسعى إلى تحقيق غاية معينة، أو يوجد لديه باعث خاص في الإقدام على ارتكاب الجريمة. يستخدم مثل هذا النوع من القصد في جرائم السرقة، حيث يتطلب القانون إرادة التملك بالإضافة إلى القصد العام.[29]

يلتقي القصد العام والقصد الخاص في جميع عناصره، ويزيد عنه في تحديد الإرادة الإجرامية لدى الجاني إما بباعث معين فقد يدفعه إلى الجريمة، وإما بنتيجة محددة يريدها.

ج-القصد المباشر: يعتبر القصد المباشر سواء كان معينا أو غير معين كلما ارتكب الجاني الفعل وهو يعلم نتائجه ويقصدها بغض النظر عما إذا كان يقصد شخصا معينا أو لا يقصد شخصا معينا، كمن يخترق جهاز حاسوب لمجني عليه بغرض تهديده دون أن يعلم من هو.

د-القصد غير المباشر: يعتبر القصد غير مباشر إذا قصد الجاني فعلا معينا ترتب عليه فعل لم يكن يقصده في الأصل، أو لم يستطع تقدير نتائجه، وذلك كقيام أحد الأشخاص باختراق جهاز حاسب آلي لأحد زملائه بغرض التلصص، فإذا بالأمر يتطور لفكرة تهديد المجني عليه والقصد الغير مباشر يسمى أيضا بالقصد المحتمل.[30]

---

(27) يراجع في ذلك:

مفهوم الإرادة في الركن المعنوي للجريمة، المنشور على منصة مؤسسة دام برس الإعلامية التواجد على الرابط التالي:

https://www.dampress.net/mobile/?page=show_det&category_id=48&id=62342

الذي تم الاطلاع عليه بتاريخ 2024/05/10 على الساعة 22:30

(28) يراجع في ذلك:

صغير يوسف، مرجع سابق، ص ص 68 70

(29) يراجع في ذلك:

بحث حول القصد الجنائي المنشور على منصة Law House المتواجد على الرابط:

https://www.law-house.net

الذي تم الاطلاع عليه بتاريخ 2024/04/18 عل الساعة 12:02

(30) يراجع في ذلك:

القصد المباشر والغير المباشر المنشور في منصة المحامي الرقمية المتواجد على الرابط

https://elmo7amy.tv/

الفرع الثاني

شروط قيام جريمة التهديد الإلكتروني

من تسمية جريمة التهديد الإلكتروني يتبين لنا النطاق الذي تقع فيه الجريمة وهو البيئة الإلكترونية، حيث أنه بالإضافة إلى شروط ثبوت المسؤولية في جريمة التهديد والمتمثلة في أن يكون التهديد أولا هناك تهديد صريح أو مبطن بإلحاق ضرر بالضحية، أن يكون التهديد جادا بحيث يثير الخوف والقلق في نفس الضحية، أن يكون التهديد موجها إلى شخص محدد ومعروف، وهناك أيضا شرط تم إضافته نظرا إلى النطاق الذي تقع فيه الجريمة وهو أن يكون قد تم التهديد عبر وسيلة إلكترونية أي من خلال الشبكة المعلوماتية أو أحد وسائل تقنية المعلومات.

في حال إذا اقترفت هذه الجريمة خارج نطاق هاتين الوسيلتين فلا نكون بصدد جريمة التهديد الإلكتروني، ويمكن اعتبار هذا كشرط مسبق لارتكاب هذه الجريمة.

أولا: الشبكة المعلوماتية WEB

تعرف شبكة المعلومات أو ما يسمى بشبكة الأنترنت حسب المجلس الفيدرالي الأمريكي لشبكات الحاسوب (FNC)The Federal Networking Council، أن مصطلح الأنترنت يشير إلى: "نظام المعلومات العالمي المرتبط ببعضه منطقيا بواسطة مجموعة عناوين متفردة ترتكز على بروتوكول الأنترنتIPأو ملحقاته الفرعية وتوابعه وأي بروتوكولات أخرى متوافقة مع بروتوكول الأنترنت، ويكون قادرا على دعم الاتصالات بواسطة حزمة بروتوكول TCP/IPأو أية بروتوكولات متوافقة، ويوفر استخدامات أو يسهل عملية الدخول بشكل عام أو خاص إلى مستوى عالي من الخدمات المعتمدة على الاتصالات والبنية التحتية المشار إليها".[31]

تعرف أيضا بأنها عبارة عن ترابط بين جهاز حاسوب أو أكثر بإحدى طرق الاتصال المتوفرة، ويتم تبادل المعلومات والبيانات فيما بين هذه الأجهزة.[32]

الذي تم الإطلاع عليه بتاريخ 10 /2024/06 على الساعة 15:55.

(31)يراجع ذلك في:

محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت (دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية)، رسالة لنيل شهادة الماجستير، قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 20.

(32)يراجع في ذلك:

ما مفهوم الشبكة المعلوماتية، المنشور على منصة موضوع، المتواجد على الرابط التالي:

https://mawdoo3.com/

الذي تم الإطلاع عليه بتاريخ 2024/05/22 على الساعة 10:31.

ومن بين التعريفات أيضا أنها "مجموعة من الأجهزة والبرمجيات تعمل معا كنظام لنقل البيانات من نقطة إلى أخرى"، وعرفها المشرع المصري في المادة 1 من قانون مكافحة جرائم تقنية المعلومات بأنها:" مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معا ويمكنها تبادل المعلومات والاتصالات فيما بينهما، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية والتطبيقات المستخدمة عليها"، وهذه الشبك تمثل أجهزة الكمبيوتر ووسائل الاتصال مملكتي عصر المعلومات وعند جمعها مع بعض داخل شبكات الحاسوب تشكلان أساس شبكة الويب الحالية والبنية الأساسية لمعلومات المستقبل.[33]

هذه الشبكة فتحت الباب على مصراعيه للانتقال الحر للبيانات والمعلومات حول العالم دون الاعتراف بالحدود السياسية والجغرافية للدول، مختصرة فيها الزمان والمكان، فهي بدورها تتألف من عدد كبير من الوسائل المختلفة لتنظيم البيانات ونقلها والوصول إليها، كما أن نطاق استخدامها متعدد، ومن بين وسائلها: البريد الإلكتروني E-mail،مواقع التواصل الاجتماعي كـ Facebook،Instagramtiktok، منتديات الدردشة....إلخ.[34]

ثانيا: وسائل تقنية المعلومات

تطرق المشرع المصري إلى تعريف تقنية المعلومات من خلال المادة الأولى من قانون مكافحة جرائم تقنية المعلومات بأنها:" أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا، كأجهزة الحاسب الآلي وأجهزة الاتصال"، تقنية المعلومات أو تكنولوجيا المعلومات (information technology) تختصر ب (IT) وحسب تعريف مجموعة تقنية المعلومات الأمريكية ITAA هي:" دراسة تصميم وتطوير وتفعيل أو تسيير أنظمة المعلومات التي تعتمد على الحواسب، وبشكل خاص تطبيقات وبنية عتاد الحاسوب"، تهتم تقنية المعلومات باستخدام الحواسيب والتطبيقات البرمجية لتحويل وتخزين وحماية ومعالجة وإرسال والاسترجاع الآمن للمعلومات.[35]

---

(33) يراجع في ذلك:

المادة 01 من من قانون مكافحة جرائم تقنية المعلومات، المتواجد على الرابط التالي:

https://manshurat.org/node/31487

الذي تم الإطلاع عليه بتاريخ 2024/06/10 على الساعة 14:09

(34) يراجع في ذلك:

محمد سعيد عبد العاطي محمد، محمد أحمد المشاوي محمد،" دور القانون الجنائي في حماية الطفل من الابتزاز الإلكتروني (دراسة مقارنة)"، **مجلة البحوث الفقهية والقانونية**، العدد 36، أكتوبر 2021، ص 142.

(35) يراجع في ذلك:

المادة 01 من قانون مكافحة جرائم تقنية المعلومات، مرجع سابق.

أما المشرع الجزائري لم يتعرض إلى تعريف تقنية المعلومات واكتفى بما عرفه الفقهاء، حيث أن هناك من عرفها على أنها الحصول على المعلومات الصوتية والمصورة والرقمية والتي في نص مدون، وتجهيزها واختزالها، وبثها وذلك باستخدام توليفة من المعدات الميكرو إليكترونية الحاسبة والاتصالية عن بعد، في يرى آخر بأنها البحث عن أفضل الوسائل لتسهيل الحصول على المعلومات وتبادلها وجعلها متاحة لطالبها بسرعة وفعالية، وبناءًا عليه فإن تقنية المعلومات لها جوانب ثلاث يمكن التمييز بينها، الجانب الأول هو تقنية تسجيل المعلومات، والجانب الثاني هو تقنية تحليل البيانات، ثم يأتي الجانب الثالث المتمثل في تقنية توصيل البيانات.[36]

يتبين ضرورة أن تقع جريمة التهديد الإلكتروني عبر شبكة المعلوماتية" الأنترنت" مثلFacebook ، Instagram، أو بواسطة أي وسيلة من وسائل التقنية الحديثة مثل التليفون المحمول أو الكمبيوتر الشخصي، وإلا انتفت عنها صفة جريمة التهديد الإلكتروني، وإن كانت من الممكن أن تشكل جريمة أخرى ستكون جريمة التهديد التقليدية المنصوص عليها في قانون العقوبات.[37]

المطلب الثاني

نطاق المسؤولية الجزائية لجريمة التهديد الالكتروني وشروطها

تعرف المسؤولية الجزائية بأنها التزام الإنسان بتحمل الآثار القانونية المترتبة عن قيامه بفعل غير مشروع يعتبر جريمة بنظر القانون، ونتيجة مخالفة هذا الالتزام هو العقوبة أو التدبير الاحترازي الذي يفرضه القانون عن الشخص، وبما أن جريمة التهديد كغيرها من الجرائم تأثرت بالتطور الهائل لتكنولوجيا الإعلام والاتصال، ما يعني أن بيئة مسرح الجريمة قد تغير من شكله التقليدي وأصبحت تتم ضمن بيئة رقمية وعالم افتراضي ما شكل عبء على الجهات المختصة في تحديد الأشخاص المسؤولة جزائيا عن جريمة التهديد الالكتروني بمعنى على من تقوم المسؤولية الجزائية في جريمة التهديد الالكتروني.

يمس هذا النوع من الجريمة كل الفئات العمرية صغيرا كبيرا شخصا طبيعيا ومعنويا، ويمكن أن تقع على الكثير من الوسائل الإلكترونية وعلى رأسها مواقع التواصل الاجتماعي.

---

(36) يراجع في ذلك:

عمار حمبلي، عثماني دليلة، جرائم تقنية المعلومات في ظل الاتفاقية العربية 2010 والتشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021-2022، ص8.

(37) يراجع في ذلك:

محمد سعيد عبد العاطي محمد، محمد أحمد المنشاوي محمد، مرجع سابق، ص 144.

الفرع الأول

نطاق المسؤولية الجزائية عن جريمة التهديد الإلكتروني

تعتبر الشبكة العالمية من أكثر المجالات التي تستخدم فيها تكنولوجيا الإعلام والاتصال الحديثة والتي تعتبر بيئة للشكل المستحدث لجريمة التهديد، تعتبر هذه الأخيرة من أحد نتائج أو إشكال الاستخدام السيئ للشبكة العالمية (الانترنت)، فالغرض الأساسي من استعمال أجهزة الاتصال الحديثة هو الاتصال السريع، ولكن هناك بعض الأشخاص ذات النفوس الضعيفة ممن تستهويه استعمال هذه الوسائل استعمالا غير مشروع لارتكاب الجرائم كجريمة التهديد الإلكتروني، فلا إشكال في قيام المسؤولية الجزائية ضد هؤلاء الأشخاص، لكن السؤال يطرح في مدى مسؤولية الأشخاص الذين يوفرون هذه الخدمة، وهو من أصعب الحالات التي يمكن تحديدها نظرًا للطابع الفني الذي يميز الشبكة وصعوبة فهم التقنيات التي تعمل بها.

عرف المشرع الجزائري مقدمي خدمة الأنترنت في المادة 2/ف.د من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنهم:" 1-أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات، 2-وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها."،[38]لذا من خلال هذا الفرع سنتطرق إلى صور المسؤولية الجنائية لمقدمي الخدمة وذلك حسب الدور الذي يقوم به عبر الشبكة.

أولا: المسؤولية الجنائية لمقدمي الخدمات الفنية

لقد واجه القانون والقضاء صعوبة في تحديد صور المسؤولية الجنائية لمقدمي الخدمات الفنية وذلك نظرا لطبيعة نشاطهم ولأنه في أغلب الأوقات لا يعترفون بها، لذا أردنا تلخيصها حسب الدور الذي يقوم به كل من مزود خدمة الاتصال، الناقل المادي، متعهد الوصول، متعهد الإيواء.[39]

1-حالات المسؤولية الجنائية لمزود خدمة الاتصال: اختلفت تسميات هذا المتعامل من تشريع إلى آخر من بينها: متعهد الوصول، مقدم خدمات الدخول، مورد منافذ الدخول، مزود الخدمة، خدمة الاتصال

---

(38)يراجع في ذلك:

المادة 2 من القانون 09-04، مرجع سابق.

(39)يراجع في ذلك:

أحمد عبد الاله عبد الحميد عبد الرحيم المراغي،" المسئولية الجنائية لمقدمي خدمات الإنترنت (دراسة تحليلية خاصة لمسئولية مزودي خدمات الاتصالات الإلكترونية"، مجلة حقوق حلوان للدراسات القانونية والاقتصادية،المجلد 42، العدد 42 - الرقم المسلسل للعدد 42 يناير 2020،ص 10 .

...إلخ، إلا أن أحسن تعبير يحقق معناه هو: مورد خدمة الدخول إلى شبكة الأنترنت لكونه يتماشى ويتلاءم مع مفهوم ومهام هذا المتعامل،[40]عرفه Christiane Feral-Schuhl بأنه المتعامل الذي يوفر لعملائه المصادر التقنية التي تسمح لهم بالدخول إلى شبكة الأنترنت وما توفره من خدمات، كما يعمل على إقامة الربط بين مختلف موردي الخدمات على الشبكة والمستخدمين.[41]

كما عرفته المادة 6-1-1 من القانون رقم 2004-575 المتعلق بالثقة في الاقتصاد الرقمي موردي خدمات الاتصال بشبكة الأنترنت أنهم " أشخاص ينصب نشاطهم على إتاحة الاتصال بخدمات الاتصال الفوري للجمهور على الخط".[42] أما بالنسبة لقانون تنظيم الاتصالات المصري رقم 10 لسنة 2003 في المادة 1 فقرة 7 عرفه بأنه: " كل شخص طبيعي أو اعتباري مرخص له من الجهاز القومي لتنظيم الاتصالات بتقديم خدمة من خدمات الاتصال بالغير".[43]

رغم اختلاف التعريفات إلا أن لها نفس الدلالة التي تقضي بأن مورد الدخول Le fournisseur d'accès هو ذلك الشخص الطبيعي والمعنوي الذي يكون مرخصا له بتقديم خدمات الاتصال، وهو يعتبر الممر الإلزامي لوصول المستخدم إلى الأنترنت.

أما المشرع الجزائري تطرق إليه ضمن أحكام القانون 09-04 في نص المادة الأولى فقرة د-1 بأنه: " أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات". وحدد شروط و كيفيات استعمالها في المرسوم التنفيذي 98-257،[44] وهو ما يقوم به المتعامل التاريخي" اتصالات الجزائر". فطبيعة الخدمة التي تقدمها هذا النوع من المؤسسات خدمة تقنية بحتة تفترض أن مقدمها لا تكون له أي علاقة بالمضامين التي تنشر أو يتم الاطلاع عليها، وهذا هو المتفق عله قضاء وتشريعا.

---

(40)يراجع في ذلك:

حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الأنترنت، د ط، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019، ص18.

(41)يراجع في ذلك:

FERAL-SCHUL Christiane, Le Droit à l'épreuve de l'internet, Ed 6, Dalloz, Paris, France, 2010, P 770.

(42)يراجع في ذلك:

محمد حمزة بن عزة، المسؤولية القانونية لمتعاملي الأنترنت (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2018-2019، ص136

(43)يراجع في ذلك:

محمد حمزة بن عزة، المرجع السابق، ص 137

(44) يراجع في ذلك:

المرسوم التنفيذي رقم98 -257 المؤرخ في 03 جمادى الأولى عام 1419 الموافق لـ25 غشت 1998 المتضمن ضبط شروط وكيفيات إقامة خدمة الأنترنت واستغلالها، ج ر ج ج، عدد 63 ، المؤرخة في 04 جمادى الأولى عام 1419 الموافق لـ 26 غشت سنة 1998

لكن هذا لا يمنع إمكانية مساءلتهم جزائيا في حالات ضيقة جدا، بالنظر إلى القانون 09-04 الذي لم يميز بين مقدمي الخدمة في نطاق فرض الالتزامات التي يجب عليهم العمل بها والواردة في المواد 11 و12 من هذا القانون، كصورة خرق الالتزامات الواردة في المادة 11 مثل ضرورة حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، الخصائص التقنية وكذا تاريخ و وقت ومدة كل اتصال ...إلخ، بحيث إذا أدت إلى عرقلة حسن سير التحريات القضائية ستشكل جنحة معاقب عليها بالحبس من 6 أشهر إلى 5 سنوات مع غرامة من 50000 دج إلى 50000 دج بالنسبة إلى الشخص الطبيعي، ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات، دون الإخلال بالعقوبات الإدارية.[45]

2-حالات المسؤولية الجنائية لمورد خدمة الإيواء: عملية إيواء البيانات والمعلومات وتخزينها خدمة من الخدمات التقنية التي تحدث داخل شبكة الأنترنت، ويطلق على المتعامل عدة تسميات باللغة العربية، منها مورد خدمة الإيواء أو مورد خدمة الاستضافة وكلاهما صحيح يعبران عن مصطلح Hébergement باللغة الفرنسية.

جاء مفهوم الاستضافة حسب نص المادة 14من التوجيه الأوروبي المتعلق بالتجارة الإلكترونية الصادر في 08 جوان 2000 على أنها تكمن في تخزين المعلومات التي يتم توريدها من طرف المستفيد من هذه الخدمات.[46] أما المشرع الجزائري فتطرق إليها من خلال القانون 09-04 في نص المادة 2 فقرة د-2 حيث جاء فيها:" أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال الذكورة أو لمستعمليها"،[47]وهو ما ينطبق على مهام مورد خدمة الإيواء وبذلك يكون هذا النص تطرق إليه دون أن يسميه، إن الطبيعة القانونية لخدمات متعهد الإيواء قد تخوله القيام بعدة مهام في نفس الوقت والتي على رأسها مهمة تخزين المعلومات، وعلى ذلك تختلف صور قيام مسؤوليته الجنائية وذلك حسب دوره.

---

(45)يراجع في ذلك:

المواد 11 و 12 من القانون 09-04،مرجع سابق.

(46)يراجع في ذلك:

المادة 14 من الأمر التوجيهي رقم 31/2000 EC/للبرلمان والمجلس الأوروبي المؤرخ 8 يونيو 2000 بشأن بعض الجوانب القانونية لخدمات مجتمع المعلومات، لاسيما في مجال التجارة الإلكترونية، في السوق الداخلية (أمر توجيهي في مجال التجارة الإلكترونية)، المتواجد على الرابط التالي:

https://www.wipo.int/wipolex/ar/legislation/details/6393

الذي تم الاطلاع عليه بتاريخ 2024/04/19 على الساعة 17:45.

(47)يراجع في ذلك:

المادة 02 من القانون 09-04 ، مرجع سابق

أ-مسؤولية متعهد الإيواء كشريك في الجريمة: لكي نقول إن متعهد الإيواء شريك في الجريمة يجب أن تثبت مساهمته في الجريمة إما عن طريق التحريض أو الاتفاق أو المساعدة أي أن يكون دوره إيجابي، ولا يمكن نفي هذه المسؤولية إلا بإثبات عكس ذلك كإثبات جهله بعدم مشروعية المضمون الإلكتروني.

حيث انتهت محكمة النقض الفرنسية إلى استحالة مساءلة مدير مركز الحاسبات الخادمة Centres Serveurs Minitel عندما يقوم بإيواء خدمات محتوى الرسائل غير المشروعة، فتخزين البيانات والمعلومات يكون لثواني، كشخص بعث رسالة تهديد إلى شخص آخر عبر البريد الإلكتروني، فتواجد هذه الرسالة في القرص الصلب لمتعهد الإيواء قد يكون لثواني، فلا يمكن معاقبته على جريمة حدثت في ثواني ولم يكن قادرا على معرفتها، إضافة إلى الكميات الكبيرة من هذه المعلومات والرسائل الإلكترونية التي تمر بقرصه الصلب يوميا والتي من المستحيل أن يقوم بمراقبتها أو التدقيق في مشروعيتها، إلا ان هذا لا يعني عدم مساءلتهم حيث تنعقد مسؤوليتهم في حالتين:

-إذا توفر لديهم العلم الفعلي بالطبيعة غير المشروعة للمحتوى ولم يخطروا السلطات أو يتصرفوا فورا لإزالة البيانات أو جعل الوصول إليها مستحيلا.

-إذا لم يبقوا على البيانات التي يمكن من خلالها التعرف إلى مدير تحرير الموقع أو المدون.[48]

ب-مسؤولية متعهد الإيواء عن جريمة الإخفاء: حيث يسأل عن جريمة الإخفاء في حالة ما إذا قام متعهد الإيواء بتسجيل المعلومات غير المشروعة على دعامة، قضت محكمة النقض الفرنسية بانتفاء الحيازة المادية للمعلومات ومن ثم لا تصلح لأن تكون محلا لجريمة الإخفاء، أما إذا تم نقل المعلومات غير المشروعة على إحدى وسائط التخزين للقرص الصلب أو أسطوانات الليزر CD فنجد أن أيا منهم دعامة مادية وتصلح أن تكون محلا لجريمة الإخفاء.[49]

ثانيا: صور المسؤولية الجنائية لمقدمي الخدمات المعلوماتية

القيام بخدمة تقديم المعلومات تعرض مقدميها إلى المساءلة الجزائية عن المحتويات غير المشروعة التي يتعاملون بها، فهم على اتصال مباشر بالمضمون الإلكتروني، وفي أغلب الحالات لا تحتاج إلى إخطار من الغير لمعرفة عدم مشروعيته، وتختلف المسؤولية الجنائية بين ناشر المعلومة ومؤلفها.

---

(48) يراجع في ذلك:

دينا عبد العزيز فهمي، "المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي"، بحث مقدم للمؤتمر العلمي الرابع تحت عنوان القانون والإعلام، كلية الحقوق، جامعة طنطا، 23-24 ابريل 2017، ص ص 31 32.

(49) يراجع في ذلك:

حدة أبو خالفة، "النظام القانوني لمتعهد الإيواء عبر الأنترنت في القانون الجزائري والأردني (دراسة مقارنة)"، **مجلة دراسات علوم الشريعة والقانون**، المجلد 45، العدد 04، الملحق 02 2018، ص 163.

1-المسؤولية الجنائية لناشر المعلومة: قد يكون الناشر الشخص الذي قام بإنشاء صفحة التواصل أو قام بتأليف المحتوى، أو وضع المعلومات على المواقع أو أرسلها عبر الشبكة، فتقع في حقه المسؤولية الجنائية المباشرة عما يتم بثه.

تفترض جرائم النشر الإلكتروني أن يكون هناك ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات، وأن يقوم هؤلاء المستخدمين بنشر أو إعادة نشر بيانات أو أي معلومات يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تقنية المعلومات، ويستوي أن تتعلق تلك البيانات أو المعلومات بمستخدمين آخرين. ويكون لناشر الموقع السلطة الكاملة على هذه المعلومات لأنه هو من قام بجمعها وتكمن هذه السيطرة في القيام بنشرها أو الامتناع عن ذلك، وبذلك فإن ناشر الموقع ملزم مراقبة محتوى الرسائل التي يصل إليه ليقرر بعدها عدم نشرها إن كانت غير مشروعة، يمكن حصر حالات المسؤولية الجنائية لناشر المحتوى فيما يلي:

-أن يكون فاعلا أصليا في جرائم النشر، بأن يقوم بتأليف المعطيات بنفسه وتسجيلها ثم نشرها على مواقع الشبكة رغم عدم مشروعيتها.

-أن يكون فاعلا أصليا في جريمة الإخفاء، بأن يقوم بتسجيل المعطيات التي تصله ونشرها مع علمه بعدم مشروعيتها.

-أن يكون شريكا في جريمة النشر، باعتباره مدير التحرير على المواقع، الذي تصل إليه المعطيات غير المشروعة، ومع علمه بعدم مشروعيتها يقوم بنشرها، أو أن يقصر في القيام بالتزام الرقابة على هذه المعطيات غير المشروعة قبل نشرها، لكن وجب أولا تحديد الشخص القائم بالنشر الإلكتروني ليتم تحديد المسؤولية الجنائية.[50]

2-المسؤولية الجنائية لمؤلف المعلومة: الشخص الذي يؤلف المعلومة غير المشروعة وينشرها على الشبكة هو أول من يجب أن يسأل عنها، فهم يلعبون دورا إيجابيا في تأليف المحتوى الإلكتروني، هناك حالة أين يكون مؤلف الرسالة شريك في الجريمة، وليس فاعلا أصليا ويكون هنا الناشر هو الفاعل الأصلي، إذ يسأل هذا الأخير جزائيا لأنه أخل بواجب التدقيق والتفحص للمعلومات التي تمر عبر شبكته،

---

(50) يراجع في ذلك:

حنان جديلي، المسؤولية الجزائية لمتعهدي الأنترنت، مذكرة لنيل شهادة الماستر، تخصص قانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة،2019-2020،ص 36.

والتأكد من مشروعيتها، ويكون مؤلف الرسالة شريكا في الجريمة لأنه يدخل باسم مستعار يصعب معه غالبا التأكد من هويته وتحديد عنوانه على شبكة الأنترنت.[51]

الفرع الثاني

شروط قيام المسؤولية الجنائية لمقدمي خدمة الأنترنت

إقرار المسؤولية الجزائية لمقدمي خدمة الأنترنت ضرورة لا مناص لها، وهذا حتى يبذل القائمين على هذه الخدمة الحيطة والحذر حول ما يمر عبر قنواتهم من محتوى قد يضر بالغير، ولذلك وضعت شروط منها موضوعية وأخرى إجرائية بتوافرها تتقرر المسؤولية الجنائية في حق مقدمي خدمة الأنترنت.

أولا: الشروط الموضوعية لقيام المسؤولية الجنائية لمقدمي خدمة الأنترنت

تفرض خدمة الأنترنت خصوصية مختلفة للمسؤولية الجنائية لمقدميها، حيث تتطلب لقيامها مجموعة من الشروط الموضوعية الخاصة.

1-العلم الفعلي بالمحتوى غير المشروع: القاعدة في هذا المجال أن المورد أو الوسيط غير مسؤول عن المعلومات المنشورة على الشبكة، بالمقابل يعد مسؤولاً إن كان يعلم بالطابع غير المشروع لها، أو كان يعلم بالظروف التي تجعل عدم مشروعيتها واضحا وظاهرا، ويكون هذا هو وجه المعرفة الفعلية.[52]

وفي قضية بروجي (prodigy case s) وهي شركة مجهزة الخدمات، في عام 1995أقرت المحاكم الأمريكية حكم يقضي بالتعويض في حق شركة برودجي لصالح الطرف المدعي، على الرغم من أن الشركة لم يكن باستطاعتها مراجعة المحتوى الإلكتروني الذي تبثه عبر الموقع، فالشركة لا تملك الأجهزة التقنية المناسبة للرقابة، لذا فالحكم الذي جاء عليها غير منصف نظرا للظروف التقنية التي تعمل بها هذه الشركة. إلا أنه يمكن الأخذ بالقوانين الخاصة بالحكم في المسؤولية الجنائية لمقدمي الخدمة، ما لم يكن لها تشريع خاص، وهذا ما اعتمده القضاء في تطبيق القوانين الأخرى حتى لا يضيع حق الضحية في التعويض.[53]

2-عدم الالتزام بالمراقبة: اتفق القضاء الأوروبي على أن يقيم مسؤولية متعهد الإيواء إذا توافر العلم مع قدرته الفنية على منع الوصول إلى المحتوى غير المشروع، أو وقف بثه، حيث أن القضاء لا يفرض الرقابة

---

(51) يراجع في ذلك:

حنان جديلي، مرجع سابق، ص 35.

(52) يراجع في ذلك:

Bernard Dubuisson, Pierre Jadoul, La responsabilité civile liée à l'information et l'information et au conseil questions d'actualité, publications des facultés Universitaires Saint-Louis, Bruxelles, 2000, p12.

(53) يراجع في ذلك:

حدة بوخلفة، مرجع سابق، ص ص64 65.

السابقة على المحتوى المعلوماتي، وإنما يلزمه بالرقابة التي تأتي بعد البث وذلك لعدة اعتبارات وحماية لسرية الاتصالات والمحافظة على سرية البيانات الشخصية.

المشرع الجزائري لم ينص على التزام مقدمي الخدمة بالمراقبة، يرى أنه نص على نوع آخر من الرقابة وهو رقابة السلطات الخاصة للمحتوى المعلوماتي، كإجراء جزائي من إجراءات التحقيق في جريمة ذات طابع معلوماتي منصوص عليه في القانون 09-04.

إذا لا وجود لالتزام الرقابة على عاتق مزودي خدمة الأنترنت، ما لا يرتب على عاتقهم أي مسؤولية جنائية في حالة وجود مضمون غير مشروع عبر قنواتهم، وهذا ينحصر فقط على مقدمي الخدمة الفنية، أما مقدمي خدمة المعلوماتية فلا ينطبق ذلك عليهم لأنهم الأشخاص المصدرة للمحتوى، فيفترض فيهم المعرفة والقدرة على رقابة هذا المحتوى قبل توريده للمستخدمين.[54]

ثانيا: الشروط الإجرائية لقيام المسؤولية الجنائية لمقدمي خدمة الأنترنت

يلتزم مقدمي خدمة الأنترنت ببعض التصرفات القانونية الإيجابية والتي نصت عليها مختلف التشريعات حيال المضمون الإلكتروني غير المشروع الذي يمر عبر قنواتهم ويهدد استقرار الحياة الخاصة للأفراد، وإلا قامت في حقه المسؤولية الجنائية، وحددت بمفهوم الشروط الإجرائية، هي الإخطار وعدم وقف البث.

1-الإخطار: ويقصد به إخطار السلطات المختصة أو الجهات المعنية، فهو ملزم بالتبليغ متى ما وجد محتوى غير مشروع، وتقوم مسؤوليته الجنائية إذا قام بأي عمل يحول دون حسن سير التحريات القضائية بموجب المادة 11 من القانون 09-04.[55]وبموجب نص المادة 8-1/6 من القانون الفرنسي حول الثقة في الاقتصاد الرقمي تأمر مقدمي خدمات الأنترنت بصورة عاجلة وبغض النظر عن صفاتهم أو طبيعة الخدمة التي يقدمونها، باتخاذ الإجراءات اللازمة لوقف بث أي مضمون ثبت عدم مشروعيته، وبالطبع تقوم مسؤوليتهم في حال عدم استجابتهم لهذا الأمر،[56]المقصود بالإجراءات اللازمة هنا هي إخطار السلطات المختصة ووقف بث المحتوى.

---

(54)يراجع في ذلك:

حدة بوخلفة، مرجع سابق، ص 76.

(55)يراجع في ذلك:

المادة 11 من القانون 09-04، مرجع سابق.

(56)يراجع في ذلك:

أحمد قاسم فراح،"النظام القانوني لمقدمي خدمات الأنترنت: دراسة تحليلية مقارنة"،مجلة المنارة، المجلد 13، العدد 9، الأردن، 2007، ص34.

أقرت الولايات المتحدة الأمريكية ف عام 2004نصوصا تقرر المسؤولية الجنائية على مزودي خدمات الأنترنت في حالة عدم الإبلاغ عن وجود مواد غير مشروعة عبر قنواتها، وهناك الإخطار الذي يكون من جانب السلطات المختصة، حيث تقوم هذه الأخيرة بإرسال إخطار إلى أصحاب المواقع أو شركات الاستضافة، بوجود محتوى غير مشروع، وإلزامهم بحذفه أو وقف بثه، نص المشرع الجزائري على هذا الإخطار بالفقرة ما قبل الأخيرة من نص المادة 394 مكرر8 من قانون العقوبات وذلك:" بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا"،[57] حيث حدد المشرع الجزائري الجهة التي تصدر هذا الإخطار وهي إما الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أو أن تكون جهة قضائية، كما نص على معاقبة كل شخص على أي نوع من الإخطارات الكاذبة، التي قد تشير بوجود احتمال اعتداء على النظام المعلوماتي أو المضمون الإلكتروني، وذلك في المادة 135 من القانون المتعلق بالبريد والاتصالات السلكية واللاسلكية.[58]

2-عدم وقف البث: يقصد به علم مقدمي خدمة الأنترنت بالمحتوى الغير المشروع بأية طريقة كانت، وعدم المبادرة بمنع بثه، أو إيقاف تداوله والعمل على محوه من الموقع الإلكتروني.[59]

نص المشرع الجزائري على هذا التصرف في المادة 120 من القانون 09-04 وأيضا في نص المادة 394 مكرر8 حيث يعاقب فيه في حال عدم وقف البث، فمقدمي خدمة الأنترنت مكلفين بحذف المحتوى غير المشروع ومنع الوصول إليه ووضع الأجهزة والتقنيات اللازمة لمحوه وإزالته من النظام المعلوماتي الذي يوجد فيه.[60]

نصت المادة 12 من التوجيه الأوروبي حول التجارة الإلكترونية على إلزام متعهد الدخول بحذف المحتوى الإلكتروني غير المشروع الذي يمر عبر قنواته، ومنع المستخدمين من الوصول إليه، أما فيما

---

(57)يراجع في ذلك:

المادة 394 مكرر 8 من قانون العقوبات، مرجع سابق.

(58)يراجع في ذلك:

المادة 13 من قانون 2000-03 المتضمن القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، الصادر في 06 أوت 2000، ج ر ج ج، عدد 48، المؤرخة في 06 أوت.

(59)يراجع في ذلك:

حدة بوخلفة، مرجع سابق، ص ص79 82.

(60)يراجع في ذلك:

حدة بوخلفة،" المسؤولية الجزائية لمتعهد الدخول عبر الأنترنت"، **مجلة الدراسات القانونية**، المجلد 06، العدد 01، 2020، ص 13

يتعلق بناقل المعلومات، فنصت المادة 13 منه بوقف بث المحتوى غير المشروع بمجرد علمه بعدم مشروعيته، وجاءت المادة 14 منه لتحمله المسؤولية إذا لم يتخذ الإجراءات اللازمة لوقف بث المحتوى.[61]

كما جاء في لائحة التجارة الإلكترونية للمملكة المتحدة، في المادة 19 منها، على عدم مسؤولية مقدمي خدمة الأنترنت، إذا قام بالأفعال واتخذ الإجراءات اللازمة لعدم بث المحتوى أو تعطيل دخول المستخدم للموقع أو إزالة المعلومات غير القانونية.

المبحث الثاني

النماذج التشريعية لجريمة التهديد الإلكتروني

الوجه الجديد لجريمة التهديد الذي أصبح إلكترونيًا يختلف عن جريمة التهديد التقليدية ومن بين هذه الاختلافات أن هذا النوع من التهديد لا يقتصر فقط على البشر بل يمتد ليلحق الأنظمة المعلوماتية والمعطيات، فالآليات التكنولوجية الحديثة لها دور في تحقيق تطور وتقدم الدول والتواصل بين الشعوب، حيث أصبح الفضاء الإلكتروني المساحة الجديدة التي تمارس فيه مختلف الأنشطة الإنسانية سواء من طرف الأفراد أو الدول.

إلا أن هذه التطورات أدت إلى ظهور تهديدات الأمنية أكثر خطورة من التهديدات الأمنية التقليدية، تتمثل في التهديدات الأمنية للمعلومات الإلكترونية إضافة إلى التهديد الواقع على الشبكة المعلوماتية (الأنترنت) واتصال جريمة التهديد بالمعطيات والأنظمة المعلوماتية جعلها تأخذ وصف الجريمة المعلوماتية وخصائصها، تعتبر هذه الأخيرة من أخطر الجرائم التي يتعامل معها العالم الحديث نظرا لمميزاتها وسهولة ارتكابها، وهي مساس بحرمة الحياة الخاصة للأفراد وجعل مختلف التشريعات منها العربية على رأسها الجزائر تتسارع إلى ردعها عبر سن القوانين وضع نصوص تشريعية تجرم و تعاقب على الأفعال التي من شأنها تهديد أمن وسلامة الفرد والدولة .

المطلب الأول

مظاهر جريمة التهديد الإلكتروني

لكي نبين وجه جريمة التهديد الإلكتروني وجب تبيان الصور التي يمكن أن تأخذها هذه الجريمة حيث يمكن أن تقع جريمة التهديد على المعطيات والأنظمة المعلوماتية في هذه الحالة نكون أمام التهديدات الأمنية للمعلومات الإلكترونية أما إذا وقع التهديد على الأشخاص بواسطة الشبكة العالمية فنكون أمام التهديد عبر الانترنت، ويدخل ضمن جريمة التهديد الإلكتروني مميزاتها التي تميزها عن جريمة التهديد

---

(61) يراجع في ذلك:

المواد 12 13 14 من الأمر التوجيهي الأوروبي في مجال التجارة الإلكترونية، مرجع سابق.

التقليدية وتدخل ضمن الجرائم المعلوماتية، سوف نتطرق في الفرع الأول صور جريمة التهديد الإلكتروني أما الفرع الثاني خصائص جريمة التهديد الإلكتروني.

الفرع الأول

صور جريمة التهديد الإلكتروني

ترتكب جريمة التهديد الإلكتروني باستعمال الوسائل الإلكترونية كالحاسوب وشبكة الانترنت، حيث تعتبر هاتين الوسيلتين من أحد الوسائل التي ترتكب بها هذه الجريمة إلا أنها ليست على سبيل الحصر لكنها الأكثر شيوعا في معظم الدول إذا من بين بعض التهديدات التي تتعلق بهذه الوسيلتين، أولا التهديدات الأمنية للمعلومات الإلكترونية في نظام المعلوماتية، وثانيا التهديد عبر الانترنت.[62]

أولا: التهديدات الأمنية للمعلومات الالكترونية في النظام المعلوماتي

إن تأمين المعلومات والمعطيات سواء للأشخاص الطبيعية أو المعنوية أمر مهم، فوجب تعزيز الأمن والتقليل قدر الإمكان من الاختراقات الأمنية.

يمكن تعريف أمن المعلومات على أنه "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية ".[63]

أما التهديدات الأمنية فمفهومها واسع ومن بين تعاريفه: هو الشخص والمنظمة والآلة أو الحدث الذي يمكن أن يلحق الضرر بالمعطيات المعلوماتية للمنظمة، أو أنه الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات سبب وجود تهديدات أمنية هو نقاط الضعف في الأنظمة المعلوماتية وقد تكون هذه التهديدات أفعالا مقصودة وقد تأتي من المصادر داخلية أو خارجية وبطريقة مباشرة أو غير مباشرة، كالتلاعب بالبيانات الموجودة على الحاسوب.

حيث تأخذ بالطريقة مباشرة بإدراج المعلومات من طرف العون المكلف بذلك كتغير تاريخ معلوم أو إدراج أسماء من أجل الحصول على مرتباتهم أو عن طريق تحويل مبالغ مالية إلى أشخاص وهمية عن طريق البنوك، أما الطريقة غير مباشرة فتأخذ صورة تغير أرقام وشيفرات الحسابات داخل الوسائط الإلكترونية.[64]

---

(62) يراجع في ذلك:

فريدة سعيد عثماني، بن عيسى نورة، المسؤولية الجزائية عن التهديد عبر الوسائل الالكترونية (دراسة مقارنة)، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، 2020-2022، ص19.

(63) يراجع في ذلك:

لمين علوطي، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، أطروحة لنيل شهادة الدكتوراه، تخصص إدارة أعمال، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، الجزائر، 2007-2008، ص239.

(64) يراجع في ذلك:

يمكن تصنيف التهديدات في أنواع مختلفة بطرق مختلفة إلا أن هدفها وغرضها مشترك وهو إلحاق الضرر بالمنظومة المعلوماتية ومن أساليب التهديدات الأمنية للمعلومات الإلكترونية هناك:

القرصنة: لديه عدة تسميات أخرى كالتجسس، الاختراق ويقصد به القدرة على الوصول لهدف معين والدخول على الأجهزة والمنظومات المعلوماتية بطريقة غير مشروعة عن طريق الثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصية الأخرين وإلحاق الضرر بهم، يطلق على المخترق مصطلح HAKERوحينما يتمكن المخترق من إحداث الأضرار كحذف ملفات مؤذية كوضع ملفات تجسسية (كأحصنة طروادة) أو فيروسات أو أي نوع من هذه الأنواع التي تعمل على تخريب Cracker.[65] يتم الاختراق عن طريق معرفة الثغرات الموجودة في النظام والتي غالبا ما تكون في المنافذ أو Ports الخاصة بالجهاز ويمكن وصف هذه المنافذ بأنها بوابات للكمبيوتر على الشبكة العالمية تسمح لها بالدخول، وعادة ما يكون غرض الفاعل قرصنة البرامج والبيانات الإلكترونية إما بإعادة إنتاجها أو نسخها للاستفادة منها أو للحصول على منفعة مادية منها.[66]

هجمات DDOS: هو نوع من الهجمات التي تسبب أضرار كبيرة ووخيمة للخوادم الخاصة بالبيانات، إذ تتسبب في زيادات غير متوقعة في حركة المرور فيها وإجراء سلوكيات غير طبيعية في النظام، أو رفض الخدمة الموزعة إلى الشبكات أخرى أو الإبطاء أو غلق النظام المعلوماتي.

نشاط المستخدم غير المصرح: هو شكل من أشكال التهديدات الداخلية حيث يحدث هذا النشاط عندما يقوم مستخدمي النظام المخولين الوصول إلى الملفات التي لا يحق لهم الوصول إليها، وضعف التحكم في الوصول غالبا ما يمكن من الوصول غير المصرح به إلى معلومات التي تكون سرية وحساسة والغاية من ذلك يكمن في سرقتها وتسريبها للعوام.[67]

الديدان Worms: تعد الديدان برامج ضارة ذاتية النسخ، ويمكن أن تنتشر بسرعة وبشكل مستقل داخل أجهزة الكمبيوتر وفيما بينها، وغالبا ما تستعمل للاتصال دفتر عناوين Outlook أو من خلال البحث عن

زوبير خلفي، الجرائم الماسة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الشيخ العربي التبسي، تبسة،2022-2023، ص24.

(65)يراجع في ذلك:

بشرى حسين الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، د ط، دار أسامة للنشر والتوزيع، الأردن، عمان،2014،ص13

(66)يراجع في ذلك:

عايدة رجا الخلايلة، المسؤولية التقصيرية الإلكترونية: المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والانترنت (3دراسة مقارنة)،ط2، دار الثقافة للنشر والتوزيع،عمان، 2011، ص101.

(67)يراجع في ذلك:

عبد الوهاب مليايي، أمن المعلومات في بيئة الاعمال الالكترونية، رسالة لنيل شهادة الدكتوراه، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011، ص101

منافذ مفتوحة على أجهزة أخرى دون الحاجة إلى مضيف أو تدخل بشري، ولذلك يمكن أن يكون تأثير الديدان أكثر خطورة من الفيروسات، مما يتسبب في تدمير الشبكات بأكملها أو باستخدام الكثير من موارد الشبكة، يمكن أيضا استخدام الديدان لنشر أحصنة طروادة على نظام الشبكة،[68]لضمان تأمين أنظمة المعلومات وجب على المسؤول أن يضع بعض الحواجز لضمان أمن تلك المعلومات وسريتها وذلك بقيامهم بالوظائف التالية:

أ-الخصوصية: يقصد بها أن تكون فعلية الوصول إلى المعلومات المتاحة في شكل إلكتروني يقتصر فقط على الأطراف المشاركة في الاتصال (أشخاص، التطبيقات، البرمجيات، الأجهزة)، حيث تعتمد الخصوصية على مبدأ التشفير الذي يمكن إجراءه على البيانات والمعلومات.[69]

ب-الجدران الناريةfirewall/Parfeu : حيث يكون على شكل برامج أو جهاز يستخدم للحماية ويعتبر من أكثر الطرق فاعلية، بحيث يمكن اتخاذها كخطوة أولية لحماية الحاسب الآلي، فلا بد من القيام بتركيب جدار حماية ناري بل دخول إلى الإنترنت والإبقاء عليه عاملا في كل الأوقات.[70]

ج-التشفيرEncryptions : أحد وسائل المعلومات المنظمة عن طريق تغيير مظهرها الإخفاء معناها الحقيقي وذلك باستعمال عدة طرق فتظهر كلمات غامضة لا معنى لها، وطريق فك الشفرة هي عكس الإجراء الذي تم استخدامه في التشفير.

د-عازل الفيروسات: هو برنامج عازل للفيروسات في الجهاز الذي يصل بين الشبكات الداخلية والعالم الخارجي مثل (الوسيط proxt)، لمنع وصول الفيروسات إلى الشبكة المحلية أو أجهزة المستفيدين.[71]

ثانيا: التهديد عبر الأنترنت

قبل الدخول في الجريمة أو صورة التهديد عبر الوسائل الإلكترونية فوجب تعريف مصطلح الأنترنت تعتبر هذه الأخيرة عبارة عن ترابط شبكات حيث تتكون من عدد كبير من شبكات الحاسوب

---

(68)يراجع في ذلك:

STOILKOVSKI Marjan, Guidelines on Cybercrime investigation, OSCE (Organization for Security and Co-operation in Europe), Tirana, Albania, 2022, P 64.

(69)يراجع في ذلك:

مريزق عدمان، عماد بوقلاشي،" الأمن المعلوماتي في ظل التجارة الالكترونية: إشارة الى حالتي تونس والجزائر"، **مجلة الاقتصاد الجديدة**، العدد 03، ماي 2011، ص12.

(70)يراجع في ذلك:

كاهنة لرول، "تحديد بعض مصطلحات الأمن المعلوماتي"، أعمال الملتقى الوطني حول الأمن المعلوماتي: مهدداته وسبل الحماية "، كلية الآداب واللغات، جامعة مولود معمري، تيزي وزو، 03-04 نوفمبر 2015، ص84.

(71)يراجع في ذلك:

مليايني عبد الوهاب، مرجع سابق، ص127

المترابطة والمتناثرة في كل أنحاء العالم، حيث يحكم هذا الترابط بروتوكول موحد يسمى تراسل الأنترنت TCP IP.[72]

بالنسبة لجريمة التهديد عبر الأنترنت فتعريفها هو نفسه تعريف جريمة التهديد التقليدية المنصوص عليها في نص المادة 284 ق ع ج، الإضافة الوحيدة هي الوسيلة المستعملة في ارتكابها حيث ترتكب بواسطة الحاسب الآلي وذلك عن طريق شبكة الأنترنت، تقوم هذه الجريمة بالمساس بالنظام المعلوماتي والاعتداء على حرمة الحياة الخاصة والمعطيات الشخصية.[73]

صفات مرتكب جريمة التهديد عبر الأنترنت:

-يجب أن يتوفر لدى الفاعل القدر الكافي من المعلومات والبيانات الشخصية الإلكترونية.

-أن تكون المعلومات الإلكترونية ذات صورة متكاملة غير متجزئة يتحقق بها معنى واضح.

-أن يكون لدى الفاعل القدرة الكافية لإيقاع ما يهدد به وتوافر الوسائل الكافية للقيام بذلك.

-أن تكون غاية الفاعل من فعله هو إلحاق الضرر بصاحب المعلومات والبيانات الإلكترونية سواء بصورة مباشرة أو غير مباشرة.

-أن يكون هدف الفاعل من فعله هو تحقيق غاية مادية أو معنوية له أو لغيره كالحصول على ترقية أو مبلغ من المال أو إجبار صاحب المعلومات السرية على القيام بفعل أو الامتناع عنه.[74]

*من جرائم التهديد عبر الأنترنت:

أ-جريمة انتحال شخصية: يقصد به قيام المجرم باستعمال شخصية أو هوية غير شخصيته الحقيقية وذلك للاستفادة من بعض تلك السمات مثلا أو ماله أو صلاحياته وهذه من الأسباب الوجيهة التي إلى الاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الأنترنت من هذا الشكل من التهديدات.

فأحيانا يكفي الحصول على الاسم والعنوان ورقم الهوية الشخص آخر،[75]انتشرت هذه الظاهرة بشكل واسع وكبير حيث نتلقى العديد من الإعلانات المشبوهة على الصفحات والبرامج الموجودة على

---

(72)يراجع في ذلك:

أسامة غربي،" جرائم الانترنت بين الجانب التقني وأساليب المكافحة"، **مجلة الحقوق والحريات**، العدد 2،2015، ص33 .

(73) يراجع في ذلك:

محمد سعيد عبد العاطي محمد، محمد احمد المنشاوي محمد، مرجع سابق، ص135.

(74)يراجع في ذلك:

سارة محمد حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الالكترونية (دراسة مقارنة)، رسالة لنيل شهادة الماجستير، تخصص قانون عام، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2020، ص44.

(75)يراجع في ذلك:

شبكة الأنترنت كإعلان عن الحصول على تطبيق مجاني حيث يطلب من المستخدم إدخال بياناته الشخصية كالاسم واللقب والعنوان أو رقم بطاقة الائتمان فيعتبر هذا الإعلان كفخ الغاية منه هو سرقة البيانات والمعلومات الشخص لانتحال شخصية الأفراد، والذي يؤدي إلى استنزاف رصيد الضحية في البنك أو سحب مبالغ مالية من بطاقته الائتمانية، فمعظم الرسائل المشبوهة التي ترسل إلى مستخدمي وسائل التواصل ومواقع التواصل الاجتماعي هي التي يكون محتواها دعوات وطلبات اشتراك لترويج عن ماركات غير معروفة .[76]

ب-إخفاء الشخصية على الأنترنت: في أغلب الأوقات يحتاج مجرم الأنترنت لإخفاء شخصيته خلال العملية التي يقوم بها، فعند إرسال خطاب تهديد بالبريد العادي لا يضع المجرم عنوانه على المظروف ولكن شبكة الأنترنت لها نظام آلي يضع عنوان المرسل في مقدمة كل أجزاء الرسالة عبر الشبكة، بالتالي يجب على المجرم أن يتجاوز هذا النظام بتغير عنوان المصدر لبروتوكول الأنترنتIP الذي يظهر في مقدمة أجزاء الرسائل ليستبدل به عنوان أخر مغلوط بحيث يصبح تتبع المصدر الأصلي للرسالة عملية صعبة ومستحيلة ويطلق على هذه العمليات إسم IP Spoofing وفي معظم الأوقات يختار المجرم عنوان لجهاز الحاسب يستطيع الوصول إليه واستخدامه حتى يستطيع معرفة ردة فعل الضحية ومدى استجابته للتهديد.[77]

ج-المطاردة الإلكترونية Cyberstalking: هي شكل جديد من جرائم الأنترنت في مجتمعنا، وهي عندما يتم ملاحقة شخص تتبعه إلكترونيا أي على الأنترنت، حيث أن المطارد الإلكتروني لا يقوم بتتبعه جسديا، إنما يقوم بتتبع نشاطات هذا الشخص(الضحية) الإلكترونية ليجمع عنه المعلومات لأجل مضايقته وتوجيه التهديدات له باستخدام الترهيب اللفظي، وهذا عبارة عن غزو لخصوصية الإنسان على الأنترنت (الخصوصية المعلوماتية).[78]

حسن طاهر داوود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000، ص84.

(76) يراجع في ذلك :

حسن طاهر داوود، المرجع السابق، ص85.

(77)يراجع في ذلك:

حسن طاهر داوود، مرجع سابق،ص86

(78) يراجع في ذلك:

HAIDAR Ali, The Basic Concept Cyber Crime, Journal of Technology Innovations and Energy, the wise publicher, April 2022, United States, p34.

الفرع الثاني

خصائص جريمة التهديد الإلكتروني

تأخذ جريمة التهديد الإلكتروني وصف الجريمة المعلوماتية وذلك نظرا لارتكابها في بيئة تقنية افتراضية فهي تقع باستعمال برامج أو أنظمة المعالجة الآلية للمعطيات وشبكة الانترنت أو كليهما ما يعني أن جريمة التهديد الإلكتروني تتمتع بنفس خصائص الجريمة المعلوماتية ومن بينها:

أولا: جريمة التهديد الإلكتروني عابرة للحدود من حيث الزمان والمكان

هذه الجريمة تتميز بصفة العالمية وارتباطها بالتقنيات الحديثة والتطور الحاصل في مجال الاتصال ألغى الحدود الجغرافية بين الدول، فبذلك تخطت الجريمة الإلكترونية حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى عدة بلدان على مستوى العالم،[79] و بذلك أن هذا النوع من الجرائم لا يعترف بالحدود الجغرافية للدول فشبكة الانترنت العالمية قد مكنت من ربط أعداد لا حصر لها من أجهزة الكمبيوتر عبر مختلف دول العالم، وهذا ما مكن الجاني من ارتكاب هذه الجريمة بحيث يكون هو في بلد و ضحيته في بلد آخر، واتصافها بالطابع الدولي راجع إلى الطابع العالمي لشبكة الانترنت التي جعلت معظم الدول في حالة اتصال دائم، ما سهل ارتكاب الجريمة من دولة إلى دولة، وهي تعتبر شكلا من أشكال الجرائم العابرة للحدود الإقليمية.[80]

خلقت هذه الخاصية العديد من الإشكالات القانونية في مسألة الاختصاص القضائي والتحديات التي تقترن به، فعليه بات من الضروري إيجاد الوسائل الضرورية والمناسبة لتشجيع التعاون الدولي لمواجهة هذا الشكل من الجرائم، والعمل على التوثيق بين التشريعات الخاصة التي تتناول هذه الجرائم.

ثانيا: جريمة سهلة الارتكاب

تحتاج الجرائم التقليدية لارتكابها وتنفيذها قوة ونوعا من المجهود العضلي، والذي يكون في صورة عنف وإيذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وغير ذلك. عكس الجرائم ذات الطابع الإلكتروني والمعلوماتي التي تتميز بالهدوء والنعومة، وهي لا تحتاج إلى العنف لارتكابها، بل يكفي أن يتوفر في مرتكبها لتنفيذها قوة علمية وقدراً من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل ذلك لا يحتاج من الوقت إلا ثوان أو دقائق محدودة منه، فكل ما يحتاجه المجرم

---

(79) يراجع في ذلك:

حمبلي عمار، عثماني دليلة، مرجع سابق، ص 25.

(80) يراجع في ذلك:

عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون الاعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022، ص13.

المعلوماتي هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير المشروعة كجريمة التهديد الإلكتروني كما أنه يحتاج إلى شبكة المعلومات الدولية (الأنترنت) بالإضافة إلى الإرادة في تحقيق الغرض الإجرامي وكل ذلك دون عنف، إذا يجدر القول إنها من الجرائم النظيفة التي تستخدم الأرقام والبيانات في ارتكابها وليس لها أثر خارجي مادي.[81]

ثالثا: قلة الإبلاغ عن جريمة التهديد الإلكتروني

تتسم الجرائم ذات الطابع الإلكتروني بالسرية و عدم الإعلان عنها أو إبلاغ ضحاياها للسلطات المختصة وذلك راجع إلى خوف المجني عليه من فضيحة أو حماية مضرة لمصلحته كما هو الحال في الجرائم التي تؤثر على خصوصية الأفراد و أمنهم كجريمة التهديد الإلكتروني كأن يكون المجني عليها امرأة تم التحرش بها وابتزازها عبر مواقع التواصل الاجتماعيFacebook،فتضطر الضحية لتلبية طلبات الجاني خوفا من تشويه سمعتها وأيضا في حالة المؤسسات المالية و الشركات التجارية فهي لا تتعاون مع جهات التحقيق وذلك حفاظا على سمعتها وثقة عملائها أكثر من الاهتمام بكشف الجريمة ومرتكبها.[82]

المطلب الثاني

النماذج التشريعية لجريمة التهديد الإلكتروني

أصبح استخدام الأنظمة المعلوماتية المقياس الذي يحدد مدى تطور الشعوب وتقدمها حيث أن تقنية النظم الاتصالات والمعلومات وفرت نوعا من السرعة في تنفيذ أهداف وخطط التنمية التي ترسمها الدول ولضمان هذه الأخيرة نهضتها وتماشيا مع عصر المعلومات وجب على هذه الدول وضع سياسة جنائية عقابية لتعاقب وتتصدى للظواهر الإجرامية التي تشكلت من هذا التطور التكنولوجي والمعلوماتي، منه فالعقوبة هي الأثر القانوني الناتج عن القيام بسلوك غير مشروع مجرم في القانون بنص تشريعي وذلك عملا بمبدأ الشرعية المنصوص عليه في قانون العقوبات الجزائري في نص المادة 01منه" لا جريمة ولا عقوبة أو تدابير أمن بغير قانون".[83]

---

(81)يراجع في ذلك:

أمينة بوشعرة، سهام مرساوي، الإطار القانوني للجريمة الالكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر، تخصص قانون خاصوعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017-2018، ص18.

(82)يراجع في ذلك:

ريمة بودراع، نعيمة بوحموش، جرائم وسائل التواصل الاجتماعي وآليات مكافحتها، مذكرة لنيل شهادة الماستر، تخصص المهن القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2022-2023، ص11.

(83)يراجع في ذلك:

سعيد عثماني فريدة، مرجع سابق، ص29.

حيث أن الصياغة التشريعية للنصوص التجريم والعقاب هي ليست مجرد إفراغ للنصوص في قوالب شكلية إنما هي أولا وقبل كل شيء فكر قانوني يرد النصوص لضوابطها القانونية التزاما بالأصول المنطقية ومن ثم يدخل فيها التثبت من اتفاق النصوص مع الفعل المجرم. لذلك تعد النصوص القانونية الجدار الذي يحمي الإنسان ويحيطه بالأمن والخصوصية فإن أي شخص يحاول كسر هذه الحواجز أو اختراق هذا الجدار فهو مدان ويستحق العقاب المقرر لفعله.[84]

وبناء على ما تناولناه سوف نحاول أن نبين العقوبات المقررة لجريمة التهديد الإلكتروني في التشريع الجزائري كفرع أول وفي التشريع المصري والأردني كفرع ثاني.

الفرع الأول

العقوبة المقررة لتهديد الإلكتروني في التشريع الجزائري

تطرق المشرع الجزائري إلى جريمة التهديد في نص المادة 284 من قانون العقوبات، إلا أن نص هذه المادة عالجت جريمة التهديد بمفهومها التقليدي، والمشرع لم يجري أي تعديلات ليتناسب هذا النص مع التطور التكنولوجي الحالي، وارتكاب هذا النوع من الجرائم في بيئة افتراضية مع عدم استحداث نصها القانوني يطرح السؤال من حيث العقوبة المقررة لها وفيما إذا كانت تشكل جريمة أخرى أو تتعدد مع جريمة أخرى.

تعتبر جريمة التهديد الإلكتروني انتهاكا لحرمة الحياة الخاصة للأفراد، حيث قام المشرع الجزائري بحماية هذه الحياة الخاصة للأفراد بصفة عامة، فهذه الحماية معترف بها في الدستور الجزائري في نص المادة 47 منه حيث تنص على ما يلي "لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته واتصالاته 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 طابع الشخصي حق أساسي يعاقب القانون على كل انتهاك لهذه الحقوق."[85]

منه فالمادة السالفة الذكر منعت انتهاك خصوصية الأفراد بأي وسيلة كانت وقامت أيضا بحماية الحياة الخاصة في قانون العقوبات في نص المادة 303 مكرر و303 مكرر1 وهذه النصوص تسري على

---

(84) يراجع في ذلك:

باقر غازي حنون، حسن حماد حميد، "جريمة الابتزاز الالكتروني (دراسة مقارنة)"، **مجلة دراسة البصرة**، العدد 42، كانون الأول 2021، ص71.

(85) يراجع في ذلك:

المادة 47 من الدستور، مرجع سابق.

الجرائم المرتكبة في العالم الافتراضي لأنها تعتبر تهديدا لحياة الأفراد الخاصة و استعمال الوسائل الإلكترونية لارتكابها يصلها مباشرة بتكنولوجيا الإعلام والاتصال، والتي نظمها المشرع الجزائري في قانون خاص وهو القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ونص في المادة الثانية منه :"يقصد في مفهوم هذا القانون بما يلي:

أ-الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: جرائم الماسة بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية."،[86] يفهم من نص هذه المادة أن كل الجرائم التي يمكن ارتكابها أو يسهل ارتكابها بواسطة منظومة إلكترونية أو نظام اتصالات إلكتروني تدخل في نطاق جرائم المعلومات، ما يعني أن جريمة التهديد بمفهومها الجديد تدخل ضمن هذه الجرائم.

أولا-العقوبة الأصلية لجريمة التهديد الإلكتروني:

يعاقب على جريمة التهديد كما تطرقنا إليها سابقا في نص المادة 284 من قانون العقوبات، على الحبس من سنتين(2) إلى عشر سنوات(10) وبغرامة من 20000 إلى 100000 دج، إذا تضمن التهديد أمرا بإيداع مبلغ من النقود أو تنفيذ أي شرط آخر.

في حالة إذا لم يتضمن التهديد أي أمر وشرط يعاقب الجاني بعقوبة الحبس من سنة إلى ثلاث سنوات(3) وبغرامة من 20000 إلى 100000 دج وهذا طبقا لنص المادة 285 من نفس القانون.[87]

حددت المواد 303 مكرر العقوبات الخاصة بانتهاك حرمة الحياة الخاصة وهي كالآتي:

في المادة 303 مكرر يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 50000 دج إلى300000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كان.

يعاقب على الشروع في هذه الجريمة أيضا بنفس العقوبة المقررة للجريمة التامة.

ويعاقب بنفس العقوبة في نص المادة 303 مكرر1 كل من احتفظ أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدام بأي وسيلة كانت التسجيلات أو الصور المتحصل عليها بواسطة الأفعال المنصوص عليها في المادة 303 مكرر.[88]

---

(86) يراجع في ذلك:

المادة 02 من القانون 09-04، مرجع سابق.

(87)يراجع في ذلك:)

المواد 284 و285 من قانون العقوبات الجزائري، مرجع سابق.

(88) يراجع في ذلك:

المواد 303 مكرر و303 مكرر 01 من قانون العقوبات، مرجع سابق.

وتقوم المسؤولية الجزائية للشخص المعنوي في هذه الجريمة طبقا للشروط المنصوص عليها في المادة 51 مكرر من قانون العقوبات الجزائري، وتكون عقوبته الغرامة حسب الكيفيات المنصوص عليها في المادة 18 مكرر والمادة 18مكرر2 عند الاقتضاء.

أما العقوبة المقررة لجريمة الاعتداء على أنظمة المعالجة الآلية للمعطيات نص عليها المشرع في نص المادة 394 مكرر من قانون العقوبات الجزائري حيث يعاقب عليها بالحبس من 6أشهر إلى سنتين(2 سنة) وبغرامة من 60000 دج إلى 200000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، و تضاعف العقوبة إذا ما ترتب عن فعل الدخول والبقاء غير المشروع في المنظومة المعلوماتية حذف أو تغير لمعطياتها، وإذا ترتب عن هذه الأفعال تخريب نظام اشتغال المنظومة تصبح العقوبة الحبس من سنة(1) إلى 3سنوات والغرامة من 100000دج إلى 300000 دج.

في نفس السياق أيضا في نص المادة 394 مكرر1 من نفس القانون "يعاقب بالحبس من سنة (1) إلى 3 سنوات وبغرامة من500000دج إلى2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".[89]

ويعاقب أيضا في نص المادة 394 مكرر2 في الأحوال الأتية:

"1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم."

بعقوبة الحبس من سنة إلى 5 سنوات وبغرامة من 1000000دج إلى 5000000دج.

وفي حالة استهداف هذه الجرائم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام تضاعف العقوبات المنصوص عليها سابقا (نص المادة 394 مكرر3).

وإذا ارتكبت الجرام المنصوص عليها في المواد 394 مكرر و394 مكرر2 من طرف شخص معنوي تحدد العقوبة بغرامة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وهذا في نص 394 مكرر 4.[90]

---

(89) يراجع في ذلك:

المواد 394 مكرر و394 مكرر01 من قانون العقوبات، مرجع سابق.

(90) يراجع في ذلك:

المواد 394 مكرر 02 ومكرر03 ومكرر04 من قانون العقوبات، مرجع سابق.

ثانيا: العقوبات التكميلية بالإضافة إلى العقوبات الأصلية المفروضة على مرتكبي جريمة التهديد وجريمة انتهاك حرمة الحياة الخاصة قرر المشرع عقوبات تكميلية تتمثل في الحرمان من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر1 لمدة لا تتجاوز 5 سنوات ويمكن أيضا نشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 من قانون العقوبات الجزائري، وهذا في حالة الشخص الطبيعي أما الشخص المعنوي فيتعرض لواحدة أو أكثر من العقوبات المنصوص عليها في المادة 18 مكرر، أما العقوبات التكميلية المقررة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات تتمثل في المصادرة والإغلاق حسب نص المادة 394 مكرر6 ق ع ج.[91]

أ-المصادرة: وهي تشمل كل الأجهزة والوسائل التي تم استخدامها في ارتكاب جريمة التهديد الإلكتروني وذلك مع مراعاة الغير حسن النية.

ب-الغلق: تشمل عقوبة الغلق من جهة غلق المواقع التي تكون محلا لارتكاب الجريمة ومن جهة أخرى غلق المواقع التي تكون محل أو المكان المستغل إذا ارتكبت الجريمة بعلم مالكها.[92]

الفرع الثاني

العقوبات الواردة في بعض التشريعات المقارنة

تتباين موقف التشريعات بشأن العقوبة المقررة لجريمة التهديد الإلكتروني حيث نصت العديد من النصوص القانونية والتشريعية على عقوباتها ونذكر منها:

أولا: العقوبات الأصلية

1-عند المشرع السعودي: حرصت المملكة السعودية والنظام السعودي إلى التصدي لأي جريمة أو جنحة تعرقل الأمن وتروع الأفراد ولو عن طريق الأنترنت والوسائل الإلكترونية فوضعت عقوبات قاسية لهذه الجرائم تنص المادة 3 من النظام مكافحة الجرائم المعلوماتية في السعودية "يعاقب بالسجن مدة لا تزيد عن خمسمائة ألف ريال أو بإحدى هاتين العقوبتين ..."، كل من يرتكب أي من الجرائم المعلوماتية الآتية:

-يتنصت على المعلومات المتبادلة بين الأفراد عبر الأنترنت.

-ابتز شخصا بنية سيئة.

-دخول إلى موقع إلكتروني بهدف تغير تصميمه أو تعكيره.

-المساس بحرية الأشخاص عبر مواقع التواصل الاجتماعي.

---

(91) يراجع في ذلك:

المادة 394 مكرر 06 من قانون العقوبات، المرجع السابق.

(92) يراجع في ذلك:

إيمان بوشعرة، سهام مرساوي، مرجع سابق، ص 94.

-التشهير بأشخاص أو تهديدهم بذلك.

ومن الملاحظ أن المشرع السعودي لم يضع حدا أدنى للعقوبة الأصلية سواء للغرامة المالية أو العقوبة السالبة للحرية، حيث جعل للقاضي السلطة التقديرية ما بين الحكم بالسجن أو الغرامة المالية أو الجمع بينهما.[93]

2-المشرع الأردني: يعاقب المشرع الأردني في نص المادة 18من القانون الجرائم الإلكترونية على جريمة التهديد الإلكتروني بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 3000 دينار ولا تزيد على 6000 دينار.[94]

3-**المشرع المصري:** يعاقب المشرع المصري على جريمة التهديد في قانون العقوبات الخاص به حسب كل حالة وذلك في نص المادة 327 على النحو الآتي: "كل من هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المؤبد أو المشدد أو بإفشاء أمور أو نسبة أمور مخدشة بالشرف وكان التهديد مصحوبا بطلب أو بتكليف بأمر يعاقب بالسجن.

ويعاقب بالحبس إذا لم يكن التهديد مصحوبا يطلب أو بتكليف بأمر.

وكل من هدد غيره شفهياً بواسطة شخص آخر يمثل ما ذكر يعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوبا بتكليف بأمر أم لا.

وكل تهديد سواء أكان بالكتابة أم شفهياً بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه".

يلاحظ من الفقرة الأولى من نص المادة السالفة الذكر أنّ المشرع المصري لم يحدد فترة السجن والحبس.[95]

ونص أيضا على جريمة التهديد الإلكتروني بشكل غير مباشر في القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات وذلك في الفصل الثالث تحت عنوان الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع في نص المادة 25 و 26 منه، و عاقب على ذلك بالترتيب على النحو الآتي: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل

---

(93) يراجع في ذلك:

الحسن بوشعير، شعيب حداد، مرجع سابق، ص 77.

(94) يراجع في ذلك:

الحسن بوشعير، شعيب حداد، مرجع سابق، ص 79.

(95) يراجع في ذلك:

المادة 327 من قانون العقوبات المصري، مرجع سابق.

الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".[96]

وعاقب أيضا في المادة التي تليه على النحو التالي:" يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه"[97].

4-المشرع الفرنسي: يعاقب المشرع الفرنسي على جريمة التهديد في نص المادة 222-17 بعقوبة السجن لمدة 6 أشهر وغرامة 7500 يورو وهذا إذا تحقق فعل التهديد.

وتعاقب المادة 222-18 إذا تم التهديد بأي وسيلة كانت وتضمن تنفيذ شرط بعقوبة السجن لمدة ثلاث سنوات(3) وغرامة تقدر ب 45000 يورو، وتشدد العقوبة لتصل السجن لمدة خمس سنوات(5) وغرامة 75000 يورو إذا كان تهديدا بالقتل. [98]

ويعاقب أيضا الشخص المعنوي على هذه الجريمة في نص المادة 222-18-2 من نفس القانون.

ثانيا: العقوبات التكميلية

1-عند المشرع السعودي: القواعد التي تحكم العقوبة التكميلية في النظام السعودي نجدها في القانون الإماراتي كونها عقوبة عينة وتخضع للسلطة التقديرية للقاضي.

نصت المادة 41 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي على: "مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصل منها أو بمحو

---

(96) يراجع في ذلك:

المادة 25 من القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات، مرجع سابق. المتواجد على الرابط التالي:
https://manshurat.org/node/31487

الذي تم الإطلاع عليه بتاريخ 2024/06/10 على الساعة 14:09

(97) يراجع في ذلك:

المادة 26 من القانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات، مرجع سابق.

(98) يراجع في ذلك:

المادة 222-17 من قانون العقوبات الفرنسي، مرجع سابق.

المعلومات أو البيانات أو إعدامها كما يحكم بإغلاق المحل أو الموقع الذي يرتكب في أي من هذه الجرائم وذلك إما إغلاقا كليا أو لمدة التي تقدرها المحكمة"[99].

2-عند المشرع الأردني: نص المشرع الأردني على العقوبات التكميلية المقررة لجريمة التهديد الإلكتروني في المادة31 من قانون الجرائم الإلكترونية الأردني حيث أنه في حال الإدانة تقضي المحكمة من تلقاء نفسها بمصادرة الأجهزة أو البرامج أو الأدوات أو الوسائل أو المواد المستخدمة في ارتكاب الجريمة، وأيضا وقف أو تعطيل أو حجب عمل أي نظام معلوماتي أو موقع إلكتروني مستخدم في ارتكاب هذه الجريمة، حذف المعلومات أو البيانات على نفقة الفاعل، إغلاق المحل الذي أستخدم لارتكاب الجريمة لمدة لا تقل عن3أشهر و لا تزيد عن سنة.[100]

ملخص

تختلف المسؤولية الجزائية للتهديد عبر الوسائل الإلكترونية من دولة إلى أخرى، وذلك حسب نصوص القوانين المطبقة في كل دولة، لكن بشكل عام اتفقت على أن تشمل عناصر المسؤولية الجزائية للتهديد الإلكتروني على ما يلي: الركن الشرعي الذي يتمثل في نص التجريم، الركن المادي سلوك الجاني المتمثل في إرسال رسالة تهديد عبر الوسائل الإلكترونية، الركن المعنوي يتمثل في نية الجاني بإلحاق الضرر بالضحية عن طريق فعل التهديد.

كي نقول أن جريمة التهديد وقعت عبر الوسائل الإلكترونية، يشترط توفر الشبكة المعلوماتية وتقنية المعلومات، وقد تنصرف المسؤولية الجزائية للتهديد عبر الوسائل الإلكترونية لتشمل أشخاص آخرين غير الجاني والمتمثلين في مقدمي خدمة الانترنت، يأخذ هذا النوع من التهديد صورة التهديدات الأمنية للمعلومات الإلكترونية في النظام المعلوماتي أو صورة التهديد عبر الانترنت الواقع على مختلف مواقع التواصل الاجتماعي، لتتنوع بذلك العقوبات المقررة للتهديد الإلكتروني لتشمل غالبا السجن، الغرامة المالية، بالإضافة إلى عقوبات تكميلية.

---

(99) يراجع في ذلك:

المادة 41 من القانون الاتحادي لمكافحة جرائم تقنية المعلومات الإماراتي، المنشور في منصة تشريعات الإمارات، المتواجد على الرابط التالي:
https://uaelegislation.gov.ae/ar/legislations/1526/download

المطلع عليه بتاريخ 2024/03/16 على الساعة 23:41.

(100) يراجع في ذلك:

المادة 31 من القانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، المتواجد على الرابط التالي:

https
://www.lob.gov.jo/?v=3&lang=ar#!/LegislationDetails?LegislationID=3398&LegislationType=2&isMod=false

الذي تم الإطلاع عليه بتاريخ 2024/05/15 على الساعة 21:18.

الفصل الثاني

إجراءات إقامة المسؤولية الجزائية عن التهديد الإلكتروني

تمر جريمة التهديد الإلكتروني كغيرها من الجرائم عبر إجراءات البحث والتحري وذلك من أجل الوصول إلى اكتشاف الجريمة وفاعلها، جريمة التهديد الإلكتروني من الجرائم الخطيرة التي تستدعي فتح تحقيق دقيق وجمع الأدلة اللازمة للإثبات تورط المتهم وتقديمه للعدالة، فيتطلب التحقيق في جريمة التهديد الإلكتروني مهارات خاصة واستخدام تقنيات متقدمة نظراً للطبيعة الرقمية التي تتميز بها، عند استلام بلاغ حول الجريمة التهديد الإلكتروني يتم اتخاذ جملة من الإجراءات الضرورية لبدء التحقيق يتضمن ذلك جمع المعلومات حول الحادثة، مثل تحليل رسائل التهديد، مواقع الويب، أو أي بيانات أخرى ذات صلة.

ويتم التعاون مع الشركات الخاصة المتخصصة في الأمن السيبراني للمساعدة في تحليل المعلومات وتحديد مصدر الهجوم، وأول الإجراءات التي تلجأ إليها السلطات المختصة في البحث والتحري عن الجريمة هي تلك الإجراءات العامة المعمول بها في كل الجرائم والمتمثلة في إجراء المعاينة، التفتيش، الخبرة الفنية، وكإجراءات خاصة خصصها المشرع الجزائري لجرائم على سبيل الحصر والتي تدخل فيها جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات والتي تطرق إليها في قانون الإجراءات الجزائية في نص المادة 65 مكرر 05 وأيضا في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي هي إجراء التسرب الإلكتروني، اعتراض المراسلات، وإجراء المراقبة الإلكتروني وحفظ سير المعطيات، ويستخلص من خلال القيام بهذه الإجراءات أدلة ذات طابع إلكتروني أطلق عليها الفقه مصطلح الأدلة الرقمية، والتي يتم الاعتماد عليها في الإثبات الجنائي في هذا الشكل المستحدث من الجرائم، إضافة إلى الشهادة التي تغير شكلها عن الشكل المتعود عليه

إلا أن جميع إجراءات جريمة التهديد الإلكتروني من أولها إلى آخرها ترافقها العديد من الإشكالات التي تعرقل سير هذه الإجراءات نظرا لطبيعتها الافتراضية والعابرة للحدود بداية من طريقة الحصول على الدليل إلى غاية المحاكمة، ثم يأتي دور تحديد الاختصاص القضائي في النظر في هذا النوع من الجرائم و دور الإنابة القضائية أيضا، و سعي مختلف الدول إلى سبل وطرق مكافحتها لجريمة التهديد الإلكتروني، وتم تلخيص هذه العناصر في هذا الفصل من خلال مبحثين، المبحث الأول تحت عنوان التحقيق والإثبات في جريمة التهديد الإلكتروني، أما المبحث الثاني المحاكمة في جريمة التهديد الإلكتروني ومكافحتها.

المبحث الأول

التحقيق والإثبات في جريمة التهديد الإلكتروني

التحقيق هو نشاط إجرائي تقوم وتباشره هيئة قضائية مختصة كل في حدود اختصاصه، والهدف من التحقيق هو جمع أدلة الجريمة بطرق موضوعية ومشروعة ثم تقدير هذه الأدلة من أجل إعداد ملف الجريمة إعدادا قانونيا والإشراف عليه قصد تقديمه للمحاكمة، تعد متابعة الجريمة

المعلوماتية بصفة عامة ومتابعة جرائم التهديد الإلكتروني بصفة خاصة، من أهم التحديات التي تواجه جهات التحقيق بالنظر إلى طبيعة الجريمة، وهذا من حيث تعلقها بمحل غير مادي، بالإضافة إلى صعوبة مراقبتها ومنع حدوثها وكذلك التحري عن مرتكبيها.

يعمل التحقيق على استخلاص الأدلة، ولا تكفي الطرق والوسائل التقليدية لاستخلاصها في الجرائم الإلكترونية لما يصاحبها من المشكلات العملية، فطبيعة الدليل المستخلص مختلف عن الأدلة التقليدية المتعود عليها وجاءت بشكل جديد وتسمية جديدة للدليل تعرف بالدليل الرقمي أو الإلكتروني، وعليه وجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم ذات الطابع الإلكتروني أو تبني وسائل جديدة للبحث والتحري تمكن من الحصول على الدليل الإلكتروني، و هذا ما قام به المشرع الجزائري على غرار باقي التشريعات المقارنة، تبنى وسائل جديدة للبحث و التحري إضافة إلى الوسائل التقليدية في الجرائم الإلكترونية، إلا أن استخلاص الأدلة في الجرائم المستحدثة يعترضه عدة عقبات من عدة جوانب سواء في البحث عنها أو في طبيعتها.

منه نريد التطرق في هذا المبحث إلى مختلف إجراءات التحقيق التي تبناها المشرع الجزائري في جريمة التهديد الإلكتروني في المطلب الأول، وفي المطلب الثاني إلى أدلة الإثبات الإلكتروني ومختلف الإشكالات الواردة على جريمة التهديد الإلكتروني.

المطلب الأول

إجراءات التحقيق في جريمة التهديد الإلكتروني

تتشابه إجراءات التحقيق في جريمة التهديد الإلكتروني مع الإجراءات التي يتم العمل بها في جريمة التهديد التقليدية حيث أن كلاهما يتطلب إجراء التفتيش، لمعاينة والخبرة الفنية وإضافة إلى هذه الإجراءات هناك إجراء مراقبة الاتصالات والتسرب وإجراء حفظ المعطيات المتعلقة بحركة السير وتعتبر هذه الإجراءات ذات طابع خاص وذلك راجع للبيئة الإلكترونية لهذه الجريمة.

الفرع الأول

إجراءات التحقيق العامة

من خلال هذا الفرع سوف نتطرق إلى الإجراءات العامة للتحقيق في جريمة التهديد الإلكتروني والتي هي المعاينة، التفتيش والخبرة الفنية.

أولا: المعاينة الإلكترونية

تعتبر المعاينة أول إجراء من إجراءات التحقيق فهي من أهم الوسائل لتكوين أول فكرة عن كيفية ارتكاب الجريمة فهي تساهم في تصوير كيفية وقوعها وتحديد ملابساتها وظروف ارتكابها، [101]حيث تتم

(101) يراجع في ذلك:

بالانتقال إلى محل الواقعة الإجرامية كقاعدة إجرائية، إلا أنه في إطار جريمة التهديد الإلكتروني يعد من الموضوعات الجديدة، فمسألة الانتقال لا تكون عبر عالم مادي وإنما عبر عالم افتراضي، فالمعاينة في الفضاء الإلكتروني تكون بالمشاهدة والرؤية بالعين لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والأثار المادية التي خلفها في ارتكاب الجريمة. [102]

هذا الإجراء من اختصاص ضابط الشرطة القضائية بإذن مكتوب من وكيل الجمهورية المختص، لتحقيق الهدف من المعاينة وجب عليه إتباع جملة من الخطوات والإرشادات المتمثلة في:

-تصوير الكمبيوتر وما يتصل به من أجهزة ومحتويات وملحقات والأوضاع العامة بصفة دقيقة مع التركيز على الأجزاء الخلفية للكمبيوتر مع تسجيل وقت وتاريخ التقاط الصور.

-عدم إجراء أي نقل للمعلومات من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجالات لقوى مغناطيسية يمكن أن تكون سبب في محو أو إتلاف البيانات المسجلة.

-مراعاة الطريقة التي تم بها إعداد النظام والأثار الإلكترونية بما في ذلك السجلات الإلكترونية التي تتزود بها شبكة المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع.

-ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام لإجراء المقارنة والتحليل لعرض الأمر على القضاء.

-التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها ورفع البصمات التي تكون لها صلة بالجريمة المرتكبة.

-وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة.

-القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية ذات صلة بالجريمة ورفع ما قد يوجد عليها من بصمات وأثار مادية.[103]

-ربط الأقراص المتحصل عليها والتي لا ربما تحمل أدلة مع جهاز يمنع الكتابة أو التسجيل عليها مما يتيح للمحققين قراءة بياناتها دون تغيرها.[104]

خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، د ط، دار الفكر الجامعي، الإسكندرية،2010، ص156

(102) يراجع في ذلك:

رشيد بن فريحة، يوسف مهوب،"التحري الجنائي في مصرح الجريمة الإلكترونية"، **مجلة جامعة القدس المفتوحة للأبحاث والدراسات**، مجلد01 ، العدد 42 ،الجزء الأول،تشرين الثاني 2017، ص 55 .

(103) يراجع في ذلك :

عيدة بلعابد، "خصوصية التحقيق في الجريمة المعلوماتية"، **مجلة الباحث الأكاديمي في العلوم القانونية والسياسية**، العدد 6، مارس 2021، ص ص 140 141.

-فصل الكهرباء عن موقع المعاينة لمنع الجاني من القيام بأي عملية محو أو إتلاف على أثار الجريمة.

-جعل المعاينة الإلكترونية سرية ومقتصرة على فئة الباحثين والمحققين ذو الكفاءة العلمية والخبرة الفنية.[105]

ثانيا: التفتيش الإلكتروني

يعد هذا الإجراء من أهم إجراءات التحقيق وهو من اختصاص قاضي التحقيق والنيابة العامة كأصل وذلك باختلاف التشريعات، إلا أنه يخول استثناءات إلى الضبطية القضائية في حالات محددة قانوناً. يختلف التفتيش في جريمة التهديد الإلكتروني عن التفتيش التقليدي في محله، حيث أنه في الجرائم المرتكبة عبر الوسائل الإلكترونية يقع على الحاسب الآلي الذي يقوم في تركيبه على مكونات مادية (Hard ware) كوحدات المعالجة المركزية processeur،وحدات الإدخال والإخراج ووحدات التخزين أو ما يسمى بوحدة التحكم (unité de control)، ومكونات أخر منطقية (Soft ware)كبرامج النظام الأساسية، البرامج التطبيقية والبيانات المعالجة آليا، كما له شبكات اتصالات بعدية سلكية ولاسلكية متواجدة على المستوى المحلي والدولي.[106]

منه التفتيش هو التنقيب والبحث في البرامج المستخدمة وملفات البيانات المخزنة للبحث عما يتعلق بالجريمة التي وقعت للوصول إلى كشف الحقيقة عن تلك الجريمة وعن مرتكبيها.[107]

يخضع تفتيش المكونات المادية لجهاز الحاسب وملحقاته لنفس إجراءات تفتيش الأشياء والأدوات المادية الأخرى من شروط وضمانات المنصوص عليها من المادة 44 إلى غاية المادة 47 من قانون إ ج ج، كمراعاة أوقات التفتيش، الإذن بالتفتيش، الأشخاص القائمين بالتفتيش والأشخاص المطلوب حضورهم عند التفتيش مع مراعاة الاختصاص المكاني وعدم فرض الأوراق المحرزة.[108]

---

(104) يراجع في ذلك:

عيدة بالعابد، مرجع سابق، ص141.

(105) يراجع في ذلك:

أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية،2015، ص ص 139 140.

(106)يراجع في ذلك:

دحمان عدلي، سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم الجنائية، جامعة زيان عاشور، الجلفة،2020-2021، ص ص 37 38.

(107)يراجع في ذلك:

محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، د ط، دار الجمهورية للصحافة، مصر،2010،ص 70.

(108) يراجع في ذلك:

المواد 47،46،45،44 من قانون الإجراءات الجزائية، مرجع سابق.

أما المكونات المعنوية للحاسب الآلي فقد قام المشرع الجزائري باستحداث نصوص قانونية جديدة أجاز من خلالها تفتيش هذه المكونات والمعطيات المعلوماتية للحاسب، من خلال نص المادة 05 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تنص على: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04أعلاه، الدخول بغرض التفتيش ولو عن بعد إلى:

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

ب-منظومة تخزين معلوماتية."[109]

أما الضبط فهو نتيجة المترتبة عن إجراء التفتيش ويكون على شكل نسخ للمعطيات الموجودة على المنظومة محل التفتيش على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية وهذا حسب نص المادة 06 من القانون 09-04.[110]

وجب على السلطة المختصة في إجراء التفتيش والضبط اتخاذ بعض الإجراءات الخاصة للحفاظ على سلامة المنقولات وصيانتها وذلك على النحو التالي:

-ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

-عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدان المعلومات المسجلة عليه.

-عدم تعريض الأقراص والأشرطة الممغنطة لدرجة الحرارة العالية ولا إلى رطوبة.

-منع الوصول إلى المعلومات التي تم ضبطها، وذلك عن طريق ترميزها أو تقيدها عن طريق وسيلة إلكترونية أخرى تمنع الوصول إلى هذه المعلومات ونص على هذا الإجراء القانون 09-04 في المادة 07.[111]

ثالثا: الخبرة الفنية الإلكتروني

تعتبر الخبرة وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل وتعزيز أدلة قائمة، كما أنها استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية،وهي المهمة الموكلة من قبل المحكمة أو الهيئة القضائية إلى شخص أو عدة أشخاص أصحاب

---

(109) يراجع في ذلك:

المادة 05 من القانون 09-04، مرجع سابق.

(110) يراجع في ذلك:

المادة 06من القانون 09-04، المرجع السابق.

(111) يراجع في ذلك:

عبد الوهاب مليياني، مرجع سابق، ص311.

اختصاص أو مهارة أو تجربة في المهنة، وتسند في جريمة التهديد الإلكتروني إلى شخص ذو خبرة في مجال الإلكترونيات ومن بينهم:

-المحلل (هو شخص يضع خطوات العمل ويقوم بتجميع بيانات نظام معين).

-المبرمجون ومدير النظام المعلوماتي.

-مهندس الصيانة والاتصالات.

-مشغل الحاسوب الآلي وشبكاته.[112]

ينقسم الخبراء وفقا للجهة التي قامت بندبهم من خبراء منتدبين يتم اختيارهم عادة من الجداول التي تعدها المجالس القضائية وخبراء استثنائيين كما هو الحال في جريمة التهديد الإلكتروني حيث يختارون بقرار مسبب وليسوا مقيدين في أي من هذه الجداول وهذا ما نصت عليه المادة 144 من قانون إ ج ج[113]، كما تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته مساعدة السلطات القضائية إنجاز الخبرات القضائية وهذا حسب الفقرة الثانية من نص المادة 14 من القانون 09-04.[114]

الفرع الثاني

إجراءات التحقيق الخاصة

يستدعي التحقيق في جريمة التهديد الإلكتروني إلى الاستعانة بأساليب التحري الخاصة لأن محل الاعتداء فيها يقع على أنظمة المعالجة الآلية للمعطيات المنصوص عليها على سبيل الحصر في المادة 65 مكرر5 من قانون إ ج ج، تتمثل هذه الأساليب في إجراء التسرب، إعراض المراسلات المنصوص عليها بموجب القانون 66-155 إ ج ج، واستحدث إجراء المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير في القانون 09-04.

أولا: التسرب الإلكتروني

تبنى المشرع الجزائري إجراء التسرب عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة حيث عرفه من خلال نص المادة 65 مكرر 12 من قانون إ ج ج بأنه "قيام ضابط عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص والمشتبه

---

(112) يراجع في ذلك:

يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة،2016-2017،ص 34.

(113) يراجع في ذلك:

المادة 144 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(114) يراجع في ذلك:

المادة 14 من القانون 09-04، مرجع سابق.

في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم...".[115]منه تنص المادة سالفة الذكر عن إجراء التسرب في الأحوال العادية، حيث يمكن تعريفه في نطاق جريمة التهديد الإلكتروني على أنه يتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الرقمي، وذلك باختراقه لمواقع معينة وثغرات إلكترونية أو اشتراكه في محادثات غرف الدردشة والظهور بمظهر كما لو كان فاعلا مثلهم، مستعملا أسماء أو صفات وهمية بغية الحصول على معلومات هامة تفيد التحقيق.[116]

ولصحة هذا الإجراء وجب على القائم به التقيد بجملة من الضوابط يجب مراعاتها قبل وأثناء مباشرته:

-إذن قضائي مكتوب وكل ما يجب أن يتضمنه من أحكام وبيانات.

-أن تتم عملية التسرب تحت الرقابة المباشرة للجهة المصدرة للإذن لضمان عدم حدوث تجاوزات وتعسف استعمال هذا الحق.

- تسبيب الإذن بإجراء التسرب.

نظرا لخطورة مهمة التسرب أحاط المشرع الجزائري القائم بالإجراء بنوع من الحماية وذلك من خلال جعله يستعمل هوية مستعارة أثناء أدائه للمهمة (المادة 65 مكرر 16 ق إج ج).[117]

ثانيا: اعتراض المراسلات

أصبح العالم بأسره يعتمد على وسائل الاتصال المرئية والمسموعة لسيما في تنفيذ الجرائم حيث لابد لهؤلاء المجرمين من التواصل فيما بينهم للاتفاق وتنسيق الخطوات الآيلة إلى ارتكاب الجريمة.[118]مكنت أجهزة التكنولوجيا الحديثة أجهزة التحقيق في جريمة التهديد الإلكتروني من مراقبة هذه الاتصالات عن بعد سواء كانت سلكية أو لاسلكية وهذا حسب نص المادة 65 مكرر5 من ق إ ج ج، ووضع المشرع الجزائري ترتيبات تقنية لمراقبة الاتصالات الإلكترونية في القانون 09-04 ضمن المواد 03 و04 منه.[119]

---

(115) يراجع في ذلك:

المادة 65 مكرر 12من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(116) يراجع في ذلك:

خلود فرحاتية، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج،2021-2022، ص 29.

(117)يراجع في ذلك:

المادة 65 مكرر 16، قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(118) يراجع في ذلك:

نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، د ط، المؤسسة الحديثة للكتاب، بيروت،2011، ص 155.

(119) يراجع في ذلك:

المواد 03 و04 من القانون 09-04 ، مرجع سابق.

يمكن تعريف عملية اعتراض المراسلات بأنها "اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المرسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض"، وهذا بمفهومها التقليدي وعند إدخال مصطلح الوسائل الإلكترونية تصبح: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"

أورد المشرع عدة قيود حال القيام بهذا الإجراء في نصوص المواد 65 مكرر5 إلى 65 مكرر10 المتمثلة في:

-ضرورة أن تتم هذه الإجراءات بناءا على إذن مكتوب من وكيل الجمهورية المختص إقليميا أومن قاضي التحقيق وتحت مراقبته المباشرة في حالة فتح تحقيق قضائي.

-توفر الإذن على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة ونوع الجريمة، مع تحديد مدة الإجراء التي لا يجب أن تتجاوز04 أشهر قابلة للتجديد حسب مقتضيات التحقيق.

-إمكانية الدخول إلى الأماكن العامة والخاصة بغير علم أصحابها وموافقتهم وفي كل وقت وهو ما أشار إليه المشرع.

-يمكن للقائم بالاعتراض المأذون به بأن يسخر كل عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو لاسلكية للتكفل بالجوانب التقنية للعملية.

-للقائم بعملية الاعتراض تحرير محضراً بعد الانتهاء من هذه العملية يضمن فيه محتوى العملية والترتيبات التقنية المتخذة، ويذكر فيه التاريخ وساعة بداية ونهاية العملية، ويقوم بنسخ المراسلات أو الصور المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف وتنسخ وتترجم المكالمات التي تتم باللغة الأجنبية عند الاقتضاء بمساعدة مترجم يسخر لهذه العملية.[120]

أ-الإلزام بمساعدة السلطات: وفقا للمادة 10من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإن مزود الخدمات يلتزم بما يلي:

- تقديم المساعدات لسلطات المكلفة بتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات.

- تمكين مزودو الخدمات من مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم من خلاله يتم معرفة المواقع التي قام بزيارتها والمعلومات التي خزنها والاتصالات التي أجراها.

---

(120) يراجع في ذلك:

إلهام بن خليفة، "مداخلة بعنوان القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"،الوطني حول (مواجهة الجريمة المعلوماتية)، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، الوادي، يوم 26 فيفري 2019،ص 5 6.

ثالثا: حفظ معطيات المتعلقة بحركة السير

هو قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في الأرشيف وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات التحقيق من الاستفادة منها واستعمالها في التحقيق.[121]

لقد أشار المشرع الجزائري إلى تعريف مقدمي الخدمات في الفقرة د من المادة 02 من القانون 09-04 على أنهم "كل كيان عام أو خاص يقدم لمستعملي القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصال وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصالات المذكورة أو مستعمليها".[122]

نص المشرع الجزائري على التزامات مقدمي الخدمات في القانون 09-04 والمرسوم التنفيذي 98-257 وهي كما يلي:

1-الإلتزامات الواردة في القانون 09-04: وهما التزامان الالتزام بمساعدة السلطات، والالتزام بحفظ المعطيات المتعلقة بحركة السير:

- يمكن جهات التحقيق من كل المعلومات التي تبحث عنها عن طريق تجميعها أو تسجيلها.
- يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.[123]

ب-الالتزام بحفظ المعطيات المتعلقة بحركة السير: تنص المادة 11 من القانون 09-04 على مراعاة طبيعة ونوعية المعطيات الخدمات يلتزم مقدمو الخدمات بحفظ:

- المعطيات التي تسمح بالتعرف على بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بتجهيز الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.[124]

---

(121) يراجع في ذلك:

عبد القادر فلاح ،" حجز وحفظ المعطيات في الجريمة الإلكترونية"، **مجلة صوت القانون**، المجلد08، العدد 01 ،2021،ص 183.

(122)يراجع في ذلك:

المادة 02 من القانون 09-04، مرجع سابق.

(123) يراجع في ذلك:

المادة 10 من القانون 09-04، مرجع سابق.

(124) يراجع في ذلك:

المادة 11 من القانون 09-04، مرجع سابق.

-أما ما يتعلق بنشطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من نفس المادة سالفة الذكر وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، منه فتحدد مدة هذا الإجراء بسنة واحدة ابتداء من تاريخ التسجيل.

2-الإلتزامات الواردة في المرسوم التنفيذي رقم 98 -257 المتضمن ضبط شروط وكيفيات إقامة خدمة الأنترنت واستغلالها تتمثل فيما يلي:

-طبقا لنص المادة الخامسة من المرسوم التنفيذي 98-257 يجب على كل من يرغب في إقامة طلبا للحصول على ترخيص بحيث يقدم عرضا بكل الخدمات التي يريد أن يقدمها.

-التزام متعهدين بالسماح للجهة التي تمنح لهم الترخيص بإجراء مراقبة للتأكد من مشروعية الخدمات، واحترام شروط استعمال هذه التراخيص وهذا ما نصت عليه المادة 17 من المرسوم سالف الذكر.

-التزام متعهدي الخدمات بحسن السيرة وكتم أسرار المستخدمين وعدم البوح بها وهذا ما أكدته المادة 14 من المرسوم التنفيذي 98 -257 المتضمن ضبط شروط و كيفيات إقامة خدمة الأنترنت و إستغلالها.

فنلاحظ أن المشرع الجزائري وفق إلى حد بعيد في فرض التزامات بالغة الأهمية بالنسبة لمقدمي الخدمات والهدف من ذلك أولا: في حماية حقوق الزبائن وضمان تقديم أحسن الخدمات في هذا الفضاء، ثانيا: تمكين السلطات القضائية المكلفة بالتحريات والتحقيقات للاستفادة من التكنولوجيات الإعلام والاتصال للكشف عن المجرم الإلكتروني، أما على المستوى الواقع فيجب مراقبة وتأكد من القيام بهذه الالتزامات في ظل التطوير السريع لتكنولوجيات الإعلام والاتصال.[125]

المطلب الثاني

طرق الإثبات في جريمة التهديد الإلكتروني

يعد الدليل الحجة والبرهان الذي يدفع به الخصم، و وسيلة الإثبات حق من الحقوق، فالدليل الجنائي أساس الإثبات، منه فنجد المشرع الجزائري قد اعتمد نظام الإثبات المختلط وفقا لنص المادة 212 من ق إ ج ج أنه "يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي..."[126]، إذا كانت جريمة التهديد الإلكتروني ذات طبيعة خاصة فإن هذا يؤثر مباشرة في أدلة إثباتها الجنائية، حيث يستخلص منها الدليل الرقمي الذي يمتاز عن غيره من الأدلة بصعوبة فهمه باعتباره يحتاج إلى خبرة ومهارة فنية لمعالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده و اختيار أفضل الطرق لضبطه.

---

(125) يراجع في ذلك:

عبد القادر فلاح، مرجع سابق، ص 186.

(126) يراجع في ذلك:

المادة 212 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

في بعض الأحيان الدليل التقني غير كافي لتكوين قناعة القاضي بل يحتاج لما يدعمه من أدلة إثبات أخرى ومن بينها الشهادة التي أخذت مفهوما جديدا عما هو متعود عليه، وهذا الشكل الجديد من الأدلة صاحبته العديد من الإشكالات إما بالنظر إلى طبيعته التقنية أو طريقة استخلاصه، منه سنتناول من خلال هذا المطلب إلى أدلة الإثبات في جريمة التهديد الإلكتروني كفرع أول وإلى الإشكالات التي تصاحب هذه الجريمة كفرع ثاني.

الفرع الأول

أدلة الإثبات في جريمة التهديد الإلكتروني

ترتكز عملية الإثبات الجنائي في جريمة التهديد الإلكتروني على الدليل الرقمي والشهادة الإلكترونية، باعتبارهما من بين أحد الوسائل القليلة لإثبات هذا النوع من الجرائم المستحدثة، لذا وجب التطرق إلى ماهية كل منهما وحجيتهما في الإثبات.

أولا: ماهية الدليل الإلكتروني ودوره في الإثبات

أصبحت وسائل الإثبات الجنائي التقليدية عاجزة عن مواجهة الجرائم الإلكترونية التي تنصب على المعلومات والبيانات المخزنة في نظام المعلومات مما أدى إلى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية حيث نتج عنها ما يسمى بالدليل الرقمي، يعتبر هذا الدليل الوسيلة الأساسية لإثبات هذا النوع من الجرائم فهو عبارة عن مكون رقمي لتقديم المعلومات في أشكال متنوعة مثل نصوص المكتوبة أو الصور أو الأصوات ...إلخ، وذلك من أجل الربط بين المجرم والجريمة والمجني عليه بشكل قانوني.[127]

1-ماهية الدليل الإلكتروني: يدخل في الماهية التعريف بالدليل الإلكتروني وخصائصه.

أ-تعريف الدليل الإلكتروني: الدليل الإلكتروني هو كل المعلومات المخزنة أو المنقولة في شكل رقمي، حيث يمكن تخزين هذه المعلومات في أقراص صلبة للكمبيوتر، أقراص مرنة، الأجهزة المحمولة، بطاقات الذاكرة، خوادم الشبكات، رسائل البريد الإلكتروني....إلخ.[128]

يعرف الدليل الإلكتروني على أنه مجالات أو نبضات مغناطيسية أو كهربائية الذي تجمع وتحلل عن طريق برامج خاصة وتطبيقات والتكنولوجيا، ويعد بمثابة جسم الجريمة المعلوماتية الذي يستعين به المحقق بتقنية المعالجة الآلية للبيانات.

ب-خصائصه: من بين ما يميز الدليل الرقمي عن غيره الأدلة نجد ما يلي:

---

(127) يراجع في ذلك:

أمينة لميز، "الدليل الرقمي كآلية لإثبات الجرائم المعلوماتية، **مجلة بحوث القانون والتنمية**، المجلد 02، العدد 03، جوان2023، ص 12.

(128) يراجع في ذلك:

GUZ Gultan, ELECTRONIC EVIDENCE, Master Thesis, Department of Private Law, Faculty of Law, University of Oslo, P06.

-يتكون من البيانات ومعلومات إلكترونية غير مرئية وغير ملموسة ولإدراكها يجب استخدام أجهزة ومعدات الحاسب الآلي (Hard Ware) واستعانة بنظم البرمجيات الحاسوب (Software).

- الدليل الإلكتروني ذو طبيعة تقنية ما يميزه عن الدليل التقليدي.

-يعد الدليل الرقمي دليل علمي، حيث يتطلب منه توافر مجال تقني للتعامل معه لذا كل ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، فالدليل العلمي يخضع لقاعدة ضرورة تعبيره عن الحقيقة.

-صعوبة التخلص من الدليل الإلكتروني.

-الدليل الإلكتروني هو مصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقميا.

-يمكن له تسجيل المعلومات عن الجاني ورصدها وتحليلها في الوقت نفسه.

-إمكانية توظيف نشاط الجاني لتوظيف أو لمحو أو إزالة الدليل من الحاسب الآلي كدليل الإدانة أمامه.[129]

2-مكانة الدليل الإلكتروني في الإثبات الجنائي

يندرج ضمن هذا العنوان شروط قبول الدليل الإلكتروني في الإثبات الجنائي وحجيته وقيمته القانونية.

أ-شروط قبول الدليل الإلكتروني: من بين شروط قبول الدليل الإلكتروني لدينا ما يلي:

- شرط مشروعية الدليل الإلكتروني وذلك حيث يتم الحصول عليه بطرق مشروعة.

- شرط مناقشة الدليل الإلكتروني هو من أهم القواعد الإجرائية على أن القاضي يجب أن يبني قناعته وأحكامه وفقا لما طرح أمامه من أدلة في الجلسة، فالدليل الذي لم يناقش أمام لقضاء لا يعتد به المادة 212 الفقرة 02 من ق إ ج ج " لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".[130]

-شرط بلوغ القضائي درجة اليقين حيث يصدر أحكامه بناءاً عن قناعته الشخصي.[131]

ب-حجية الدليل الإلكتروني في الإثبات الجنائي: فيقصد به قوته الاستدلالية في إبراز الحقيقة ونسب الفعل الإجرامي إلى شخص معين، تتوقف القيمة القانونية التي يتمتع بها الدليل على مشروعيته

---

(129) يراجع في ذلك:

عبير بعقيقي، فيصل نسيغة،"الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04 "، **مجلة العلوم القانونية والسياسية**، المجلد 09،العدد 02، جوان 2018، صص36 37.

(130) يراجع في ذلك:

المادة 212 فقرة 2 من قانون العقوبات الجزائري، مرجع سابق.

(131) يراجع في ذلك:

زهية معمش، نسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة، بجاية،2012-2013، ص 72 73.

ومصداقيته.[132]فمسألة تقيم الدليل الجنائي في إثبات الوقائع الجرمية مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها.[133]

يتبين موقف المشرع الجزائري في مسألة قبول الدليل الإلكتروني في مجال الإثبات الجنائي على أنه أخذ بنظام الإثبات الحر شأنه شأن النظم اللاتينية كفرنسا وبلجيكا والأردن وسوريا في هذا المجال، وهذا وفقا ما نصت عليه المادة 212 من ق إ ج ج.[134]

ثانيا: الشهادة الإلكترونية ودورها في الإثبات

هي من أهم الإجراءات والتدابير القضائية التي لا تختلف عن الشهادة التقليدية إلا من حيث الوسيلة المستخدمة لأدائها لقد تبني المشرع الجزائري فكرة الشهادة الإلكترونية في القسم الجزائي بموجب الأمر رقم 15-02 المتضمن قانون الإجراءات الجزائية وذلك من خلال وصفها على أساس أنها آلية إجرائية تستهدف إرساء نظام خاص بالشهود، منه فإن المشرع لم يبين لنا القواعد النظرية التي يمكن الاستناد إليها لضبط مفهومها.

1-**تعريف الشهادة الإلكترونية:** لم يضع المشرع الجزائري تعريف خاص بالشهادة الإلكترونية غير تلك القواعد المقررة لحماية الشهود التي تعتبر من أحدث المفاهيم التي ظهرت نتيجة الثورة التكنولوجية خاصة في مجال الإجراءات القضائية وذلك لاعتمادهم على تكنولوجيا الحاسوب والأنترنت في إدارة الخصومة القضائية.[135]

2-**تعريف الشاهد الإلكتروني:** غالبا ما يكونون الشهود من البيئة الافتراضية وهم أشخاص لهم دراية وخبرة في مجال التكنولوجيا المعلومات والاتصال ونذكر على سبيل المثال: المبرمجون، القائم على تشغيل الحاسوب، مهندسون الصيانة والاتصالات مزودو خدمات الأنترنت والاستضافة، وللاستشارة فقد ألزم المشرع الجزائري بموجب المادة 10 الفقرة الأولى من القانون 09-04 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية وإمدادهم بكل المعلومات المتعلقة بمحتوى الاتصالات.[136]

---

(132)يراجع في ذلك:

عبد القادر فلاح، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد04، العدد 02،جانفي2020، ص1701.

(133)يراجع في ذلك:

ابتسام بوباعية، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون الإعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022، ص 58.

(134)يراجع في ذلك:

المادة 212 قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(135)يراجع في ذلك:

نور الهدىقادري،" الشهادة الإلكترونية وحجيتها في الإثبات "، **مجلة الفكر القانوني والسياسي**، المجلد 07، العدد 01،2023، ص1594.

(136)يراجع في ذلك:

يمكن تعريف الشاهد في جريمة التهديد الإلكتروني أنه ذلك الشخص الفني ذو الخبرة والتخصص في تكنولوجيا الحاسوب والعلوم، ومن له المعلومات المهمة واللازمة للوصول إلى نظام المعالجة الآلية للمعطيات، إذا كان التحقيق يتطلب ذلك، وهذا يسمى بالشاهد المعلوماتي.[137]

3-مكانة الشهادة الإلكترونية في الإثبات: من هنا نبين خصائص الشهادة الإلكترونية ومن ثم سلطة قاضي الموضوع في تقديرها:

3-1-خصائصها:

-حجيتها غير قاطعة أي قابلة لإثبات نقيضها بشهادة أخرى.

-حجيتها غير ملزمة للقاضي، لأنه له السلطة التقديرية الكاملة في تقدير قيمتها لأنه له الحق بترجيح شهادة على شهادة أخرى وأن يأخذ بنتيجة دون أخرى ولو كانت محتملة.

- الشهادة الإلكترونية وتكون عبر الوسائط الإلكترونية هي الوسيلة الوحيدة التي تميزها عن الشهادة التقليدية لأنها تتم عبر الوسائل الإلكترونية الحديثة (أي أنها تتم عن بعد).[138]

3-2-حجية الشهادة الإلكترونية: تبعا للمعنى السالف بيانه إحدى الأدلة التي يمكن للقاضي الاستناد إليها في إثبات نمط معين من الجرائم تبعا لما هو مقرر بموجب نص المادة 65 مكرر19 من قانون الإجراءات الجزائية الجزائري غير أنه يخضع لبعض من الضوابط والقواعد التي تحقق للشهادة الإلكترونية قيمتها في الإثبات في حدود اقتناع القاضي الجزائي.[139]

سلطة القاضي الجزائي في الاستناد إلى الشهادة الإلكترونية يتباين نطاق السلطة المقررة للقاضي كدليل مستحدث للإثبات الجنائي بتباين أنظمة الإثبات السائدة لهذا يتبين أن المشرع الجزائري اعتمد على نظام الإثبات الحر كأصل عام منه ينقسم مضمون هذه الفقرة تبعا لتوجه التالي خضوع الشهادة الإلكترونية لحرية القاضي الجزائي في الإثبات وسلطة القاضي في قبول الشهادة الإلكترونية من عدمها.

فتيحة سويسي، "التكيف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها"، مداخلة مقدمة في الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية ،18 جانفي2022، ص 11.

(137)يراجع في ذلك:

AI SALEH Ibtisam," The Procedural Framework For The Electronic Blackmail Crime In The Jordanian Criminal Legislation", **Journal of Legal, Ethical and Regulatory Issues**, Volume 24, Special Issus 6, 2021, P4.

(138) يراجع في ذلك:

نور الهدى قادري، مرجع سابق، ص 1595.

(139)يراجع في ذلك:

المادة65 مكرر19من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

يقينية الشهادة الإلكترونية في المواد الجزائية هي من أهم القواعد التي تبنى عليها نظرية الإثبات في المادة الجزائية والتي تقضي بلوغ درجة من اقتناع القاضي التي تعني القطعية لا مجال لشك فيها ومن ضوابط بناء قناعة القاضي هناك ضوابط متصلة بمحل الاقتناع والضوابط المتعلقة بدرجة الاقتناع.[140]

الفرع الثاني

الإشكالات الواردة حول جريمة التهديد الإلكتروني

تتنوع الصعوبات التي تواجه السلطات القضائية في البحث والتحري والإثبات في جريمة التهديد الإلكتروني وهذا راجع لارتكابها في بيئة تقنية وافتراضية، فبالرغم من الجهود المبذولة لمكافحة هذا الشكل من الجرائم المستحدثة التي ترتكب باستعمال الوسائل الإلكترونية و وضع آليات تشريعية لمواجهتها، وإجراء تعديلات متواصلة في القواعد الإجرائية لتطوير أساليب مكافحتها، إلا أن هذا غير كافي فلا يزال هناك معوقات تعترض عملية استخلاص الأدلة و الحصول عليها واكتشاف مرتكبي الجريمة، ويمكن تجميلها في صعوبات تتعلق بالدليل الإلكتروني وصعوبات تتعلق بالتحقيق في الجريمة.

أولا: الصعوبات المتعلقة بالدليل الإلكتروني

الدليل الرقمي من الموضوعات الحديثة التي فرضت نفسها في الإثبات الجنائي لأنه مصاحب وملازم لاستخدام التطور التكنولوجي في المعلومات في ارتكاب الجرائم، ما نتج عنه العديد من الإشكالات القانونية في التعامل معه منها ما يتعلق بالمصطلحات التي تدخل في نطاقه وأيضا في طبيعته ونذكر منها:

1-المصطلحات المستعملة

نظرًا للطابع التقني والحديث لجريمة التهديد الإلكتروني فإنها تطرح إشكالاً عمليًا عند تطبيق النصوص القانونية، يتعلق بالمصطلحات التقنية إذ تتضمن بعض النصوص القانونية المجرمة مصطلحات غامضة المفهوم مما يعيق فهم هذه النصوص وتطبيقها الجيد، إذ أنه لم يقم المشرع الجزائري بتعريف المصطلحات الواردة في المواد القانونية المتعلقة بتجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات لأنها تعتبر مصطلحات حديثة وذات طابع تقني، ما يؤدي إلى عدم تحقيق الأمن القانوني والقضائي، كمثال نأخذ نص المادة 394 مكرر 2 إذ وردت فيها عبارات غامضة في تبيان السلوك المادي للجريمة والتي هي: بحث، تصميم، توفير، تجميع مما يثير صعوبة في تصور الجريمة وتحديد الفعل المجرم.[141]

---

(140) يراجع في ذلك:

عادل بوزيدة، " دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية الجزائري"، **مجلة النبراس للدراسات القانونية**، المجلد01، العدد 01، سبتمبر2016،ص 144.

(141) يراجع في ذلك:

المادة 394 مكرر2 من قانون العقوبات الجزائري، مرجع سابق.

استبدال مصطلح "المعطيات" Donnéesالواردة لدى تعريف الجرائم المدرجة ضمن أحكام المواد 394 إلى 394 مكرر 1 بمصطلح " معطيات معلوماتية" تماشيا مع أحكام القانون 09-04، ضمانا لصياغة قانونية صحيحة.[142]

توحيد المصطلحات المستعملة التي تفيد نفس المعنى كمصطلح "نظام" و " منظومة".[143]

2-الطبيعة غير المرئية للدليل الإلكتروني

من أكثر العوائق التي تواجه المحققين في الجرائم الإلكترونية هو عدم وجود دليل مرئي يمكن قراءته وفهمه، وذلك لأن البرامج والبيانات التي تقع عليها الجريمة تكون غير قابلة للإدراك الحسي، وهذا ما يميزه عن الجرائم التقليدية فهو يفتقد على الآثار المادية.

فهذا النوع من الجرائم يعتمد في موضوعه على التشفير والكلمات السرية والنبضات والتي يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها او يستدل من خلالها على الجناة،[144]فالبيانات غير المرئية لا تفصح عن شخصية معينة، وغالبا تكون مسجلة إلكترونيا بكثافة بالغة وبصورة مرمزة على دعائم أو وسائل للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها إلا إذا توفرت لديه الخبرة.[145]

3-الطبيعة الديناميكية للدليل الإلكتروني:

من مميزات جريمة التهديد الإلكتروني أنها عالمية، وذلك لأن آثارها تتجاوز الحدود الوطنية للدولة إلى غيرها من الدول، حيث أنه لا يتطلب من المجرم الانتقال على مسرح الجريمة وقطع المسافات، والمرور على الحواجز الأمنية وتسلق الأسوار لارتكاب الجريمة، لأنه يرتكبها وهو خلف مكتبه دون الحاجة إلى مغادرة مكانه، فمثلا مع التطور الهائل لوسائل الاتصال يمكن للمجرم أن يضع فيروس ويصيب به الملايين من الأجهزة والنظم لعدد كبير من البلدان.[146]

---

(142)يراجع في ذلك:

المواد394 إلى 394 مكرر1 من قانون 09-04 ،مرجع سابق.

(143)يراجع في ذلك:

فتيحة سويسي، مرجع سابق، ص ص 22 23.

(144) يراجع في ذلك:

بوشارب هانية، شول بن شهرة،" صعوبة عملية استخلاص الدليل الإلكتروني"، **مجلة الدراسات القانونية والسياسية**، المجلد 09، العدد 01، جانفي 2023، ص 68.

(145)يراجع في ذلك:

الطيبي البركه،"إشكالية الإثبات في الجرائم الإلكترونية"، **مجلة آفاق علمية**، المجلد 11، العدد 01، 2019، ص 269

(146) يراجع في ذلك:

عبد الوهاب مليياني، مرجع سابق، ص131.

4-سهولة محو الدليل الإلكتروني أو تعديله أو تدميره:

الصعوبات التي تعترض عمليات الإثبات في الجرائم الإلكترونية سهولة محو وتعديل أو تدمير أدلة الإدانة في فترة قياسية تقاس باللحظات والثواني، حيث أنه يمكن للجاني أن يمحو الأدلة القائمة ضده بمجرد إدخاله لبعض البيانات في نظام الحاسوب حتى يتم محو البيانات بالكامل في لمح البصر، كما يمكنه بمجرد كبسة زر أن يقوم بإلغاء الأوامر الصادرة للجهاز، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز، وما أن يحس الجاني بأن أمره سينكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يصعب على السلطات من كشف الجريمة.[147]الهدف من المحو السريع للأدلة عدم استطاعة السلطات من إقامة الدليل ضد الجاني، وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي أو في الأجهزة. ومن أمثلة عن هذا:

قيام أحد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب عن إدخال أمر النسخ أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة.

حدثت بدولة الإمارات العربية المتحدة أن قام مشغل حاسب آلي بتهديد المؤسسة التي يعمل بها لتنفيذ مجموعة من المطالب، وذلك بعد ما قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة، وإزاء رفض الشركة الاستجابة لمطالبه أقدم على الانتحار مما سبب صعوبة بالغة في استرجاع البيانات التي كان قد حذفها.[148]

قيام عصابة إيطالية محترفة باختراق أنظمة الحاسب الآلي، من خلال تصميمها جهاز يمحو تلقائيا جميع آثار الخطوات والتعاملات السابقة التي استخدمتها في اختراق نظم الحاسبات الآلية الخاصة بشركات معينة، وفي جميع أنحاء العالم.[149]

5-إعاقة الوصول إلى الدليل الإلكتروني:

تجدر الإشارة أنه من الصعب ملاحقة مرتكبي الجرائم الإلكترونية لأنهم يلجؤون إلى إخفاء هوياتهم الخاصة عند استخدام شبكة الإنترنت من خلال استعمال العديد من البرامج والتطبيقات التي تعمل على طمس هويته.[150]

---

(147)يراجع في ذلك:

هانية بوشارب، بن شهرة شول، مرجع سابق، ص ص 71 72.

(148) يراجع في ذلك:

خالد ممدوح إبراهيم، مرجع سابق، ص ص 65 66.

(149) يراجع في ذلك:

بوشارب، بن شهرة شول، مرجع سابق، ص72.هانية

(150) يراجع في ذلك:.

لعرقلة جمع أدلة الإدانة يعملون إحاطة الدليل الإلكتروني بوسائل الحماية الفنية وذلك بترميزه وتشفيره لتعطيل أي محاولة للوصول إليه أو استنساخه، فالمعلومات والبيانات المخزنة إلكترونيا محاطة بجدار من الحماية الفنية يمنع من الاطلاع عليها واستنساخها.[151]ومن بين الأدوات التي تستخدم لهذا الغرض برنامج (بسيفون pasiphon) وشبكة (تورTor) هدفها عرقلة تتبع عنوان بروتوكول الأنترنت (IP) لهذا المستخدم.

يزداد الأمر صعوبة حينما تكون المعلومات المحملة في عناوين(IP) غير حقيقية أو زائفة وهذا ممكن حين استخدام الحزم المعلوماتية(Packet) عنوان IP زائف، بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاءت من كمبيوتر آخر، كاستخدام الجاني الحواسب الموجودة بالأماكن العامة أو اللجوء إلى مقاهي الأنترنت، لأن جل هذه الأخيرة لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم، أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن ارتكابها وبين حدوث النتيجة الإجرامية، ما يفسح المجال لحدوث تغييرات أو عبث في الآثار المادية للجريمة أو زوال بعضها ما يلقي الغموض على الدليل، و هو ما استغله المجرمون لطمس هوياتهم. [152]

ثانيا: الصعوبات المتعلقة بالتحقيق

من مميزات الجرائم التقليدية أنه عند ارتكابها تخلف أثارا مادية فعلية، إلا أن هذا لا ينطبق على الجرائم المرتكبة بالوسائل الإلكترونية، فهي شكل مستحدث من الإجرام يرتكب في عالم افتراضي لا يترك المجرم فيها وراءه آثار مادية، وإنما تكون ذو طبيعة تقنية يتطلب لاكتشافها نوع من الخبرة الخاصة في المجال المعلوماتي وهذا هو الحال في جريمة التهديد الإلكتروني، حيث يشكل هذا النوع من الجرائم تحديا لجهات التحقيق في الكشف عنها والبحث فيها فمحل الاعتداء يكون شيء معنوي غير ملموس وليس مادي، إضافة لذلك غالبا ما تطول الفترة الزمنية بين وقوع الجريمة واكتشافها ما يصعب الأمر أكثر وهذا عائد لعدة أسباب منها يعود على الجهات المتضررة كقلة الإبلاغ عن الجريمة...إلخ، نقص الخبرة لدى جهات التحقيق، إشكالات تتعلق بالمساعدة القضائية والتعاون الدولي.

خلود فراحتية، مرجع سابق، ص 34.

(151)يراجع في ذلك:

كريم معروف، "المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية"، **المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي**، المجلد 04، العدد 02، 2022، ص161.

(152)يراجع في ذلك:

هانية بوشارب، شول بن شهرة، مرجع سابق، ص 73.

1-عوائق تتعلق بالجهات المتضررة

قد يكون هناك عدة أسباب تدفع بالجهات المتضررة إلى عدم التقدم إلى الجهات القضائية لتقديم إبلاغ أو شكوى حول تعرضهم لأي شكل من أشكال جريمة التهديد الإلكتروني ما يعيق عملية التحقيق وهذا عائد إلى:

-عدم إدراك خطورة الجريمة وإغفال جانب التوعية لإرشاد المستخدمين على خطورتها، لأن هناك نوع من التطبيقات تقدم لعملائها خدمات أسرع بدون عوائق على حساب الأمن.

-الامتناع عن الإبلاغ من طرف الأشخاص الميسورين أو صغار السن خوفا من المجتمع المحيط بهم وخشية من الفضيحة.[153]

-الامتناع عن التبليغ حفاظا عن السمعة الشخصية أو المصداقية التجارية كما هو الحال في الشركات مثلا وذلك لما يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني، وعدم اتخاذها الاحتياطات الأمنية لحماية معلوماتها.

-خوف بعض الأشخاص من الحرمان من خدمات معينة تتعلق بالنظام المعلوماتي وتعد التقنية المستخدمة في نظم المعلومات مجال استثمار ولذا تتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني.[154]

-عدم تجاوب الضحايا أحيانا مع مصالح الضبطية القضائية المختصة في حالة إنذارهم بوجود هجوم سيبراني محتمل على النظام المعلوماتي التابع للشركة أو المؤسسة لوجود ثغرة في النظام المعلوماتي sécurité de faille إلا أن صاحب الشركة التجارية لا يتخذ أي إجراءات لتعزيز أمن النظام المعلوماتي للشركة، مما يؤدي لوقوع الهجوم السيبراني بصفة فعلية.

2-عوائق تتعلق بجهات التحقيق

-صعوبة الوصول إلى الأدلة الإلكترونية لأنها غالبا تتطلب المساس ببيانات أخرى محاطة بالخصوصية الإلكترونية والاصطدام بالحق في الخصوصية المعلوماتية عند القيام بإجراءات التحقيق: كالتسرب الإلكتروني، التفتيش الإلكتروني، الرقابة الإلكترونية، يتطلب تقييد اللجوء إلى هذه الإجراءات بشروط صارمة حفاظا على حرمة الحياة الخاصة للأفراد.

---

(153) يراجع في ذلك:

خالد ممدوح إبراهيم، مرجع سابق، ص76.

(154) يراجع في ذلك:

خالد ممدوح إبراهيم، المرجع السابق، ص77.

-نقص المهارة الفنية والخبرة الكافية المطلوبة في التحقيق والتعامل مع هذا النوع من الجرائم مقارنة بالمجرمين الذين يتمتعون بشكل كبير من الاحترافية والذكاء، لاسيما وأن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، حتى أنهم اختصروا هذه المصطلحات بالحروف اللاتينية لتكون لهم لغة تعرف بلغة المختصرات Acronyms.[155]

3-عوائق تتعلق بالمساعدة الدولية:

اختلاف التشريعات والنظم القانونية الإجرائية للدول نتج عنه عدم وجود نموذج موحد للتعامل مع النشاط الإجرامي، ما يؤثر مباشرة على إجراءات جمع الأدلة الإلكترونية، مثلا الإجراء الذي يعتبر مشروعا في دولة ما قد تعتبره دولة أخرى خارج إطار الشرعية الإجرائية، ما يترتب عنه لاحقا عدم مشروعية الدليل الإلكتروني، بطيء إجراءات الإنابة القضائية الدولية بين جهات التحقيق فيما يتعلق بتقديم الطلب وانتظار الرد يعرقل سير التحقيقات في جريمة التهديد الإلكتروني، حيث أن الفترة التي تكون بين الطلب والرد يمكن من شأنها أن تؤدي إلى إتلاف أو ضياع الدليل الإلكتروني.

المبحث الثاني

المحاكمة في جريمة التهديد الإلكتروني ومكافحتها

تتسم جريمة التهديد الالكتروني بالطابع الدولي ولا تعرف معنى الحدود الجغرافية وذلك راجع لوقوعها في بيئة رقمية، ولأن شبكة الأنترنت جعلت معظم الدول في اتصال دائم، فهي جريمة يمكن أن تكون داخلية أو دولية أو ذات بعد دولي، داخلية عندما تقع كاملة في نطاق إقليم دولة معينة، ودولية عندما يكون أحد أطرافها شخصا دوليا، وتكون ذات بعد دولي عندما ترتكب داخل إقليم دولة معينة إلا أن آثارها تمتد خارج إقليم تلك الدولة، وهنا يكمن الإشكال في أي دولة تختص قضائيا بالنظر في الجريمة ومتابعتها.

غالبًا تستدعي إجراءات التحقيق والمتابعة في هذا الشكل من الجرائم تمديد الاختصاص للأشخاص المكلفين بذلك، إلا أنه في بعض الحالات لا يسمح القانون بذلك، حيث وضع هذا الأخير آلية قانونية تسعى وتضمن السير الحسن والجيد لإجراءات التحقيق والمتابعة الجزائية وتتمثل هذه الآلية القضائية في إجراء الإنابة القضائية.

سعت مختلف الدول لضمان سير كل هذه الإجراءات القانونية ومكافحة الجرائم الإلكترونية إلى إنشاء هيئات ومنظمات وطنية ودولية لهذا الغرض، وأيضا التوقيع على اتفاقيات ومعاهدات تسمح بها بتقديم العون والمساعدة لبعضها البعض، سنتناول جميع هذه النقاط من خلال هذا المبحث.

---

(155) يراجع في ذلك:

خالد ممدوح إبراهيم، مرجع سابق، ص69.

المطلب الأول

الاختصاص والإنابة القضائية في جريمة التهديد الالكتروني

الطبيعة الخاصة لجريمة التهديد الإلكتروني تتطلب تجاوز المعايير التقليدية، الأمر الذي جعل البعض يرى بأن تطبيق القواعد الكلاسيكية على الجرائم ذات الطابع الإلكتروني لا يتلاءم مع تحديد محل وقوع الجريمة في العالم الافتراضي، ولا يتلاءم مع المبادئ الأساسية التي تحكم مسألة الاختصاص والطبيعة العابرة للحدود ستنعكس عليها، لمعالجة هذه النقطة وجب التطرق إلى مختلف مبادئ التي تحكم الاختصاص القضائي وموقف الفقه والمشرع الجزائري من مسألة الاختصاص القضائي لجريمة التهديد الإلكتروني وأيضا الإنابة القضائية.

الفرع الأول:

الاختصاص القضائي في جريمة التهديد الإلكتروني

يقصد به مباشرة سلطة المتابعة والتحقيق والحكم في الجريمة وفقا للقواعد والحدود التي يرسمها القانون، وعلى رأس مبادئ الاختصاص القضائي مبدأ الإقليمية وتليه ثلاثة مبادئ أخرى تطبق على جريمة التهديد الإلكتروني وهي مبدأ العينية، مبدأ الشخصية، مبدأ العالمية أو الصلاحية الشاملة،[156] وهذا ما سنراه من خلال هذا الفرع إضافة إلى موقف الفقه والمشرع الجزائري وغيره من التشريعات المقارنة من مسألة تنازع الاختصاص القضائي في جريمة التهديد الإلكتروني.

أولا: مبادئ الاختصاص القضائي

1-مبدأ الإقليمية: يقصد بهذا المبدأ أن القانون الجزائي لدولة ما هو الذي يطبق على كل جريمة ترتكب على إقليمها، سواء كان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية، وسواء كان مواطنا أو أجنبيا، يسود هذا المبدأ معظم التشريعات المقارنة،[157]وطبقا له تعود سلطة التحقيق والحكم إلى محكمة المكان الذي وقعت فيه الجريمة أو جزء منها، وهناك ثلاثة آراء فقهية حول تحديد المحكمة المختصة، الرأي الأول يرى أنه يعود على المحكمة التي تقع فيها الجريمة، أما الرأي الثاني فيقول أنه يعود على مكان تحقق النتيجة الجرمية، لم يسلم هذين الرأيين من الانتقادات لعدم اتفاقهما مع مبدأ العدالة، فبرز اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط الإجرامي(الأعمال التنفيذية) وكذلك المكان الذي تحققت فيه النتيجة الجرمية، ما يعني أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر ركنها المادي.[158]

---

(157) يراجع في ذلك:

QUEMENER Myriam, Cybercriminalité, Droit Pénal Appliqué, édition économica, Paris ,2010, P 157.

(158) يراجع في ذلك:

2-تطبيق المبادئ الأخرى على مسألة الاختصاص في جريمة التهديد الإلكتروني: استعمال الوسائل الإلكترونية في ارتكاب الجرائم أتاح فرصا للخروج على مبدأ الإقليمية وتبني معايير جديدة لفض تنازع الاختصاصات كمعيار العينية، معيار الشخصية والعالمية.

أ-مبدأ العينية: يقصد بمبدأ العينية تطبيق القانون الجزائي على الجرائم التي تمس بالمصالح الأساسية للدولة، والمرتكبة خارج إقليمها أيا كانت جنسية مرتكبها، وهذا المبدأ أعطى للدولة الحق في الحماية والدفاع على مصالحها من أي اعتداءيقصد من هذا المبدأ انعقاد الاختصاص لقضائي للدولة التي تم الاعتداء على مصالحها.[159]

ب-مبدأ الشخصية:يقصد بمبدأ الشخصية كملاحقة القانون الوطني للأشخاص الذي يحملون جنسية الدولة، أينما وجدوا وليحكم أفعالهم الإجرامية المرتكبة في بالخارج ويطبق مبدأ الشخصية بطريقتين: إيجابية وسلبية، ويقصد بالطريقة الايجابية تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها، وهذا لتجنب فرار المجرم الذي يسيء السمعة دولته، أما الطريقة السلبية فيقصد بها تطبيق القانون الجنائي على كل جريمة يكون مجني عليه حاملا لجنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها وأيا كانت جنسية الجاني وهذا لضمان حماية رعايا الدولة من الاعتداءات الجرمية عليهم تجدر الإشارة أن المشرع الجزائري نص على الاختصاص الشخصي في ق إ ج ج.[160]

ج-مبدأ العالمية أو الصلاحية الشاملة: ينطوي هذا المبدأ على نوع من التعاون الدولي في مكافحة الإجرام، فهو يضمن عدم إفلات المجرمين الذين سولت لهم أنفسهم ارتكاب الجرائم في دولة ما، ثم الفرار إلى دولة أخرى تملصا من المسؤولية، وعليه فالأجنبي الذي يرتكب جريمة دولة ويلقى القبض عليه في دولة أخرى، يمكن محاكمته في الدولة التي ألقي القبض عليه، فيها بشرط أن لا تطلب الدولة التي أرتكب فيها الجرم تسليمه هلا بناء على ما تقدم، فإننا لا نجد مانعا من تطبيق مبدأ الإقليمية ومبدأ العينية ومبدأ الشخصية ومبدأ العالمية، على سائر الجرائم المعلوماتية الأخرى، لأن القواعد الإجرائية الجزائية يمكن

مريم عراب ، مرجع سابق، ص ص 277 278.

(159)يراجع في ذلك:

طيب وردي، الاختصاص القضائي في جرائم الأنترنت، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، 2014-2015، ص ص 38 39.

(160)يراجع في ذلك:

محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت (الأحكام الموضوعية والأحكام الجزائية)، د ط، منشورات حلبي الحقوقية، بيروت، 2011، ص 220.

تفسيرها تفسيرا موسعا إضافة إلى إمكانية اللجوء إلى القياس عند فقدان النص الإجرائي وذلك بخلاف القواعد الموضوعية[161].

ثانيا: موقف الفقه والمشرع الجزائري والتشريعات المقارنة من مسألة تنازع الاختصاص القضائي في جريمة التهديد الإلكتروني

مسألة الاختصاص لا تثير أي إشكال عندما تقع جريمة التهديد الإلكتروني داخل إقليم الدولة، وإنما ينشأ الإشكال عندما تمتد مجريات التحقيق والتحري في الجريمة إلى خارج إقليم تلك الدولة.

1-موقف الفقه من مسألة تنازع الاختصاص القضائي: تباينت المعايير الفقهية التي اعتمدت في شأن تحديد المحكمة المختصة بالنظر في الجرائم عبر الانترنت وبواسطة الوسائل الإلكترونية كجريمة التهديد الإلكتروني إلى ثلاثة معايير وهي:

أ-معيار الاختصاص المكاني: تعتمد أغلب التشريعات في تحديد المحكمة المختصة، إتباع ثلاثة ضوابط هي، مكان وقوع الجريمة أو محل إقامة المتهم أو مكان إلقاء القبض عليه، وفي حالة اجتماع أكثر من ضابط، تكون المحكمة التي ترفع إليها الدعوى أولا هي المختصة بالنظر في الدعوى. حيث يمثل السلوك الإجرامي والنتيجة الإجرامية شطري الجريمة في إطار الجرائم المرتكبة عبر الإنترنت، ومن ثم فإن سلطات ومحاكم مكان النشاط الإجرامي، ومكان النتيجة تكون مختصة، وعلى ذلك فإذا تم بث الفيروس المعلوماتي (السلوك الإجرامي) في مكان، وتحققت النتيجة (تدمير المعلومات) في مكان آخر وألقي القبض على الجاني في مكان ثالث، فإن الاختصاص ينعقد لمحاكم إحدى هذه الأماكن.

ينتقد بعض الفقه فكرة المساواة بين هذه المحاكم، حيث يجب أن ينظر إلى اختصاص محل ارتكاب الجريمة، كاختصاص رئيسي يقدم على غيره، ويتبعه اختصاص محل الإقامة، ثم اختصاص مكان إلقاء القبض على المتهم.[162]

ب-معيار القانون الأكثر ملائمة: نظرًا للطبيعة الخاصة للجرائم المعلوماتية والأضرار الناجمة عنها التي تمتد لتشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى الأمر الذي دفع إلى القول بأنه يجب التوسيع في تفسير قاعدة اختصاص محكمة وقوع الفعل (حصول الضرر)، ليجعل الاختصاص لمحكمة الدولة الأكثر تعرضا للضرر بشكل فعلي، مع التركيز على مبدأ التخلي أو التنازل عن الاختصاص بخلاف ذلك، وجعل الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى المعلومة من هذه الدولة، أصبح أمرا غير كافي من الناحية القانونية، لإعلان اختصاصها، أخذ هذا المعيار بعين الاعتبار

---

(161) يراجع في ذلك:

محمد لموسخ،" تنازع الاختصاص في الجرائم الإلكترونية"، مجلة دفاتر السياسة والقانون، العدد 02، جوان 2009، ص159.

(162) يراجع في ذلك:

صغير يوسف، مرجع سابق، ص144.

نقطة الاتصال المميزة والسلطة الفعلية، أي باختصاص قضاء الدولة التي قانونها هو الأكثر تعرضا للانتهاك بسبب الفعل الجرمي.[163]

ج-معيار الضرر المرتقب: صاحب ظهور شبكة الإنترنت وجود عالم إفتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، وهذا العالم الافتراضي لا يخضع لأي سلطة إقليمية، وبالتالي ترتب على هذه الحالة أن الضرر الذي تسببه الجريمة المرتكبة عبر الإنترنت يمكن أن يحدث في أي دولة تكون متصلة بالإنترنت، وهذا هو معيار الضرر المرتقب أو الافتراضي.

2-موقف المشرع الجزائري من مسألة تنازع الاختصاص القضائي: سارع المشرع الجزائري إلى بسط الاختصاص القضائي وتوسيعه من خلال قانون الإجراءات الجزائية وذلك بجواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجاء أيضا المرسوم التنفيذي رقم 06-348 متضمنا تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ليجسد فعليا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بأنظمة المعالجة الآلية.[164]

أ-الاختصاص المحلي لوكيل الجمهورية: وفقاً لنص المادة 37 من ق إ ج ج، فإنه يتحدد الاختصاص المحلي للنيابة بمكان وقوع الجريمة أو محل إقامة أو محل القبض على أحد الأشخاص المشتبه في مساهمتهم في الجريمة و لو حصل هذا القبض لسبب آخر، وبالتالي فإن اختصاص وكيل الجمهورية لا يتعدى مكان وقوع الجريمة أو مكان القبض على الأشخاص المشتبه في مساهمتهم في الجريمة أو محل إقامة أحد هؤلاء الأشخاص، لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر، فإن المشرع الجزائري أجاز بتمديد الاختصاص المحلي لوكيل الجمهورية بموجب المادة 37 فقرة 02من قانون الإجراءات الجزائية إلى دائرة الاختصاص المحاكم الأخرى مع ترك كيفية ترك تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص[165].

ب-الاختصاص المحلي لقاضي التحقيق: يتحدد الاختصاص طبقاً للمادة 40 ف01 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم على اقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض حصل لسبب أخر، غير أن المشرع

---

(163) يراجع في ذلك:

صغير يوسف، مرجع سابق، ص145.

(164) يراجع في ذلك:

المرسوم التنفيذي رقم 06-348 مؤرخ 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رج ج رقم 63، المؤرخة في 08 أكتوبر 2006.

(165) يراجع في ذلك:

المادة 37 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

الجزائري قام بإلغاء الفقرة02و03من المادة 40 [166]في التعديل الجديد وأصبحت تنص الفقرة 02 على جواز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.ونستخلص من هذا أن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى مع ترك كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر بعد ذلك.[167]

أما فيما يخص ضباط الشرطة القضائية، فطبقا للمادة16 فـ1 من ق إ ج ج، إنهم يمارسون اختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة، وفي حالات الاستعجال لهم مباشرة مهامهم في كافة اختصاص المجلس القضائي الملحقين به أو كافة الإقليم الوطني بناء على أمر من القاضي المختص وبعد إطلاع وكيل الجمهورية التابعين له.[168]

ج-الاختصاص المحلي لجهات الحكم: نصت المادة 329 من ق إ ج ج على أنه تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ولو كان القبض وقع لسبب آخر، وتختص استثناءا محكمة محل المحكوم عليه وفقا للأوضاع المنصوص عليها في المادتين 552 و553ق إ ج ج،[169] ويجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة محاكم أخرى عن طريق التنظيم في الجرائم الماسة بالمعالجة الآلية للمعطيات كجريمة التهديد الإلكتروني.[170]

ويمكن أيضا أن يمتد الاختصاص القضائي لجهات الحكم في حالة امتداد جريمة التهديد الإلكتروني إلى خارج الإقليم الجزائري، وذلك عملا بنص المادة 15 من القانون 09-04 التي تنص على:" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائية بالنظر في الجرائم المتصلة في تكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندا يكون

---

(166)يراجع في ذلك:

المادة40 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(167)يراجع في ذلك:

ليلة حرزون، أسماء هدروق، التنظيم القانوني للجريمة الإلكترونية طبقا لأحدث التعديلات في القانون، مذكرة لنيل شهادة الماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية،2021-2022، ص55.

(168)يراجع في ذلك:

عراب مريم، مرجع سابق، ص284.

(169)يراجع في ذلك:

المواد 552 و553 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(170)يراجع في ذلك:

المادة 329 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".[171]

3-موقف التشريعات المقارنة من مسألة الاختصاص القضائي لجريمة التهديد الإلكتروني: بالرغم من اللجوء معظم التشريعات إلى مبدأ إقليمية النص الجزائي والمبادئ الأخرى المشار إليها لحل مسألة الاختصاص القضائي المعلوماتي إلا أن طريقة تبنيها تختلف من دولة إلى أخرى.[172]

أ-موقف المشرع الفرنسي: تضمن قانون العقوبات الفرنسي لعام 1992 القواعد المتعلقة بتنازع الاختصاص من حيث المكان.

والمنصوص عليه في المواد 113 إلى 7/113وقد تضمنت هذه القواعد مبادئ الإقليمية والعينية والشخصية التي قام القضاء الفرنسي بتطبيقها على جرائم الأنترنت فجاء في مضمون التشريع الفرنسي أنه يطبق على جرائم المرتكبة داخل الإقليم الجمهورية الفرنسية وهذا حسب نص المادة 113 فقرة 5 من قانون العقوبات، وبالرجوع للمادة 2/113 من نفس القانون يكفي فقط تحقق أحد الأركان المكونة للجريمة لتطبيق النص الفرنسي، وهذا ما حكمت به محكمة باريس في حكمها بتاريخ 2002/02/26.[173]

والذي قضت فيه بأن القاضي الفرنسي مختص في الجرائم المعلوماتية وذلك ومتى تحقق أحد أركان الجريمة على الإقليم الفرنسي كما يطبق النص الفرنسي أيضا على الرسائل الغير مشروعة المرسلة عبر شبكة الأنترنت في فرنسا مهما ما كان الموقع المرسل في العالم، فبمجرد تلقي المرسل عليه الرسالة يشكل ذلك النتيجة الإجرامية والتي تعد أحد أركان الجريمة المعلوماتية، وهذا ما قضت به الغرفة الجزائية لمحكمة النقض في قرار لها بتاريخ 2007/02/07.

ب-موقف الاتفاقيات الدولية حول مسألة تنازع الاختصاص: لا تثار مشكلة تنازع الاختصاص على مستوى الداخلي للدول، وإنما المسألة تطرح عندما يعطي الاختصاص لأكثر من دولة بسبب اختلاف الجنسية وتعدد المكان الذي ارتكبت فيه الجريمة، والحل الأمثل لهذه المشكلة هو إبرام الاتفاقيات الدولية الثنائية أو متعددة الأطراف التي تتوحد من خلالها وجهات نظر الدول وتحدد ضوابط الاختصاص

---

(171) يراجع في ذلك:

المادة 15 من القانون 09-04، مرجع سابق.

(172) يراجع في ذلك:

زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى، عين مليلية، الجزائر، ص 174.

(173) يراجع في ذلك:

QuémènerMyriam, JoelFerry, opt-cit page223.

الإقليمي لكل دولة وتظهر معالم هذا التعاون في قبول تفويض الاختصاص في اتخاذ إجراءات التحقيق وجمع الأدلة والاعتراف بالأحكام الجنائية الأجنبية.[174]

ب-1-توصيات المجلس الأوربي والإصلاحات الجديدة في مجال الجرائم المعلوماتية: نظرًا للتطور السريع في مجال تكنولوجيا الكمبيوتر والانترنت، أصدر المجلس الأوربي التوصية رقم 90/13 في 11/09/1995 تناولت المشاكل الإجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، جاء فيها لأن يفترض التحقيق من الإجراءات إلى الأنظمة حاسب إلى أخر قد تكون موجودة خارج الدولة وتتطلب التدخل السريع، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء ولذلك كانت الحاجة ملحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات، كما يجب أن تكون هناك إجراءات سريعة ومناسبة، ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة ويتعين أن تسمح السلطة الأخيرة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها وهذا كله لا يأتي إلا بالاتفاقيات دولية.

ب-2-الاتفاقية الأوروبية بودابست حول الجريمة الافتراضية: تتسم نصوصها بالمرونة وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم، وتكفل استخدام الوسائل الفعالة في البحث والتحقيق وما يتعلق بالنصوص الخاصة بالتعاون الدولي، نصت المادة 22 [175]من هذه الاتفاقية إلى المبادئ التي يجب اعتمادها من قبل الأطراف 383 لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذه الاتفاقية وهذه المبادئ هي:

***مبدأ الإقليمية**: نصت الاتفاقية على هذا المبدأ في الفقرة 1 البند "أ" من المادة 22 وطلبت من كل دولة طرف في هذه الاتفاقية أن تعاقب على الجرائم المنصوص عليها إذا ارتكبت الجريمة ضمن نطاق الجغرافية للدول مثال: يعد هذا الاختصاص منعقد إذا كان نظام الحاسوب العائد للمتعدي ضمن الإطار الإقليمي ولو كان المعتدي مقيم خارج الدولة، أو إذا كان نظام الحاسوب العائد للضحية في إطار الإقليمي للدولة، كما يعد الاختصاص الإقليمي متوفر إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة.

***مبدأ النسبية للاختصاص المكاني(إقليم اعتباري):** نصت الاتفاقية على هذا المبدأ في الفقرة 1 البندين أ" و "ب" من المادة 22 وطلب من كل دولة طرفا في هذه الاتفاقية أن تكون مختصة جزائيا بالجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقا لقانون فيها. وعلى الرغم من ضرورة التعاون الدولي وتضافر الجهود من أجل تفعيله، إلا أن هناك العديد من العقبات التي تعترض سبيله من أبرزها: عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الالكترونية، عدم وجود توافق بين قوانين

---

(174)يراجع في ذلك:

Cour de cassation chamber criminelle, feverier 2007,voir Quémener Myriam Joel Ferry opt-cit,p223.

(175)يراجع في ذلك:

المادة 22من الاتفاقية الأوروبية بودابست، مرجع سابق.

الإجراءات الجزائية للدول بشأن تحقيق في تلك الجرائم والنقص الظاهر في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء[176].

* **مبدأ الجنسية**: نصت الاتفاقية على هذا المبدأ في الفقرة 1 البند د من المادة 22، وطلبت من كل دولة طرف في هذه الاتفاقية أن تكون مختصة جزائيا عندما يرتكب مواطنو أي من هذه الدول جريمة في الخارج، إذا كان هذا السلوك يشكل الجريمة وفقا للدولة التي ارتكبت على أرضها الجريمة.

* **مبدأ التعاون الدولي في مكافحة الإجرام أو الصلاحية الشاملة أو العامية**: نصت الاتفاقية على هذا المبدأ في الفقرة 3 من المادة 22 والتي تنص بأنه في حال رفض أي دولة طرف في هذه الاتفاقية تسليم مرتكب الجريمة المتواجد على أرضها وعلى أساس مبدأ الجنسية فيجب على هذه الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة وفقا لقانونها الوطني وإذا كانت جريمة الحاسوب تدخل في اختصاص أكثر من دولة من الدول الأطراف مثل جريمة الاحتيال وجرائم العدوان الفيروسي، فإن على هذه الدول التشاور فيما بينها لتحديد المكان الملائم للمحاكمة.

كما نصت الاتفاقية أنه يحق لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر، والتي ينوي الطرف الطالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو لدخول بأي طريقة مماثلة أو الحصول أو الكشف على البيانات.

ب-3- القانون العربي الإسترشادي النموذجي بشأن مكافحة الجرائم التقنية وأنظمة المعلومات 2004: تناول القانون العربي النموذجي بشأن مكافحة جرائم الكمبيوتر والأنترنت مسألة تنازع الاختصاص القضائي الدولي وذلك في المادة 22 من هذا القانون تحت عنوان إطار تطبيق القانون حيث نصت: تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية إذا ارتكبت كليا أو جزئيا داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بالنظر في الدعوى المترتبة على تلك الجرائم، وعلى الدول العربية عقد اتفاقيات لتبني المعيار الأول بإتباع في حالة تنازل الاختصاص بين الدول، كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات وقد تناول هذا النص مسألتي القانون الواجب التطبيق والمحاكم المختصة بشأن الجرائم المعلوماتية، يلاحظ من النص المادة السالفة الذكر أنه لكي أخد بمبدأ شخصية القانون الجنائي، النص الجنائي وعلى ذلك أيا كان نوع الجرائم المعلوماتية وسواء وقعت على الشبكة

(176) يراجع في ذلك:

محمد طارق عبد الرؤوف الخن، المرجع السابق، ص ص 200 201.

المعلوماتية داخلية أو عن طريق الانترانت وسواء كان ذلك داخل الدولة أو خارجها شرط أن يكون القانون الوطني صالحا للتطبيق عليها فإن المحاكم الوطنية هي المختصة دون غيرها بالنظر في هذه الجرائم[177].

ب-4- الاتفاقية العربية لمكافحة الجرائم التقنية المعلومات رقم 19 لسنة 2012: تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة الجرائم التقنية المعلوماتية والوقاية من أخطارها والتحقيق فيها وملاحقة مرتكبيها.

بالنسبة لمسألة الاختصاص نصت المادة 30 من الاتفاقية على أنه تلتزم كل دولة طرف في تبني الإجراءات الضرورية لمدّ اختصاصها في الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت: في إقليم الدولة الطرف، أو على متن سفينة تحمل علم الدولة الطرف، على متن طائرة مسجلة تحت قوانين الدولة الطرف، من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي فيه مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأي دولة، إذا كانت الجريمة تمس أحد المصالح العليا للدولة، تلتزم كل دولة طرف بتبني إجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 31/1 من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضر في إقليم تلكمه إلى الدولة الطرف ولا يقوم بتسلمه إلى طرف آخر بناءا على جنسية بعد طلب التسليم.

وإذا ادعت أكثر من دولة طرف في الاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو مصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف تقدم الدولة الأسبق في الطلب التسليم.[178]

الفرع الثاني

الإنابة القضائية

تعرف الإنابة القضائية بالتفويض أو أنها تكليف بالمهمة التي تصدرها سلطة مختصة بالتحقيق إلى سلطة أخرى لتنفيذ جزء من إجراءات التحقيق، هي إجراء من إجراءات التحقيق وتستند على مبدأ الملائمة الإجرائية التي تبررها الكفاءة في مباشرة الإجراءات، إذ نصت عليه المادة 68 فقرة 05 من قانون الإجراءات الجزائية "وإذا كان من المتعذر على قاضي التحقيق أن يقوم بنفسه بجميع إجراءات التحقيق

---

(177) يراجع في ذلك:

طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي والنظام القانوني لحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2015، ص 576.

(178) يراجع في ذلك:

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم 19 لسنة 2012 المنشور على الصفحة رقم(2580) الجريدة الرسمية رقم (5162) بتاريخ2012/06/17.

جاز له أن يندب ضابط الشرطة القضائية للقيام بتنفيذ أعمال التحقيق اللازمة ضمن الشروط المنصوص عليها في المواد 138 إلى 142.[179]

ومضمون هذه المواد جواز ندب أي قاضي من قضاة المحكمة أو ضابط شرطة قضائية في دائرة اختصاص المحكمة ينتدب ضابط الشرطة القضائية كما يجوز انتداب أي قاضي من قضاة المحكمة، بينما خارج دائرة اختصاص المحكمة ينتدب أي قاضي من قضاة التحقيق والذي يجوز له أن ينتدب أي أحد من ضباط الشرطة القضائية في دائرة اختصاصه وذلك في إطار التفويض بعد الإنابة حسب المادة 138 من قانون الإجراءات الجزائية، فإن الإنابة القضائية هي تفويض قاضي التحقيق لقاضي من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختصة للقيام بإجراء واحد أو بعض من إجراءات التحقيق الابتدائي ماعدا الاستجواب والمواجهة يلجأ عادة إلى الإنابة القضائية في بعض الحالات كوجود شاهد مقيم خارج اختصاص القاضي المنيب أو تطلب الأمر إجراء تحقيق أو معاينة في منزل أو معاينة في منزل كائن بدائرة اختصاص محكمة أخرى، أو إذا كان المتهم أو الضحية يقيمان في مكان بعيد عن المكان الذي يعمل فيه قاضي التحقيق ويحتاج قاضي التحقيق في إجراء تحقيق حول سلوكهما وتكون الإنابة عادة للحصول على تقرير لحالة المتهم الاجتماعية والأخلاقية، وذلك باختيار الإجراءات المناسبة التي تراها جهة التحقيق مفيدة لإظهار الحقيقة من الجهة المختصة باعتبارها جهة مستقلة.[180]

لصحة أمر الإنابة القضائية يجب أن يتوفر على جملة من البيانات الأساسية ونذكر منها: التوقيع الختم والتاريخ، صفة واسم مصدر الأمر واسم المصدر إليه.

من بين الشروط المتعلقة بالإنابة القضائية:

-أن تكون الإنابة خاصة وذلك بالرجوع إلى نص المادة 139 ق إ ج ج.[181]

-أن تتضمن الإنابة القضائية نوع الجريمة ومحل المتابعة المادة 138 ق إ ج ج.

أولا: أهمية الإنابة القضائية: تكمن أهمية الإنابة القضائية في أنها نوع من التعاون وتبادل الخبرات في المجال القضائي وهذا ما سيتضح في هذه النقاط:

-أن ضابط الشرطة القضائية عندما يقوم بتنفيذ الإنابة القضائية لا يتصرف بصفته عضوا من أعضاء الشرطة القضائية، بل أن منزلته ترتفع المرتبة القاضي لأنه حل محله، فاستظهاره لمحضر الإنابة يجسد

---

(179) يراجع في ذلك:

المادة 68 والمواد 138 إلى 142، قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(180) يراجع في ذلك:

كمال بوشليق، "النظام القانوني للإنابة القضائية في التشريع الجزائري"، **المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية**، المجلد 12، العدد 03، 2020، ص 465.

(181) يراجع في ذلك:

المادة 139 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

له سلطة شرعية وقانونية ذات أهمية وتدرج له في ملفه، أي بمعنى آخر الإنابة القضائية تجعل من ضابط الشرطة القضائية يكسب صفة قاضي التحقيق، لأنه قام بعمل قضائي يخص القاضي نفسه.

- أنه في حالة عجز قاضي التحقيق، أو أن القضية محل المتابعة تحتاج إلى سرعة في إنجازها وتعذر على القاضي مباشرتها، لبعد المسافة يلجأ إلى هذا الإجراء ويندب من ينوب عنه للقيام بهذا العمل ضباط الشرطة القضائية.

-هي مظهر من مظاهر التعاون التي يمارسها قاضي التحقيق ومساعديه، إذ أنه يعطي البعض من صلاحياته لهم.

ثانيا: سلطة إصدار أمر الإنابة القضائية

بما أنه إجراء من إجراءات التحقيق فإن المشرع الجزائري خول إلى جهات التحقيق سلطة إصدار أمر الإنابة القضائية إلى كل من قاضي التحقيق على مستوى المحكمة ولقضاة غرفة الاتهام باعتبارها جهة ثانية للتحقيق، وهذه الصفة لا يشترط توافرها أثناء إصدار أمر الندب وإنما يجب أن يستمر حتى تمام تنفيذ مقتضاه وإلا كان باطلا وعلى ذلك سنتطرق لسلطة إصدار الإنابة القضائية بالرجوع إلى نص المادة 138 ق إ ج[182]، نجدها قد اشترطت على أن يتمتع الشخص الذي يخول له القانون سلطة إصدار الإنابة القضائية بصفة قاضي التحقيق الذي يختص بالتحقيق الابتدائي كدرجة أولى يتبع التحقيق الذي تجربه جهات التحقيق وجمع الاستدلالات أو ما يعرف بالتحقيق الأولى أو التمهيدي الذي يسبق عادة التحقيق القضائي والذي تتولاه الشرطة القضائية[183].

1-قاضي التحقيق: ولأن التحقيق في الجرائم كأصل يكون من اختصاص قاضي التحقيق إلا أنه قد تستدعي ظروف التحقيق، أن يلجأ قاضي التحقيق إلى الإنابة القضائية نظرا لتعدد الأعمال التحقيق وتشعبها وهذا ما نصت عليه المادة 68 ف 6 ق إ ج مع مراعاة الشروط المنصوص عليه في نص المواد 138-142 ق إ ج[184].

2-غرفة الاتهام: تعد غرفة الاتهام من أهم غرف المجلس القضائي، ولقد حدد المشرع الجزائري الغرفة الاتهام تشكيلة جماعية وجعل تعيينها بقرار صادر من وزير العدل تنص المادة 176 من ق إج على أن تتشكل في كل مجلس قضائي غرفة اتهام واحدة على الأقل حسب ما تقتضيه ظروف العمل ويعين رئيسها ومستشارها لمدة ثلاث سنوات بقرار من وزير العدل طبقا للمادة السالف ذكرها، حسب المادة 178 ق إ

---

(182) يراجع في ذلك:

المادة 138 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(183) يراجع في ذلك:

جلال ثروت، النظم الإجراءات الجنائية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 373.

(184) يراجع في ذلك:

المادة 68 فقرة 6و المواد 138 و142 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

ج[185]فإن غرفة الاتهام تنعقد إما باستدعاء من رئيسها وإما بناء على طلب النيابة العامة كلما اقتضت الضرورة ذلك.

من خلال الأحكام العامة الواردة في الباب الثالث في قانون الإجراءات الجزائية يتبين لنا أن غرفة الاتهام دور مهم تلعبه في مجال القضاء الجنائي واختصاصات واسعة تمارسها منها ما يتعلق بدورها كجهة للتحقيق وجهة استئناف ودور آخر تلعبه بصفتها هيئة للرقابة والاتهام.

تعتبر غرفة الاتهام الجهة المختصة بالأعمال التكميلية وذلك ما جاء في نص المادة «يمكن لغرفة الاتهام أن تأمر بإجراء تحقيق تكميلي يقوم به إما أحد أعضائها أو قاضي تحقيق تابع لدائرة اختصاصها» وهذا طبقا للمواد 186-187-189-190-191-192 من ق إج ج[186].

حيث نصت المادة 190 من ق إج ج على: يقوم بإجراء التحقيقات التكميلية طبقا للأحكام المتعلقة بالتحقيق السابق إما أحد أعضاء غرفة الاتهام وإما قاضي التحقيق التي تندبه لهذا الغرض ويجوز للنائب العام في كل وقت أن يطلب الاطلاع على أوراق التحقيق على أن يردها خلال خمسة أيام، يفهم من خلال مضمون المادة أن الجهة المختصة بإجراء التحقيقات التكميلية تكون إما من طرف أحد أعضاء غرفة الاتهام أو من طرف قاضي التحقيق الذي تنيبه للقيام بهذه الإجراءات[187].

3-رئيس محكمة الجنايات: وذلك عندما يأمر بإجراء أعمال في إطار التحقيق التكميلي كأن يكون ملف التحقيق ناقصا أو عند ظهور عناصر جديدة فيه تتطلب مزيدا من التحريات، وتدقيق تمحيص بعض جوانب وملابسات القضية، وهذا حسب الفقرة الأولى من المادة 276 من ق إج. التي تنص على أنه" يجوز لرئيس محكمة الجنايات إذا رأى أن التحقيق غير واف أو استكشف عناصر جديدة بعد صدور قرار الإحالة أن يأمر باتخاذ أي إجراء من إجراءات التحقيق"، بمعنى أنه في حالة ما إذا كان التحقيق غير تام أو أنه يحتاج إلى مزيد من البحث فهنا يظهر دور رئيس محكمة الجنايات لإصدار أمر الإنابة لاستكمال مجريات التحقيق[188].

4-المحكمة جهة الحكم: ويكون ذلك عندما تريد سماع محبوس خارج دائرة المحكمة من طرف القاضي المختص محليا.

---

(185) يراجع في ذلك:

المواد 176 و178، من قانون إجراءات الجزائية الجزائري، مرجع سابق.

(186) يراجع في ذلك:

المواد 186 187 189 190 191و 192من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(187) يراجع في ذلك:

المادة 190 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(188) يراجع في ذلك :

المادة 276 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

5-المحكمة العليا:إذا وكل إليها النظر في جناية ارتكبها قاضي أو موظف أثناء ممارسة وظائفه، ومن خلال ما ذكرناه يتبين أن سلطة إصدار الإنابة القضائية مبدئيا يتمتع بها قاضي التحقيق، أي التحقيق الأولي يكون من طرفه، أما الجهات الأخرى التي تم ذكرها مثل رئيس محكمة الجنايات والمحكمة العليا هي مختصة بالتحقيقات التكميلية فقط[189].

ثالثا: سلطة تنفيذ أمر الإنابة القضائية:

يشترط قبل البدء في تنفيذ الإنابة القضائية أن يتأكد ضابط الشرطة القضائية الموجه إليه أمر الندب أن هذا الأخير يدخل في اختصاصه المحلي والنوعي، أي أنه يتأكد من أن القضية التي انتدب فيها تكون ذات صلة باختصاصه، وفي حالة بيان أن الإجراء محل الندب خارج اختصاص المندوب جاز له ردها إلى القاضي مع ذكر الأسباب، وفي هذه الحالة تنتقل كل الميزات والسلطات التي كان يتمتع بها القاضي إلى الشخص المندوب ضابط الشرطة القضائية. وهذا ما أكدت به المادة 139 من ق إ ج ج الفقرة الأولى،[190] بما أن المندوب في حالة الندب تنتقل إليه جميع السلطات التي كان يتمتع بها قاضي التحقيق قبل إعطاء أمر الندب، فإنه يلزم عليه عند قيامه بإجراءات التحقيق إتباع القواعد الإجرائية التي نص عليها القانون بالنسبة لهذه الإجراءات أي القواعد التي كان يلتزم به القاضي التحقيق في حالة عدم اللجوء إلى الندب، لذا يجوز له سماع الشهود واستدعائهم للإدلاء بشهادتهم وهذا ما نصت عليه المادة 140من ق إ ج ج استثناء: معروف أن سلطة المنوب تتحدد بحدود سلطة النادب لذا لا يملك أكثر مما يملك الأمر بها، غير أنه أحيانا قد تتجاوز سلطات المندوب أمر الإنابة القضائية دون الرجوع إلى قاضي التحقيق مثل: الحق في اللجوء مباشرة إلى طلب مساعدة القوة العمومية في تنفيذ مهمتهم، وهذا ما أدلت به المادة 17الفقرة الأخيرة من ق إ ج ج، أي بمعنى آخر تشير هذه المادة أنه في حالة الضرورة يمكن لضابط الشرطة القضائية أن ينفذ أمر دون إذن مسبق من قاضي التحقيق[191]وتنتقل ضمانات التحقيق مع إجراء الإنابة القضائية السرية و التدوين.

رابعا: أنواع الإنابة القضائية

يوجد نوعين من الإنابة القضائية وهي على النحو الآتي:

---

(189) يراجع في ذلك:

عمارة فوزي، قاضي التحقيق، رسالة لنيل شهادة دكتوراه في العلوم، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الإخوة منصوري، قسنطينة، 2009-2010، ص 220.

(190) يراجع في ذلك:

المادة 139 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

(191)يراجع في ذلك :

احسن بوسقيعة، التحقيق القضائي،ط2، الديوان الوطني للأشغال التربوية، الجزائر، 2002،ص 113.

1-الإنابة القضائية الداخلية: الإنابة القضائية الداخلية هي التي لا تملك صبغة الدولية، أي هي الإجراء الاستثنائي الذي يلجأ إليه القضاة في حالة الضرورة، بمعنى تخص القضاة أو المحاكم داخل الوطن الواحد، والتي تعرف بأنها وسيلة تحقيق وضعت تحت تصرف قاضي التحقيق بعد إخطاره بالقضية من أجل السماح له من انتداب قضاة أو ضباط شرطة قضائية للقيام بإجراءات لا يمكنه القيام بها بنفسه يتبين من خلال التعريف أنه يتم اللجوء إلى أمر الإنابة من طرف القاضي في حالة عدم إمكانه من القيام بالإجراء المطلوب منه من خلال التعريف استنتجنا تطابق مصطلح الإنابة القضائية باعتباره مصطلح قانوني مع استخلاف القاضي باعتباره مصطلح شرعي[192].

2-الإنابة القضائية الدولية: توجد عدة تعاريف لهذا المصطلح لذا سنذكر منها ما هو أدق وأشمل الإنابة القضائية الدولية هي طلب من السلطة القضائية المنيبة إلى السلطة المنابة قضائية كانت أم دبلوماسية، أساسه التبادل، باتخاذ إجراء من إجراءات التحقيق أو جمع الأدلة في الخارج وكذا أي إجراء قضائي آخر يلزم اتخاذه للفصل في المسألة المثارة، أو المحتمل إثارتها في المستقبل أمام القاضي المنيب ليس في مقدوره القيام به في نطاق دائرة اختصاصه يستنتج من خلال التعريف أن الإنابة القضائية الدولية هي نوع من التعاون القضائي المتبادل بين الدول، والتي يلجأ إليها القاضي في حالة عدم قدرته على مباشرة إجراءات التحقيق داخل دائرة اختصاصه.

خامسا: الإجراءات التي يجوزفيها إجراء الإنابة القضائية

الإجراءات التي يجوز فيها الندب:

1-سماع الشهود: بما أن القانون منح لقاضي التحقيق السلطة العليا في التحقيق، لذا فهو يسعى إلى إظهار الحقيقة بكافة الطرق القانونية، إذاً يجوز له أن يسمع كل شخص يرى فائدة من سماع شهادته ويتعين على الشاهد أن يحضر ويؤدي اليمين القانونية إن كان ذلك لازما فإذا امتنع الشاهد عن الحضور دون مبرر، جاز القاضي التحقيق أن يأمر بإحضاره جبرًا، أما إذا تعذر عليه الحضور لسبب فهنا على القاضي إما الانتقال إليه وإما يعطي أمر بالندب السماع هذا الشاهد، وهذا حسب المادة 89 من ق إ ج ج الفقرة الأولى منها يتعين على كل شخص استدعي بواسطة أحد أعوان القوة العمومية لسماع شهادته أن يحضر ويؤدي اليمين عند الاقتضاء ويدلي بشهادته 97 ق إ ج ج يفهم من المادة أن حضور الشاهد للإدلاء بشهادته ضروري لإتمام إجراءات التحقيق، وتخلفه يؤدي إلى عقابه لأن فيه تعطيل الحقوق الناس، ومنه يجوز القاضي التحقيق أن يندب غيره للقيام بهذا الإجراء[193].

---

(192) يراجع في ذلك:

أحمد الشافعي، البطلان في قانون الإجراءات الجزائية (دراسة مقارنة)، ط5، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006، ص135.

(193) يراجع في ذلك:

المواد 89 و97 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

2-إجراء توقيف للنظر: يمكن الضابط الشرطة القضائية في حالة الضرورة أن يوقف شخصا للنظر ويجب أن يقدمه خلال 48 ساعة أمام قاضي التحقيق في الدائرة التي يجرى فيها تنفيذ الإنابة القضائية وفي حالة امتناع الشخص للحضور تم إحضاره جبراً.

3-إجراء التفتيش: ونظرا لأهمية التفتيش سواءً كان تفتيش أشخاص أو مسكن. فإنه ينبغي لصحته أن يتم بحضور المتهم إن كان في حالة الحبس. أما إذا تعذر حضوره أو امتنع مع عدم تعين شخصا ينوب عنه، فهنا يلجأ المحقق أي ضابط الشرطة القضائية إلى تسخير شاهدين الإمكانية إقباله على المهمة، يسمح لضابط الشرطة القضائية القيام بعملية التفتيش وذلك بشرط أن ينص محضر الإنابة القضائية على هذا الإجراء، ويستطيع ضابط الشرطة القضائية تفتيش أي مسكن إذا كانت الإنابة القضائية ذات طابع عام إذا تضمنت العبارة التالية البحث في كل مكان عن كل الأشياء التي يمكن كشفها مفيدًا للحقيقة[194].

المطلب الثاني

مكافحة جريمة التهديد الإلكتروني

عرفت دول العالم تطور في مجال الإعلام والاتصال ما أدى إلى بروز وظهور أشكال عديدة من الجرائم وذلك ما دفع الدول لتصدي لها وذلك من خلال المعاهدات الاتفاقيات التي تنظمها وتصدي لها وردعها تشريعياً عن طريق سن النصوص القانونية واستحداث أجهزة خاصة للحد من انتشارها وذلك حماية الأفراد والمؤسسات من التهديدات الإلكترونية التي تستهدف سرقة المعلومات الشخصية، البيانات الحساسة، أو التسبب في تعطيل الأنظمة الإلكترونية، وتشمل استراتيجيات مكافحة هذه الجرائم تعزيز الوعي الأمني بين الأفراد والمؤسسات، وتطوير التشريعات والسياسات الضامنة للحماية الإلكترونية، وتعزيز التعاون بين القطاع العام والخاص في مجال الأمن الإلكتروني، واستخدام تقنيات التشفير وحلول الأمان الرقمي لتقوية الحماية الإلكترونية.

كما تشمل أيضًا تدريب الكوادر الأمنية على التعرف والتصدي للتهديدات الإلكترونية والتحقيق في حالات جرائم التهديد الإلكتروني منه نبين أهم الاتفاقيات الدولية والعربية التي تقوم بالتصدي لهذه الجريمة ودور الهيئات المتخصصة في مكافحاتها.

---

(194) يراجع في ذلك:

سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، د ط، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 1999، ص 553.

الفرع الأول

مكافحة جريمة التهديد الإلكتروني انطلاقا من الاتفاقيات الدولية والعربية

بما أن جريمة التهديد الإلكتروني من الجرائم الخطيرة والمستحدثة العابرة للحدود الدولية ما دفع بها إلى ظهور تعاون دولي لمكافحتها وذلك من خلال جملة من الاتفاقيات والمعاهدات منها اتفاقيات المجلس الأوروبي لسنة 2004،القانون العربي النموذجي الاسترشادي لمكافحة للجريمة المعلوماتية الدولية من بين أهمها اتفاقية بودابست في سنة 2001 والاتفاقية العربية في سنة 2010.

أولا: مكافحة جريمة التهديد الإلكتروني من خلال الاتفاقيات الدولية

1-اتفاقية بودابست 2001: تعد أول محاولة قانونية دولية لمعالجة مشكلة تزايد الجرائم السيبرانية،[195] حيث رسمت سياسة جزائية مشتركة لمكافحة الجرائم التي ترتكب في بيئة افتراضية.

هي أول معاهدة ملزمة متعددة الجنسيات وكان لها دورا مهما على المستوى الدولي في مكافحة الجرائم السيبرانية بدأ المجلس الأوروبي يعمل في جرائم الكمبيوتر منذ السبعينات وفي1989 قدم مجلس أوروبا مبادئ توجيهية للهيئات التشريعية الوطنية في توصيتها، تم التوقيع عليها من قبل 30 دولة وذلك بتاريخ 2001/11/23، برغم أن هذه المعاهدة أوروبية إلا أنه تم التوقيع عليها من طرف دول ليست أعضاء في المجلس أوروبا مثل اليابان وكندا والولايات المتحدة الأمريكية وجنوب إفريقيا، تضمنت هذه الاتفاقية 48 مادة التي تأكد ضرورة أخذ تدابير التشريعية لمكافحة جرائم الحاسوب ومخاطرها على الدول.[196]

***أهداف اتفاقية بودابست:**

-السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية ودول المنظمة لهذه الاتفاقية.

-التأكيد على أهمية التعاون الدولي والإقليمي في ميدان مكافحة الجرائم الإلكترونية، وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة الإجرام الإلكتروني.

-ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكاته، وأنشطة إساءة استخدامها بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة والإطار الإجرائي لها.

---

(195) يراجع في ذلك:

اتفاقية بودابست لسنة 2001، المنشورة على منصة مجلس أوروبا، المتواجدة على الرابط التالي:
https://rm.coe.int/budapest-convention-in-arabic/1680739173

الذي تم الإطلاع عليه بتاريخ 2024/05/20 على الساعة 19:30.

(196) يراجع في ذلك:

Chat Le Nguyen, Wilfred Glomma , Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: “Law on the book’s“ “ law in action” computer law & security review n40 (2021) , p02.

-تحقيق التوازن بين حماية حقوق الإنسان الأساسية المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان وحرياته لعام 1950 والعهد الدولي للحقوق المدنية والسياسية لعام 1966،[197]

الاتفاقيات الأخرى الدولية الخاصة بالحقوق المتصلة بالرأي وحرية الوصول إلى المعلومات وحرية البحث والتلقي والنقل للمعلومات والأفكار، مراعاة الحق في الخصوصية وحيازة المعلومات والاستفادة منها فهي اتفاقية تهدف إلى احترام حقوق الإنسان والحد من تعرضه لجرائم الأنترنت.[198]

2-اتفاقية المجلس الأوروبي: هي من أحدث الاتفاقيات لمكافحة الجريمة المعلوماتية على المستوى الدولي، والتي صدرت عن المجلس الأوروبي بعد أن وقعت عليها 32 دولة ودخلت حيز التنفيذ بتاريخ 2004/07/01 و من بين أهم الجرائم التي تناولتها هذه الاتفاقية الجرائم الماسة بالنظام المعلوماتي مبنية أساليب التحقيق فيها، والمتمثلة في كل من الجرائم المرتكبة ضد و سرية تكامل وتوافر البيانات أو نظم الحسابات كجرائم التدخل و الاختراق على أجهزة الحسابات الآلية، والجرائم المتصلة بالمحتوى والمتعلقة بالجرائم الخاصة بالإنتاج أو النشر غير المشروع عبر النظم المعلوماتية...إلخ[199].

***أهداف اتفاقية المجلس الأوروبي:**

-توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

-توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونيا.

-جمع معلومات عن حركة البيانات وعن إمكانية وجود تدخل في محتواها.

-تتضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.[200]

إضافة إلى هذه الاتفاقيات ظهرت عدة جهود دولية لمواجهة الجرائم المعلوماتية في التشريع الدولي:

2-أ-جهود الأمم المتحدة : تؤكد على ضرورة تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشار وتفاقم آثارها، وقد حظيت الجرائم المعلوماتية باهتمام مؤتمرات الأمم المتحدة حيث عقدت مؤتمرين، المؤتمر الثالث عشر سنة 2015بدولة قطر كان موضوعه الرئيسي هو "إدماج ومنع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية

---

(197) يراجع في ذلك:

محمد طارق عبد الرؤوف الخن، المرجع السابق، ص205.

(198) يراجع في ذلك:

سليمان قطاف، "الآليات القانونية والموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 06، العدد 01، 2022/03/31، ص ص337 338.

(199) يراجع في ذلك:

علي حسن الطوالبة،الجرائم الالكترونية: جرائم الحسابات الإلكترونية، ط01، دار الفكر الجامعي، الإسكندرية ،2005،ص 100.

(200) يراجع في ذلك:

فاروق خلف، "الآليات القانونية لمكافحة الجريمة المعلوماتية"، **مجلة الحقوق والحريات**، العدد 02، 2015، ص13.

والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي، ومشاركة الجمهور" والمؤتمر الثاني عشر سنة 2010تحت عنوان "استراتيجيات شاملة لتحديات عالمية "من بنوده ما يلي:

من بينها: جرائم الأنترنت،[201] حيث دعت لجنت منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها.

*من أهم القرارات الصادرة عنها:

1-القرار (121/45) العام 1990، نشر الدليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

2-القرار رقم (63/55) المؤرخ في 2000/12/04، والقرار رقم (121/56) المؤرخ في 2001/12/19 بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات".

3-القرار رقم (239/57) في 2003/01/31 والقرار رقم (199/58) المؤرخ في 2004/01/30 بشأن "إنشاء ثقافة عالمية للأمن السيبراني".[202]

2-ب-جهود الاتحاد الدولي للاتصالات : يضم 192 دولة و 700 شركة في القطاع الخاص و المؤسسات الأكاديمية منبرا استراتيجيا للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة ، ومن أهم أهدافه:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بجرائم الأنترنت.

2-ج-جهود المنظمة الدولية للشرطة الجنائية الإنتربولOIPC : تعتبر أكبر منظمة شرطية في العالم، والتي تضم 186 عضو، ومن بين اللغات الرسمية لهذه المنظمة الإنجليزية والفرنسية والإسبانية والعربية ولها 6 مكاتب إقليمية و في مجال الإجرام المعلوماتي يؤدي دور مهم الذي يتمثل في التعليم والتدريب موظفي هيئات تنفيذ القانون على الصعيد العالمي وفي سياق الجهود المبذولة بالخصوص على سرقة البيانات Phishing التي يحاول المجرمون من خلالها الحصول على المعلومات الحساسة ككلمات السر، وتفاصيل بطاقات الائتمان البنكية عبر البريد الإلكتروني أو برامج التخاطب المباشر عن طريق الادعاء بأنهم ممثلين شرعيين لشركات التجارية أو باستحداث رموز البرامج الخبيثة التي يستخدمونها لسرقة

---

(201) يراجع في ذلك:

أمال بيدي، "جهود الأمم المتحدة في مكافحة الجريمة السيبرانية"، **مجلة البحوث و الحقوق و العلوم السياسية**، المجلد08 ،العدد01 ،سنة2022،ص 305 .

(202)يراجع في ذلك:

أمال بيدي، مرجع سابق، ص ص 306 307 .

التفاصيل الهوية واستغلال الشبكات الإلكترونية للارتكاب جرائم النصب والاحتيال والتهديد الإلكتروني...إلخ.[203]

تهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في دول الأعضاء وعلى نحو فعال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم دول الأعضاء، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول منها جرائم الأنترنت.[204]

كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى G8 وذلك بوضع استراتيجيات لمواجهة هذا النوع من الجرائم من خلال إنشاء مركز الاتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة و7 أيام في الأسبوع على مستوى مصالح الشرطة في الدول الأعضاء، واستخدام وسائل حديثة في تلك المكافحة كاستخدام برنامج للتحليل والمقارنة وتزويد شرطة الدول بكتيبات إرشادية حول الجرائم المعلوماتية وكيفية التدريب على مكافحة والتحقيق في جرائم المعلوماتية بما فيه جرائم التهديد الإلكتروني.

ثانيا: مكافحة جريمة التهديد الإلكتروني في الاتفاقيات العربية

وذلك عبر:

1-الاتفاقية العربية لمكافحة الجريمة الإلكترونية لسنة 2010: جاءت هذه الاتفاقية التي وافق عليها مجلسي الوزراء الداخلية و العدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة بجامعة الدول العربية بتاريخ 2010/12/21 كمبادرة عربية لمكافحة الجرائم الإلكترونية وذلك في إطار مواكبة الجهود المبذولة على مستوى الدولي، بهدف تعزيز التعاون بين الدول العربية و تدعيمه في مجال مكافحة جريمة تقنية المعلومات، التي أدت إلى ظهور العديد من القوانين لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية والأردن وقطر والإمارات والعراق وسلطنة عمان ...إلخ.[205]

---

(203)يراجع في ذلك:

مختار شبيلي، الجهاز العالمي لمكافحة الجريمة المنظّمة،ط2، دار هومة، الجزائر، 2016، ص ص273 274.

(204)يراجع في ذلك:

مصطفى قرزان، عبد القادر زرقين، "الآليات الدولية لمكافحة الجريمة الإلكترونية"، **مجلة صوت القانون**، المجلد 08، العدد02، 2022/06/16، ص 1226.

(205) يراجع في ذلك :

مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق 08 . سبتمبر سنة 2014 يتضمن التصديق على الإتفاقية العربية لمكافحة جرام تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2012، منشور في ج ر ج ج، العدد 57 ، المؤرخة في:04 ذو الحجة عام 1435 الموافق 28 سبتمبر 2014 .

وقد جاءت مضامين هذه الاتفاقية مطابقة للاتفاقية بودابست خاصة على المستوى القواعد الإجرائية، التي استوجبت على الدول الأطراف ملائمتها مع قوانينها الوطنية فيما يخص الأبحاث الجنائية لتدابير التحفظ على بيانات الكمبيوتر.[206]

2-القانون العربي النموذجي الإسترشادي لمكافحة الجريمة المعلوماتية: يعد هذا القانون خطوة فعالة في مجال مكافحة الجريمة المعلوماتية خاصة في المجتمعات العربية التي عرفت كغيرها من الدول انتشار هذه الجريمة العابرة للحدود، وقد كان هذا القانون ثمرة عمل مشترك قدم بشكل مشروع لمكافحة الجريمة المعلوماتية من قبل كل من مجلس وزراء الداخلية العرب في نطاق الأمانة العامة لجامعة الدول العربية، وقد تم اعتماد هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته 19 بالقرار رقم 495 –د-19-2003/10/08،ومجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم 417 –د-21 /2004 ، كما حدد القانون النموذجي الإطار التجريمي و العقابي للأفعال التي من شأنها أن تشكل خطراً على المنظومة المعلوماتية أو سلامة نقل البيانات عبر شبكة الأنترنت.

الفرع الثاني

الهيئات والأجهزة المختصة في مكافحة جريمة التهديد الإلكتروني

تسعى كل دولة لضمان أمن وسلامة المجتمع لذا أنشأت هذه الهيئات لمكافحة الجرائم الإلكترونية و من بينها جريمة التهديد الإلكتروني، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدث، حيث تتولى مهمة البحث والتحري عنها وكشف غموضها، إذ سميت هذه الأخيرة بشرطة الإنترنت تتميز بالخبرة والمعرفة بتقنيات التحقيق في هذه الجرائم، وتختلف تماما عن الشرطة التقليدية لكونها لا تعتمد على التدريبات المادية التي يتلقاها رجال الشرطة في الجرائم العادية، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لهم لتولى مهمة البحث والتحري في العالم الافتراضي، على كلا الصعيدين الداخلي والدولي مجسدة بذلك مظاهر التعاون الشرطي الدولي من أجل التصدي الأمثل لهذه الجرائم، فتتمثل هذه الوحدات والأجهزة لدراسة وحدات البحث والتحري عن الجرائم الإلكترونية، في حين خصصنا وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى والدولي والعربي والوطني.

أولا: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الدولي:

تسعى كل دولة على مكافحة الجرائم الإلكترونية داخل إقليمها راصدة لذلك عتادها فعلى المستوى التقني قد قامت أغلب الدول بتوفير أساليب وطرق حديثة ومتطورة لحماية مجتمعاتها من

---

(206) يراجع في ذلك:

طاهر ياكر، "مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، **مجلة الصدى للدراسات القانونية والسياسية**، المجلد 04، العدد04، ص 16.

مختلف الانتهاكات التي تحدث نتيجة التطور التكنولوجي، أما على المستوى البشري فقد أسست أغلب دول العالم الأجنبية منها والعربية وحدات خاصة تعمل على مكافحة الجرائم الإلكترونية، وتتولى مسائل التحري والتحقيق بشأنها.

نتيجة تطور أغلب الدول الأجنبية في المجال التكنولوجي والذي أسفر عن ظهور وتنامي الجرائم والانتهاكات الإلكترونية كما سبق وأشرنا، فإنه قد سعت أغلب هذه الدول إلى تحديث تشريعاتها الداخلية بما فيها الإجرائية عن طريق استحداث بعض الأجهزة والوحدات المختصة بمتابعة هذا النوع من الجرائم والتحري بشأنها وذلك على مستوى كل من الدول الأنجلوساكسونية وكذا اللاتينية.[207]

1-على مستوى الدول الأنجلوساكسونية: من أبرز الدول التي بادرت بإنشاء شرطة متخصصة في مكافحة جرائم الإنترنت نجد المملكة المتحدة أو انجلترا، الولايات المتحدة الأمريكية، وكندا، سنتطرق لكل منها فيما يأتي:

أ-المملكة المتحدة (انجلترا):قامت كغيرها من الدول المهددة بالاعتداءات السيبرانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في مجال البحث والتحري عن الجرائم الإلكترونية، حيث تضم هذه الوحدة نحو 80 مفتشا من رجال شرطة وجمارك ذو درجة عالية من الخبرة والكفاءة في المجال التقني والمعلوماتي يتمركز هؤلاء الضباط في مدينة لندن وفي جميع المفتشيات الإقليمية التقليدية المتواجدة في إنجلترا، حوالي 40 منهم يمارسون مهامهم ضمن الوحدة الوطنية لمكافحة جرائم التقنية العالية، والباقي مقسمون على الوحدات المحلية الأخرى.

يتمثل دورها في متابعة مرتكبي الجرائم الإلكترونية بصفة عامة والجرائم الجنسية الواقعة على الأحداث والقصر بصفة خاصة إلى جانب هذه الوحدة تم إنشاء وحدة أخرى تختص بمكافحة الجريمة الإلكترونية على مستوى الشرطة المركزية "PCEU" والتي تختص بتحليل وتطوير المعلومات الإستخباراتية حول الجرائم الإلكترونية، وإنشاء شبكة تعاونية بين مؤسسات الدولة لتبادل المعلومات بشأن تطور هذه الجرائم، كما تقوم بالتحقيق في الحوادث الإلكترونية وتقديم الدعم والمشورة لسلطات إنفاذ القانون والأجهزة الشرطية في إنجلترا[208].

وقامت المملكة المتحدة بتأسيس وكالة وطنية لمكافحة الجريمة أطلق عليا اسم "NCA" تختص بمكافحة الجريمة المنظمة والاتجار بالبشر والأسلحة والجريمة الاقتصادية، وجرائم الاحتيال الدولي،

---

(207)يراجع في ذلك:

الشراقي حسام محمد نبيل، الجرائم المعلوماتية: جرائم الاعتداء على التوقيع الإلكتروني (دراسة مقارنة)، د ط، دار الكتب القانونية، مصر،2013، ص 747 .

(208) يراجع في ذلك:

نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، د ط، دار الفكر الجامعي، الإسكندرية، 2006، ص 111

وجرائم المخدرات، وكذا الجرائم الإلكترونية، حيث تم تأسيسها نتيجة تصاعد الجرائم خاصة المرتبطة باستخدام التكنولوجيات الحديثة والجرائم المنظمة وذلك سنة 2013 لتحل بذلك محل وكالة مكافحة الجريمة المنظمة والخطيرة"SOCA" ، وهي تضم ثمانية فروع تضم بذلك أكثر من 4000 ضابط، ونظرا لأهمية لما تقوم به هذه الوكالة من عرقلة أنشطة المجرمين وتقديمهم للعدالة فإنها تعتبر نقطة اتصال للمملكة المتحدة مع وكالة الإنتربول الدولية والأوروبول وكذا وكالات إنفاذ القانون الدولية الأخرى، ولعل من أبرز الأمثلة عن هذا التعاون هي عملية كاثريك "Catterick"والتي تتعلق بالتهديد الذي قامت به شركات القمار عبر الإنترنت في سنة 2004.[209]

ب-**الولايات المتحدة الأمريكية:** نتيجة تزايد جرائم الإنترنت سارعت هي الأخرى بإنشاء عدة أجهزة ووحدات شرطة متخصصة في مكافحة هذا النوع من الإجرام والحد من خسائره، تتمثل فيما يلي:

ب-1-مكتب التحقيقات الفيدراليFBI : يعتبر مكتب التحقيقات الفيدرالي وكالة حكومية تابعة لوزارة العدل الأمريكية تعمل كوكالة استخباراتية داخلية وقوة لتطبيق القانون في الدولة، حيث تأسست عام 1908 تحت اسم مكتب التحقيقات وتم تغييره إلى الاسم الحالي في عام 1935، مقره بواشنطن عاصمة أمريكا ويضم أكثر من 400 مكتب تحقيق مركزي منتشرة عبر عدة مدن داخل الو م أ. بالإضافة إلى 60 مكتب تحقيق دولي في القنصليات و السفارات الأمريكية حول العالم .[210]

يعمل هذا الجهاز على حماية الو م أ والدفاع عنها وتحقيق العدالة الجنائية، ذلك من خلال مكافحة الهجمات الإرهابية والإلكترونية والمنظمات الإجرامية المختلفة. ونظرا للطابع التقني للجرائم الإلكترونية عني هذا المكتب بتوفير التدريب اللازم لمكافحة هذه الجرائم من خلال تنظيم دورات متخصصة مدة كل منها أربعة (04) أسابيع تعقدها أكاديمية هذا المكتب في كوانتيكو وفيرجينيا، تقوم من خلالها بتزويد محققي الشرطة والعاملين في سلطات إنفاذ القانون بصفة عامة بمهارات ومعارف حول البرمجة والحوسبة وكيفية التعامل مع هذا النوع من المسارح الافتراضية[211].

من أشهر العمليات التي قام بها هذا المكتب العملية المعروفة باسم I LOVE YOU التي وقعت في عام 2000 حيث تم هجوم الشركات والأفراد في جميع أنحاء العالم من قبل فيروس "أنا أحبك" والذي

---

(209)يراجع في ذلك :

هشام محمد فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية (دراسة مقارنة)، د ط، مكتبة الآلات الحديثة، مصر،1994، ص 48.

(210)يراجع في ذلك:

مقال حول مكتب التحقيقات الفيدرالي منشور على موقع الموسوعة الحرة" ويكبيديا"، الرابط

https://ar.wikipedia.org/wiki/

،تاريخ الاطلاع2024/05/24،على الساعة 20:00

(211)يراجع في ذلك:

محمد سيد سلطان، قضايا أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، الإمارات المتحدة، 2012، ص 49.

تسبب في عدة خسائر كبيرة، حيث يستهدف هذا الفيروس البريد الإلكتروني للضحية والذي يحمل ملفا مرفقا يسمى هو في الأصل عبارة عن فيروس خبيث وليست رسالة حب، حيث يقوم بسرقة كلمات المرور ونسخ الملفات المتواجدة على جهاز الضحية، كما يرسل نسخ منه تلقائيا إلى جميع جهات الاتصال الموجودة في دفتر عناوينMicrosoft Outlook ، وعلى إثر هذا الهجوم تم التعاون بين كل من المركز القومي الأمريكي ومكتب التحقيقات الفيدرالي وكذا مكتب التحقيقات الفلبيني بالتحقيق في الحادث وتم التعرف على المشتبه فيه والذي يدعى "أونيل دي جوزمان" وهو رجل فليبيني الأصل وطالب مختص في التعامل مع الحواسيب الآلية[212].

-ب-2- **المركز الوطني لحماية البنية التحتية:** تم إنشاء هذا المركز التابع للمباحث الفيدرالية الأمريكية في 1998،يتكون من فريق سري يصل عدد أعضائه إلى 125 رجل حكومي، تعود نشأة هذا الفريق إلى تقرير جمعية العمل حول جرائم الإنترنت والمقدم إلى الرئيس الأمريكي "بيل كلينتون" والذي حددت من خلاله البنية التحتية التي تعتبر محلا للهجمات والاعتداءات عبر الإنترنت إضافة إلى هذه الأجهزة تم إنشاء وكالة متخصصة في مكافحة القرصنة المعلوماتية تابعة لمكتب التحقيقات الفيدرالي مهمتها التنسيق مع المركز الوطني لحماية البنية التحتية ومحاربة جميع أشكال القرصنة والاحتيال المعلوماتي، وكذا نيابة جرائم الحاسوب والاتصالات [213].

2-على مستوى الدول اللاتينية: من أبرز الدول اللاتينية التي بادرت بإنشاء شرطة متخصصة في مكافحة جرائم الإنترنت نجد كل من فرنسا، اسبانيا، ألمانيا، وروسيا، سنتطرق بالتفصيل لكل منها حسب ما يلي:

أ-فرنسا: يعتبر النظام الفرنسي من الأنظمة الأكثر تطورا وتماشيًا مع الجرائم المستحدثة والجرائم الإلكترونية، من خلال تبني الحكومة الفرنسية استراتيجية أمنية حديثة ومتطورة لمواجهة هذه التهديدات، وهذا من خلال العمل على تقوية القدرات الخاصة في مجال الأمن السيبراني وهو ما تجسد في إنشاء وحدات متخصصة في مجال مكافحة الجرائم الإلكترونية إلى جانب الوحدات التقليدية الأخرى،من أبرز هذه الوحدات نجد:

أ-1-الوحدات التابعة للشرطة القضائية: نجد على مستوى مصالح الشرطة القضائية الفرنسية الوحدات التالية:

---

(212) يراجع في ذلك:

هروال نبيلة هبة، مرجع سابق، ص 110.

(213) يراجع في ذلك:

القانون رقم 57-1426 المؤرخ في 1957/12/31، المتضمن تحديد أعضاء الضبط القضائي، الجريدة الرسمية للجمهورية الفرنسية عدد 20، الصادرة بتاريخ 1958/01/08، المعدل والمتمم بالقانون رقم 21-1109 المؤرخ في 2021/08/24.

أ-1-1-المركز الوطني لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالاتL'office central de lutte contre la cybercriminalité liée aux technologies de l'information L.O.C.L.C.T.I.C: يعتبر هذا المكتب من أقدم المكاتب المختصة بمكافحة الجرائم الإلكترونية على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية يساعده في نشاطه كل من وزارة الدفاع ووزارة الاقتصاد والمالية والصناعة، [214]المديرية العامة للجمارك، وكذا المديرية العامة للمنافسة والاستهلاك وقمع الاحتيال كما يتمتع باختصاص وطني يتحدد نطاقه في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، كما أنه يضم مجموعة كبيرة من ضباط الشرطة القضائية الذين يتمتعون بالخبرة الكافية في مجال الأنظمة المعلوماتية، وهم مقسمون على الوحدات التالية[215]:

- **La section opérationnelleوحدة العمليات:** تختص هذه الوحدة بالتحري في القضايا الإجرامية ذات الصلة بكل ما هو معلوماتي والكشف عن مرتكبي هذه الجرائم عن طريق تنسيق وتنشيط عمليات ملاحقة هؤلاء المجرمين.[216]
- **وحدة المساعدات التقنيةla plateforme d'assistance technique:** وهي عبارة عن بنية مجهزة ومزودة بأحدث التجهيزات الإلكترونية المتطورة والوسائل ذات المستوى التكنولوجي العالي، حيث تعمل على مساعدة مصالح التحري والتحقيق في الكشف عن الأدلة الإلكترونية وتحليلها وكذا توفير الرقابة التكنولوجية، كما تقوم بتكوين الضباط والمحققين في مجال التحقيق في الجرائم الإلكترونية.
- **وحدة التحليل والتوثيق العملي:la cellule d'analyse et de documentation** تعمل هذه الوحدة في معالجة البلاغات وتحليلها لمساعدة المصالح القضائية الأخرى في نشاطها، حيث تتكون هذه الوحدة من منصتين منصة فاروس(Pharos) ، ومنصة(Info-Escroqueries) .

---

(214) يراجع في ذلك:

نبيلة هبة هروال، مرجع سابق، ص 115 .

(215)يراجع في ذلك:

ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة لنيل شهادة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، باتنة، 2015 2016، ص 161.

(216)يراجع في ذلك:

CHAMPAGNAT Adeline, L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, revue de cybercriminalité cybermenace et cyberfraude, sous la direction de Irénebouhadana et William grilles, Edition IMODEV, paris, France, 2012, p 164.

- **وحدة العلاقات الدولية:** تعمل هذه الوحدة على ربط الاتصالات مع مختلف المصالح التي تعمل بالاشتراك مع هذا المركز من خلال تقديم وتبادل كل المعلومات اللازمة للتعرف أو البحث عن مرتكبي هذه الجرائم، كما تجدر الإشارة إلى أن هذا المركز يمثل لفرنسا نقطة الاتصال المركزية في التبادلات الدولية.[217]

أ-2-المديرية الفرعية لمكافحة الجريمة الإلكترونية lasous direction de la lutte contre la cybercriminalité(S.D.I.C : تضم وزارة الداخلية الفرنسية عدة مديريات وأجهزة أمنية على رأسها المديرية المركزية للشرطة القضائية (DCPI)والتي تتفرع عنها المديرية الفرعية لمكافحة الجريمة الإلكترونية هذه الأخيرة هي المسئولة عن محاربة الجرائم الإلكترونية بمختلف أصنافها، تم إنشاؤها بموجب مرسوم من رئيس الجمهورية في أفريل 2014، تضم هي الأخرى عدة أجهزة متخصصة تقوم كل منها بنشاط معين أولها مكتب للتنسيق الاستراتيجي مسئول عن الاتصالات الداخلية والخارجية في مجال مكافحة الجرائم الإلكترونية، ومكتب الإنترنت مسئول عن جمع المعلومات من مقدمي الخدمات لصالح أجهزة الشرطة الوطنية، ومكتب التدريب الأولي على مكافحة هذه الجرائم، بالإضافة إلى قسم للتحليل الفني للهجمات السيبرانية يعتمد في عمله على التقنيات المتطورة لتحليل واكتشاف الدليل الإلكتروني والتنبيه بمخاطر الإنترنت بصفة عامة.

أ-3-المديرية العامة للاستخبارات الداخليLa direction centrale du renseignement (D.C.R.I): تختص هذه المديرية بقمع الجرائم على مستوى كامل التراب الوطني الفرنسي، وتلك التي تنشأ أو تكون مدعومة من قبل قوى خارجية أجنبية، والتي من شأنها الإضرار بأمن البلاد والمصالح الأساسية فيها، كالتجسس والإرهاب المعلوماتي.[218]

أ-4- الوكالة الوطنية لأمن الأنظمة المعلوماتية: أنشأت هذه الوكالة في فرنسا في 07 جويلية 2009 مقرها باريس، وتعتبر وكالة وزارية تخضع المصالح الوزير الأول، أما عن تشكيلة هذه الوكالة فهي تضم إدارة تتكون من مكتب وخلية للأمن السيبراني، تتفرع عنهما عدة أجهزة مسئولة عن عمليات المراقبة والخبرة التقنية وكذا الاستراتيجيات المتبعة في تحقيق أمن الأنظمة المعلوماتية،[219] وتتمتع هذه الأخيرة بصلاحيات

---

(217) يراجع في ذلك:

QUEMENER Myriam,La Coopération Entre Les Organes de Lutte Lontre la Cybercriminalité Pour Une Stratégie de Cyber Sécurité Français، Revue de Lamy Droits des Affaires ,Num° 87, France, 2013، P02.

(218) يراجع في ذلك:

المديرية العامة للاستخبارات الداخلي، المنشور على منصة ويكيبيديا،المتواجد على الرابط التالي:

https://ar.wikipedia.org/wiki/

الذي تم الاطلاع عليه بتاريخ 2024/06/12 على الساعة 12:38.

(219) يراجع في ذلك:

الضبط الإداري والقضائي معا، إذ تختص باقتراح القوانين والتنظيمات الخاصة بأمن الأنظمة المعلوماتية وتسهر على ضمان تطبيق النصوص حسب المعايير المحددة سلفاً، كما تعمل على كشف الهجمات السيبرانية التي تستهدف هذه النظم والوقاية منها من خلال تطوير برامج حماية أمنية، وتحليل هذه الهجمات والتحري عن مرتكبها وتقديم نتائج هذه التحقيقات إلى السلطات المختصة، كما أنها تقوم دائما بتوعية أفراد المجتمع كافة بخطورة هذه الجرائم وضرورة التبليغ عنها، وبهذا فهي تلعب الدوريين الوقائي والردعي معا.

أ-5- فرق البحث والتحري عن جرائم الغش المعلوماتي: زيادة على ما تقدم توجد هناك فرق مختصة بالبحث والتحري عن بعض الجرائم الإلكترونية، والتابعة المحافظة شرطة باريس وضواحيها، أولها فرقة البحث والتحري عن الجرائم الماسة بالبرمجيات والاعتداء على حقوق المؤلف والملكية الفكري (B.E.F.T.I) إذ تضم هذه الفرقة حوالي 30 شرطياً في صفوفها يختصون بمهمة التحري عن الجرائم الماسة بحقوق المؤلف وجرائم التقليد، وتنقسم بدورها إلى ثلاثة فرق أو خلايا تتمثل في خلية البحث والتحقيق خلية المبادرة، خلية الدعم حيث تدعم أي جهة أخرى تتولى مسألة البحث والتحري في المسائل الإلكترونية إلى جانب هذه الفرقة توجد أيضا تحت سلطة محافظة باريس فرقة لمكافحة جرائم الغش المتعلقة بوسائل الدفع الإلكتروني (B.F.M.D) حيث تضم هي الأخرى حوالي 50 شرطيا مختص بمهمة التحري في المسائل الإلكترونية.[220]

ب-الوحدات التابعة لمصالح الدرك الوطني والجمارك: لقد سخرت الحكومة الفرنسية إلى جانب رجال الشرطة القضائية قوات درك وطنية لمواجهة الجرائم الإلكترونية، أعطى القانون لخلية الجمارك المعلوماتية صلاحيات واسعة لكشف هذا النوع من الجرائم، إذ تقوم في سبيل ذلك بمراقبة عمليات التبادل الإلكتروني للسلع والمنتجات، وكذا القيام بعمليات الشراء مباشرة من المواقع الإلكترونية والقيام بأسلوب التسرب ضمن الأقمار الإلكترونية، حيث ينعقد اختصاصها على كل من المستويين الوطني المركزي والإقليمي.[221]

-قسم الأنترنت التابع للمصلحة التقنية للبحوث القانونية والوثائقية.

-القسم المعلوماتي الإلكتروني التابع لمعهد البحوث الجنائية للدرك الوطني.

-المركز الوطني لتحليل الصور ومركز مكافحة الجرائم الرقمية.

نبيلة هبة هروال، مرجع سابق، ص 129.

(220) يراجع في ذلك:

ربيعي حسين، مرجع سابق، ص ص 163 166.

(221) يراجع في ذلك:

SCHOEN Gérard, Ladouane face à La cybercriminalité, Revue deCybercriminalité Cybermenace et Cyberfraude, sous La direction de IrèneBouhadana et William Dgilles, Edition Imodev, paris, France, 2012, pp 169 170.

ثانيا: وحدات البحث والتحري عن الجرائم الإلكترونية على المستوى الدول العربية

إن معظم الدول العربية سارعت لإنشاء فرق مختصة لتصدي الأمثل للجرائم الإلكترونية من بين أهم الدول العربية نجد المملكة العربية السعودية ومصر والأردن بصفة عامة والجزائر بصفة خاصة.

1-على مستوى المملكة العربية السعودية: في إطار تنامي ظاهرة الإجرام الإلكتروني في المملكة العربية السعودية بشكل كبير ومستمر، ونتيجة الضعف السلطات القضائية التقليدية في مواجهة هذا النوع من الإجرام، قامت الحكومة السعودية بتأسيس وحدات وفرق مختصة لمحاربة هذا النوع من الجرائم هذا من جهة، ومن جهة ثانية استحدثت تطبيقات وأرقام متعددة لاستقبال بلاغات المواطنين حول هذه التهديدات من بين أهم هذه الوحدات والأقسام نجد قسم مكافحة الجرائم الإلكترونية التابع المديرية الأمن العام للمملكة،[222] والذي يختص باستقبال البلاغات والتحري في هذه الجرائم وذلك نظرا لخبرة موظفيه في التعامل مع هذه التهديدات والطبيعة التقنية لها، وتعقبه للمجرمين المعلوماتيين والكشف عنهم وتوجيههم للقضاء، كما أسست الحكومة السعودية هيئة لمكافحة الابتزاز الإلكتروني وهي عبارة عن هيئة حكومية متخصصة في متابعة جرائم الابتزاز الواقعة من داخل المملكة أو خارجها، وذلك من خلال فريق كبير من المختصين في معالجة الابتزاز والتهديد بطريقة تقنية، كما تمتلك فريق تقني يعمل على تعقب المجرمين والقبض عليهم وإحالتهم للنيابة العامة، بحيث تتيح هذه الهيئة رقما خاصا للمواطنين لتقديم بلاغاتهم كما تتيح لهم إمكانية التواصل مع محامي مختص في الجرائم الإلكترونية وعرض للتمكن من مساعدتهم وتقديم الاستشارة القانونية لهم بخصوص هذه الجرائم.[223]

وفقا لتقارير عديدة قامت بها الأجهزة الأمنية فإن قضايا الابتزاز والتهديد الإلكتروني وكذا قضايا تخزين المواد الإباحية تحتل نسبة 76% من الجرائم الإلكترونية الواقعة بالسعودية تليها قضايا التحويلات البنكية غير المشروعة والاستخدام غير المشروع البطاقات الائتمان وتزويرها، تليها جرائم الفدية التي تمس المؤسسات والشركات الكبرى.

---

(222)يراجع في ذلك:

مقال حول هيئة مكافحة جرائم الابتزاز الإلكتروني منشور على الموقع الرسمي لوزارة الداخلية للمملكة العربية السعودية، والمتواجد على الرابط التالي:

https://www.moi.gov.sa

الذي تم الاطلاععليه بتاريخ 2024/05/29 على الساعة21:00.

(223)يراجع في ذلك:

الشرطة السعودية تستعد لمواجهة ملف الجرائم الإلكترونية، المنشور على منصة العربية نت،المتواجد على الرابط التالي:

https://www.alarabiya.net/saudi-today/2013/12/05

الذي تم الاطلاع عليه بتاريخ 2024/05/29 على الساعة 21:18.

فقد تعرضت المملكة العربية السعودية ودولة قطر عام 2013 إلى هجمات إلكترونية استهدفت كل من شركة أرامكو السعودية للنفط وشركة رأس غاز القطرية، وهجمات أخرى على مواقع الإلكترونية حكومية منها وزارة الداخلية أدت إلى تعطيل بعض المرافق مؤقتا.

2-على مستوى دولة الأردن: تناط مهمة الضبط القضائي في الأردن بجهاز الضابطة العدلية طبقا لقانون أصول المحاكمات الجزائية وينقسم موظفو الضابطة العدلية إلى طائفتين تبعا لنوع الجريمة أو طبيعتها، الطائفة الأولى هي من أوكل لها ممارسة الضبط في جميع أنواع الجرائم ويطلق عليها أعضاء الضابطة العدلية ذو الاختصاص العام، وهم من ورد ذكرهم في المادتين 08 و 09 من قانون أصول المحاكمات الجزائية، أما الطائفة الثانية وهي من خصها القانون بضبط بعض الجرائم دون غيرها، و نشأة شركة "ترينت مايكرو" حول المختصون في التحري وضبط الجرائم الإلكترونية، حيث استجابة للتسارع والتطور الكبير الذي يشهده العالم في مجال الجريمة وخاصة الإلكترونية أنشأت مديرية الأمن العام بالمملكة الهاشمية الأردنية إدارة مخصصة للبحث الجنائي عام 1948 وكانت أولى مهامها منع الجرائم والقبض على المجرمين وحراسة حيث كانت تعرف باسم دائرة تحري المجرمين.[224]

تضم هذه الوحدة مجموعة من الضباط والخبراء المدربين والمؤهلين لملاحقة هذا النوع من الإجرام والتصدي له ،من خلال الكشف عن الجناة وملاحقتهم عن طريق التحقق من الحسابات والمواقع والبرامج التي استخدمها المجرمين في تنفيذ جرائمهم، إذ تعتمد هذه الوحدة في تحرياتها على وسائل جد متطورة تمكنها من معرفة صاحب الحساب أو الموقع ومكان تواجده، كما تقوم بتعزيز التعاون الدولي مع الجهات الدولية الأخرى في العديد من البلدان في مجال مكافحة هذا النوع من الإجرام، ومن مهامها أيضا القيام بدوريات إلكترونية متجددة، وبشكل دائم على المواقع الإلكترونية ومواقع الاجتماعي المراقبة أي منشور من شأنه أن يشكل جريمة إلكترونية، كالعبارات الماسة والأخلاق العامة، أو خطابات الكراهية والخطابات الماسة بأمن الدولة وغيرها.

وفي سبيل التواصل مع هذه الوحدة قد خصصت مديرية الأمن العام الرقم التالي "065633404 للإجابة عن جميع استفسارات المواطنين واستقبال بلاغاتهم المتعلقة بالجرائم الإلكترونية، والرقم "192" للتبليغ جرائم الابتزاز والتهديد الإلكتروني خصيصا، أو عن طريق التواصل معهم عبر "jenaee.dept@psd.gov.jo"مديرية الأمن العام عبر بريدها الإلكتروني التالي وقد عالجت هذه الوحدة منذ إنشائها العديد من قضايا الإجرام الإلكتروني جرائم الاحتيال واختراق الأنظمة وسرقة البيانات وكذا البريد الإلكتروني، حيث تمكنت وحدة مكافحة (ج إ) على مستوى إدارة البحث الجنائي بإلقاء القبض على أحد الأشخاص بعد أن ثبت تورطه في إنشاء صفحات وهمية على مواقع التواصل واستخدامها للإساءة

(224) يراجع في ذلك:

حسن الربيعي، مرجع سابق، ص 130 .

للمواطنين والشخصيات العامة والتشهير بهم ونشر الإشاعات والأكاذيب عليهم،[225] وهذا بعد تلقي الإدارة عدة بلاغات وشكاوى ضد شخص مجهول ينشر هذه التهديدات عبر صفحات الإنترنت، وبعد تشكيل فريق من المختصين تم تتبع منشورات هذا الشخص لغاية الوصول إليه وتحديد مكانه وتم القبض عليه، كما تجدر الإشارة أنه تقوم هذه الوحدة في سبيل التحذير من الجرائم الإلكترونية على نشر الوعي والثقافة الإلكترونية والدعم والإرشاد عن طريق موقعها الإلكتروني أو صفحتها على مواقع الاجتماعي، أو عن طريق المحاضرات التي يتم إلقائها من طرف الضباط والخبراء في الجريمة الإلكترونية وذلك على مستوى كل من المدارس،[226] والمعاهد والجامعات وحتى الجمعيات، تجنبا لوقوع المواطنين وخاصة فئة الأطفال ضحية لهذه الجرائم.

3-على مستوى دولة الجزائر بصفة خاصة: تسند مهمة البحث والتحري في الجرائم بصفة عامة إلى جهاز الضبطية القضائية، حيث عني قانون الإجراءات الجزائية الجزائري بتحديد الأشخاص الموكل إليهم مهام الضبط القضائي، المادة 12 فقرة 01[227] من ق إ ج ج يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون الذين تسند إليهم بعض مهام الضبط القضائي، وقد جاءت المادة 15 من ذات القانون محددة لمن تثبت لهم صفة الضبطية القضائية والمواد 21 و28،[228] محددتان الموظفين المخول إليهم بعض المهام لضبطية القضائية الخاص بحيث قسم القانون هؤلاء الضباط إلى فئتين أساسيتين تتمتع الأولى بمتابعة جميع أنواع الجرائم وتعرف بالضبطية القضائية ذات الاختصاص العام، في حين تتمتع الفئة الثانية بالتحري في بعض الجرائم الخاصة وتعرف بالضبطية القضائية ذات الاختصاص الخاص.

بظهور الجرائم المستحدثة والإلكترونية أصبح جهاز الضبطية القضائية غير قادرا على التصدي لمثل هذه الجرائم نظرا الضعف خبرته ومعرفته في هذا المجال، لهذه الأسباب ونظرا للخصوصية التي تتمتع بها هذه الجرائم، أصبح واجبا العمل على تكوين وتأهيل الضباط في مجال التحري عن الجرائم الإلكترونية لتطوير كفاءاتهم ومهامهم من أجل التصدي الأمثل لهذه الجرائم ومحاربة مرتكبيها.

---

(225) يراجع في ذلك:

غادة الشيخ،" الفضاء الإلكتروني مسرح جديد للجرائم ضحاياه مراهقون"، مقال منشور في جريدة الغد المتواجد على الرابط التالي: https://alghad.com

الذي الاطلاع عليه بتاريخ 2024/05/21 على ساعة 13:30.

(226) يراجع في ذلك:

غادة الشيخ، الفضاء الإلكتروني مسرح جديد للجرائم ضحاياه مراهقون، المرجع السابق.

(227) يراجع في ذلك:

المواد 12 و15 من قانون الإجراءات الجزائية الجزائري، المرجع السابق.

(228) يراجع في ذلك:

المواد 21و 28 من قانون الإجراءات الجزائية الجزائري، مرجع سابق.

وفي هذا الإطار قامت الحكومة الجزائرية بإنشاء واستحداث أجهزة خاصة للبحث والتحري في الجرائم الإلكترونية وذلك على مستوى كل من مديرية الأمن الوطني، والقيادة العامة للدرك الوطني، وكذا المديرية العامة للجمارك، سنتعرف عليها بالتفصيل في النقاط الآتية:

1-الوحدات التابعة للمديرية العامة للأمن الوطني: في إطار تجسيد سياسة أمنية فعالة للتصدي للجرائم الإلكترونية بادرت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية والعمل على استحداث وحدات متخصصة تعمل على مكافحة هذا النوع من الجرائم، حيث استحدثت أربع (04) مصالح مختصة في شكل نيابة تمثلت في نيابة مديرية الشرطة العلمية والتقنية نيابة المديرية الاقتصادية والمالية، نيابة القضايا الجنائية مصلحة البحث والتحليل.

2-الوحدات التابعة للقيادة العامة للدرك الوطني: بما أن الدرك الوطني أحد الأجهزة الأمنية المكلفة بردع وضبط الجريمة، والمحافظة على الأمن والنظام العموميين، فقد ساير التطور الإجرامي الذي يشهده العالم اليوم من خلال توفير الوسائل المادية وتأهيل الضباط المختصين في مكافحة الإجرام المعلوماتي وذلك بإنشاء العديد من الهياكل والوحدات المتخصصة في التحري والتحقيق في هذا النوع من الجرائم،[229] إلى جانب بعض المصالح التي تختص بالتحري في جميع الجرائم بصفة عامة نذكر من بينها المصالح والمراكز العلمية والتقنية المصلحة المركزية للتحريات الجنائية، هياكل التكوين الوحدات المتخصصة ووحدات الإسناد، والوحدات الإقليمية، إضافة إلى هذه المصالح وفي سبيل مكافحة الجريمة الإلكترونية يضع الدرك الوطني بعض الوحدات والمراكز المتخصصة في هذا النوع من الجرائم.

أ-المعهد الوطني للأدلة الجنائية وعلم الإجرام: يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-432[230] المؤرخ في 29 ديسمبر 2004 ببوشاوي بالجزائر العاصمة وذلك في إطار عصرنة قطاع الدرك الوطني يتكون هذا المعهد من (11) إحدى عشرة دائرة متخصصة في مجالات مختلفة، تهدف جميعها إلى إنجاز عمليات الخبرة والتكوين والتعليم وتقديم المساعدات التقنية وغيرها ومن بين هذه الدوائر دائرة الإعلام والإلكترونيك التي أوكلت لها مهام تحليل الأدلة الرقمية المتحصل عليها من الجرائم الإلكترونية، حيث تنقسم هذه الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات أو الأدلة ،تتمثل هذه المخابر في:

---

(229) يراجع في ذلك :

حسين ربيعي، مرجع سابق، ص ص 180 181.

(230) يراجع في ذلك:

المرسوم الرئاسي رقم 04-432 المؤرخ في 29ديسمبر 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج ر ج ج عدد 84، المؤرخة في 29 ديسمبر 2004.

أ-1-1-مخبر الإعلام الآلي: يقوم هذا المخبر بتحليل ومعالجة حوامل المعطيات الرقمية الموجودة بالأجهزة الإلكترونية مثل الهاتف الشريحة القرص الصلب ذاكرة الفلاش...الخ، والقيام بتحديد التزوير الرقمي للبطاقات البنكية.

أ-1-2-مخبر الفيديو: يختص هذا المخبر بمقارنة الصور والفيديوهات وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد، وذلك عن طريق أجهزة فيديو بوكس وحوامل الفيديو الرقمية والممغنطة كونيتك استوديو ماكس ثلاثة أبعاد وموزع لحفظ شرائح الفيديو، كما يحتوي مخبر الفيديو على أربع قاعات، قاعتان للتحليل، قاعة للتخزين، وقاعة موزع.

أ-1-3-**مخبر الصوت:** يختص هذا المخبر بتحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة، كما يقوم بتحديد الشخص المتكلم وتحديد شرعية التسجيلات الصوتية، وذلك عبر أجهزة الازدواجية والتنصت والشبكات الإعلامية المختصة بمعالجة وتحسين التسجيلات الصوتية، وكذا أجهزة نسخ الأقراص المضغوطة وأجهزة التصليح، ويحتوي هو الآخر على 05 قاعات، ثلاثة منها مخصصة للتحليل، وقاعة للتخزين، وقاعة موزع، من خلال ما يحتويه هذا المعهد من دوائر ومخابر فرعية مختصة تقنيا فإنه يساهم بشكل فعال في مكافحة الجرائم الإلكترونية، وذلك لما يقوم به من مهام حيث يتولى في هذا الشأن القيام بالخبرات العلمية والتقنية لدعم أجهزة التحري والتحقيق وذلك بطلب منها، إذ تساعد الخبرات والتحليلات التي يقوم بها هذا المعهد على تحديد هوية مرتكبي هذه الجرائم.[231]

كما يقوم بدعم هذه الوحدات عن طريق الخبراء المؤهلين بمعاينة هذه الجرائم، إذ يتم التواصل بين أجهزة الشرطة القضائية وهذه المخابر عن طريق إرسالية تتضمن طلب تحليل الأجهزة المتحصل عليها من طرف الشرطة، والتي قد تتمثل في دعائم تخزين رقمية مثل القرص المرن والقرص لأجهزة أو مرتكبيها أو أماكن تواجدها، والتي من شأنها مساعدة الضباط في عملية التحقيق، مع الإشارة إلى أن نتائج هذه الخبرة قد تأخذ وقتا طويلا يدوم لعدة أشهر، وفي هذه المدة يواصل ضباط الشرطة التحريفي الجريمة في انتظار وصول نتائج الخبرة، فضلاً عن هذا يشارك المعهد في الأبحاث والدراسات المتعلقة بالوقاية من جميع أشكال الإجرام بما فيها الإجرام المعلوماتي، وبهذا يكون المعهد قد ساهم في وضع واقتراح سياسة ناجعة لمكافحة الإجرام بأنواعه[232].

ب-المركز الوطني لمكافحة الجريمة الإلكترونية: جاء هذا المركز نتيجة استراتيجية مؤسسة الدرك الوطني في تعقب الجرائم والإسراع في صدها إيمانا منها بأن المعلوماتية أصبحت وسيلة لتطور بعض الجرائم، وقد

---

(231) يراجع في ذلك:

عياش هواري، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، كلية الحقوق، جامعة بسكرة، 2016، ص 03.

(232) يراجع في ذلك:

هواري عياش، مرجع سابق، ص 08.

تم إنشاؤه في الجزائر العاصمة سنة 2004، يضم هذا الأخير مجموعة من الوحدات والأقسام تقوم بمهام التحري في هذا النوع من الجرائم،[233] وهي كالتالي:

ب-1--وحدة الحماية والتحليل: تسهر هذه الوحدة على تحليل المخزون المعلوماتي على مدار 24 ساعة، وحماية بنك المعلومات المفتوحة والمتداولة عبر شبكة الإنترنت، وهي تضمن بهذا مهمة المراقبة العامة للمضمون المعلوماتي.

ب-2-خليةالمساعدة ومعالجة الحوادث المعلوماتية:خلية المساعدة ومعالجة الحوادث المعلوماتية تسهر هذه الخلية على الوقاية من مخاطر المعلوماتية وتقديم المساعدة للمواطنين في تخطي الجرائم الإلكترونية على مستوى المؤسسات والمرافق الحكومية للدولة.

ب-3-الوحدة المركزية للتنسيق والتعاون: وتتفرع عن هذه الوحدة عدة وحدات فرعية موجودة على مستوى المجموعات الولائية والمتمثلة في الوحدات المحلية لمحاربة الجريمة الإلكترونية. إذ تعمل بالتنسيق مع الوحدة المركزية في مجال تبادل المعلومات والخبرات في التحري عن هذه الجرائم وتحليل الأدلة الرقمية.من خلال هذه الوحدات والمهام المنوطة بها نستنتج أن المركز الوطني لمكافحة الجرائم الإلكترونية يضطلع بمهمتين أساسيتين أولهما قبلية وتتعلق بالوقاية من مخاطر المعلوماتية وتجنب الوقوع فيها إضافة إلى عمليات التوعية والتحسيس التي يقوم بها المركز، والثانية بعدية تتمثل في ردع الجرائم بأنواعها.

وتجدر الإشارة أنه قد تم إنشاء مكتب خاص بمكافحة الجريمة الاقتصادية على مستوى هذا المركز عالج من خلاله حوالي 20 جريمة اقتصادية ومالية خلال سنة 2017، إلى جانب هذا المكتب وعلى مستوى نفس المركز تم إنشاء مكتبا آخرا خاصا بحماية الأحداث عبر الإنترنت ليكمل مهام الفرق الخاصة بحماية الأطفال التي استحدثتها قيادة الدرك الوطني، حيث يقوم هذا المكتب بتقديم الدعم التقني للوحدات الإقليمية في مجال التحري عن الجرائم الواقعة على الأطفال، وقد عالج هذا الأخير حوالي 100 جريمة الإلكترونية كان ضحاياها أطفال ومراهقين من ضمن 1000 قضية تمت معالجتها سنة2017.[234]

ج-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: يعتبر مركز الوقاية من جرائم الإعلام الآلي نقطة اتصال وطنية في مجال دعم أعمال البحث والتحري عن الجرائم الإلكترونية وجرائم الإعلام الآلي، وهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستعمال القيادة الدرك الوطني، تم إنشاؤه سنة 2015 بيتر مراد رايس بالجزائر العاصمة، حيث يتولى المهام التالية:

---

(233) يراجع في ذلك:

حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، مرجع سابق، ص ص 182 183.

(234) يراجع في ذلك:

ربيعي حسين، مرجع سابق، ص ص184 185.

-القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.

-مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال، والبحث عن الأدلة عبر شبكة الإنترنت والأجهزة الإلكترونية.

-المشاركة في عمليات التحري من خلال التسرب عبر شبكة الانترنت لفائدة مصالح الدرك الوطني والسلطات القضائية.

-العمل على ضمان المراقبة الدائمة والمستمرة لشبكة الإنترنت.

وفي إطار مكافحة الجرائم الإلكترونية عالج هذا المركز سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم الإلكترونية تنوعت بين جرائم التهديد والتحريض جرائم الاختراق والقرصنة جرائم التحرش الجنسي بالأطفال وتحريضهم على الفسق والدعارة جرائم إهانة رموز وطنية وهيئات حكومية، جرائم النصب والاحتيال، جرائم الاعتداء على حرمة الحياة الخاصة... الخ.

كما تم إنشاء بعض المصالح الأخرى على نفس المستوى المركزي من بينها مديرية الأمن العمومي والاستغلال وهي عبارة عن هيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال البحث والتحري عن الجرائم الإلكترونية، وكذا المصلحة المركزية للتحريات الجنائية والتي تعمل على التحري في جميع أنواع الجرائم بما فيها الجرائم الإلكترونية والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.[235]

ملخص

تتميز جريمة التهديد عبر الوسائل الإلكترونية بحداثتها، مما يستدعي إلى إجراءات تحقيق ذات طبيعة خاصة تتم في بيئة إلكترونية، منها ما نص عليه المشرع الجزائري في قانون الإجراءات الجزائية والقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وترتكز عملية الإثبات الجنائي في هذا النوع من الجرائم على الدليل الرقمي المستخلص من إجراءات التحقيق إضافة إلى الشهادة الإلكترونية، إلا أن هذه الجريمة واجهتها العديد من الصعوبات منها ما تعلق بالدليل الإلكتروني وما تعلق بالسلطات القضائية خاصة أثناء مرحلة التحقيق.

---

(235) يراجع في ذلك:

عز الدين عز الدين، قيادة الدرك الوطني الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر2015، جامعة بسكرة، الجزائر، ص 29.

ويتحدد الاختصاص القضائي في جريمة التهديد الإلكتروني بناءا على مبادئ كرستها معظم التشريعات، وفي بعض الأحيان في هذا الشكل من الجرائم يستدعي الأمر اللجوء إلى إجراء الإنابة القضائية وذلك في حالة ما تعدت آثار الجريمة خارج نطاق المحكمة المختصة.

وتمت مكافحة هذه الجريمة من خلال التوقيع على العديد من المعاهدات والاتفاقيات، بالإضافة إلى استحداث أجهزة خاصة للحد من انتشارها.

خاتمة

ختاما لما تم التطرق إليه سابقا نجد أن التطور الذي نعيشه في هذا العصر خاصة ما تعلق بالثورة المعلوماتية نتج عنه العديد من المشكلات والأخطار التي تكون مصاحبة بشكل عفوي لكل تطور حضاري، فدخول الأنترنت عالمنا وانتشارها انتشارا كبيرا لدى مختلف أطياف المجتمع أدّى على ظهور الجريمة الإلكترونية التي أصبحت تشكل خطرا على كل مستخدمي هذه التقنية وهذا بسبب غياب الرقابة على مستخدمي الشبكات المعلوماتية. من صور الجرائم الإلكترونية لدينا جريمة التهديد الإلكتروني، حيث تعد آفة عصرية تلقي بظلالها القاتمة على المجتمعات، وتشكل تحديا كبيرا يهدد أمن وسلامة المجتمع الرقمي أي يهدد الأفراد في أمنهم النفسي وخصوصيتهم وممتلكاتهم.

اتفقت مختلف التشريعات أنّ لهذا الشكل من الجرائم نوع من الخصوصية سواء من الناحية الموضوعية أو الإجرائية، يطلق عليها تسمية الجرائم الناعمة وذلك لخلوها من العنف، وتتميز حسبما تم التطرق إليه سابقا بأنها عابرة للحدود وأنّ طبيعة الدليل المستخلص منها تقني، وهذا ما يفرض نمط تحقيق وتحري مختلف عن النمط المتعود عليه في الجرائم التقليدية، فتختلف بذلك الوسائل ويتطلب وجود خبير في الإعلام الآلي في عملية التحقيق الجنائي لما له من كفاءة ودراية بعالم المعلوماتية والفضاء الإلكتروني، ومن جانب آخر اللجوء إلى أساليب تحقيقية خاصة مناسبة لطبيعة الدليل بغية إثبات الجريمة ونسبتها لفاعل محدد، وهنا تكون الأدلة الرقمية مناسبة لذلك، إضافة إلى الأشياء الجديدة التي جاءت بها جريمة التهديد الإلكتروني منح الخبير صفة الشاهد، او الذي تم إعطاءه تسمية الشاهد الإلكتروني.

وبالتالي من خلال هذا البحث وصلنا إلى جملة من النتائج تتلخص فيما يلي:

- الحاجة إلى تحديث النص الخاص بجريمة التهديد النصوص عليه في المادة 384 من ق ع ج، وإضافة الوسائل الإلكترونية إلى الوسائل المستعملة في ارتكابها.
- قصور قواعد القانون الجنائي في مواجهة تهديد حياة الأشخاص عبر الوسائل الإلكترونية، وعدم تحديد مفهوم لجريمة التهديد الإلكتروني وصورها.
- ربط جريمة التهديد الإلكتروني بالأنظمة المعلوماتية دون تحديد دقيق للمفهوم.
- جريمة التهديد الإلكترونية من صور الجرائم الإلكترونية، إذ تتم باستخدام شبكة الأنترنت وأجهزة الاتصال الحديثة.
- توسع نطاق المسؤولية الجزائية في جريمة التهديد الإلكتروني ليشمل عدة أطراف كمقدمي خدمة الاتصال.

- لجريمة التهديد الإلكتروني وسائل وطرق مختلفة لارتكابها كالهواتف النقالة والحواسب المحمولة.
- جريمة التهديد الإلكتروني جريمة تقع على أنظمة المعالجة الآلية للمعطيات، ويمكن ارتكابها عبر عدة طرق كالاختراق والقرصنة ....
- جريمة التهديد الإلكتروني ذات طابع دولي عابرة للحدود الوطنية فهي عالمية الوجود.
- تعديل قانون العقوبات الجزائري فيما يخص جرائم الاعتداء على الأنظمة المعلوماتية رقم 05-24، وإصدار قانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- اصطدام القاضي الجنائي بمبدأ الشرعية الجنائية عند تطبيق النص التقليدي لجريمة التهديد الإلكتروني.
- لجوء المحاكم إلى تطبيق النصوص الجنائية التقليدية على قضايا التهديد الإلكتروني على الرغم أنّ تلك النصوص لا تشمل على صور جريمة التهديد الإلكتروني.
- اختلاف التشريعات في مقدار العقوبة المقررة لجريمة التهديد الإلكتروني.
- استحداث أساليب تحري خاصة للبحث في الجرائم ذات الطابع المعلوماتي.
- الحاجة إلى أجهزة وخبرات متخصصة وفرق عمل متكاملة الخبرة لجمع أدلة الإثبات في جريمة التهديد الإلكتروني.
- صعوبة تحديد هوية المجرم المعلوماتي، واستحالة الوصول إلى أدلة مادية.
- صعوبة الحصول على الدليل الإلكتروني.
- ظهور مفهوم جديد للشهادة يتناسب مع الطابع الإلكتروني لجريمة التهديد الإلكتروني.
- وجود عدة صعوبات تعيق عمل إجراءات مكافحة الجريمة الإلكترونية بالشكل الصحيح، ومن أبرزها اختلاف القوانين من دولة إلى أخرى من حيث إجراءات التحري والاختصاص القضائي بين الدول، وإجراءات الإنابة القضائية.
- سعي مختلف التشريعات إلى مكافحة جريمة التهديد الإلكتروني عبر تعزيز أجهزتها الأمنية ووضع قوانين خاصة واستحداث هيئات تفيد نفس الهدف.
- التوقيع على اتفاقيات تهدف إلى التعاون الدولي.

من هذه النتائج وصلنا إلى الاقتراحات التالية:

- من الأجدر تعديل القوانين العقابية القائمة لمواجهة ما قد يرتكب من أفعال غير مشروعة عن طريق تكنولوجيا الإعلام والاتصال بشكل دائم، وذلك لأن هذه الأخيرة في تطور مستمر.
- تعديل المادة 284 من ق ع ج المتعلقة بجريمة التهديد، كون هذه الجريمة أصبحت ترتكب بواسطة وسائل إلكترونية وذلك بإضافة عبارة "الأنترنت" أو "تكنولوجيا الإعلام والاتصال".
- تشديد العقوبة في التهديد المرتكب عبر الوسائل الإلكترونية، لتحقيق الردع، لأنها أصبحت من الجرائم الأكثر انتشارا حول العالم.
- ضرورة استحداث نصوص قانونية إجرائية تتلاءم مع مجال الضبط والتحقيق في المجال الافتراضي، وإنشاء رقابة فعلية لأنه من المتوقع أن تكون جريمة التهديد عبر الوسائل الإلكترونية أكثر تطورا مستقبلا.
- تهيئة متخصصين للتفتيش والتحقيق الإلكتروني، ونقترح أن تسمى بشرطة مكافحة جرائم الحاسوب.
- توفير أدوات حماية تقنية تعمل على تقليص عمليات جمع البيانات الشخصية التي تتم دون علم المستخدم.
- تعديل قانون الإجراءات الجزائية على وجه الاستعجال من خلال إدراج قسم خاص بأعمال البحث والتحقيق في الجرائم الإلكترونية، لتسهيل الأمر على جهات التحقيق.
- إعطاء الضبطية القضائية المزيد من الوسائل التقنية المتطورة مع ضرورة التكوين والتأهيل المتواصل، وإمكانية الاستعانة بأهل الخبرة والاختصاص، تماشيا مع تطور التكنولوجي.
- زيادة المدة الزمنية المحددة لحفظ البيانات الموجودة لدى مزودي خدمات الاتصال لتسهيل التصدي للجريمة والتعرف على مرتكبيها.
- وضع آليات ردعية تتماشى مع التطورات الحاصلة من خلال فتح المجال للأصحاب الخبرات من خارج القطاع الأمني للمشاركة في مكافحة الجريمة الإلكترونية بمختلف أشكالها.
- نشر ثقافة السلامة المعلوماتية من خلال حملات توعوية للعموم على مستوى وسائل الإعلام، وإعلام مستخدمي الأنترنت بالمخاطر التي تهددهم وسبل الوقاية منها، بالإضافة إلى تشجيع الإبلاغ عنها.

- تحقيق التوازن بين الحرية الشخصية وضمان إرساء الأمان الرقمي، لضمان الحماية من التدخلات غير المشروعة أو التعسفية.
- إنشاء هيئة عامة مستقلة للحفاظ على الأمن السيبراني للدولة.
- التنسيق مع مختلف دول العالم والعمل على الاستفادة من تجارب الدول الرائدة في مجال مكافحة الجرائم المعلوماتية من أجل التصدي لها بصفة عامة، وجريمة التهديد الإلكتروني بصفة خاصة نظرا لطبيعتها العابرة للحدود، وذلك عبر تعزيز وتفعيل التعاون الدولي من خلال إبرام المزيد من الاتفاقيات الدولية على المستوى الإقليمي والعالمي.

قائمة المراجع

I-المراجع باللغة العربية

أولا: الكتب

1- إبراهيم خالد ممدوح، فن التحقيق في الجرائم الإلكترونية، د ط، دار الفكر الجامعي، الإسكندرية، 2010.

2- أحسن بوسقيعة، التحقيق القضائي، ط2، الديوان الوطني للأشغال التربوية، الجزائر، 2002.

3-أحمد الشافعي، البطلان القانوني في قانون الإجراءات الجزائية (دراسة مقارنة) ، ط5، دار هومة للنشر والتوزيع، الجزائر، 2006.

4-أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 2015.

5-بشرى حسين الحمداني، القرصنة الإلكترونية أسلحة الحرب الحديثة، د ط، دار أسامة للنشر والتوزيع، الأردن، عمان، 2014.

6- جلال ثروت، النظم الإجرائية الجنائية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 1997

7- حدة بوخلفة، المسؤولية الجنائية لمقدمي خدمات الأنترنت، د ط، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2019.

8- حسام محمد نبيل الشراقي، الجرائم المعلوماتية : جرائم الاعتداء على التوقيع الإلكتروني (دراسة مقارنة) ، د ط، دار الكتب القانونية، مصر، 2013

9- حسن طاهر داوود، جرائم نظم المعلومات، د ط، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000.

10- زهراء عادل سلبي، جريمة الابتزاز الإلكتروني (دراسة مقارنة) ، د ط، شركة دار الأكاديميون للنشر والتوزيع، عمان، الأردن، 2020.

11- زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى، عين مليلية، الجزائر،2011.

12- طارق إبراهيم الدسوقي. عطية، الأمن المعلوماتي والنظام القانوني لحماية المعلوماتية، د ط، دار الجامعة الجديدة، الإسكندرية، 2015.

13- عايدة رجا الخلايلة، المسؤولية التقصيرية الإلكترونية : المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والأنترنت (دراسة مقارنة) ، ط2، دار الثقافة للنشر والتوزيع، عمان، 2011

14- عبد المنعم سليمان، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، د ط، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، .1999

15- علي حسن الطوالبة،الجرائم الالكترونية: جرائم الحسابات الإلكترونية،ط01،دار الفكر الجامعي، الإسكندرية،2005.

16- محمد سيد سلطان، قضايا أمن المعلومات وحماية البيئة الإلكترونية، د ط، دار ناشري للنشر الإلكتروني، الإمارات المتحدة، .2012

17-محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الأنترنت : الأحكام الموضوعية والأحكام الجزائية، د ط، منشورات حلبي الحقوقية، بيروت، 2010.

18- محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، د ط، دار الجمهورية للصحافة، مصر، .2010

19- مختار شبيلي، الجهاز العالمي لمكافحة الجريمة المنظمة، ط2، دار هومة للنشر والتوزيع،الجزائر، 2016.

20- مصطفى خالد الرواشدة ، جريمة الابتزاز الإلكتروني في القانون الأردني، د ط، مركز الكتاب الأكاديمي، عمان، الأردن، .2020

21- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة) ، د ط، دار الفكر الجامعي، الإسكندرية، .2006

22- نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، د ط، المؤسسة الحديثة للكتاب، بيروت، 2011

23- نظام توفيق المجالي ، شرح قانون العقوبات القسم العام : دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية، ط6، دار الثقافة للنشر والتوزيع، عمان، .2005

24-هشام محمد فريد رستم، الجوانب الإجرائية لجرائم المعلوماتية (دراسة مقارنة) ، د ط، مكتبة الآلات الحديثة، مصر، 1994.

ثانيا: الأطروحات والمذكرات الجامعية

أ-رسائل الدكتوراه:

1- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة لنيل شهادة الدكتوراه، تخصص قانون العقوبات والعقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 01، باتنة، 2016.-2015

2- عبد الوهاب ملياني، أمن المعلومات في بيئة الاعمال الإلكترونية، رسالة لنيل شهادة الدكتوراه، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، .2011

3- فوزي عمارة، قاضي التحقيق، رسالة لنيل شهادة الدكتوراه في العلوم، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الإخوة منصوري، قسنطينة، 2009-.2010

4- لمين علوطي، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، أطروحة لنيل شهادة الدكتوراه، تخصص إدارة الأعمال، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، 2008.-2007

5- محمد حمزة بن عزة، المسؤولية القانونية لمتعاملي الأنترنت (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، تخصص علوم قانونية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2018-2019.

ب-المذكرات الجامعية:

1- سارة محمد حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الماجستير، تخصص قانون عام، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، 2020.

2- طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي (دراسة مقارنة)، رسالة لنيل شهادة الماجستير، تخصص قانون عام، كلية القانون والعلوم السياسية، جامعة كركوك، العراق، .2021

3- محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت (دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية)، رسالة لنيل شهادة الماجستير، قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، .2004

4- يوسف صغير، الجريمة المرتكبة عبر الأنترنت، رسالة لنيل شهادة الماجستير، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013

5- ابتسامبوبعاية، التحقيق في الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون الإعلام الآلي والأنترنت، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022.

6- الحسن الحسن، شعيب حداد، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مذكرة لنيل شهادة ماستر مهني في القانون العام، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022-2023

7-الزوبير خلفي، الجرائم الماسة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الشيخ العربي التبسي، تبسة، 2022-2023.

8- أمينة بوشعرة، سهام مرساوي، الإطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2017-2018.

9-أمال برحال، جريمة الابتزاز الإلكتروني عبر الوسائل الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة،2020

10- خلود فرحاتية، دور الدليل الرقمي في إثبات الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون إعلام آلي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022.

11-دحمان عدلي، سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، 2020-2021.

12- ريمة بودراع، نعيمة بوحموش، جرائم وسائل التواصل الاجتماعي وآليات مكافحتها، مذكرة لنيل شهادة الماستر، تخصص المهن القانونية والقضائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2022-2023.

13- زهية معمش، غانم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر، تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة، بجاية، 2012-2013.

14- طيب وردي، الاختصاص القضائي في جرائم الأنترنت، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الطاهر ملاي، سعيدة، 2014-2015.

15- عبد الرؤوف بوديسة بجاد، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2021-2022.

16- عمار حمبلي، دليلة عمار، جرائم تقنية المعلومات في ظل الاتفاقية العربية 2011 والتشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021-2022.

17- فريدة سعيد عثماني، نورة بن عيسى، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية (دراسة مقارنة)، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة يحي فارس، المدية، 2021.-2020

18- ليلة حرزون، أسماء هدروق، التنظيم القانوني للجريمة الإلكترونية طبقا لأحدث التعديلات في القانون، مذكرة لنيل شهادة الماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2021-2022

19- يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2016-2017.

20-دحمان عدلي، سعد الدين ثامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم الجنائية، جامعة زيان عاشور، الجلفة،2020-2021..

ثالثا: المقالات والمجلات

1-أحمد قاسم فراح، "النظام القانوني لمقدمي خدمات الأنترنت (دراسة تحليلية مقارنة)"، **مجلة المنارة**، المجلد 13، العدد 09، 2007، ص ص 1-16.

2-أسامة غربي، "جرائم الأنترنت بين الجانب التقني وأساليب المكافحة"، **مجلة الحقوق والحريات**، العدد 02، 2015، ص ص 33-50.

3-أمال بيدي، "جهود الأمم المتحدة في مكافحة الجريمة السيبرانية"، **مجلة البحوث والحقوق والعلوم السياسية**، المجلد08، العدد01،سنة2022، ص ص 299-316.

4-أحمد عبد الاله عبد الحميد عبد الرحيم المراغي،" المسئولية الجنائية لمقدمي خدمات الإنترنت (دراسة تحليلية خاصة لمسئولية مزودي خدمات الاتصالات الإلكترونية"، مجلة حقوق حلوان للدراسات القانونية والاقتصادية، المجلد 42، العدد 42 -الرقم المسلسل للعدد 42 يناير 2020،

5-الطاهر ياكر، "مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية"، **مجلة الصدى للدراسات القانونية والسياسية**، المجلد 04، العدد 04، 2022، ص ص 1-39.

6-الطيبي البركه،"إشكالية الإثبات في الجرائم الإلكترونية"، **مجلة آفاق علمية**، المجلد 11، العدد 01، 2019، ص ص 266-284.

7-أمينة لميز، "الدليل الرقمي كآلية لإثبات الجرائم المعلوماتية"، **مجلة بحوث القانون والتنمية**، المجلد 02، العدد 03، جوان 2023، ص ص 10-18.

8-باقر غازي حنون، حسن حماد حميد، "جريمة الابتزاز الإلكتروني (دراسة مقارنة)، **مجلة دراسة البصرة**، العدد 42، كانون الأول 2021، ص ص 48-.92

9-حدة أبو خالفة، "النظام القانوني لمتعهد الإيواء عبر الأنترنت في القانون الجزائري والأردني (دراسة مقارنة)"، **مجلة دراسات علوم الشريعة والقانون**، المجلد 45، العدد 04، الملحق 02 ، 2018، ص ص 157-167.

10-حدة بوخالفة، "المسؤولية الجزائية لمتعهد الدخول عبر الأنترنت"، **مجلة الدراسات القانونية**، المجلد 06، العدد 01، 2020، ص ص 1-17.

11-رشيد بن فريحة، يوسف مهوب،"التحري الجنائي في مسرح الجريمة الإلكترونية"، **مجلة جامعة القدس المفتوحة للأبحاث والدراسات**، مجلد01 ، العدد 42 ،الجزء الأول،تشرين الثاني 2017، ص ص 52-60.

12-سليمان قطاف، "الآليات القانونية والموضوعية لمكافحة الجرائم الشيبانية في ظل اتفاقية بودابست والتشريع الجزائري"، **المجلة الأكاديمية للبحوث القانونية والسياسية**، المجلد 06، العدد 01، 2022/03، ص ص 334-358.

13-سكينة فروج، عبد الرحمان خلفي، "أثر النتيجة الإجرامية على التفريد العقابي"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد 07 ، العدد02، ديسمبر 2022

14-عادل بوزيدة، "دور الشهادة الإلكترونية في الإثبات الجزائي على ضوء قانون الإجراءات الجزائية الجزائري"، **مجلة النبراس للدراسات القانونية**، المجلد 01، العدد 01، سبتمبر 2016، ص ص 134-151

15-عبد القادر فلاح، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد 04، العدد 02، جافني 2020، ص ص 1689-1708.

16-عبد القادر فلاح،" حجز وحفظ المعطيات في الجريمة الإلكترونية"، **مجلة صوت القانون**، المجلد08، العدد 01 ،2021، ص ص 177-194.

17-عبير بعقيقي، فيصل نسيغة، "الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04"، **مجلة العلوم القانونية والسياسية**، المجلد 09، العدد 02، جوان 2018، ص ص 34-.49

18-عيدة بلعابد، "خصوصية التحقيق في الجرائم المعلوماتية"، **مجلة الباحث الأكاديمي في العلوم القانونية والسياسية**، العدد 06، مارس 2021، ص ص 130-.158

19-فاروق خلف، "الآليات القانونية لمكافحة الجريمة المعلوماتية"، **مجلة الحقوق والحريات**، العدد 02، 2015، ص ص 7-21.

20-كريم معروف، "المشكلات الإجرائية التي تواجه المحقق الجنائي في الجرائم السيبرانية"، **المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي**، المجلد 04، العدد 02، 2022، ص ص 1-10.

21-كمال بوشليق، "النظام القانوني للإنابة القضائية في التشريع الجزائري"، **المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية**، المجلد 12، العدد 03، ص ص 571-580.

22-محمد سعيد عبد العاطي محمد، محمد أحمد المشاوي محمد، "دور القانون الجنائي في حماية الطفل من الابتزاز الإلكتروني (دراسة مقارنة)"، **مجلة البحوث الفقهية والقانونية**، العدد 36، أكتوبر 2021، ص ص 123-178.

23-محمد لموسخ، "تنازع الاختصاص في الجرائم الإلكترونية"، **مجلة دفاتر السياسة والقانون**، العدد 02، 2009، ص ص 151-167

24-مريزق عدمان، أ.بوقلاشي عماد، "الأمن المعلوماتي في ظل التجارة الإلكترونية: إشارة إلى حالتي تونس والجزائر"، **مجلة الاقتصاد الجديدة**، العدد 03، ماي 2011، ص ص 07-25.

25-مريم عراب، "جريمة التهديد والابتزاز الإلكتروني"، **مجلة الدراسات القانونية المقارنة**، المجلد 07، العدد 01، 2021، 1205-1234.

26-مصطفى قرزان، زرقين عبد القادر، "الآليات الدولية لمكافحة الجريمة الإلكترونية"، **مجلة صوت القانون**، المجلد 08، العدد 02، ص ص 1222-1244.

27-نور الهدى قادري، "الشهادة الإلكترونية وحجيتها في الإثبات"، **مجلة الفكر القانوني والسياسي**، المجلد 07، العدد 01، 2023، ص ص 1592-1604.

28-هانية بوشارب، بن شهرة شول، "صعوبة عملية استخلاص الدليل الإلكتروني"، **مجلة الدراسات القانونية والسياسية**، المجلد 09، العدد 01، جانفي 2023، ص ص 67-77

رابعا: الملتقيات

1- إلهام بن خليفة، "مداخلة بعنوان القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال"، الملتقى الوطني حول (مواجهة الجريمة المعلوماتية)، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخظر، الوادي، يوم 26 فيفري 2019، ص ص 1-15.

2- دنيا عبد العزيز فهمي، "المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي"، بحث مقدم للمؤتمر العلمي الرابع تحت عنوان (القانون والإعلام)، كلية الحقوق، جامعة طنطا، 23-24 أبريل 2017، ص ص 212-.382

3- عز الدين عز الدين، "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها"، بحث مقدم إلى أعمال الملتقى الوطني حول (الجريمة المعلوماتية بين الوقاية والمكافحة)، 16-17 نوفمبر 2015، جامعة بسكرة، الجزائر.

4- فتيحة سويسي، "التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها"، مداخلة مقدمة في الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، 18 جانفي 2020، ص ص 1-.32

5- كاهنة لرول، "تحديد بعض مصطلحات الأمن المعلوماتي"، أعمال الملتقى الوطني حول (الأمن المعلوماتي: مهدداته وسبل الحماية) ، كلية الآداب واللغات، جامعة مولود معمري، تيزي وزو، 03-04 نوفمبر 2015، ص ص 75-86.

6- هواري عياش، "مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ومكافحتها"، المعهد الوطني الأدلة الجنائية وعلم الإجرام، كلية الحقوق، جامعة بسكرة، 2016، ص ص 1-15.

خامسا: النصوص القانونية

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996، منشور بموجب المرسوم الرئاسي رقم 96-438، مؤرخ في 07 ديسمبر سنة 1996، ج ر ج ج عدد 76، صادر في 08 ديسمبر سنة 1996، معدل ومتمم بالقانون رقم 02-03، مؤرخ في 10 أفريل سنة 2002، يتضمن التعديل الدستوري، ج ر ج ج عدد 25، صادر في 14 أفريل 2002، معدل ومتمم بالقانون رقم 08-19، مؤرخ في 15 نوفمبر سنة 2008، يتضمن التعديل الدستوري، ج ر ج ج عدد 63، صادر في 16 نوفمبر سنة 2008، معدل ومتمم بالقانون رقم 16-01، مؤرخ في 06 مارس سنة 2016، يتضمن التعديل الدستوري، ج ر ج ج عدد 14، صادر في 07 مارس سنة 2016، معدل بالتعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020 في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، صادر بموجب المرسوم الرئاسي رقم 20-442، مؤرخ في 30 ديسمبر سنة 2020، ج ر ج ج عدد 82، صادر في 30 ديسمبر 2020.

2-قانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر ج ج رقم 47، المؤرخة في 16 أوت 2009.

3-القانون رقم 2000-03 المتضمن القواعد العامة المتعلقة بالبريد والاتصالات السلكية واللاسلكية، الصادر في 06 أوت 2000، ج ر ج ج، عدد 48، المؤرخة في 06 أوت 2000.

4-الأمر رقم 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية الجزائري، ج ر ج ج رقم 48، الصادر بتاريخ 1966/06/10، معدل ومتمم.

5-الأمر رقم66-156، مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966، يتضمن قانون العقوبات، ج ر ج ج عدد 49 صادر في 21 صفر عام 1386 الموافق 11 يونيو سنة 1966، معدّل ومتمّم.

6-المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004، المتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، ج ر ج ج عدد 84، المؤرخة في 29 ديسمبر 2004.

7-مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 الموافق 08 .سبتمبر سنة 2014 يتضمن التصديق على الإتفاقية العربية لمكافحة جرام تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2012، منشور في ج ر ج ج، العدد 57 ، المؤرخة في:04 ذو الحجة عام 1435 الموافق 28 سبتمبر 2014.

8-المرسوم التنفيذي رقم 06-348 مؤرخ في 5 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر ج ج رقم 63، المؤرخة في 08 أكتوبر 2006.

9-المرسوم التنفيذي رقم98 -257 المؤرخ في 03 جمادى الأولى عام 1419 الموافق لـ25 غشت 1998 المتضمن ضبط شروط وكيفيات إقامة خدمة الأنترنت واستغلالها، ج ر ج ج، عدد 63 ، المؤرخة في 04 جمادى الأولى عام 1419 الموافق لـ 26 غشت سنة 1998.

سادسا: المو اقع الإلكترونية

httpsM//mawdoo3.com.
http://www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html
http://WWW.un.org/arabic/documents/instruments/subj_ar.asp.
https://ar.wikipedia.org/wiki/

https://www.alarabiya.net/saudi-today/2013/12/05

https://www.moi.gov.sa

https://www.psd.gov.jo/index.php/ar/2020-02-05

https://alghad.com

https://x.com/Law3li/status/1197221360092745730

https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719

https://trc.gov.jo/EchoBusV3.0/SystemAssets

https://elmo7amy.tv/wp-content/uploads/2023/04/كود-العقوبات-المصرى-pdf.pdf

https://www.mohamah.net/law

https://www.dampress.net/mobile/?page=show_det&category_id=48&id=62342

https://www.law-house.net

https://mawdoo3.com/

https://www.wipo.int/wipolex/ar/legislation/details/6393

https://manshurat.org/node/31487

https://uaelegislation.gov.ae/ar/legislations/1526/download
https://www.lob.gov.jo/?v=3&lang=ar#!/LegislationDetails?LegislationID=3398&LegislationType=2&isMod=false
https://rm.coe.int/budapest-convention-in-arabic/1680739173

https://ar.wikipedia.org/wiki/
https://www.moi.gov.sa

https://www.alarabiya.net/saudi-today/2013/12/05

https://alghad.com

II-المراجع بالغة الأجنبية

1-AI SALAH Ibtisama, « Le cadre procédural pour le crime de chantage électronique dans la législation pénale jordanienne », Journal of Ethical and Regulatory Issues, Volume 24, Numéro Spécial 6, 2021, PP

2-CHAMPAGNAT Adeline, l'office central de lutte contre la criminalité liée auxtechnologies de l'information et de la communication, revue de cybercriminalité cyber menace et cyber fraude, sous la direction de lrènebouhadana et William grilles, Edition IMODEU, Paris, 2012.

3-CHAT Le Nguyen, GLOMMA Wilfred, Diffusion of the Budapest Convention on cybercrime and development of cybercrime legislation in pacific island countries: «law on the book's" " law action" computer law and security review, 2021.

4-DUBUISSON Bernard Pierre Jadoul, la responsabilité Civile liée à l'information et au Conseil- questions d'actualités, publication des facultés Universitaires Saint-Louis, Bruxelles, 2000.

5-FERAL-SCHUL Christiane, le droit à l'épreuve, 6m éditions, Dalloz, Paris, France, 2010.

6-GÜLTAN Güz, Electronic Evidence, master thesis, Department of private law, faculty of law , university of Oslo.

7-HAIDAR Ali, the Basic Concept Cybercrime Journal of Technology Innovations and Energy, the wise publicher, April 2022, United States.

8-QUEMENER Myriam, cybercriminalité, droit pénal appliqué, édition èconomica, Paris, 2010.

9-QUEMENER Myriam, La coopération entre les organes de lutte contre la cybercriminalité pour une stratégie de cyber sécurité français, revue de Lamy droits des affaires, num 87, France, 2013.

10-SCHOEN Gérard, La douane face à la cybercriminalité • Revue de cyber criminalité opbermenace et cyber fraude, Sous la direction de Irenebouhadana et William dgilles, édition lmodev, Paris, 2012.

الفهرس

الملخص:

أصبحت جريمة التهديد الإلكتروني مع التطور التكنولوجي صورة من صور الجرائم الإلكترونية، التي تخترق المجتمع وتهدد أمنه واستقراره. كما تسبب في هدم أهم ركائزه المتمثلة في الحريات الفردية المكرسة في متن القوانين الوطنية والدولية، والمحافظة على الأسرة والمجتمع بشكل عام. ولعل جوهر تجريم التهديد الإلكتروني وأساسه يكمن فيما يتضمنه من تهديد وضغط على إرادة المجني عليه، للقيام بأعمال ما كان ليقوم بها لو كانت إرادته حرة، سواء أكانت تلك الأعمال مشروعة أم غير مشروعة. وهو ما ذهبت إليهمعظم الدولالعربية والأجنبية إلى الإسراع بتجريم هذه الظاهرة، سواء بالنص عليها في قوانين خاصة بالجرائم الإلكترونية، أوبتعديل نصوصها التقليدية وتضمينها تجريم التهديد الإلكتروني والعمل على مكافحتها بكل الوسائل.

Résumé :

Avec l’innovation de la technologie, la menace par voie électronique est devenue une forme de cybercriminalité qui menace la sécurité de la société. Cela a également peut provoquer la destruction de la préservation de la famille et de la société en général.

Les bases de la criminalisation des menaces par voie électronique résident dans la menace et la pression qu’elles contiennent sur la volonté de la victime, d'accomplir des actes qu'elle n'aurait pas accomplis si sa volonté était libre, que ces actes soient légaux ou illégaux. C'est ce qu'ont fait la plupart des pays arabes et étrangers, pour accélérer la criminalisation de ce phénomène, soit en le stipulant dans des lois spécifiques aux crimes électroniques, soit en modifiant leur textes traditionnels et en incluant la criminalisation des menaces électroniques et en œuvrant pour la combattre par tous moyens.