جامعة آكلي محند اولحاج– البويرة–
كلية الحقوق والعلوم السياسية
قسم القانون العام

جريمة الابتزاز والتهديد عبر الانترنت في التشريع الجزائري

مذكرة تخرج لنيل شهادة ماستر في الحقوق

تخصص: قانون جنائي وعلوم جنائية

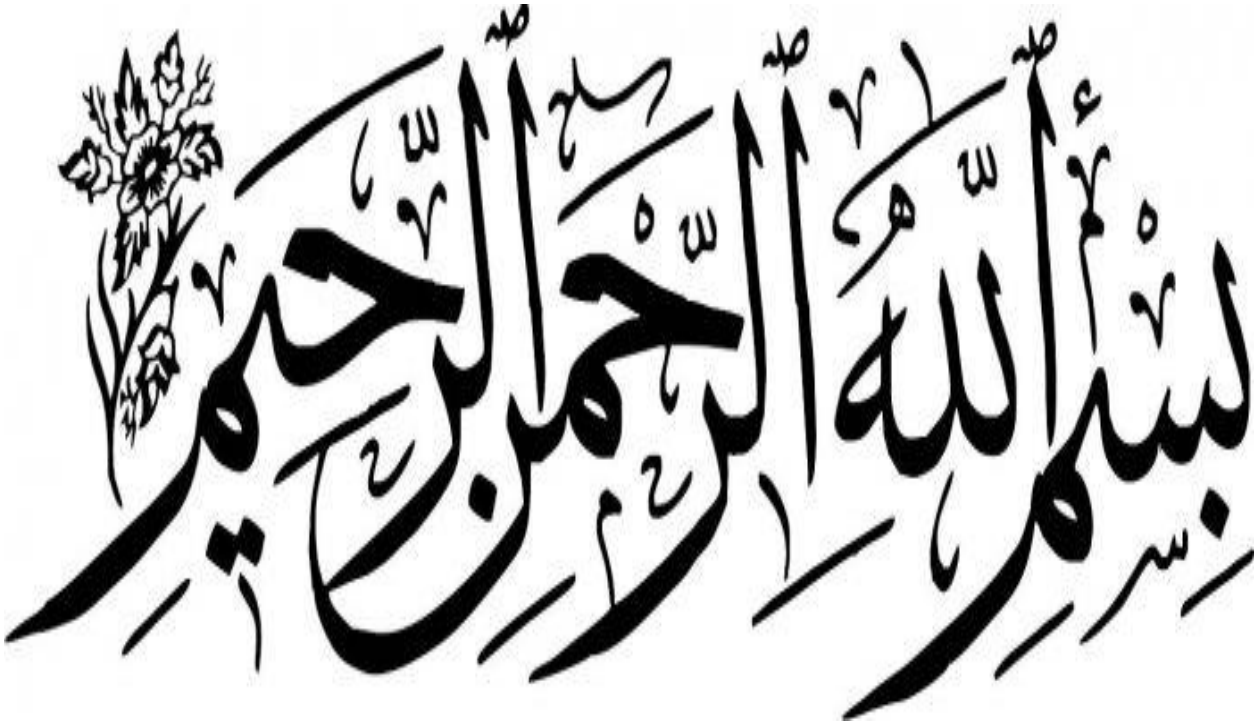
إعداد الطالبتان:
- صفاح زكية
- إبراهيمي ويداد

إشراف الأستاذة:
أ. غضبان نبيلة

أعضاء لجنة المناقشة

الاستاذة : د/ عيساوي فاطمة ..... رئيسا
الاستاذة: د/ غضبان نبيلة .....مشرفا ومقررا
الاستاذة : د/ آيت بن عمر صونيا ..... ممتحنا

السنة الجامعية:2024/2023


بسم الله الرحمن الرحيم

شكر وعرفان

الشكر والحمد لله الذي منحنا القدرة على إنجاز هذه المذكرة وأنار لنا دربنا ووفقنا وأنعم علينا بنعمة

طلب العلم وفتح لنا أبواب البحث العلمي.

والشكر موصول إلى لجنة المناقشة وإلى كل أستاذ أفادنا بعمله

كما نرفع كلمة الشكر إلى الدكتورة المشرفة "د. نبيلة غضبان" على سعة صدرها.

شكرا لكم على المساهمة في إنجاز هذا الموضوع.

كما نشكر كل من مدّ لنا يد العون من قريب أو من بعيد.

إهداء

أهدي ثمرة جهدي ...

إلى روح جدتي دريسي الزهرة وإخوتي سيدعلي وبلال رحمهم الله عز وجل سائلة المولى تعالى أن يتغمدهم بواسع رحمته ويسكنهم فسيح جناته.

إلى التي صبرت وسهرت وتعبت ... إلى أمي الغالية أمدها الله بالصحة والعافية وأطال الله في عمرها.

إلى سندي بعد الله عز وجل ... أبي أمده الله بالصحة والعافية وأطال الله في عمره.

سندي ومسندي وضلعي الثابت الذي لايميل ... أختي الوحيدة مريم.

إلى الذين شد الله عضدي بهم ... إخوتي مهدي، هشام.

إلى جدي وجدتي أطال الله في عمرهم.

سندي وأمهاتي بعد أمي ... إلى عماتي مباركة، سعيدة، حياة.

وإلى جميع عائلتي وأصدقائي.

زكية

إهداء

أهدي ثمرة جهدي المتواضع ...

إلى من لا يمكن للكلمات أن توفي حقهما إلى الوالدين الكريمين رزقنا الله برهما وأطال الله في عمرهما " أبي وأمي"

إلى سندي في الحياة " زوجي"

إلى قرة عيني إبني " آدم "

إلى نفسي القوية العظيمة التي تحملت كل الفترات وأكملت رغم كل الصعوبات

إلى إخوتي الأعزاء

ولكل من أعطاني يد العون من قريب أو من بعيد وساعدني في إنجاز هذه المذكرة .

ويداد

مقدمة

مقدمة:

يعرف العصر الذي نعيش فيه اليوم بعصر المعلومات، وهو العصر الذي يعرف انفجارا في حجم المعلومات وسرعة وسهولة انتشارها وتداولها بين الأشخاص، وقد ساهم هذا الانتشار المذهل للتكنولوجيا الحديثة وبشكل خاص الحاسوب والهواتف الذكية والتي تساعد في نشر وتبادل المعلومات في أشكال مختلفة من صور وملفات وأحاديث ... وغيرها.

وقد ساهم هذا التطور المعاصر في تبادل المعلومات إلى إحداث سلوكيات مشروعة وغير مشروعة في جميع المجالات التي تتعلق بالفرد والمجتمع وقد يؤدي الاستخدام المفرط لهذه المواقع إلى تدني المنظومة القيمية نتيجة للتأثير بالثقافات المفتوحة، فنظرا لتقدم وتطور التكنولوجيا وظهور ما يسمى بوسائل التواصل الاجتماعي وعلى رأسها الفايسبوك والتويتر والأنستغرام ...الخ والتي أدت إلى سرعة انتشار الأخبار حتى أصبح العالم قرية صغيرة، وإلى كثرة انتشار الصور حتى أصبحت الصورة تضاهي ألف كلمة هذا ما أدى إلى ظهور العديد من الجرائم الإلكترونية والتي تمس حرمة الحياة الخاصة وعلى رأسها جريمة الإبتزاز والتهديد عبر الانترنت.

أصبحت جريمة الإبتزاز والتهديد الإلكتروني ظاهرة تخترق المجتمع وتهدد دعائمه وتضرب في مقتل أهم أهداف أي مجتمع متحضر في تحقيق الأمن لأفراده، فقد يسعى المجرمين في هذا المجال إلى التعدي على حقوق الأفراد في الخصوصية واستغلالهم على غير وجه حق والضغط على الضحية بكشف أسرار من شأنها أن تضره مما يؤدي به إلى الانصياع والإذعان لرغبة الجاني وتحقيق مطالبه المشروعة وغير المشروعة تحت الإكراه والخوف من الفضيحة ،و هذا ما أدى بالمشرعين في العديد من الدول إلى سن قوانين تجرم السلوك الإجرامي المتمثل في جريمة الإبتزاز والتهديد الإلكتروني.

والمشرع الجزائري لم يتطرق لهذه الجريمة بصفة خاصة غير أنه قام على تطوير المنظومة القانونية فيما يخص المعلوماتية ،حيث أصدر تشريعات تواكب التطور الحاصل في المجال التكنولوجي ،و من أبرز هذه التعديلات ما ورد في القانون 15/04 المؤرخ في 10 نوفمبر 2004 المتضمن "جرائم المساس بأنظمة المعالجة الآلية للمعطيات "،ثم القانون 04/09 المؤرخ في 05 سبتمبر 2009 المتضمن "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا

الإعلام والاتصال "،و كذا القانون رقم 07/18 المؤرخ بتاريخ 10 جوان 2018 المتعلق "بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي".

وبالرجوع إلى قانون العقوبات الجزائري نجده أدرج جريمة التهديد في الباب الثاني، القسم الثاني تحت عنوان "التهديد" وأيضا القسم الخامس تحت عنوان (الإعتداء على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار).

إن هذا النوع من الجرائم المتصلة بالانترنت هو ظاهرة إجرامية حديثة النشأة اكتنفها العديد من الغموض والذي أدى إلى القول بأنها جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها ،لذا تراءى لنا الخوض والبحث في هذا الموضوع من أجل الاستزادة العلمية في هذا المجال والعمل على بيان خطورة الجرائم الإلكترونية وبالتحديد التهديد والإبتزاز وما قد تؤدي إليه من أخطار جسيمة على حياة الشخص بصفة خاصة وعلى الأمن والنظام داخل الدولة وخارجها بصفة عامة.

أما عن أسباب اختيارنا لهذا الموضوع فتعود بالأساس إلى أسباب ذاتية كون الموضوع يعالج ظاهرة إجرامية تهدد المجتمع واستقراره، وأسباب موضوعية نابعة من طبيعة الموضوع والذي يعد موضوع حيوي بحاجة إلى المزيد من التأمل والدراسة والرغبة في إضافة نوعية في هذا المجال، بالإضافة ان جريمة الابتزاز والتهديد سجلت معدلات هائلة في مختلف دول العالم وبالخصوص في الجزائر، وأكثر الفئات المستهدفة في هذه الجريمة هم الفتيات مما أدى إلى دق ناقوس الخطر ومحاولة إيجاد سبل لمكافحتها والحد منها.

ما مدى نجاعة النصوص القانونية التي جاء بها المشرع الجزائري لمواجهة جريمة الابتزاز والتهديد عبر الانترنت؟

وللإجابة على هذه الإشكالية تم تقسيم الموضوع إلى فصلين ،حيث نتطرق في الفصل الأول إلى الجانب المفاهيمي لجريمة الإبتزاز والتهديد عبر الانترنت ،في حين سيخصص الفصل الثاني للإطار القانون لجريمة الإبتزاز والتهديد عبر الانترنت.

وبالنسبة للدراسات السابقة فعلى الرغم من أهمية الموضوع وحيويته إلا أنه لم ينل ما يستحقه من العناية والاهتمام، فلم نجد المراجع الكافية لدراسة الموضوع جريمة الابتزاز والتهديد عبر الانترنت خاصة الدراسات المتعلقة بالتشريع الجزائري فهي قليلة نوعا ما مقارنة بالتشريعات المقارنة.

أما عن المناهج المتبعة في دراستنا لهذا الموضوع فتتمثل في المنهج الوصفي وذلك من خلال التعريف بجريمة الإبتزاز والتهديد عبر الانترنت والوقوف على عناصرها ،و المنهج التحليلي للوقوف على الحماية القانونية التي وفرها المشرع لمواجهة هذه الجريمة ومن ثم حماية هذا الحق من خلال تحليل مختلف النصوص القانونية المتعلقة بالموضوع.

رفصل الاول

الإطار المفاهيمي لجريمة الابتزاز والتهديد عبر الانترنت

بعد انتشار الانترنت وتوسع استخدام التكنولوجيا ليشمل العالم برمته – حيث يستخدم حوالي 5،18 مليار شخص في العالم الانترنت ما يمثل نسبة تقارب 64،6% من سكان العالم البالغ عددهم 8،03 مليار نسمة – أصبحت التطبيقات والبرامج الالكترونية جزءا لا يتجزأ من حياة المجتمعات، هذا الانتشار المذهل ساهم في تعزيز التواصل الحضاري وكسر حواجز العزلة الاتصالية بين الشعوب.

مع كل هذه الفوائد هناك ايضا جوانب سلبية، فقد ساعد هذا التطور الذي جلبته التكنولوجيا في نقل بعض الانشطة الاجرامية من العالم الواقعي إلى عالم الافتراضي وبما أن هذا العالم غير مراقب بنفس الطريقة التي يتم فيها مراقبة العالم المادي، فإنه أصبح بمثابة ملاذا للأنشطة الاجرامية.

من بين هذه الانشطة نجد التعدي على خصوصية الأفراد واستغلالها في اغراض غير شرعية، حيث يمارس الجناة الضغط على الافراد بواسطة استغلالهم بصورهم أو معلومات شخصية وتهديهم بنشرها على الانترنت اذا لم يتم الوفاء بمطالبهم كما يمكنهم استخدام التهديد بالتشهير أو الاساءة لسمعة الأفراد أو المؤسسات كوسيلة لابتزازهم لتحقيق مكاسب مادية أو معنوية .

وبالرغم من أن التهديد والابتزاز لهما وجود في العالم الحقيقي،إلا أن الانترنت قد أعطى لهم مساحة أكبر للعمل دون أن يلفت انتباه السلطات الأمنية والقضائية .

المبحث الأول

مفهوم جريمة الابتزاز والتهديد عبر الانترنت

في نهاية القرن العشرين وبداية القرن الواحد والعشرين ازداد الطلب على شبكة المعلوماتية، أصبحت الدول تتسارع وتتنافس على تطور تكنولوجيا الاتصال بصفة عامة وشبكة الانترنت بصفة خاصة.

وفي يومنا هذا هناك عدة طرق لاتصال شبكة الانترنت للحصول وتبادل البيانات الخاصة الاتصال وإرسال الرسائل القصيرة فقط بل وصلت الى تطبيقات التعارف ومواقع التي وصلت لمرحلة من التقدم حيث جمعت عدة استخدامات ومواصفات تتعدى مرحلة التواصل الاجتماعي والمنصات التي تسمح بالتفاعل وتبادل والمشاركة، مما يجعلها تحتل الصدارة من حيث عدد المستخدمين بحيث وصل عدد مستخدميها 4,74 مليار مستخدم[1] منها Facebook و Instagram و Telegram و Imo .

كثيرا ما نجد من الأشخاص يضعون معلوماتهم الشخصية وصورهم وفيديوهاتهم في هذه المواقع والمنصات حتى إنها قد تكون سرية في بعض الأحيان ، وتكون عرضة للمتطفلين والهاكرز[2] الأسوء من ذلك ان الكثير من المراهقين والأطفال كانوا صيدا سهلا للابتزاز والتهديد والتغرير من قبل مجرمي الانترنت.

1- مات أليغرين، إحصائيات واتجاهات وسائل التواصل الاجتماعي[تحديث 2024] تم تحريره والتحقق من صحته بواسطة فريق WSR ،8 مايو 2024، مقال منشور علعلى موقع الكتروني ،رابط الموقع الالكتروني: WWW.Websiterating.com تاريخ الإطلاع: 2024/05/31، ساعة 12:25.

2- يصنف مجرمو الانترنت إلى: الهاكر: ويسمون بقراصنة الكمبيوتر وهم نوعان: 1 الهاكر الأمن: يستخدمون الحاسوب والانترنت لإختراق نظم الأمن والشبكات دون تخريب أو إتلاف، 2 الهاكر: وهو المخترق ذي النوايا الإجرامية يقوم بما هو سيئ كالتخريب والإرهاب والسرقة. المحترفون: تهدف اعتداءاتهم إلى تحقيق الكسب المادي أو لأغراض سياسية أو لتعبير على مواقفهم يتميزون بالتنظيم والتخطيط للأنشطة الإجرامية يتمتعون بسعة الخبرة والإدراك الواسع للمهارات التقنية. الحاقدون: تهدف إعتداءاهم للثأر والإنتقام تكون أغلب منشطاتهم باستخدام تقنية زرع الفيروسات والبرامج الضارة. طائفة صغار السن: ويطلق عليهم صغار نوابغ المعلوماتية وهم صغار السن مولعون بالحواسيب والاتصالات.

شكلت الجرائم التي ترتكب عبر الوسائط الالكترونية والتي عرفت بالجرائم الناعمة او جرائم العصر والجرائم المستحدثة تحديا كبيرا أمام الجهات القضائية وحتى أمام فقهاء القانون .

فتطرقنا في المطلب الأول: إلى مفهوم الابتزاز والتهديد المرتكب عبر الشبكة الانترنت والمطلب الثاني: طرق ووسائل الابتزاز والتهديد عبر الشبكة العنكبوتية.

المطلب الأول

تعريف جريمة الابتزاز والتهديد عبر الانترنت

تعتبر جريمة الابتزاز والتهديد من الجرائم التي تهدد الأمن والاستقرار تتجلى هذه الجريمة في قيام الجاني بتهديد الضحية بإفشاء أسرار أو معلومات خاصة أو بإلحاق ضرر به أو بأقاربه أو بممتلكاته، وذلك بهدف الحصول على مكاسب مالية أو حتى معنوية، تطور التهديد والابتزاز بتطور وسائل التواصل والتكنولوجيا، في الماضي كانت تتم هذه الجريمة بطرق تقليدية مثل الرسائل الخطية أو المواجهات المباشرة، ولكن مع دخول عصر التكنولوجيا شهدت هذه الجريمة كغيرها من الجرائم تحولا حيث أصبحت الانترنت ووسائل التواصل الاجتماعي ساحة جديدة لممارسة أفعالهم لمميزات تمنحها هذه التكنولوجيا.

وتكمن خطورة التهديد هنا في جعل ضحاياهم يقبلون على الانتحار أو القتل من قبل عائلاتهم في الوقت الذي يعرف احجام عن الابلاغ ورفع قضايا على المجرمين لأنه غالبا ما تكون هذه التهديدات والابتزازات محرجة للضحايا[1].

وقبل الخوض في غمار التحليل نحاول وضع تعريف للابتزاز والتهديد في الفرع الأول وفي الفرع الثاني تعريف الابتزاز والتهديد عن طريق الانترنت.

1- عبد المهين سالم بكر، الوسيط في شرح قانون الجزاء الكويتي القسم الخاص، مطبوعات جامعة الكويت، الكويت، 1979.

الفرع الأول: تعريف الابتزاز والتهديد:

أولا: تعريف الابتزاز blackmail:

أ/التعريف اللغوي للابتزاز: كلمة الابتزاز من أصل الفعل الثلاثي بزّ بالتشديد على الزاي فيقال:بز الشيء يبزه بزا بمعنى: اغتصبه ، والبز هو السلب أخذ الشيء بجفاء وقهر،و ابتززت الشيء أي سلبته [1]، قال الهروي: عرضته على الأزهري فقال هذا لاشيء كالابتزاز. وفي حديث " فيبتز ثيابي ومتاعي " أي يجردني منها ويغلبني عليها[2].

ب/التعريف الاصطلاحي لجريمة الابتزاز: تعددت التعاريف التي قدمها الفقه لهذه الجريمة فقد عرفه البعض على انه الضغط الذي يباشره الشخص على إرادة شخص آخر بحمله على ارتكاب جريمة معينة[3].

أي أن الهدف من الابتزاز هو الحصول على أسراره أو أشياء تخص حياته الشخصية قد تؤدي بالضحية إلى عقوبات أو القتل من طرف العائلة او غير ذلك .

وهناك من عرف الابتزاز على أنه الحصول على معلومات سرية أو صورة شخصية أو مواد فلميه تخص الضحية واستغلالها لأغراض مادية أو القيام بأعمال غير مشروعة كالحصول على المال أو منافع من الشخص وابتزازه بواسطة التهديد بفضح أسراره التي يمتلكها[4].

---

[1]- أبو الفضل جمال الدين محمد بكر(ابن المنظور)، معجم لسان العرب، دار صابر، لبنان، المجلد الثاني،حرف الباء.

[2]– محب الدين أبي فيض الزبيدي، تاج العروس من جواهر القاموس، دار الفكر، المجلد الثاني، باب (الزاي: السين) بيروت، 2005، ص 13.

[3]– أمال برحال، جريمة الابتزاز عبر الوسائط الالكترونية، مذكرة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، 2019-2020،ص 8.

[4]– محمد بن المحسن بن شلهوب، جريمة الابتزاز الالكتروني -دراسة مقارنة-، بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية شعبة الأنظمة، جامعة الإمام محمد بن سعود الإسلامية، 2011، ص 59.

وفي تعريف آخر عرف الابتزاز على أنه القيام بتهديد شخص بفضح أمره ما لم يستجيب المهدد إلى تنفيذ طلبات المبتز وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس بالشرف أو الكرامة أو تتعلق بحرمة الحياة الخاصة للشخص الذي تم ابتزازه[1].

ثانيا تعريف التهديد the threat:

أ/ التعريف اللغوي للتهديد: يقال هدده يهدده تهديدا أي خوفه وتوعده بالعقوبة او الجزاء[2].

ب/ التعريف الاصطلاحي لجريمة التهديد: هناك عدة تعارف منها:

1- التهديد هو كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء او نسب أمور مخدشة للشرف ، وقد يحمله التهديد تحت تأثير ذلك الخوف إلى إجابة الجاني إلى متى اصطحب التهديد بطلب[3].

2- هو الوعيد بشر يصيب المجني عليه مهما كانت الوسيلة التي توسل بها الجاني ، سواء بالاعتداء على نفسه أو ماله او عرضه ، مما يحدث الرعب في نفسه فكل فعل مادي او حتى قول يشكل اعتداء على حرية وامن المجني عليه يعتبر تهديدا[4].

3- هو ترويع المجني عليه وإلقاء الرعب في قلبه بتوعده بإنزال شر معين به[5].

ومن هذه التعريف يتضح إن الابتزاز والتهديد هو عملية ضغط وممارسة الإكراه المعنوي من طرف المبتز أو المُهدِد على المُهدد ،وذلك بالضغط على إرادته بأشياء تمس ماله أو شرفه واعتباره أو أسرار تمس خصوصيته.

فيكون إما كتابا أو شفهيا ، فالكتابي بقيام الجاني بإرسال رسائل نصية مكتوبة على الورق أو رسالة نصية عبر الجوال وذلك عبر شريحة الهاتف أو عبر احد الوسائل التواصل الاجتماعي أو عبر الحاسب الآلي ،لدفع الجاني بالقيام بالفعل أو الامتناع عن القيام بالفعل.

---

[1]- ممدوح رشيد مشرف العنزي، الحماية الجنائية للمجني عليه من الابتزاز الالكتروني، مجلة العربية للدراسات الأمنية، المجلد 33، العدد 70، الرياض، 2017، ص 199.

[2]- أبو الفضل جمال الدين محمد بكر(ابن المنظور)، المرجع السابق، ص 36.

[3]- حسن صادق المرصفاوي، شرح قانون العقوبات، القسم الخاص، منشأة المعارف الإسكندرية، 1975، ص 14.

[4]- نجم محمد صبحي، الجرائم الواقعة على الأشخاص، ط 01، مكتبة دار الثقافة، القاهرة، 1994، ص 153.

[5]- الدرة ماهر عبد الشويش، شرح قانون العقوبات، القسم الخاص، ط 02، شركة العاتك لصناعة الكتاب، القاهرة، 2009، ص 223.

أما الشفهي يتحقق بتلقي المجني عليه التهديد مباشرة من الجاني او بالإشارة أو التلميح يسعى من خلاله إلقاء الرعب والاضطراب في نفس الجاني[1].

وبالرجوع للمشرع الجزائري فقد أدرج جريمة التهديد في القسم الثاني تحت عنوان التهديد من قانون العقوبات في المواد 284 و285 و286 و287 وفي الفصل الثالث للجنايات والجنح ضد الاموال القسم الأول السرقات وابتزاز الأموال من ذات القانون في المادة 371، فعدد المشرع في هذه المواد أنواع التهديد والعقوبات وهي: التهديد بواسطة محرر، التهديد الغير المصحوب بشرط أو أمر، التهديد الشفهي المصحوب بأمر أو شرط، التهديد بأي عمل من أعمال العنف، التهديد بالتشهير[2].

الفرع الثاني: تعريف جريمة الابتزاز والتهديد عبر الانترنت وخطورته

تطور التهديد والابتزاز بتطور الوسائل التكنولوجيا، حين كانت مسرح هذه الجريمة أرض الواقع انتقلت إلى المسرح الافتراضي وشبكة معلوماتية لامتناهية لا يحكمها نظام ولا قانون، كل مزياها التطور والسرعة وسهولة التلاعب ومحو أي آثار لجريمة حدثت من خلالها، فالتهديد التقليدي في غالب الأحيان يكون الهدف منه مادي يترك آثار نفيسة مثل الخوف والتوتر، أما التهديد والابتزاز الالكتروني يخلف آثار نفسية وعاطفية يكون له آثار تقنية مثل تسريب معلومات والصور على الانترنت التي لها صيت أوسع وسرعة أكبر في انتشار الأخبار.

أولا: تعريف جريمة الابتزاز والتهديد عبر الانترنت:

جريمة الابتزاز والتهديد عبر الشبكة المعلوماتية هي إحدى صور الجرائم الالكترونية (cyber-crimes)والتي تتكون من شقين، الشق الأول cyber وتعني السريانية والشق الثاني crimes وتعني الجرائم.

ويستخدم مصطلح الالكترونية لوصف فكرة أن هذه الجرائم تقوم وتتم من خلال التقنيات الحديثة now advanced technology، وقد اصطلح على تعريف بأنها: المخالفات التي ترتكب ضد الفرد أو مجموعة من الأفراد ويقصد بها إيذاء سمعة الضحية أو أذى مادي أو عقلي بالاستخدام

[1]– ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 208.

[2]– أنظر المواد من 284 إلى 287 والمادة 371 من أمر رقم 66–156 مؤرخ في 18 صفر 1386 الموافق ل8 يونيو 1966 ، المتضمن قانون العقوبات المعدل والمتمم، ج ر عدد 49.

شبكة الاتصال (الانترنت) بواسطة غرف الدردشة ،البريد الالكتروني...إلخ، باستخدام الهواتف الذكية أو الحاسب الآلي[1] ، وعرفها الأستاذ mass:"تتمثل بالاعتداءات غير القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح للفاعل او الخسارة للمجني عليه"[2]، وحديثا تبنى المؤتمر الأمم المتحدة العاشر لمنع الجريمة المعلوماتية بأنها:"أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية"[3].

وهذه التقنية أحدثت تغيرات في مجال الجريمة والسلوكيات الإجرامية حيث نتج عن تكنولوجيا استحداث جرائم جديدة إلى جانب طرق جديدة لاقتراف الجرائم الكلاسيكية, فالجرائم التقليدية تمتاز بالعنف وأذى مباشر للضحية كالقتل والضرب والسرقة ... ،على غرار الجرائم التكنولوجيا تكون ناعمة ولا تسبب أذى جسدي مباشر كالسرقة مثلا أصبحت معلوماتية كالاختراقات المصرفية او اختراق نظام الحاسوب او البريد الالكتروني لأخذ المعلومات والملفات والعديد من الجرائم وكذلك الجرائم التي تمارس على الأشخاص كالقذف او الشتم أو التشهير او التهديد والابتزاز .... فكل هذه الجرائم ليست وليدة العصر فماهو وليد العصر أنها أصبحت عن بعد عبر العالم الافتراضي من مواقع وبرامج وغرف الدردشة .

و الجريمة المراد دراستها في بحثنا جريمة الابتزاز والتهديد عبر شبكة الانترنت.

فالتهديد والابتزاز الكتروني يكون باستعمال وسائط الكترونية، فهو عملية ترهيب لضحية بنشر صوره وفيديوهاته أو تسريب معلومات تخص الضحية بمقابل مادي او استغلالي وعادة ما يتم الإطاحة بالضحايا عن طريق البريد الالكتروني ووسائل التواصل الاجتماعي لأنها أكثر انتشارا واستخداما[4].

[1]– مريم عراب، جريمة الابتزاز والتهديد الالكتروني، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، جامعة أحمد بن بلة، وهران 02، الجزائر، 2021، ص 1207.

[2]– محمد أمين شوابكة، جرائم الحاسوب والانترنت، ط 01، مكتبة دار الثقافة للنشر والتوسيع، الأردن، 2000، ص 9.

[3]– محمد أمين شوابكة، المرجع السابق، ص 10.

[4]– رامي احمد الغالبي، جريمة الابتزاز الالكتروني وآلية مكافحتها في جمهورية العراق، مجلة ثقافتنا الأمنية، الإصدار الثاني، وزارة الداخلية العراقية، مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019، ص 29.

وكما ذكرنا سابقا بعد انتشار هستيريا التواصل الاجتماعي وانتشار وسائل التواصل أصبح مستخدميها يضعون ثقتهم في تلك البرامج ويضعون أشياء عنهم من غير البيانات الخاصة كالاسم واللقب والعنوان والبريد الالكتروني، بل وصلت إلى الصور والفيديوهات الخاصة او حميمية تعتبر موثقة لحياة الخاصة لصاحبها ومن خصوصياته.

لم يعرف المشرع الجزائري الحياة الخاصة ولم يعرفها أي تشريع وحتى محكمة حقوق الإنسان امتنعت عن تقديم تعريف واضح وشامل ودقيق لمفهوم الحياة الخاصة حيث اعتبرت أن مفهوم الحياة الخاصة هو مفهوم واسع وغير قابل لأي تعريف شامل، فحاول الفقهاء وضع تعريف شامل للحياة الخاصة من بينهم الفقيه الفرنسي «نيوسن مارتن» حيث يرى أن الحياة الخاصة هي حق ينطوي عنصر الذاتية في الإنسان والتي تتعلق بشخصه وأمنه وطمأنينته بعيدا عن تدخل الآخرين، أما مؤتمر الحق في الحياة الخاصة المنعقد في الإسكندرية فقد عرف حرمة الحياة الخاصة "بأنها حق الشخص في ان يحترم الغير في كل ما يعد من خصوصياته سواء كانت مادية أم معنوية أم تعلقت بحرياته على إن يتحدد ذلك بمعيار الشخص العادي وفقا للعادات والتقاليد والنظام القانوني القائم في المجتمع ومبادئ الشريعة الإسلامية [1]،ويدخل في نطاق الحياة الخاصة للأفراد كثير من العناصر التي تعني الفرد وعائلته مثل علاقاته العاطفية وحياته الزوجية ،كما يضاف إلى هذه الأمور عناصر أخرى لصيقة بشخصية الإنسان مثل حق الفرد في إسمه وصورته وفي سرية مراسلاته ،و حقه في عدم الكشف عن أحواله الصحية والمهنية وفي حرية قضاء أوقات فراغه .... الخ [2] ، ونجد مبدأ سرية الحياة الخاصة وحمايتها في كل المواثيق الدولية والتشريعات، فهي حق مكفول في الدستور الجزائري فلا يجوز انتهاك حرمة حياة المواطن وحرمه وشرفه ويحميها القانون[3]. وردع الأفعال الماسة بها في عدة نصوص

[1]– صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا « الإعلام والاتصال»، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2014-2015، ص 12-13.

[2]– عبد العزيز النويري، المخاطر القانونية للانترنت على حرية التعبير والحياة الخاصة، مجلة التواصل، العدد 26، جامعة الحاج لخضر، باتنة، 2010، ص 67.

[3]– أنظر المادة 39 و47 من مرسوم الرئاسي 20– 442 المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري،

ج ر عدد 82 لسنة 2020.

في قانون العقوبات وقانون الإعلام .. ففي قانون العقوبات في نص المواد 303و 303 مكرر،303 مكرر 01[1].

نطاق خصوصية الفرد في العالم الافتراضي تختلف بحيث أنه يحق للأفراد او المجموعات أو المؤسسات ان يحددوا لأنفسهم مدى وصول المعلومات المرتبطة بحياتهم الخاصة للآخرين[2].

والحصول على الأشياء سابقة الذكر والتي تعتبر من خصوصية صاحبها وأسراره يكون إما عن طريق التغرير والإغواء تمس خاصة فئة الأطفال والمراهقين والشباب عن طريق الصداقة او المواعدة وتكون بكسب ثقة الضحية فيقوم هذا الأخير بإرسال أو إفشاء أسراره أو ملفاته الخاصة ،أي أن يلعب المبتز على مشاعر وعواطف الضحية عن طريق الشات من أمثلتها أن يقوم الشاب بالتعرف على فتاة عبر احد المواقع التواصل الاجتماعي مثل الفايسبوك أو انستغرام بالصوت والصورة ويقوم بتصوير الفتاة أثناء محادثه ويحفظها لديه وبعد ذلك يقوم بمصارحتها بأنه قام بالتقاط صورة او تسجيل فيديو لها ولتصديقه يقوم بإرسال الصورة في مراسلاتهم او عبر البريد الالكتروني وبمقابل هذا الفعل يطلب منها تصوير جسدها أو الالتقاء بها أو تسديد مبلغ مالي وذا لم تستجب لطلبه يهددها بنشر صورتها على شبكة الانترنت مما يجعلها تقبل على تطبيق طلبه. فأكثر من يتعرض لهذه الابتزازات والتهديدات هم فئة النساء وهذا ما أكدته دراسة لشركة Eversave 2009 نتائجها أن 85% من النساء يتعرضن للمضايقات على الفايسبوك[3].

والطريقة الثانية تكون عن طريق الاختراق وتكون بدون علم المجني عليه وخارجة عن إرادته عكس الطريقة الأولى ، يقوم بها فئة يطلق عليهم اسم المخترقون ، فهو مجرم معلوماتي يكون طفل أو رجل أو أنثى يتميزون بالخبرة والإدراك الواسع للمهارات التقنية أي يتمتع بالذكاء والمعرفة في مجال الحاسب الآلي والانترنت ، وتهدف اعتداءاتهم في الأساس الى تحقيق كسب

[1]– أنظر المواد من 303 إلى 303 مكرر 1 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

[2]– حسام الدين الاهوائي، الحق في احترام الحياة الخاصة (الحق في الخصوصية) دراسة مقارنة، ط 02، دار النهضة العربية، 2014، القاهرة، ص 272.

[3]– حسني عوض، آثار مواقع الاجتماعي في تنمية المسؤولية المجتمعية لدى الشباب، برنامج التنمية الاجتماعية والأسرية، جامعة القدس، فلسطين، ص 12.

مادي غير مشروع[1]، فأصحاب هذه الطريقة يكون الهدف من اختراق البريد الالكتروني أو الحسابات الشخصية الحصول على أسرار الضحية وابتزازه وتهديده بمقابل مادي على غرار الطائفة الأولى في أغلب الأحيان يكون المقابل جنسي، وتمارس هذه الطريقة في الغالب الأحيان على الشخص الاعتباري بقيام المخترق بابتزاز شركة كبرى بعد سرقة أسرارها ومساومتها عليها مقابل مبالغ مالية ضخمة .

والأدهى من ذلك إن منصات التواصل الاجتماعي تدخل في خصوصيات حيث ذهب بعض الملاحظين امر انتهاك الخصوصية في facebook لم يعد يقتصر على محتويات المستخدمين من الصور والفيديوهات بل تجاوز ذلك ليصل إلى أرقام هواتفهم إذ يطلب facebook حاليا من كثير من المستخدمين إدخال رقمهم الهاتفي بذريعة التحقق من هوية المستخدم [2] ،والكثير من المواقع الشخصية تطلب رقم الهاتف مما يترتب عليها سهولة حصول المبتز المخترق عند اختراقه للحساب على الرقم هاتف الضحية وزيادة الضغط والإكراه عليه وقد تؤدي به لاختراق عدة حسابات في مختلف المنصات المسجلة برقم الذي حصل عليه.

ثانيا: خطورة جريمة الابتزاز والتهديد عبر الانترنت:

جريمة الابتزاز والتهديد تشكل خطرا كبيرا بسبب آثارها الجسيمة والمتعددة، وهي على النحو التالي:

أ- خطورة جريمة الابتزاز والتهديد عبر الانترنت على المجتمع:

تعتبر جريمة الابتزاز والتهديد من أخطر الجرائم ومن أكثر الجرائم تأثيرا على الضحية، وهذا ما يخلف آثار على الأسرة والمجتمع وكما ذكرنا أن أغلب ضحايا هذه الجريمة من شريحة النساء، بما أن المرأة هي الأم والمدرسة وهي حجر الأساس للحفاظ على العائلة ومن العائلة يأتي صلاح المجتمع.لأن جريمة التهديد تأثر بشكل مباشر على العرض والشرف بانصياع الفتيات إلى رغبة المجرمين وإقامة علاقة جنسية خارج إطار الزواج, وقد ينتج عن ذلك حمل

[1]- حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الانترنت مقال منشور على موقع الكتروني، رابط الموقع: http://www.eastlaws.com ، ص 6.

[2]- ممدوح بن يحيى الخليوي، دور مواقع التواصل الاجتماعي في زيادة جريمة الابتزاز ضد المرأة من وجهة نظر طالبات الجامعات السعوديات، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، كلية العدالة الجنائية، قسم الدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، 2014، ص 57-58.

الفتاة وقد يترتب عنه قيامها بالإجهاض أو قتل الطفل ، وقد تقوم بالتخلص من الطفل بإيداعه في ملاجئ أو الشارع فيصبح من أولاد الشوارع والمنحرفين فيكون مصيره إما السجن أو القتل[1].

في مثل هذه القضايا وصمة عار توصم بيه العائلة وتؤدي إلى قتل وغسل العار الذي لحق بها.

ب- خطورة الابتزاز والتهديد عبر الانترنت على الأمن:

جريمة الابتزاز والتهديد وعلى نحوها من الجرائم الأخرى تؤثر تأثيرا مباشرا على الأمن في البلد لأنها تحدث اضطراب في شعور المجتمع بالأمان بتفشي الفساد والانحلال الأخلاقي، كما أن هذه الجريمة قد تصل بالضحية للدعارة والتسلط على أموال الناس كما تؤدي كذلك الى ارتفاع معدل جرائم القتل والانتحار[2] حيث يقوم المبتز بقتل ضحيته وتصويره لها. فإذا ما تم تداول صورة الجريمة يقوم أهل الضحية بقتل المبتز المعتدي انتقاما منه[3].

ج- خطورة الابتزاز والتهديد عبر الانترنت على الضحية:

جراء عملية الضغط التي يمارسها المجرم والإكراه يتعرض المجني عليه للأمراض نفسية وعصبية كالاكتئاب ,الترهيب النفسي ,القلق والتوتر,الشعور بالذنب ,الصعوبة في النوم ,هجران المجتمع, النظرة العدائية للمجتمع, وقد تحول شخصيته الى شخصية ناقمة على المجتمع فقد تكون ردت فعل لما لحقه من ضرر بأن يمارس الجريمة التي تعرض لها على غيره، فقد تلازمه هذه الأعراض طوال حياته ويصبح شخص غريب الأطوار فقد تدفع به ضغوطات المبتز إلى الإنتحار أو ترك العمل[4].

---

[1]- أمال برحال، المرجع السابق، ص 31.

[2]- ممدوح بن يحيى الخليوي، المرجع السابق، ص 36.

[3]- محمد بن المحسن بن شلهوب، المرجع السابق، ص 59.

[4]- نسرين عبد الحمين نبيه، الإجرام الجنسي، ط 01، دار الجامعة الجديدة، الإسكندرية، 2008،ص 39.

المطلب الثاني

وسائل وطرق التهديد والابتزاز عبر الانترنت

بعد تحول العالم وأصبح عالما رقميا تسوده الرقمنة فأصبح التواصل عبر تقنيات رقمية منها البريد الالكتروني والمنصات الاجتماعية، وتطبيقات المراسلة الفورية فستغل البعض هذه الوسائل على الإعتداء على خصوصية الآخرين والإعتداء على أموالهم والإحتيال عليهم .

ويكون باستدراج الضحية عبر أحد المواقع التواصل الاجتماعي أو بعض تطبيقات الهواتف الذكية وإغرائهم لإرسال صورهم أو تصويرهم من خلال كاميرا الهاتف الذكي أو عن طريق اختراق البريد الالكتروني أو حساب الشات، فهذا مفاده أن وسائل وطرق التهديد والابتزاز عبر الانترنت عديدة.

وهذا ما سنتطرق عليه في هذا المطلب وذلك من خلال تقسيم وسائل الابتزاز والتهديد عبر الانترنت (الفرع الأول)، وطرق الابتزاز والتهديد عبر الشبكة العنكبوتية (الفرع الثاني).

الفرع الأول: وسائل الابتزاز والتهديد عبر الانترنت

التهديد والابتزاز التقليدي يحدث عادة وجها لوجه أو عن طريق الهاتف أو رسائل ورقية تتضمن تهديدا بفعل الشيء معين (مثل الإيذاء الجسدي أو الإضرار بالممتلكات).

لكن يختلف الأمر بالنسبة لجريمة الكترونية بحيث يتم إيقاع واستدراج الضحايا الابتزاز والتهديد عبر الانترنت غالبا باستعمال الهاتف الذكي وتطبيقاته والحاسب الآلي ولواحقه والبريد الالكتروني ومواقع التواصل الاجتماعي عن طريق شبكة الانترنت.

أولا- الحاسب الآلي: هو جهاز يعمل الكترونيا بعد برمجته لتنفيذ عمليات حسابية ومنطقية والقيام بمقارنات على مجموعة من البيانات الداخلة إليه ، حيث يقوم بتخزينها واسترجاعها وينتج من معانيها معلومات أو تقارير بأسلوب مبوب ومرتب بسرعة ودقة عالية مما يوفر الجهد والوقت والتكاليف [1]. وهناك من عرفه بأنه:"مجموعة متداخلة من الأجزاء لديها هدف مشترك من

[1]- محسن بن سلمان الخليفة، جرائم الحاسب الآلي وعقوبتها في الفقه والنظام، مذكرة لنيل درجة الماجستير في التشريع الجنائي الإسلامي، كلية الدراسات العليا قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، 1423-1424، ص 21-22.

خلال أداء التعليمات المخزنة، وهو آلة حاسبة الكترونية ذات سرعة عالية ودقة كبيرة، يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على نتائج المطلوبة [1].

وتعرف نظم الحاسب الآلي بأنها كل مكونات الحاسب الآلي المادية (hardwere) والتي تشمل الأجزاء الملموسة من الحاسب الآلي الشاشة، وحدة المعالجة المركزية، الفأرة لوحة المفاتيح، المودم و(software) تشمل البرامج التي تقود الحاسب الآلي لأداء عملياته ،فبرز اتجاهين يعرفان برامج الحاسب الآلي اتجاه ضيق واتجاه واسع.

فالاتجاه الضيق يعرف برامج الحاسب الآلي بأنها"مجموعة التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح بتنفيذ مهمة محددة"[2]، أما المفهوم الواسع فعرف برامج الحاسوب بأنها:"كافة البيانات الأخرى الملحقة بالبرنامج والتي تساعد على سهولة فهمه وتطبيقه وهي تعتبر بمثابة وصف تفصيلي له متضمنة مراحل تطبيقه وهذه البيانات عبارة عن تعليمات موجهة من المبرمج الذي تولى إعداد البرنامج إلى العميل الذي تعامل مع الة"[3].

ثانيا/ الهاتف الذكي وتطبيقاته : هو جهاز يحتوي خدمات تقنية بنظام تشغيل متعدد المهام ويدعم التطبيقات التطور والمشاركة والبيع والشراء والخدمات المكتبية والانترنت.

أهم مكوناته:

1. **نظام التشغيل:**هو الواجهة التي تفعل ما يحتويه الهاتف من أبرزها نظام الاندرويد تديره شركة (Google Android)و نظام التشغيل los وتديره شركة (Apple) .
2. **المعالج:** يعمل على معالجة البيانات .
3. **الذاكرة:** هي مسؤولة عن تخزين وحفظ البيانات والمعلومات[4].

---

[1]– مريم عراب، المرجع السابق، ص 1212.

[2]– خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسوب الآلي في ضوء حماية الملكية الفكرية، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص 16.

[3]– شحاتة غريب شلقامي، الحق الأدبي لمؤلف برامج الحاسب الآلي، دار النهضة العربية، القاهرة، 2004، ص 18.

[4]– أشواق بلباي، فطيمة أعراج، تفاعلية التطبيقات الالكترونية في الهواتف الذكية –اليوتيوب نموذجا–، مذكرة مقدمة ضمن متطلبات شهادة الماستر في الإعلام، كلية العلوم الاجتماعية والانسانية، شعبة العلوم والاتصال تخصص سمعي بصري، جامعة الشهيد حمه لخضر، الوادي،2019-2020، ص 20.

4. **التطبيقات:** هي برامج مصممة لتعمل على الهواتف الذكية تكون محملة مسبقا على الهاتف أو تحميلها تعمل بالاتصال بالانترنت .

5. **الاتصال:** يكون باستخدام شريحة SIM أو احد التطبيقات الموجودة على الهاتف ويكون ذلك بالاتصال بالانترنت.

ثالثا/ الانترنتInternet *:* هي اختصار لكلمتين إنجليزيتين هما الأولى International والثانية networkويقصد بها شبكة الاتصال الدولية بالمعنى اللغوي والاصطلاحي هي عبارة عن استغلال متقدم للحاسب الآلي مترابط من خلال الاتصالات الدولية مع وجوب توافر تقنية خاصة ، وهو شبكة ضخمة تتكون من عدد كبير من الشبكات الحاسب الآلي المنتشرة في أنحاء العالم ومرتبط ببعضها البعض عن طريق خطوط الهاتف أو عن طريق الأقمار الصناعية بحيث يمكن مشاركة المعلومات فيما بين المستخدمين عن طريق برتوكول موحد يسمى «بروتوكول تراسل الانترنت»[1].

وتعرف جرائم الانترنت بأنها نشاط إجرامي تستخدم فيه التقنية الالكترونية والحاسب الآلي وشبكة الانترنت ،بطريقة مباشرة او غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف [2].

و عملية الابتزاز والتهديد عبر الانترنت هي صورة من صور جرائم الانترنت تتم عبر الأجهزة والمواقع والوسائل والتطبيقات التي تتيحها الانترنت وغالبا ما تكون عبر البريد الالكتروني ومواقع التواصل الاجتماعي.

1- البريد الالكتروني: في بادئ الأمر كانت الانترنت كشبكة عسكرية، لكن سرعان ما تطورت وانتشرت لتصبح وسيلة اتصال رئيسة للعالم .

كانت تستخدم لتيسير التواصل بين المراكز البحثية والعلماء، ومن هنا تطورت خدمات البريد الالكتروني لتمكين الباحثين في مراكز البحث العلمي حتى لا يحتاج الباحث للسفر والتنقل لعرض بحثه أو البحث والاطلاع وتبادل المراجع والمعلومات، ثم توسعت استخداماتها لتشمل

[1]– احمد عبد الإله هلالي، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية، ط 01، دار النهضة العربية، القاهرة، 2003، ص 44.

[2]– يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية مدرسة الدكتوراه« القانون الأساسي والعلوم السياسية»، جامعة مولود معمري، تيزي وزو، 2013، ص 9.

جميع فئات المستخدمين[1]، وسيلة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة لاتصال(الانترنت) في ثوان معدودة .

فيمكن تعريفه هو طريقة من طرق إرسال الرسائل عبر شبكة الانترنت من جهاز الكتروني (حاسوب، هاتف) إلى آخر. يشبه البريد الالكتروني البريد التقليدي الذي يعتمد على الصناديق البريدية لكل مشترك، لكن بدلا من ذلك يتم تخصيص مساحة في وحدة التخزين في الجهاز الالكتروني المتصل بشبكة الانترنت لكل مستخدم[2].

تتكون هذه العناوين البريدية من شقين الشق الأول يكون اسم صاحب البريد أما اسمه الحقيقي أو رمز او اسم مستعار أو رموز من شروطه لا يكون متكرر أو حساب مفتوح من قبل تليه إشارة@ أما بعدها اسم مقدم خدمة البريد الالكتروني من أبرزها Gmail، yahoo،Proton، Zoho يتبعه نقطة تتبعها رمز للهيئة المستخدمة.

Com: يدل على النشاط الخاص بالشركات التجارية.

edu: يرمز للجامعات.

Gov: يشير إلى الهيئات الحكومية.

Org: المنظمات العالمية[3].

بما أن البريد الالكتروني صندوق الرسائل الخاصة لمستخدمه، فله حماية قانونية كالصندوق الرسائل التقليدي، فترتيبا على هذا فيخضع لحماية قانونية وفقا لمبدأ حرمة المراسلات التقليدية فقد كرسته الاتفاقيات الدولية ورسمته التشريعات ضمن مصاف الحقوق الدستورية مما يقضي جواز مراقبة المراسلات أو إفشاء سريتها إلا في الأحوال التي يسمح القانون بذلك[4]، كما يمكن حماية البريد الالكتروني عن طريق الدعوى بحماية علامة تجارية،

---

[1]– عبد الرحمان بن عبد الله السند، جرائم نظم المعلومات، مطابع أكادمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2000، ص 97.

[2]– مصطفى عليان رابحي، البريد الالكتروني، مجلة الأمن والحياة، العدد 234، المملكة العربية السعودية، 2000، ص 66.

[3]– تهاني السبيت، ماهو البريد الالكتروني، مقال منشور على البريد الالكتروني، رابط الموقع: WWW.C4arab.Com ،مقال منشور بتاريخ 2001/01/21، ص5.

[4]– أنظر الفقرة 2 من المادة 47 من الدستور الجزائري.

دعوى تقليد العلامة وأيضا الاعتداء على العلامة المميزة التي تدخل في اختصاص السلطة العامة مثال: استخدام العنوان الالكتروني لأحد النقابات بدون وجه حق أو صفة[1].

2- مواقع التواصل الاجتماعي: هي تقنيات موجودة على شبكة الانترنت يستخدمونها للتواصل والتفاعل مع بعضهم البعض.

ومستخدموها يستطيعون إنشاء محتوى وتبادل الرسائل والصور أو إنشاء فيديوهات لمشاركة أفكارهم ومواهبهم ... والأكثر نشاطا هي شبكة الفايسبوك facebook وتويتر twitter وانستغرام Instagram وتيك توك Tik tok وكل وسيلة تقدم لمستعمليها خصائص وميزات.

وغالبا ما يتم تعريف مواقع التواصل الاجتماعي على أنها أدوات والمنصات التي تسمح بإجراء المحادثات على شبكة الانترنت .فهي إذن مواقع الكترونية اجتماعية على الانترنت تشكل ركيزة للإعلام البديل او الجديد ،وكل هذا يتم عن طريق خدمات التواصل المباشر مثل إرسال الرسائل والصور ومقاطع الفيديو والموسيقى والاطلاع على الملفات الشخصية ومعرفة أخبارهم ومعلوماتهم [2]. ومن أشهرها:

أ- ميتا (فيسبوك سابقا):

وقد وصل عدد مستخدميه إلى 2,9 مليار مستخدم ففي النصف الأول من سنة 2022 كان لدى فيسبوك معدل 1,97 مليار مستخدم نشط يوميا بزيادة سنوية قدرها 3% كما بلغ عدد المستخدمين النشطين شهريا 2,97مليار فأمضى مستخدمو المنصة عبر الهاتف وقتا معدله 19,4 ساعة شهريا على التطبيق.

ب- يوتيوب YouTube:

تحتل منصة يوتيوب المرتبة الثانية لأكثر المنصات امتلاكا لعدد المستخدمين بعدد مستخدمين بلغ 2 مستخدم في ابريل /نيسان,5 مليار 2022.

ج-منصة الوات ساب whatsapp

---

[1]- عبد الهادي فوزي العوضي، لجوانب القانونية للبريد الالكتروني، ط 01، دار النهضة العربية، مصر، 2005، ص 41-42.

[2]- سامي حمدان الرواشدة، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي: دراسة في القانونين الانجليزي والأمريكي، المجلة الدولية للقانون، جامعة قطر، 17 جانفي 2017، ص 6.

جاء تطبيق وات ساب ضمن المرتبة الثالثة وصل عدد مستخدميه حول العالم الى 2 مليار في يوليو/تموز **2022.**

د_ انستغرام Instagram

ـجاءت منصة انستغرام في مرتبة الرابعة ضمن قائمة تطبيقات التواصل الأكثر جذبا للمستخدمين بإجمالي عدد يصل إلى 1,4 مليار.

ثم تليها باقي المنصات «كالتيك توك » و«تيليجرام »و «سناب شات»... الخ الاطلاع على الملفات الشخصية ومعرفة أخبارهم ومعلوماتهم [1].

الفرع الثاني: طرق الابتزاز والتهديد عبر الانترنت .

بعد استدراج الضحية عبر احد الوسائل المذكورة التي أتاحتها شبكة النت تليها مرحلة ماهي الطريقة التي تدفع الضحية لرضوخ للتهديد؟

هي كل الأشياء التي تمس وتعتبر خصوصية وتابعة لحياة الخاصة للشخص وتسبب إحراج له ومن نقاط ضعفه قد تؤدي به إلى تطبيق العقوبة عليه سواء عقوبات من طرف الدولة كأسرار وملفات سرية أكثر ما تمس الأشخاص الاعتبارية، أو محادثات أو تسجيلات صوتية أو مرئية لبيع المخدرات او الانضمام لعصابات الأحياء ... أكثرهم فئة الرجال وخاصة الشباب ويكون الهدف من الضغط والتهديد مادي، أو عقوبات من طرف العائلة والمجتمع وأكثر الضحايا هن نساء والأحداث، كمحادثات صور تسجيلات صوتية وتسجيلات مرئية من خلال مميزات المواقع التي تتيحها الانترنت كتطبيق المسنجر. فغالبا ما يكون الهدف منه غير أخلاقي (زنى ، لواط):

وهذه تعريف أبرزها:

[1]– رماح الدلقموني، وسائل التواصل الاجتماعي حقائق وأرقام، مقال منشور في موقع الكتروني، رابط الموقع: WWW.aljzeera.net تاريخ الإطلاع: 2024/06/01، 14:30.

أولا/ الصورة: في تعريفها اللغوي معناها الشكل بمعنى المشابهة والمقارنة[1]. ووردت الصورة في قول الله تعالى في القرآن الكريم ﴿وصوركم في أحسن صوركم ﴾[2] وأيضا في ﴿و في أية صورة ما شاء ركبك﴾[3] ويقصد بها تصوير الله تعالى للإنسان في هيئة تدرك بالبصر والبصيرة[4] .

وفي الفقه الجنائي عرفت الصورة بأنها امتداد ضوئي لجسم الإنسان[5].

و الحق في الصورة إعتبره المشرع من الحقوق اللصيقة بالشخصية واقر لها حماية وأربطها ضمن الحياة الخاصة للفرد وهذا ما ظهر جليا في نص المادة 303 مكرر1 من ق ع فجرم المشرع التقاط الصور أو اخذها وتخزينها (الاحتفاظ بها) ونشرها للجمهور[6] .

ثانيا/ التسجيلات الصوتية: هي عملية حفظ أصوات وتخزينها باستخدام أجهزة رقمية متنوعة من اجل إعادة سماعها حين تدعو الحاجة لذلك مثل المحادثات الصوتية على الانترنت والهاتف[7] إن بعض الهواتف تتميز بالتقنية العالية مزودة ببرامج والتي تعرف ب Spay call ويمكن من خلالها تسجيل كل التفاصيل الصوتية للمكالمة الواردة إلى الهاتف وكذلك يقوم بتخزين رقم الطرف الآخر في الحديث الهاتفي[8] . فتقنيات الهاتف الذكي ومن خلال مميزاته الجد متطور ميزة المشاركة ما يوجد داخله وما تم تخزين فيه مشاركته في فضاء الانترنت . وجرمه المشرع في نص المادة 303مكرر الفقرة1.

---

[1]– أحمد بن فارس بن زكرياء القزويني الرازي، كتاب مجمل اللغة معجم لغوي من الأصول، حققه أبو الحسن عمرو بن شهاب الدين، دار الفكر، لبنان، 1994، ص 319.

[2]– سورة التغابن الآية 3.

[3]– سورة الانفطار الآية 8.

[4]– الراغب الأصفهاني المعروف أبي القاسم الحسين بن محمد ، المفردات في غريب القرآن، ط 01، المؤسس الإعلامي للمطبوعات، 2009، ص 381.

[5]– محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص جرائم الاعتداء على الأشخاص، دار العربية، القاهرة، 1978، ص 776.

[6]– أنظر المادة 303 مكرر 1 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

[7]– خالد الحمد مسره، الدليل الرقمي ومعايير جودته في الإثبات الجنائي، مركز الكتاب الأكاديمي، ط 01، الأردن، 2014، ص 42.

[8]– الحسني عباس عمار، التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات ،دراسة مقارنة، ط 01، المركز العربي للنشر والتوزيع، مصر، 2017، ص 159.

ثالثا/ التسجيلات المرئية Vidéo : عرف التسجيل المرئي هو توثيق مشاهد متحركة وهناك من ذهب في تسميته بالتصوير المتحرك[1] ، هو تجميع ما بين الصورة والصوت وتوثيق للحظة التي يعيشوها صاحبها وتعرف بمقاطع فيلمية او مقاطع فيديو يتم تسجيلها بواسطة التقنيات الحديثة الكاميرا الخاصة بالهاتف أو الكاميرا المستقلة يتم إرسالها بإرادة الحرة للضحية أو خارج إرادته بتسجيله عند مكالمته بأحد الوسائل الالكترونية على الانترنت كتطبيق المسنجر او الفايبر أو تسجيله في الواقع دون علمه وإرساله لديه عبر حساباته على الشبكة العنكبوتية ، هذا الأمر يمكن أن يحدث سواء كان الأشخاص معروفين لبعضهم البعض أي سبق لهم التواصل من قبل أم لا، ويعود ذلك إلى إتاحة الكثير من الأشخاص لبياناتهم الشخصية عبر حساباتهم الخاصة (الإسم، اللقب، مكان الإقامة، مكان العمل أو الدراسة ...) مما يسهل الوصول إليهم.

رابعا/ المحادثات Conversations: هي تلك الأحاديث التي يتفوه بها الفرد[2] مع الطرف الآخر إما ان تكون مباشرة عن طريق المكالمات او غير مباشرة تكون مكتوبة ضمن وسائل التواصل الاجتماعي أو البريد الالكتروني يستطيع الجاني الاحتفاظ بها عن طريق خاصية في الهواتف الذكية وهي لقطة الشاشة Screenshot.

[1]– الحسني عباس عمار، المرجع السابق، ص 23.

[2]– أمال برحال، المرجع السابق، ص 40.

المبحث الثاني

تجريم الابتزاز والتهديد عبر الانترنت

رغم نجاح الشبكات الاجتماعية ومواقع التواصل الاجتماعي بفضل الميزات التي توفرها للمستخدمين بالتواصل المشاركة والتفاعل وتبادل المعلومات عبر شبكة الانترنت ففي المقابل تعد مسرحا مهيئا لجرائم الالكترونية . وأدت إلى تفشي الكثير من الظواهر السلبية منها المضايقات والفساد والانحلال الأخلاقي خاصة المجتمعات الإسلامية التي كانت تعرف نوعا من التحفظ في الاختلاط والعلاقات الخارجة عن إطار الزواج تبعا بالقيم الإسلامية وتعاليم الدين الإسلامي الحنيف.

فقد ساهمت هذه الوسائل الحديثة التي تعتبر وسيلة للإعلام الجديد لسهولة انتشار الأخبار فيها ولكثرت مستعمليها والنشطاء فيها فستعمل هذه الميزة ذو النفوس الإجرامية للوصول لمبتغاهم باستدراج الضحية والضغط عليها وابتزازها وتهديدها بنشر الصور وفيديوهات ... على هذه المنصات، ، وغالبا –كما ذكرنا سابقا أشياء تعتبر من خصوصية الشخص– ولهذا فقد أولت التشريعات والقوانين والاتفاقيات حماية خاصة للحياة الشخصية للشخص وصنفتها من الجرائم الخطرة نظرا للضرر الذي تلحقه هذه الجريمة للفرد في شرفه و حياته ونفسيته .

المطلب الأول: أركان جريمة التهديد والابتزاز عبر الانترنت، والمطلب الثاني: عقوبات جريمة الابتزاز والتهديد عبر الانترنت.

المطلب الأول

أركان جريمة الابتزاز والتهديد عبر الانترنت.

إن الابتزاز والتهديد عبر الانترنت، الذي يتم عبر الوسائل الالكترونية يشكل نوعا من الترهيب والضغط على الأفراد بهدف إجبارهم بالقيام بأعمال يطلبها الجاني أو الإمتناع عن القيام بشيئ حتى لو كانت هذه الأوامر مشروعة، وتصنف جرائم التهديد في التشريع الجزائري تحت تصنيف الجنح .

وعلى الرغم من حداثة الجريمة إلا أن الابتزاز والتهديد عبر الانترنت يعتبر جريمة كأي جريمة أخرى تقوم على ثلاث أركان، الركن الشرعي، الركن المادي، الركن المعنوي.

الركن الشرعي وهو الذي يحدد تنظيم القانوني للجريمة، الذي يشمل الفعل المجرم والعقوبة المنصوص عليها، الركن المادي وهو المظهر الخارجي الذي تظهر فيه الجريمة في العالم الخارجي يتمثل في بالقيام بالفعل أو الإمتناع عنه، الركن المعنوي كل ما يتعلق بنية الجاني.

الفرع الأول: الركن الشرعي لجريمة التهديد والابتزاز عبر الانترنت.

الابتزاز والتهديد عبر الشبكة العنكبوتية كغيرها من الجرائم تخضع لمبدأ الشرعية، الذي هو مبدأ يقوم عليه القانون الجنائي المعاصر وهو مبدأ كفلته التشريعات والاتفاقيات الدولية ويعرف كذلك بشرعية الجرائم والعقوبات وهو ركن أساسي إذ لا جريمة ولا عقوبة تطبق إلا بنص تشريعي ، وأنه لا يمكن توجيه اتهام من قبل السلطات القضائية ضد أي فرد لارتكابه فعلا ما لم يكن منصوص ومجرم ومنضم له عقوبات في القانون ، فالفرق بين المشروعية والشرعية ،حيث إن الشرعية تتمثل في حصر مصادر التجريم والعقاب في النصوص القانونية محددة فهي تتعلق بالشروط الشكلية والموضوعية التي تضمن شروط صحة النص . ويقصد بالمشروعية انتفاء التعارض بين الواقعة القانونية وبين نصوص التجريم فهي تنصرف إلى أسباب الإباحة فالمشروعية تتعلق بالفعل في حين إن الشرعية تتعلق بالنص[1]، كما يقصد بمبدأ الشرعية في مجال القانون الجزائي ان لهذا القانون مصدرا واحدا وهو القانون المكتوب[2] .

وطبقا لنص المادة الأولى من ق ع التي نصت على مبدأ الشرعية إذ لا يتخذ أي إجراء قضائي ضد أي فرد إلا وكان الفعل الصادر منه مجرم في القانون[3] ، فقد حمى المشرع الجزائري حياة الخاصة للأفراد وجرم كل أشكال التعدي عليها وظهر هذا جليا في الدستور الجزائري[4] فأولى لها حماية خاصة لخصوصيته وشرفه كون المجتمع الجزائري مسلم ومحافظ وأن جريمة الابتزاز والتهديد غالبا ما يكون مفادها التطفل في خصوصيات الغير والاستحواذ على أشياء حساسة من أجل الوصول لغاية في أكثرها تكون غير أخلاقية وعاقب التعدي عليها

[1]– منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر والتوزيع، الجزائر، 2019، ص 77

[2]– احسن بوسقيعة، الوجيز في القانون الجزائري العام، ط 10، دار هومة، الجزائر، 2018، ص 49.

[3]– أنظر المادة 01 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

[4]– أنظر المادة 39 من الدستور الجزائري، مرجع سابق الذكر.

في المادة 303 مكرر و303 مكرر 1 من ق ع ج ،حيث جرمت المادة 303 مكرر سلوك التعدي على الحياة الخاصة للفرد بالتقاط وتسجيل ونقل الأحاديث الخاصة والسرية ،و التقاط الصور أو نقلها او تسجيل بأي تقنية كانت دون علم ورضا صاحبها، وركز على الصورة وعاقب في المادة 303 مكرر1 على استغلالها .التقاطها والاحتفاظ بها أو وضعها أو سمح بأن توضع في متناول الجمهور، فحق الخصوصية في مجال الرقمنة يمكن تعريفه انه حق الأفراد أن يحددوا لأنفسهم متى وكيف وإلى مدى يمكن للمعلومات الخاصة ان تصل للآخرين[1].

فلا يوجد نص تشريعي مباشر لجريمة التهديد والابتزاز الالكتروني فالبرجوع إلى نص المادة 2 فقرة ب من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تنص على الجرائم المرتكبة عبر منظومة معلوماتية أو نظام الاتصالات الالكترونية[2] وبما ان المادة تشمل كل الجرائم التي تقع باستخدام تكنولوجيا الإعلام والاتصال فإنها تحتوي على جريمة التهديد بواسطة منظومة معلوماتية[3] ، فالنصوص القانونية المتعلقة بجريمة التهديد التقليدية صالحة لتطبيقها على جريمة التهديد والابتزاز على الانترنت ، فتعتبر جريمة التهديد بالتشهير من أكثر أنواع الجرائم نص عليها المشرع في نص المادة 371 من ق ع.

الحياة الخاصة ليست الواقعة الوحيدة التي يمكن بالتهديد عن الكشف عنها لأنه توجد وقائع أخرى ليست لها علاقة بالحياة الخاصة ، وعليه فإن الحياة الخاصة واقعة من الوقائع التي يمكن أن يسلط عليها التهديد.

---

[1]- سهام عكوش، الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري، المجلة السياسية العالمية، المجلد 06، العدد01، جامعة امحمد بوقرة، بومرداس (الجزائر)، 2022، ص 1300.

[2]- أنظر المادة 02 فقرة "ب" من قانون رقم 09-04 مؤرخ في شعبان عام 1430 الموافق ل 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 44 صادر في 16 غشت 2009.

[3]- يحيى التومي، جرائم الاعتداء ضد الأشخاص باستخدام تكنولوجيا الإعلام والاتصال، أطروحة من أجل نيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق ، جامعة الجزائر01، 2017-2018.

الفرع الثاني: الركن المادي لجريمة الابتزاز والتهديد عبر الانترنت.

الركن المادي للواقعة الإجرامية يقصد به «**فالركن المادي للجريمة هو وجهها الخارجي الظاهر وبه يتحقق الاعتداء على المصلحة المحمية قانونا وعن طريقه تقع الأعمال التنفيذية للجريمة ... وبالتالي الركن المادي هو ما يدخل في البناء القانوني للجريمة من عناصر مادية ملموسة يمكن إدراكها بالحواس...، الركن المادي في غالبية الجرائم يتحلل إلى ثلاثة عناصر سواء تمثل في الفعل أو مجرد امتناع ، والنتيجة يكون سبب حدوثها هذا السلوك سواء كانت نتيجة مادية يمكن إدراكها في العالم الخارجي أو مجرد نتيجة بالمفهوم القانوني وان ترتبط هذه النتيجة برابطة أو صلة أو علاقة سببية وهي العناصر العامة لركن المادي لكل جريمة تامة**»[1].

أولا: عناصر الركن المادي:

1/السوك الإجرامي: هو كل فعل أو تصرف أو موقف صادر من شخص يضر بمصلحة فيعاقبه بها القانون.

وفي جريمة الابتزاز والتهديد عبر فضاء الانترنت يكون سلوك المجرم ايجابي بحيث إن الجاني يقوم بتوجيه الإكراه المعنوي والتهديد بنشر الصور والفيديوهات ومحادثات ومعلومات .. سواء بالقول أو الكتابة أو أي فعل يحدث الرعب والخوف في نفس الضحية (المادة 371 من ق ع ج) « كل من تحصل بطريق التهديد كتابة او شفاهة ...» والمادة (286 من ق ع) إذا كان التهديد مصطحب بشرط وأن يكون مكتوب بطريقة مباشرة أو غير مباشرة كاستعمال رموز وإشعارات ....[2]، فغالبا ما يكون التهديد الشفهي أقل حده من التهديد الكتابي لأنه عادة ما يصدر في حالة غضب وهيجان ، لكن الأخطر والأدهى إن يدخل على الصورة أو الفيديو الذي تحصل عليه تغييرات وتعديلات (مونتاج) بالحذف أو الإضافة حتى تتماشى مع الغرض وإحداث تهويل أكثر في نفس الضحية وإخضاعها للطلب.

---

[1]– ناصر حمودي، الأحكام العامة لقانون العقوبات والنظرية للجريمة، محاضرات في القانون الجنائي العام، موجهة لطلبة السنة الثانية جذع مشترك، ليسونس، كلية الحقوق والعلوم السياسية، جامعة العقيد اكلي محند اولحاج، ص 162-165.

[2]– أنظر المادة 371 و286 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

واعتبر المشرع الجزائري كل من قام بتسهيل الإذاعة أو النشر فاعلا أصليا للجريمة[1].

2/ النتيجة: هو الاثر المترتب على السلوك الإجرامي للمجرم ، والمفهوم القانوني للنتيجة فيتمثل في الاعتداء على المصالح والحقوق المحمية قانونا[2].

غير أن النتيجة قد لا تكون عنصر لازما في الركن المادي لبعض الجرائم وتسمى جرائم الخطر والتي يقوم ويكتمل ركنها المادي بمجرد إتيان السلوك ، ومن بين هذه الجرائم جريمة التهديد والابتزاز الالكتروني, فهي جريمة قائمة بذاتها لا تستوجب تحقق النتيجة ويقصد بالنتيجة تحقق ما هدد به الجاني أو تحقق الطلب الذي عرضه على الضحية فإن القانون يعاقب على فعل التهويل، الرعب والخوف الذي انعكس على نفسية الضحية اثر فعل الجاني،بالإضافة إلى الإكراه المعنوي والضغط ، فيكفي لتحقيق النتيجة أن يكون التهديد جديا لا تهديدا عابرا .

3/العلاقة السببية: هي الصلة التي تربط السلوك الإجرامي بالنتيجة المحظورة قانونا .

وتكون العلاقة السببية في جريمة الابتزاز والتهديد عبر النت في تنفيذ الجاني تهديده بالنشر والعلانية في مواقع على شبكة الانترنت لمعلومات تتعلق بالشخص المجني عليه[3] .

ويقوم عنصر السببية في جريمة الابتزاز والتهديد عبر النت في الرضوخ لطلبات الجاني بدافع الخوف الذي أحدث في نفس الضحية مثال طلب المبتز المال من الضحية وحدث التسليم بدافع الخوف وأن يكون هذا التهديد سببا في إحتقار وإهانة للمجني عليه فإذا حدث تسليم المال لأسباب أخرى إنتفت العلاقة السببية[4]

إذن يتحقق الركن المادي بعناصره العامة الثلاثة: السلوك الإجرامي أو الجرمي، النتيجة العلاقة السببية.

فجريمة الابتزاز والتهديد الالكتروني تتطلب سلوك إجرامي ويتم عبر مواقع التواصل الاجتماعي أو البريد الالكتروني، يعتبر كل تهديدا سواء كتابتا أو شفاهة أو رموزا أو إشعارات او صورا من

---

[1]– سيهام عكوش، المرجع السابق، ص 1301.

[2]– ناصر حمودي، المرجع السابق، ص 168.

[3]– فاطمة العرفي، الحماية القانونية للحق في الخصوصية للأطفال من جلريمة التشهير عبر مواقع التواصل الاجتماعي في القانون الجزائري، مجلة الاجتهاد القضائي، المجلد 12، العدد 02، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة ، أكتوبر 2020، ص 534.

[4]– رامي أحمد الغالبي، المرجع السابق، ص 41.

شأنها إلقاء الرعب والخوف في قلب المهدد، ولا يهم إن كان الجاني ينوي تحقيق النتيجة أم لا فقد يجب أن يكون التهديد جديا لا هزليا فكذلك لا يهم من أين حصل على الصور .... فيمكن أن يكون حصل عليها بالاختراق حساب الضحية على الانترنت أو عثر عليها في جهاز الضحية المسروق أو المعثور عليه كما لاشترط أن يتم التهديد وسيلة معينة فيمكن أن يتم عن طريق غرف الشات أو عن طريق البريد الالكتروني أو رسالة صوتية ،كما لا يهم أن كان الابتزاز لمصلحة مشروعة أو غير مشروعة فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد بإرغام المجني عليه لقيام بذلك الفعل[1] .

ثانيا: صور الركن المادي لجريمة الابتزاز والتهديد عبر الانترنت

تعتبر جريمة الابتزاز والتهديد عبر الانترنت من الجرائم الخطر ذات صور مختلفة، فليست منحصرة في صورة واحدة فهي تتنوع بتنوع الهدف والضحية.

أ/ صور الابتزاز والتهديد عبر الانترنت بالنظر إلى الهدف أو منفعة المجرم:

يختلف الهدف باختلاف الجريمة.

1/ هدف جنسي: الهدف الجنسي من أكثر الأهداف انتشارا يستهدف فئة النساء والأحداث وخاصة شريحة المراهقين، ويتحقق عن طريق قيام الجاني بفضح ونشر أسراره ، وينقسم الابتزاز الجنسي إلى قسمين: الابتزاز الجنسي الواقعي بقيام المجرم بالاستحواذ على معلومات الضحية أو الالتقاط الصور أو مقاطع فيديو او مقاطع صوتية عن طريق استغلال عواطف الضحية وقد يصل الأمر إلى حصول المبتز على رقم هاتف ولي أمر الضحية ثم تهديدها بنشر وفضح العلاقة وصور ... إذا لم تنصع إلى رغباته الجنسية .

أما الابتزاز الجنسي الالكتروني يتحقق عن طريق وسائل الاتصال الالكترونية وفضاء الانترنت والمبتز في هذا النوع يعتبر مجرما خفيا يسعى للحصول على معلومات تخص الضحية[2].

2/ هدف مادي: من أهم وأكثر الأهداف انتشارا وهي تحقيق أو حصول على أموال أو منفعة عينية ذات قيمة من المجني عليه[3] ، ويقوم بطريقتين إما بطريقة مباشرة أو غير مباشرة .

---

[1]– مريم عراب، المرجع السابق، ص 1208.

[2]– ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 201.

[3]– أمال برحال، المرجع السابق، ص 14.

فالطريقة المباشرة يتم بطلب مباشر من المجني عليه بتحويل مبلغ مالي بشكل مستمر إليه أو لغيره، اما نشر ما بحوزته من معلومات وأشياء حرجة عن الضحية أما بالطريقة الغير مباشرة فيتحقق عن طريق طلب المبتز من المجني عليه تسديد مبالغ مالية اقترضها من أحد البنوك أو عند الغير وتسديد ديون مستحقة للمبتز[1].

3/ هدف انتقامي: عائد هذا الهدف إلى جانب النفسي للمجني عليه ، حيث يستمتع المجرم بأذية المجني عليه واستماعه لتوسلاته وانه سيقوم بتنفيذ طلباته تجنبا للفضيحة بنشر صوره وإلحاق أذى به وإساءة سمعته بنشرها على شبكة الانترنت [2].

4/ هدف نفعي:ويتحقق بدفع الضحية لتحقيق منفعة أو مصلحة تعود على المجني عليه قد تكون عمل غير مشروع كترويج للمخدرات او تزوير أوراق ..، أو عمل مشروع كالحصول على وظيفة.

ب/ صور الابتزاز والتهديد عبر الانترنت بالنظر للضحية:

وهي ما تعلق بفئات المستهدفة:

1/ النساء: فئة النساء وخاصة المراهقات ، يمثلن الهدف الشائع للتهديدات عبر الانترنت ، حيث يتعرضن للابتزاز بشكل شائع بواسطة صورهن الشخصية أو صور لمحاثات عبر أحد مواقع التواصل او البريد الالكتروني أو مقاطع فيديو خادشة للحياء ،هذا النوع من التهديدات ينتشر بشكل واسع .

وغالبا ما يتجاوبن مع مطالب المبتزين خوفا من العواقب السلبية والتشهير، وخاصة في المجتمعات العربية والمسلمة ،حيث تعتبر قضايا الشرف والعار قضايا حساسة، فخوفا من الأهل تمتنع الضحية عن الإبلاغ وترضخ لطلبات المبتز[3] .

---

[1]– المطلق نورة بنت عبد الله بن محمد، ابتزاز الفتيات أحكامه وعقوبته في الفقه الإسلامي، جامعة الإمام محمد بن سعود الإسلامية، الرياض، ص 12.

[2]– ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 202.

[3]– الحمين عبد العزيز بن الحمين بن أحمد، الابتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم، الأسباب، العلاج)، جامعة الملك سعود، 2011، ص 61.

2/ الأحداث: وهم فئة التي لا تتعدى أعمارهم 18 سنة ويتم استغلالهم بالضغط عليهم بتهديدهم بنشر صورهم أو مقاطع فيلمية وصوتية تلحق بالضحية عقوبات واحتقار ، وتستهدف هذه الفئة من اجل تحقيق مطامع جنسية أو استعمالهم في عمليات غير مشروعة كالترويج للمخدرات في المدارس وإيصالها بين أعضاء العصابات لأنهم فئة يحميها القانون وفرض عليهم حماية خاصة وبعيدين عن شبهات .

3/ الرجال: جريمة الابتزاز والتهديد عبر الانترنت لم يسلم منها تمس حتى فئة الرجال،تقوم بتهديد الضحية بكشف أسراره قد تكون متعلقة بحياته الشخصية أو مجال عمله أو بعلاقاته الإجتماعية، بهدف تحقيق مكسب مالي أو ضغط عاطفي أو إسغلال مكانة ووظيفة الضحية، يمكن أن يكون مبنيا على إشاعة أخبار كاذبة أو صور للشخص أو صور محادثات ورسائل لتشويه سمعته وقد تصل أضرارها لطلاق أو تعريضه لعقوبات . وقد يتضمن كذلك التهديد بالعنف أو الإضرار بممتلكاته .

فقد يتم إستهدافهم من قبل الرجال والنساء ،بسبب معلومات خاصة تتعلق بأعمالهم أو عائلاتهم أو علاقاتهم الشخصية ،في حال حدوث الابتزاز، يمكن أن يتعرض الفرد إلى أضرار كبيرة تتعلق بشرفه وسمعته ومركزه في المجتمع مما ينتج عنها تأثيرات سلبية تمتد إلى حياته الشخصية والمهنية والإجتماعية .

4/ الشخصيات الاعتبارية: قد يستغل المخترقون الوصول الذي يحصلون عليه من خلال اختراق حسابات الشخصيات الاعتبارية للقيام بأعمال غير قانونية، مثل السطو على مواقع الإلكترونية والتهديد بنشر أ فضح المعلومات السرية التي يحصلون عليها . بعض المجرمين قد يكونون سابقين للعمل في هذه الشركات ،وقد يستعملون معرفتهم السابقة بالحسابات والبيانات لتهديد الشركات بالانتقام أو المطالبة بالأموال كجزء من عملية انتقامية أو أسباب مالية.

وبعبارة أخرى، المخترقون والأشخاص الذين يستخدمون المعرفة الداخلية للكيانات الاعتبارية بدافع انتقامي يهددون الشركة المستهدفة في غالب الأحيان للحصول على مبالغ مالية [1].

[1]– ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 200.

الفرع الثالث: الركن المعنوي:

هو الركن النفسي للجريمة، المتمثل في توفر صلة نفسية بين الفاعل وماديات الجريمة (الركن المادي) يتحقق بموقف الإرادة من الفعل المادي، وهو الموقف الذي قد يتخذ صورة القصد كما قد يتخذ صورة الخطأ[1].

فجريمة الابتزاز والتهديد جريمة عمديه تصدر عن إرادة وعلم الجاني، ومرتكبها يكون على دراية وإلمام واسع بستخدام الوسائل التقنية وشبكة الأنترنت فلايعقل أن يكون التهديد عن طريق الخطأ، ويكون الجاني عالم أن الواقعة والفعل المراد تحقيقه مجرم ومصلحة يحميها القانون ويلحق أذى بالغير وإرادته الكاملة في تحقيق النتيجة والوصول إلى مبتغاه ، ويقصد هنا بعلمه هو انصراف عناصر الركن النفسي - العلم والإرادة- إلى تحقيق الهدف، والمصلحة التي يحميها القانون هي الحياة الخاصة وخصوصية الفرد من جميع الاعتداءات التي تمس بأمن المجتمع والفرد بحث ان التهديد يبث الرعب والخوف والهلع في نفس الفرد وعائلته وماله .

وبما أن جريمة التهديد والابتزاز عبر شبكة النت تتطلب دراية وعلم بكيفية استعمال الوسائل التكنولوجيا والانترنت، فلا يمكن أن يرتكبها الجاني بدون قصد فلا يشترط أن يكون القصد خاصا[2]

ومن هذا يتحقق القصد الجنائي العام والخاص في جريمة الابتزاز والتهديد عبر الانترنت .

المطلب الثاني

العقوبات المقررة لجريمة الابتزاز والتهديد عبر الانترنت

بما أن جريمة الابتزاز والتهديد عبر النت من الجرائم التي تهدد الأمن والمجتمع، كما أنها تمس الأفراد وخصوصياتهم، لذا استوجب على المشرع حماية خاصة بها وذلك بتوقيع المناسبة على المجرمين والتي تضمن من خلالها تحقيق الردع الخاص للمجرم من جهة وتحقيق الردع العام للمجتمع من جهة أخرى بما أن العقوبة وسيلة للوقائية وعلاجية.

ولقد تنوعت العقوبات بين عقوبات أصلية وأخرى تكميلية.

[1]– ناصر حمودي، المرجع السابق، ص 218.

[2]– محمد بن المحسن بن شلهوب، المرجع السابق، ص 104.

الفرع الأول: العقوبات الأصلية

نظرا لأهمية القانون الدستوري كبوابة أساسية لتنظيم الحياة القانونية في الدولة الجزائرية، فقد تم ضمان الحق في الحياة الخاصة ضمن نطاق الحقوق الأساسية التي تكفلها الدستور. وبالتالي، يعتبر الحق في الحياة الخاصة حقا محميا بصفة صريحة ومستقلة، ويتضمن الدفاع عنه من أي اعتداء عليه، بما في ذلك اعتداءات على المراسلات وأشكال أخرى من التعديات.

في نص المادة 39 تعد حرمة الحياة الخاصة من القيم الأساسية التي تكفلها الدولة[1]، حيث يجب على الدولة ومؤسساتها القانونية ضمان عدم انتهاك هذا الحق الأساسي للفرد. يتجلى ذلك من خلال توفير الحماية اللازمة والتي تشمل تشريعات صارمة وآليات تنفيذية فعالة للتصدي لأي مساس بحرمة الحياة الخاصة.

وتأتي هذه الحماية في إطار القانون الدستوري الذي يعتبر الوثيقة الأساسية لتنظيم الحياة السياسية والقانونية في الدولة. ومن خلال تضمين الحق في الحياة الخاصة كجزء لا يتجزأ من حقوق الإنسان الأساسية، يلزم الدستور الجهات الحكومية باتخاذ كافة الإجراءات الضرورية لحماية هذا الحق ومنع أي انتهاكات له.

و في فحوى المادة 47 كل فرد له الحق في:

1. حماية حياته الخاصة وشرفه.

2. سرية مراسلاته واتصالاته الشخصية.

هذه الحقوق الأساسية يجب أن تكون مضمونة ومحمية بواسطة السلطات القانونية[2].

وبالإضافة إلى القانون الدستوري، يعتبر القانون المدني المرجع الرئيسي لتنظيم في المجتمع. وقد تم تسمية حقوق الفرد في هذا السياق بمصطلح "الحقوق اللصيقة في الشخصية"، بالنظر إلى عدم وجود نص صريح في القانون المدني الجزائري يحمي الحق في الحياة الخاصة كحق مستقل، يمكن استنتاج أن هذا الحق مشمول بشكل عام ضمن الحقوق الشخصية الأخرى. يشار إلى ذلك في المادة 47 من القانون المدني الجزائري والتي تعني أن أي شخص يتعرض لاعتداء

[1]– أنظر المادة 39 من الدستور الجزائري، مرجع سابق الذكر.

[2]– أنظر المادة 47 من الدستور الجزائري، مرجع سابق الذكر.

غير مشروع على أي من حقوقه الأساسية يحق له طلب وقف هذا الاعتداء والحصول على تعويض عن الضرر الذي تكبده[1].

بموجب المادة 46 من القانون المدني الجزائري، لا يجوز التنازل عن حقوق الحريات الشخصية، بما في ذلك الحياة الخاصة. لذا، يحق للمتعدي على هذا الحق رفع دعوى للمطالبة بوقف الاعتداء والحصول على التعويض عن الضرر[2].

وبناء على ذلك، فإن الشخص المتعرض لأي اعتداء على حقه في الحياة الخاصة يحق له رفع دعوى قضائية للمطالبة بوقف هذا الاعتداء والحصول على التعويض عن الضرر الذي لحق به، سواء بموجب الدستور أو القانون المدني.

تم تعزيز حماية الحياة الخاصة وفقا لقانون العقوبات من خلال استخدام التقنيات الحديثة في القسم الخامس، الذي يتناول الاعتداءات على الشرف، واحترام الأفراد، وحياتهم الخاصة، وكشف الأسرار، بهدف الحفاظ على سمعة الأفراد. كما تشمل حماية الحياة الخاصة من جريمة التشهير عبر منصات التواصل الاجتماعي، مما يعني استمرار سريان هذه النصوص على الجرائم التي ترتكب في العالم الافتراضي، بما في ذلك جريمة التهديد المنصوص عليها في القسم الثاني "التهديد" والمادة 371 التي تجرم الابتزاز.

العقوبات المفروضة على جريمة التهديد تختلف حسب نوع الجريمة، وتم تنظيمها في قانون العقوبات بالمواد من 284 إلى 287، بالإضافة إلى المادة 371 التي تعنى بجريمة الابتزاز. بفضل الصياغة المطاطية التي إستخدمها المشرع، يمكن تطبيق هذه النصوص بمرونة لتشمل الابتزاز والتهديدات عبر الإنترنت[3].

وتكون العقوبات المقررة كما يلي:

التهديد بواسطة محرر: بموجب المادة 284 من قانون العقوبات، يعاقب كل من يهدد بجرائم القتل أو السجن أو أي اعتداء آخر على الأشخاص، أي بالإعدام أو السجن المؤبد . وفي حال

---

[1]– أنظر المادة 47 من الأمر رقم 58–75 مؤرخ في 20 رمضان عام 1395 الموافق ل26 سبتمبر 1975، المتضمن قانون المدني المعدل والمتمم، ج ر عدد 78، سنة 1975.

[2]– أنظر المادة 46 من قانون المدني المعدل والمتمم، المرجع ذاته.

[3]– سيهام عكوش، المرجع السابق، ص 1303.

تضمن التهديد إيداع مبلغ من المال في مكان معين أو تنفيذ أي شرط آخر، يحكم على المرتكب بالحبس لمدة تتراوح بين سنتين وعشر سنوات، ويُفرض عليه غرامة مالية تتراوح بين 20.001 و100.000 دينار جزائري. بالإضافة إلى ذلك، يمكن فرض عقوبة الحرمان من حقوق معينة ومنعه من الإقامة لمدة تتراوح بين سنة وخمس سنوات.

التهديد غير المصحوب بشرط: وفقا للمادة 285 من القانون الجزائري، يعاقب الفاعل بالسجن لمدة تتراوح بين سنة وثلاث سنوات في حالة التهديد غير المصحوب بشرط أو أمر محدد، دون أن يكون مصحوبا بأي شروط أو أوامر. ويفرض عليه غرامة مالية تتراوح بين 20.001 و100.000 دينار جزائري. كما يمكن الحكم عليه بالحرمان من الإقامة لمدة تصل إلى خمس سنوات كحد أقصى.

التهديد الشفهي: وفقا للمادة 286 من قانون العقوبات، يتعلق التهديد الشفهي بالحديث المصحوب بشرط أو أمر شفهي. في حالة التهديد الشفهي، يتم تطبيق عقوبة الحبس لمدة تتراوح بين ستة أشهر وسنتين، بالإضافة إلى غرامة مالية تتراوح بين 20.001 و100.000 دينار جزائري. كما يمكن أن يُمنع الفاعل من الإقامة لمدة لا تقل عن سنة ولا تزيد عن خمس سنوات.

التهديد بأعمال عنف أخرى: وهو كل تهديد بالاعتداء أو العنف الغير منصوص عليه في المواد من 284 إلى 286 من ق ع ، وهذا حسب المادة 287 من ذات القانون[1].

المادة 371: كل من يحصل بطريق التهديد، سواء كان ذلك كتابيًا أو شفهيًا أو بالكشف عن أسرار أو بهدف الحصول على الأموال أو الأوراق المالية أو التوقيعات أو المستندات المشار إليها في المادة 370 من هذا القانون، أو بأية منفعة مادية أخرى أو لأي غرض آخر، أو يشرع في ذلك، يكون قد ارتكب جريمة الابتزاز. يعاقب على هذا الفعل بالحبس لمدة تتراوح بين سنتين وخمس سنوات، وبغرامة تتراوح بين 500.000 دينار جزائري و1.000.000 دينار جزائري[2].

وجرم الافعال الاعتداء على الحياة الخاصة بموجب المادة 303 مكرر و303 مكرر1 و303 مكرر 2 من القانون أعلاه نصت هذه المواد على أن يعاقب كل من تعدى على حياة الخاصة للغير بأي وسيلة تقنية كانت ، أو حفظ الصورة أو السماح بوضعها للجمهور بالحبس من 06

[1]– أنظر المواد من 284 إلى 287 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

[2]– أنظر المادة 371 من قانون العقوبات المعدل والمتمم، المرجع ذاته.

أشهر إلى 03 سنوات وغرامة من 50.000 إلى 300.000، ويعاقب على الشروع بنفس العقوبات للجريمة التامة[1].

الفرع الثاني: العقوبات التكميلية

العقوبات التكميلية تفرض على الأفراد الطبيعية أو المعنوية كعقوبة إضافية إلى جانب العقوبة الأساسية.

أولا العقوبات التكميلية على جرائم التهديد:

المادة 284 من ق ع أحالة إلى المادة 14 من ذات القانون بالزيادة على العقوبات الأصلية يجوز للمحكمة عند قضائها في جنحة وفي حالات التي يحددها القانون أن تحضر على المحكوم عليه ممارسة حق أو أكثر من الحقوق الوطنية وذلك لمدة لا تزيد عن 5 سنوات وتسري هذه العقوبة من يوم انقضاء العقوبة السالبة للحرية أو الافراج عن المحكوم عليه[2]. وهذه الحقوق مذكورة على سبيل الحصر في المادة 09 مكرر 01 مثل العزل من المنصب العمومي، الحرمان من حق في الانتخاب، الحرمان من حق الترشح في الانتخابات ... وغيرها من الحقوق[3] بالإضافة إلى المنع من الإقامة عن مدة لا تزيد عن 05 سنوات.

ثانيا: العقوبات التكميلية المنصوص على جرائم الاعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار:

أجازت المادة 303 مكرر 02 من ق ع للمحكمة حرمان المحكوم عليه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 09 مكرر 01 لمدة أدناها سنة وأقصاها 05 سنوات كما يجوز لها نشر حكم الإدانة ، وحكم مصادرة الوسائل المستعملة في ارتكاب الجريمة ملازم للعقوبة الأصلية[4].

---

[1]– أنظر مواد من 303 مكرر إلى 303 مكرر 02 من قانون العقوبات المعدل والمتمم، مرجع سابق الذكر.

[2]– أنظر المادة 14 من قانون العقوبات المعدل والمتمم، مرجع ذاته.

[3]– أنظر المادة 09 ، من قانون العقوبات المعدل والمتمم، مرجع ذاته.

[4]– أنظر المادة 303 مكرر 02، من قانون العقوبات المعدل والمتمم، مرجع ذاته.

ثالثا: العقوبات التكميلية على جرائم السرقات وابتزاز الأموال:

نصت المادة 371 من قانون سابق الذكر على العقوبات الأصلية لجريمة الابتزاز والحصول على أموال عن طريق التهديد (المذكورة أعلاه) ، وأضافة عقوبات تكميلية بحرمان الجاني من الحقوق الواردة في المادة 09 مكرر 01 من ق ع لمدة تتراوح من سنة إلى 05 سنوات.

الفصل الثاني

الإطار الإجرائي لجريمة الابتزاز والتهديد عبر الانترنت

رغم أن الجريمة الالكترونية سريعة ومتطورة وغامضة فسعت التشريعات المعاصرة لتتدارك وتلحق هذا التطور وخاصة ما يخص الجانب الإجرائي وقواعد المتابعة القضائية، ومنها الدول العربية فالمشرع الجزائري تدارك وتدخل لمواجهة هذا النوع من الجرائم .

ففي سنة 2004 تطرق لها بموجب قانون 04-15 وبعده قانون 09-04 الذي يعتبر القانون الأساسي للجرائم الالكترونية بحيث أعطى اهتمام خاص بالجانب الإجرائي والوقائي للجريمة المعلوماتية وخصها بإجراءات خاصة تمييزها عن الجرائم الأخرى وتبنى مبدأ عدم انتهاك الحياة الخاصة بموجب قانون 18-07 الصادر سنة 2018 أولى حماية الأشخاص الطبيعيين ومعطياتهم الشخصية عند التفتيش .

فالجرائم الالكترونية تنقسم إلى قسمين جرائم ترتكب بواسطة الانترنت كالتهديد بالتشهير والسب والقذف ... وغيرها ، وجرائم ترتكب على الانترنت كاختراق منظومة معلوماتية وتعديل أو حذف معطيات شخصية والقرصنة وتدمير مواقع وغيرها من الجرائم ، فالمشرع أعطى لها أهمية تواتي خطورتها بسنه عدة قوانين صارمة لكن بالمقابل أغفل على الجرائم التي ترتكب عبر الانترنت وخاصة الماسة بخصوصية الفرد وحرمته وخاصة أن القاضي وجهاز القضاء ككل مقيد بمبدأ الشرعية إذ لا توجد جريمة ولا إجراء وجزاء إلا بنص تشريعي يجرم ويعاقب عليه .

ونظرا لخصوصية جريمة الابتزاز والتهديد عبر الانترنت وأهمية المرحلة الإجرائية من البحث والتحري وخاصة الصعوبات التي تثار في مرحلة الإثبات والتي تجعلها صعبة تطبيق النصوص القانونية للجريمة التقليدية .

المبحث الأول
التحقيق في جريمة الابتزاز والتهديد عبر الانترنت

مواجهة جريمة التهديد والابتزاز عبر الإنترنت، تتطلب التصدي لها جهودا متكاملة تتخذ من الآليات القانونية والإجرائية الفعالة أساسا لها، لكن تعترض عمليات التحقيق في هذه الجرائم صعوبات متعددة تتطلب جهودا إضافية للتغلب عليها. فالطابع الرقمي للجريمة يجعل من تحديد الجناة وجمع الأدلة الرقمية صعبا ومعقدا، حيث يمكن أن يتم تنفيذ الهجمات من مواقع مجهولة أو باستخدام هويات مزيفة.

عند تعرض الضحية لجريمة الابتزاز والتهديد عبر الانترنت، يتقدم بشكوى أمام الضبطية القضائية يتم تحويله إلى رئيس خلية مكافحة الجرائم الالكترونية، للاستماع إلى أقواله فيقوم بتدوين المعلومات التي تساعد في التحقيق عند المعاينة التقنية لحساب المجني عليه في سرية تامة، باعتماد التحقيق الجنائي على التتبع الفني الرقمي كوسيلة دليليه غير مادية، والتي تستند بشكل أساسي على الأدلة الرقمية لتثبت الجريمة، يتسنى للشرطة القضائية قبل بدء التحقيقات المطلوبة، اللجوء إلى المستشارين المتخصصين لاستشارتهم والاستفادة من خبراتهم في تحليل الأدلة الرقمية.

فتناولنا في هذا المبحث مرحلة التحقيق في جريمة الابتزاز والتهديد عبر الانترنت، إجراءات التحقيق في جريمة الابتزاز والتهديد عبر الانترنت (المطلب الأول).

دور الهياكل الخاصة في التحقيق في جريمة الابتزاز والتهديد عبر الانترنت (المطلب الثاني).

المطلب الأول

إجراءات التحقيق في جريمة الابتزاز والتهديد عبر الانترنت

عند تسليم التقرير الذي يشير إلى وقوع جريمة ابتزاز وتهديد الكتروني من رجال الضبطية القضائية، يتم إشعار وكيل الجمهورية بالموضوع. استنادا إلى ذلك، يتم الحصول على إذن بالتفتيش من وكيل الجمهورية، ومن ثم ينتقل الضباط الشرطة القضائية إلى موقع الجاني ويقومون بإيقافه وضبط الأجهزة المستخدمة في ارتكاب الجريمة، يتم بعد ذلك سماع أقوال المشتبه به ومواجه بالتقرير والأدلة المتاحة[1].

وتشمل مرحلة التحقيق في جريمة الابتزاز والتهديد عبر الانترنت على اجراءات تقليدية واجراءات مستحدثة.

قد تواجه الأجهزة الأمنية والقضائية جملة من صعوبات في مرحلة التحقيق، حيث تتغير التقنيات والأساليب المستخدمة من قبل المتسللين بشكل مستمر. هذا يتطلب وجود خبراء متخصصين في التحقيق الرقمي وتطبيق تقنيات التحقيق الحديثة لضمان جودة الأدلة وصحتها في المحاكم.

الفرع الأول: إجراءات التحقيق التقليدية في جريمة الابتزاز والتهديد عبر الانترنت

جريمة الابتزاز والتهديد عبر الانترنت لا تختلف كثيرا عن الجرائم التقليدية من ناحية الاجراءات التحقيق، تعتمد على أساليب تقليدية منها المعاينة والتفتيش بالإضافة إلى الضبط .

فالاختلاف الجريمة الالكترونية عن الجريمة التقليدية يتمحور في اختلاف مسرح الجريمة من مسرح مادي إلى عالم افتراضي رقمي ومجرم ذكي يقابلهم اختلاف في الكوادر الفنية القضائية التي تستلم اجراءات التحقيق.

اولا/المعاينة: المعاينة في جرائم تقنية المعلومات تشمل الانتقال إلى مكان وقوع الجريمة لجمع الأدلة الرقمية والمادية، وتحديد الفاعل. تتطلب هذه المعاينة سرعة ودقة[2]، ويجب أن تتم بواسطة

[1]– سيهام عكوش، المرجع السابق، ص 1306.

[2]– أنظر المادة 42 من أمر 66–155 مؤرخ في 08 جوان 1966 الموافق ل18صفر 1386 المتضمن قانون الاجراءات الجزائية الجزائري، المعدل والمتمم، ج ر عدد 51، سنة 1966.

خبراء متخصصين. تشتمل شروط صحة المعاينة على التحكم في موقع الجريمة، وترتيب المعاينة بدقة، والتحفظ على الأدلة بمبدأ المشروعية وفقا لقانون إ.

في الجرائم التقليدية، تكون مسرح الجريمة المادي يتضمن المكونات المحسوسة مثل الأدوات والأشياء المتعلقة بالجريمة. أما في الجرائم الالكترونية، يتعامل المعاينون مع البيانات الرقمية داخل بيئة الحاسوب والانترنت وتتطلب هذه المعاينة خبرة خاصة للتعامل مع الأدلة الرقمية بفعالية ودقة.

ويقصد بمعاينة مسرح الجريمة الالكتروني: معاينة الآثار التي يتركها مستخدم الشبكة الالكترونية، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكل الاتصالات التي تمت من خلال الحاسوب الآلي والشبكة الالكترونية[1].

ضوابط المعاينة في جرائم تقنية المعلومات:

أ/ الضبط في مسرح الجريمة التقليدي: يتميز بأنه خارج بيئة الحاسوب ويتكون أساسا من الأدوات والأشياء الملموسة التي وقعت فيها الجريمة. قد تترك الجرائم التقليدية آثارا مادية مثل البصمات أو الأدلة الشخصية أو وسائط تخزين رقمية[2]، يتم تفحص هذه الأشياء بواسطة مأموري الضبط القضائي لتحديد صلاحية المسرح وجمع الأدلة. يتم وضع الأختام في الأماكن التي تمت فيها المعاينة والتحفظ على الأدلة المادية وإخطار النيابة العامة بها. هذا النوع من المعاينة يتم بسهولة بسبب وجود الأدلة المادية الملموسة، على عكس المعاينة الإلكترونية التي قد تتطلب التعامل مع عناصر غير مادية[3].

ب/ الضبط في مسرح الجريمة الافتراضي: مسرح الجريمة الإلكتروني يتميز بأنه داخل البيئة الإلكترونية، ويتألف من البيانات الرقمية التي تتحرك وتتنقل داخل أنظمة الحاسوب وشبكة

[1]– ابراهيم خالد ممدوح، فن التحقيق الجنائي في الجرائم الالكترونية، ط 02، دار الفكر الجامعي، الإسكندرية، 2010، ص 165.

[2]– محمد بن نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 77.

[3]– سعيد سالم المزروعي، عبد الرحمان عزمان، اجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا لتشريع الإماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، المجلد 02، العدد 13، أكتوبر 2018، ص 111.

الإنترنت، بما في ذلك الذاكرة والأقراص الصلبة. لاستخراج الأدلة الرقمية من هذا المسرح، يتطلب ذلك خبراء متخصصين في التحليل الرقمي[1].

تظهر في هذه الجرائم تحديات عدة تجعل المعاينة أقل فعالية، بما في ذلك ندرة الأدلة المادية التي قد تكون محدودة على الأدوات المعلوماتية والبرامج، بالإضافة إلى كثافة الأشخاص الذين يترددون على المسرح الإلكتروني، مما يعطي فرصة للتلاعب بالأدلة الرقمية[2].

ثانيا/التفتيش: التفتيش في السياق القانوني يعد جزءا من إجراءات التحقيق، ويهدف إلى جمع الأدلة المادية والمعنوية المتعلقة بالجريمة ومحل تنفيذها، وتحديد ما يساهم في كشف الحقيقة[3]. يمكن تعريف التفتيش فيما يتعلق بالمعلومات على أنه البحث في الأجهزة الرقمية أو الشبكات للعثور على دلائل تثبت وقوع الجريمة وتتبعها للمتهم[4].

شروط التفتيش تنقسم إلى موضوعية وشكلية، حيث يتطلب الموضوعية وجود محل للتفتيش وسبب له، وأن يتم التفتيش بقرار قضائي صادر عن السلطة المختصة. بالنسبة للتفتيش في الجرائم الإلكترونية، يشمل ذلك الأجهزة والشبكات ولو عن بعد والأفراد المرتبطين بالجريمة الرقمية[5].

أما الشروط الشكلية، فيشترط وجود محضر تفتيش وجودا للتفتيش في الجرائم الرقمية وتسمى محاضر الشرطة القضائية وتكمن أهميتها في القيمة الممنوحة لها كوسيلة إثبات من جهة ومن خطورة الصلاحيات الممنوحة بموجبها لضباط الشرطة القضائية [6]، ويتم تنفيذه في أوقات من الساعة الخامسة صباحا إلى الثامنة مساءا، غير أنه يمكن كسر هذه القاعدة في الحالات الاستثنائية كجرائم المخدرات، الجريمة المنظمة عبر الحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، الإرهاب ... ، المنصوص عليها في ق إ ج التي تبين أن المشرع أجاز

---

[1]– محمد بن نصير السرحاني، المرجع السابق، ص 77.

[2]– سعيد سالم المزروعي، عبد الرحمان عزمان، المرجع السابق، ص 118.

[3]– على حسن طوالبة، التفتيش الجنائي على النظم الحاسوب والانترنت، عالم الكتب الحديثة، الأردن، 2004، ص 11.

[4]– سماح حمودي، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية، العدد 08، الجزء 01، المركز الجامعي، بريكة، جوان 2017، ص 328.

[5]– عز الدين عثماني، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد 04، جانفي 2018، ص 58.

[6]– المرجع ذاته.

التفتيش في الجرائم المتعلقة بالمعالجة الآلية للمعطيات[1]. ويشترط أيضا وجود المتهم أو ممثل له أثناء التفتيش، وإذا كان غير ممكن يجب تعيين ممثل أو شهود غير موظفين في التحري.

أ/ اجراءات التفتيش في الجرائم الالكترونية: تعد اجراءات التفتيش من صلاحيات سلطة التحقيق، ويناط لضباط الشرطة القضائية القيام بها في حالات استثنائية، ويقوم المفتش في إطار البحث عن الجرائم التي تقع باستخدام تكنولوجيا الاعلام والاتصال. بمجموعة من الاجراءات منها:

اجراءات التفتيش في نظام معلوماتي خاص بالمتهم: في حالة وجود جريمة داخل نظام المعلومات الخاص بالمتهم، يجرى التفتيش وفقا للشروط القانونية، لجمع الأدلة المتعلقة بالجريمة، مثل البرامج والملفات المشتبه فيها، وهذا ما يكثر في جرائم التزوير والتزييف وغيرها. تتضمن هذه العملية فحص الأجهزة ووسائط التخزين المتعددة كأجهزة الماسح الضوئي وطباعات ملونة التي تم استخدامها في ارتكاب الجريمة، مما يمكن من الحصول على دليل يثبت ارتكاب الجريمة[2].

اجراءات التفتيش في نظام معلوماتي غير خاص بالمتهم: وهو ما نجده في الجرائم التي ترتكب باستخدام الشبكات ، حيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في نظام المعلوماتي الجريمة ، في هذه الحالة تتطلب اجراءات التفتيش والضبط الدخول في نظام معلوماتي لشخص آخر. وقد نص ق إ ج أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المنصوص عليها في القانون، أو في حالات طلب المساعدة من الداخل وهو مدعى المشرع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن وكذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم [3].

ثالثا/ الضبط: في قانون الاجراءات الجزائية، يعرف الضبط بوضع اليد على الأشياء المرتبطة بالجريمة والتي تساعد في كشف الحقيقة عنها وعن مرتكبها. يتم الضبط فقط على الأشياء

---

[1]– أنظر المادة 47 من قانون الاجراءات الجزائية المعدل والمتمم، مرجع سابق الذكر.

[2]– عز الدين عثماني، المرجع السابق، ص 60.

[3]– المرجع السابق، ص 61.

المادية، حيث لا يمكن الضبط على الأشخاص أو الأشياء المعنوية. يشترط لصحة الضبط أن يكون الشيء مفيدا في كشف الحقيقة، ويتم توجيهه فقط للأشياء وليس للأشخاص[1].

أ/ الضبط في الجريمة المعلوماتية:

- الأدلة المادية التي يجوز الضبط فيها: فالأدلة المادية التي يجوز ضبطها في الجرائم العالم الإفتراضي، والتي لها قيمة خاصة في إثبات الجرائم ونسبها إلى المتهم هي: الأوراق والمستندات الرسمية سواء تحضيرية أم أصلية أساسية أو قانونية أيضا جهاز الحاسوب وملحقاته وأقراص الليزر وأسطوانات والشرائط الممغنطة[2]، البطاقات الممغنطة وبطاقات الائتمان والهواتف، ألواح الذكية .... وغيرها.

- ضبط مكونات المادية للحاسب الآلي: ويقصد به المكونات الملموسة للحاسب الآلي وملحقاته ومنها: وحدة المعالجة المركزية ولوحة المفاتيح والشاشة والفأرة بالإضافة إلى الأقراص والأشرطة المغناطسية ولوحة الدوائر الإلكترونية ،أجهزة الاتصال عبر شبكة الانترنت كجهاز المودم[3]. وكذلك وحدة الذاكرة الرئيسية ، وحدة التحكم ، وحدة المخرجات وكذلك ضبط وحدات التخزين الفرعية ،وحدة المدخلات[4].

- ضبط المكونات المعنوية للحاسب الآلي: وهو كل ما يخص برامج وبيانات ومعلومات وما تحويه من رسائل وصور ومعلومات وملفات.

ضبط برامج وبيانات الحاسب الآلي: تنص المادة 06 من القانون 09-04 على ضرورة حجز المعطيات المحل البحث، وأيضا المعطيات الضرورية لفهمها، وذلك على أجهزة تخزين إلكترونية يتم اكتشافها من قبل السلطات عند التفتيش في المنظومة المعلوماتية. ويجب وضع هذه المعطيات في الأحراز، مع ضرورة الحفاظ على سلامتها في المنظومة المعلوماتية. كما

---

[1]– أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة، 2007، ص 164.

[2]– عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط 02، منشورات الحلبي الحقوقية، بيروت، لبنان، ص 373.

[3]– عبد الله الحسين على حمودة، سرقة المعلومات المخزنة في الحاسب الآلي، ط 02، دار النهضة العربية، القاهرة، 2001، ص 398-399.

[4]– وحدة المخزنات وما تشمله: كلوحة الشاشة والطباعة. وحدات التخزين الفرعية: تشمل أقراص ممغنطة بنوعيها المرن والصلب الأشرطة الممغنطة. وحدة المدخلات وما تشمله: كلوحة المفاتيح ونظم ادخال المرئي ونظام القراءة.

يجوز استخدام الوسائل التقنية لتشكيل أو إعادة تشكيل هذه المعطيات، شريطة عدم المساس بمحتواها.

أما المادة 07 من نفس القانون، فتنص على أنه في حالة عدم القدرة على إجراء الحجز بسبب أسباب فنية، يجب على السلطة المختصة بالتفتيش استخدام التقنيات اللازمة لمنع الوصول إلى محتوى المعطيات أو نسخها، مع الاحتفاظ بها من قبل الأشخاص المصرح لهم بذلك.

بالنسبة للمادة08، فتتعلق بالمعطيات التي تحتوي على محتوى جريمة، حيث يجب على السلطة المباشرة بالتفتيش إصدار أمر بتكليف شخص مؤهل فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة لمنع الوصول إلى محتوى هذه المعطيات.

تنص المادة 09 على أن المعلومات المتحصل عليها عن طريق المراقبة وفقا للقانون، لا يجوز استخدامها إلا في حدود الضرورة التي يقضيها التحري أو التحقيق[1].

تعكس هذه النصوص اهتمام المشرع الجزائري بالتحديات التي تواجه عمليات ضبط البيانات المعلوماتية، حيث يظهر استخدام مصطلح "حجز" بدلاً من "ضبط"، مما يشير إلى الاعتراف بأن المعطيات المعلوماتية تختلف عن الأشياء المادية وتستوجب معاملة خاصة[2].

ضبط الرسائل ومراقبة الاتصالات الالكترونية: سهلت ثورة المعلومات الاتصال بين الأفراد، وأثرت على مختلف جوانب الحياة. ومع ذلك، أدت هذه التطورات أيضا إلى زيادة جرائم انتهاك الخصوصية الشخصية، خاصة عبر وسائل الاتصال الإلكترونية[3]. لحماية هذه الخصوصية،

[1]– أنظر المواد من 06 إلى 09 من قانون 09-04 المؤرخ في 14 شعبان 1430الموافق ل5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر عدد 47، الصادرة بتاريخ 16 أوت 2009.

[2]– فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة لنيل على شهادة الدكتوراه في الحقوق، فرع قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر01، 2010-2011، ص 350.

[3]– علي محمود على حموده، الأدلة المتحصلة من الرسائل الالكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد 01، دبي –الإمارات العربية المتحدة– 26-28 نيسان 2003، ص 32.

أقرت العديد من الدول تشريعات دستورية تحظر انتهاك الخصوصية في المراسلات، مثل الدستور الجزائري الذي ينص على سرية المراسلات والاتصالات بمختلف أشكالها[1].

ومع ذلك، تسمح القوانين الإجرائية في بعض الحالات بضبط المراسلات ومراقبة المحادثات الهاتفية، وذلك لحماية حقوق المجتمع والأمن العام.

فسنبين في النقاط التالية ضبط المراسلات الالكترونية:

البريد الالكتروني: من بين الجوانب الهامة المتعلقة بالبريد الإلكتروني، يجب المحافظة على سريته، مما أدى إلى ظهور برامج تشفير خاصة تجعل الرسائل غير قابلة للوصول إليها إلا بوجود الشفرة الصحيحة. تمثل البرامج المشفرة تطورا في عمليات التراسل عبر البريد الإلكتروني[2].

هناك جدل فقهي حول طبيعة الرسائل الإلكترونية مقارنة بالرسائل الورقية، حيث يرى البعض أن الرسائل الإلكترونية مجرد موجات كهرومغناطيسية تختلف تماما عن المستندات الورقية، بينما يعتبرها آخرون مستندات تقليدية. يلاحظ أن هناك تضاربا في بعض الأحكام المتعلقة بحق الإطلاع على هذه الرسائل، وذلك وفقا للنصوص التقليدية[3].

في القانون الجزائري، تم تضمين مصطلحات تقنية جديدة في قوانين جديدة تتعلق بضبط الرسائل الإلكترونية في بعض الجرائم، مثل الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات. هذه النصوص تختلف عن النصوص التقليدية بتركيزها على جوانب تقنية تسمح لقاضي التحقيق أو ضابط الشرطة القضائية بالتدخل في المراسلات وتسجيل الأصوات والصور[4]. ويظهر ذلك من خلال المادة 65 مكرر 5 من قانون الإجراءات الجزائية، التي تسمح في حالات معينة بتنفيذ أساليب تحريات خاصة في بعض الجرائم، مثل الجرائم المعلوماتية، بموافقة وكيل الجمهورية وتحت إشرافه.

---

[1]– أنظر المادة 47 فقرة 02 من الدستور الجزائري.

[2]– علي محمود على حموده، المرجع السابق، ص 33.

[3]– فايز محمد راجح غلاب، المرجع السابق، ص 352.

[4]– أنظر المواد من 65 مكرر 05 إلى 65 مكرر 10 من قانون الاجراءات الجزائية المعدل والمتمم.

وتنص المادة 03 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على أنه يمكن، وفقا لقواعد محددة في القانون، ومع مراعاة سرية المراسلات والاتصالات، لمستلزمات التحقيقات القضائية وحماية النظام العام، تطبيق ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتسجيلها وتحليلها في الحالات التي تقتضي ذلك[1].

التنصت والمراقبة الالكترونية لشبكات الحاسب الآلي: يقصد من مراقبة المحادثات الهاتفية وتسجيلها أنها جزء من إجراءات التحقيق التي تشرف عليها السلطة المختصة، بهدف البحث عن أدلة قانونية تثبت ارتكاب جريمة من قِبل شخص مشتبه به، أو لتحصيل أدلة تعزز القضية ضده. يتم اتخاذ مثل هذه الإجراءات الاستثنائية عندما تكون الجريمة ذات درجة من الخطورة تبرر ذلك[2].بموجب تعديل قانون العقوبات سنة 2006 أدرجت نصوص قانونية تتعلق بالتدابير المتعلقة بمراقبة المراسلات وتسجيل الأصوات والتقاط الصور، والتي تشمل عدة أحكام تم توضيحها في المواد مكرر 5 إلى مكرر 10 من المادة 65. هذه الأحكام تشمل:

- لا يمكن إلغاء الإجراءات التقنية في حالة اكتشاف جرائم أخرى بشكل غير مباشر.
- يجب أن يتضمن الإذن التفصيلات الكاملة لتحديد المراسلات المراد التقاطها والأماكن المستهدفة ونوع الجريمة المبررة للاستخدام الجائز لهذه التدابير، ويجب أن يكون الإذن مكتوبًا وصحيحًا لمدة لا تزيد عن أربعة أشهر وقابل للتجديد.
- يحق للوكيل العام أو قاضي التحقيق أو ضابط الشرطة القضائية تكليف موظف مؤهل لتنفيذ الجوانب التقنية للعمليات.
- يجب توثيق جميع عمليات الاعتراض أو التسجيل بمحاضر، بما في ذلك إعداد الترتيبات التقنية وتسجيل الأصوات والصور، مع تحديد توقيت بداية ونهاية كل عملية[3].

[1]– أنظر 03 من قانون 09–04، مرجع سابق الذكر.

[2]– علي محمود على حموده، المرجع السابق، ص 34.

[3]– أنظر المواد 65 مكرر 05 إلى 65 مكرر 10 من قانون الاجراءات الجزائية المعدل والمتمم.

ومع ذلك، لم تشمل هذه الأحكام بشكل صريح مراقبة الاتصالات الإلكترونية. لذا، أدرجت في القانون رقم 09-04 والذي يتضمن ترتيبات تقنية لمراقبة الاتصالات الإلكترونية[1]، وتتمثل هذه المراقبة في نوعين: المراقبة الوقائية التي تهدف إلى منع الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، والمراقبة القضائية التنظيمية[2].

الفرع الثاني: اجراءات التحقيق المستحدثة في جريمة الابتزاز والتهديد عبر الانترنت:

أصبحت الطرق التقليدية التي جاء بها ق إ ج غير كافية للوصول إلى دليل فيما يخص هذا النوع الاجرامي المستجد والذي يحتاج إلى طرق وتقنيات جديدة تتناسب مع طبيعته، فنظرا للطبيعة الخاصة للجرائم الالكترونية في عناصرها ووسائل وتقنيات ارتكابها فقد قام المشرع بسن نصوص اجرائية جديدة تواكب الحاصل في هذا المجال خاصة فيما يتعلق بمسألة التحقيق والإثبات.

اولا / التسرب الالكتروني: تعتبر عملية "التسرب" من الإجراءات الجديدة في البحث وتحقيق في الجرائم، وتأتي ضمن إطار مرسوم رئاسي رقم 02-05 والمادة 56 من قانون 06-01 المتعلق بمكافحة الفساد. يسمح هذا الإجراء بجمع الأدلة من خلال تسليم المراقب أو استخدام أساليب تحرٍ خاصة مثل الترصد الإلكتروني والاختراق، بموافقة السلطات القضائية المختصة[3].

بالرغم من وجود بعض الغموض في تفسير المادة، يفهم من مصطلح "التسرب" أن ضابط الشرطة القضائية أو موظفو الشرطة القضائية يقومون بمراقبة الأشخاص المشتبه فيهم بارتكاب جريمة معينة، وذلك من خلال التظاهر بالتعاون معهم بهدف استخلاص المعلومات أو الأدلة[4].

في جرائم الإنترنت، يمكن تطبيق هذه العملية من خلال تكليف ضابط الشرطة القضائية أو أحد أعوان الشرطة القضائية، بالمشاركة في محادثات غرف الدردشة أو حلقات النقاش عبر

---

[1]- ويقصد بالجرائم المرتبطة بتكنولوجيا الاعلام والاتصال في قانون 09-04 في المادة 02 فقرة"أ" هي جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات(الدخول الغير مصرح به، التخريب، حذف،...) وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

[2]- زهية معيش، نسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2012-2013، ص 34.

[3]- أنظر المادة 56 من قانون رقم 06-01 مؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته، ج ر عدد 14، الصادة في 08 مارس 2006.

[4]- أنظر المادة 65 مكرر 12 من قانون الاجراءات الجزائية المعدل والمتمم.

الإنترنت، حيث يتظاهر المتسرب بتواجده تحت اسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل مثلهم. يهدف المتسرب إلى استخلاص المعلومات منهم حول كيفية ارتكابهم للجرائم، بهدف جمع الأدلة[1].

ثانيا / اعتراض المراسلات والمراقبة الالكترونية:

أ / اعتراض المراسلات: تم سن هذا الإجراء بموجب المواد من 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجنائية. يتيح القانون للقاضي التحقيق، بإذن كتابي، وتحت إشرافه، أن يأمر ضابط الشرطة القضائية بإعتراض المراسلات الإلكترونية دون موافقة الطرف المعني، لتسجيل الكلام أو التقاط الصور في الأماكن الخاصة أو العامة لتنفيذ التحقيقات الجنائية[2]. تشترط الضمانات القانونية وجود مبرر شرعي وإذن من السلطة القضائية، وتحديد مدة 4 أشهر للاعتراض، قابلة للتجديد وفقا لمتطلبات التحقيق[3].

ب / المراقبة الالكترونية: لم يعرفها المشرع الجزائري، عرفها المشرع الأمريكي بأنها عملية الاستماع إلى محتوى الاتصالات الصوتية عبر استخدام أجهزة إلكترونية أو أية وسائط أخرى[4]. ولقد حددت المادة 03 من قانون 09-04 كيفية مراقبة الاتصالات، ومنه فإن عملية مراقبة الاتصالات الالكترونية حددها المشرع على سبيل الاستثناء في الحالات المحددة حصرا في المادة 04 من قانون 09-04[5]، تتم بطريقة سرية، وضع ترتيبات تقنية للمراقبة وتسجيلها في حينها[6].

ثالثا / حفظ المعطيات المتعلقة بحركة السير(إلتزامات مقدمي الخدمات):

يتمثل أحد الإجراءات التحفظية المهمة التي نص عليها في قانون الإجراءات الجنائية في إصدار قاضي التحقيق، سواء بناءا على طلب من النيابة العامة أو بشكل تلقائي، تدابير

---

[1]– مريم عراب، المرجع السابق، ص 1227.

[2]– أنظر المادة 65 مكرر 05 من قانون الاجراءات الجزائية المعدل والمتمم.

[3]– أنظر المادة 65 مكرر 07 من قانون الاجراءات الجزائية المعدل والمتمم.

[4]– عبد القادر فلاح، آية عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية اثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 04، العدد 02، جامعة الجيلالي بونعامة، خميس مليانة، 2019، ص 1699.

[5]– أنظر المادة 04 من قانون 09-04.

[6]– أنظر المادة 03 من قانون 09-04.

تحفظية أو أمنية إضافية خلال جميع مراحل الإجراءات، زيادة على حجز الأموال المتعلقة بالجريمة[1]. ونظرا لمرونة الدليل التقني في العالم الافتراضي، حيث يمكن للمتهم إزالة الأدلة عن بعد، فإنه يتوجب وضع إطار قانوني لحفظ المعطيات المتعلقة بالتحقيقات الجنائية، وقد قضى بذلك قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/22. ويتعهد مقدمو الخدمات بتقديم المساعدة للسلطات القضائية، وفقا للالتزامات المحددة في المادة 10 من القانون 09-04 وبناء على ذلك فإن الرسائل الإلكترونية التي تصل مقدم الخدمة ولم يطلع عليها بعد تحفظ في حالة تخزين إلكتروني، قابلة للمسح أو الاحتفاظ بها بناء على تقدير مقدم الخدمة.

يلتزم مقدمي الخدمات بتقديم المساعدة للسلطات القضائية المختصة، وقد حددت المادة 10 من ذات القانون هذه الالتزامات بما يلي:

الالتزام بجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، ويتم تبادلها عن طريق خدمات الانترنت المختلفة سواء الويب أو الايمايل...وغيرها[2].

الالتزام بوضع المعطيات المراد حفظها تحت تصرف السلطات، وقد حددت المادة 11 من نفس القانون طريقة الحفظ ، ومدة الحفظ والتي تقدر من تاريخ التسجيل[3].

الالتزام بحفظ السر المهني عند القيام بجمع أو تسجيل المعطيات أو عند القيام بحفظها[4].

وبناءا على ما تقدم فإن المراسلة بالبريد الالكتروني والتي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها بعد فإنها تستقر في حالة تخزين الكتروني لدى مزود الخدمة إما أن يقوم بمسح تلك الرسالة أو تخزينها[5].

---

[1]- أنظر المادة 40 مكرر 05 من قانون الاجراءات الجزائية.

[2]- مريم عراب، المرجع السابق، ص 1227.

[3]- أنظر المادة 11 من قانون 09-04.

[4]- أنظر المادة 10 من قانون 09-04.

[5]- مريم عراب، المرجع السابق، ص 1228.

الفرع الثالث: الصعوبات التي تواجه اجراءات التحقيق في جريمة الابتزاز والتهديد عبر الانترنت

يعتبر اجراء التحقيق في جريمة الابتزاز والتهديد عبر الانترنت أمر ليس بالهين، بسبب الصعوبات التي تثيرها هذه الجريمة في شبكة وهمية وهذا يأثر بشكل مباشر على فقدان الثقة في القضاء وزيادة انتشار هذه الجريمة.

اولا/ نقص خبرة جهات التحقيق: مكافحة الجرائم في العالم الرقمي تتطلب ذكاء ومرونة، حيث يمكن للمجرمين بسهولة إخفاء الأدلة وتلاعب بالبيانات. يعتبر التحقيق في هذا المجال تحديا، نظرا لنقص الخبرة لدى جهات الاختصاص، وقلة التدريب على التعامل مع الأدلة الإلكترونية وتقنيات البحث والتحليل. هذا الواقع يمثل ثغرة كبيرة في النظام الجنائي، حيث يجب تعزيز الاستعداد والتدريب للتأكد من أن رجال القانون مجهزون تجهيزا جيدا للقيام بالتفتيش والمعاينة في بيئة افتراضية.

المحقق الجنائي في هذا المجال يجب أن يمتلك فهما عميقا للتكنولوجيا الحديثة، يجب أن يتعامل مع المكونات المادية للأجهزة مثل الطابعات والماسحات الضوئية والكاميرات، لتحديد ارتباطها بالأجهزة الأصلية وتقييم الوسائط المستخدمة لتخزين الأدلة الرقمية. هذا يشمل التحقق مما إذا كانت الأدلة جزءا من الجريمة أم لا.

بالإضافة إلى ذلك، يجب أن يكون المحقق قادرا على تقديم تحليلات فعالة لتقديم الأدلة الموثوقة في المحاكم، ومنع تلاعب المجرمين بالبيانات الرقمية[1]. تعد هذه المهارات الحديثة أساسية لمواجهة جرائم االالكترونية ومنها جريمة الابتزاز والتهديد عبر الانترنت.

ثانيا / نقص الوعي بالإبلاغ عن الجريمة: جريمة الابتزاز والتهديد عبر الانترنت غالبا ما تتعلق بأمور حساسة ومخالفة للأخلاق العامة، مما يجعل الكثير من الضحايا يترددون في الإبلاغ، خاصة إذا كانت الضحية امرأة، نظرا لأن المجتمع الجزائري يعتبر هذه القضايا مسيئة فتخشى الضحية من ردت فعل العائلة والمجتمع. بالإضافة إلى ذلك، تتجنب الشركات والمؤسسات المالية الإفصاح عن حالات الابتزاز خوفا من التأثير السلبي على سمعتها والخسائر المحتملة، مما يعوق جهود الأمن في مكافحة هذه الجريمة.

[1]– مريم عراب، المرجع السابق، ص 1215-1216.

ثالثا / فقدان آثار الجريمة: جرائم المعلوماتية تختلف عن الجرائم الأخرى بطبيعتها غير المادية، إذ يتم ارتكابها في عالم افتراضي غير ملموس. البيانات والمعلومات المتعلقة بها قد لا تحتوي على آثار أو بصمات يمكن من خلالها تحديد مرتكبي الجريمة[1]، وبالإضافة إلى ذلك يعتبر الدليل في العالم الرقمي سهلا للإزالة والتلاعب به.

رابعا/ تنازع الاختصاص: المشرع الجزائري عالج مشكلة الاختصاص في قانون الاجراءات الجزائية فقد حدد من خلال هذه النصوص مجال اختصاص المحاكم ووكلاء الجمهورية وقضاة التحقيق ، إما لمكان وقوع الجريمة ، محكمة إلقاء القبض ، أو محكمة موطن إقامة المدعى عليه[2].

فهذه المجالات المحددة كقاعدة عامة فقد حددها المشرع لكل الجرائم ووسع رقعة الاختصاص ليشمل دوائر اختصاص محاكم أخرى أو لكافة الاقليم الوطني عن طريق التنظيم في الجرائم المخدرات ، الجريمة المنظمة عبر الوطنية ،إرهاب ، تبييض أموال ، جرائم الماسة بالأنظمة المعالجة الآلية للمعطيات ، الجرائم المتعلقة بالتشريع الخاص بالصرف .

رغم فطنة المشرع الجزائري لتدارك مشكلة الاختصاص وتسريع وتسهيل وصول الجهات القضائية وسع مجال مهام جهات التحقيق في جرائم المعلوماتية ، فتظل هذه القاعدة عاجزة على أن تطبق على جرائم الالكترونية لإخلاف طبيعتها وبيئتها ، فالجريمة الالكترونية ترتكب عبر عالم افتراضي كذلك عبر وسائل تقنية متطورة تربطها شبكة إيصالات لامتناهية غير ملموسة وهمية متاحة للجميع وغير تابعة لأي نظام حكومي أو سياسي[3] . فيصعب تحديد مكان الشخص ولا حتى التعرف على شخصيته الحقيقة (الاسم واللقب والموطن). إن الانترنت عكس غيرها من وسائل الاتصالات لا تعرف حدودا جغرافيا، سواء بالنسبة للمرسل

[1]– أحمد آيت طالب، العلاقة بين الإرهاب المعلوماتي والجريمة المنظمة، الدورة التدريبية في مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، قسم البرامج التدريبية، القنطيرة، المملكة المغربية 9-2006/04/13، ص 16.

[2]– أنظر المواد 37، 40، 329 من قانون الاجراءات الجزائية المعدل والمتمم.

[3]– عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل الدكتوراه، علوم في القانون الخاص، جامعة ابوبكر بلقايد، تلمسان، 2018، ص 316.

أو المستقبل أي يستطيع كل مستعمل للحاسب الآلي معلومات بدون اي اعتبار لحدود الجغرافية[1]، وهذا ما آثار تنازع الاختصاص دوليا.

فاختلاف التشريعات والنظم القانونية التي خلفها غياب السيطرة على شبكة الانترنت وعدم تبعيتها لأي نظام وعدم اعترافها بأي حد جغرافي حتى سميت غابة بلا قانون، خلفت تنازع الاختصاص عند حدوث جرائم تخص هذه الشبكة وتكون تمس أكثر من دولة فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل شخص من جنسية أخرى، مما يعرض هذه الجريمة لاختصاص الدولة الثانية بموجب مبدأ الشخصية، بالإضافة إلى ذلك يمكن أن تشكل هذه الجريمة تهديدا مباشرا لأمن وسلامة دولة أخرى وبالتالي يمكن للدولة المتضررة التدخل وفقا لمبدأ الاختصاص العيني لحماية مصالحها. كما تثير فكرة تنازع الاختصاص القضائي تحديات إضافية، خاصة عند تأسيس الاختصاص على أساس إقليمي، حيث يتطلب ذلك تنسيقا دوليا فعالا وتطوير إجراءات قانونية مشتركة لضمان تحقيق العدالة[2]، كما لو قام الجاني ببث الصورة الخليعة ذات طابع الإباحي من إقليم دولة معينة في دولة أخرى ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة[3].

خامسا/ صعوبة /لإنابة القضائية الدولية: الإنابة القضائية الدولية تستند إلى الواجبات والإلتزامات التي ينص عليها القانون الدولي، وتشمل تنفيذ التحقيقات لصالح السلطات القضائية المختصة في الدولة الطالبة، وذلك مع احترام حقوق وحريات الإنسان المعترف بها دوليا. وعلى الجانب المقابل، تتعهد الدولة الطالبة بتقديم المساعدة والتعامل بالمثل، واحترام النتائج القانونية التي تتوصل إليها. لكن إجراءات الانابة القضائية تعرف بطء وتعقيدا[4] وهذا ما يتعارض مع سرعة الجريمة وسرعة إختفاء الدليل.

---

[1]– طارق عثمان، الحماية الجنائية للحياة الحاصة عبر الانترنت دراسة مقارنة، مذكرة لنيل الماجستير قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، فرع الماجستير قانون جنائي، جامعة محمد خيضر، بسكرة، 2006-2007، ص 28.

[2]– محمد هشام فريجة، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الالكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، العدد 24، كلية الحقوق والعلوم السياسية، جامعة المسيلة، جوان 2018.

[3]– حسين بن سعسد بن سيف الغافري، المرجع السابق، ص 53.

[4]– أمال برحال، المرجع السابق، ص 84.

سادسا/ صعوبات تحديد قانون واجب التطبيق:

- مبادئ تحديد قانون واجب التطبيق: تقسم المبادئ التقليدية في تحديد القانون الواجب التطبيق إلى ثلاث مبادئ رئيسية: المبدأ الإقليمي للنص الجنائي، والمبدأ العيني للنص الجنائي، والمبدأ الشخصي للنص الجنائي. يتمثل المبدأ الإقليمي في تطبيق التشريع الجنائي الوطني على الجرائم المرتكبة داخل الحدود الوطنية، بغض النظر عن جنسية الفاعل، بينما ينص المبدأ العيني على تطبيق القانون الوطني على بعض الجرائم بشكل معين، حتى لو لم تحدث داخل الإقليم الوطني، وبغض النظر عن جنسية المرتكب[1] أما المبدأ الشخصي فيتعلق بتطبيق القانون الوطني بناء على جنسية المرتكب. ومع ذلك، تعتبر هذه المبادئ محدودة فيما يتعلق بالجرائم المرتكبة عبر الإنترنت، حيث تفقد الجرائم الإلكترونية هويتها الجغرافية، مما يجعل تطبيق هذه المبادئ غير فعال.

- إنتفاء المبادئ التقليدية أمام خصوصية جريمة الابتزاز والتهديد عبر الانترنت: إن المبادئ التي تحكم الجريمة التقليدية تنتفي أمام خصوصية جرائم الانترنت عامة وجريمة الابتزاز والتهديد خاصة، وهذا راجع لعدم تبعية شبكة الانترنت لأي كيان أو نظام أو جهة محددة وأنها لاتوجد لها رقابة أو سيطرة فلا يوجد لها نص جنائي يأطرها ، فالقاوانين الجنائية التي تطبق على هذه الشبكة تتفاوت من دولة إلى أخرى.و تتعدد بتعدد الدول المرتبطة بها بعتبار أن القانون الجنائي يتعلق بسيادة الدولة[2].

سابعا / قصور التعاون الدولي: يعتبر التعاون الدولي في جريمة الابتزاز والتهديد عبر الانترنت صعب وهذا راجع لأسباب التالية:

عدم وجود نموذج اجرامي موحد: في العديد من الحالات، يكون هناك اختلاف في التعريفات القانونية والتصنيفات لجرائم الابتزاز والتهديد عبر الإنترنت بين الدول المختلفة. هذا الاختلاف يجعل من الصعب على الدول التعاون مع بعضها البعض في مكافحة هذه الجرائم بشكل فعال

[1]– عبد الرحمان هيان الرشيد الغازي، الحماية القانونية من الجرائم المعلوماتية (الحاسب والانترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، 2004، ص 499.

[2]– يوسف صغير، المرجع السابق، ص 144.

فتثار اشكالية تحديد القانون الواجب التطبيق هل يعود للدولة التي ارتكبت فيه الجريمة أم الدولة التي ظهرت فيها آثار الضارة وكذلك تعارض القوانين من الناحية الموضوعية والاجرائية[1].

تنوع واختلاف النظم القانونية الإجرائية: كل دولة تملك نظاما قانونيا مختلفا، مما يعني وجود اختلافات في الإجراءات القانونية والقوانين المعمول بها. هذا يؤدي إلى تعقيد عمليات التعاون القضائي الدولي ويمكن أن يؤثر على سرعة وفاعلية التحقيقات والملاحقات الجنائية.

عدم وجود قنوات اتصال: إن النقص في القنوات الرسمية والفعالة للاتصال والتواصل بين السلطات القضائية في الدول المختلفة يعرقل تبادل المعلومات والبيانات ذات الصلة فيما يتعلق بالجرائم عبر الإنترنت. هذا العائق يزيد من صعوبة اجراءات التحقيق وجمع الأدلة لمكافحة هذه الجرائم[2].

هذه العوامل تجعل من التحديات الرئيسية التي تواجه التعاون القضائي الدولي في مجال مكافحة جرائم الابتزاز والتهديد عبر الإنترنت.

المطلب الثاني

دور الهياكل الخاصة في التحقيق في جرائم الانترنت

بعد إنشاء الآليات الإجرائية لمكافحة جريمة الابتزاز والتهديد عبر الإنترنت، ومن مرحلة جمع الأدلة والتحقيق الجنائي إلى إثبات الجريمة والتعامل مع الدليل الرقمي، وضع المشرع وسائل فعالة لمكافحة والوقاية من هذه الجرائم. يتجسد هذا في إنشاء هياكل خاصة تقوم بدعم جهود الكشف عن الحقائق، بالتعاون مع الجهات القضائية لتحديد الجاني. تعمل هذه الهياكل، التي تتمتع بخبرة واسعة في التعامل مع جرائم الإنترنت، لتكوينها من الخبراء والكوادر المتخصصة في هذا المجال. تلعب هذه الهياكل دورا حيويا في المساعدة الفنية، بما في ذلك اتخاذ الإجراءات التقنية والتدابير الوقائية اللازمة، وتقديم التحقيقات المتقدمة.

[1]– عزيزة رابحي، المرجع السابق، ص 329.

[2]– يوسف صغير، المرجع السابق، ص 135.

الفرع الأول: الوحدات الخاصة (جهاز الأمن والدرك الوطني):

إن مكافحة جرائم الإنترنت بشكل فعال، وخاصة جريمة الابتزاز والتهديد، تواجه تحديات تتجاوز الوسائل التقليدية. لقد جعلت هذه الجرائم الحديثة الجزائر تتخذ جميع الإجراءات الضرورية لمنع انتشارها وتفاقمها.

تحمل مكافحة هذه الجرائم مسؤولية كبيرة، وتتطلب استخدام وسائل متطورة. لذا، يعتمد الحل على جهود الأجهزة الأمنية والقانونية، حيث يعتبر جهازي الأمن والدرك الوطني الجهات الرئيسية في هذا المجال.

اولا: جهاز الأمن: تقوم قوات الشرطة بتحري عن الجرائم وضبطها، وتستقبل البلاغات وتجري التحقيقات الأولية. بعد ذلك، تحال القضايا إلى الجهات القضائية المختصة للبث فيها ومباشرة الإجراءات القانونية اللازمة[1].

هذه الجهود المشتركة بين الأجهزة الأمنية والقانونية تعتبر أساسية لمنع انتشار جرائم الإنترنت وحماية المجتمع منها بشكل فعال. لذا، قامت المديرية العامة للأمن الوطني بوضع استراتيجية عمل متكاملة تركز على تدريب ضباط الشرطة القضائية لمواجهة هذا النوع الجديد من الجرائم الإلكترونية. كما تم إنشاء مخابر الشرطة العلمية والتقنية، حيث تلعب دورا حيويا في مساعدة السلطات التحقيقية عن طريق استخدام التقنيات الحديثة وتحليل البيانات المخزنة في الأجهزة الإلكترونية المشتبه في استخدامها في ارتكاب الجريمة. هذه الإجراءات تساهم بشكل كبير في تعزيز قدرة السلطات على الوصول إلى الحقيقة وتسهيل التحقيقات الجنائية في مجال مكافحة الجرائم الإلكترونية[2]. وتتمثل هذه المخابر على المستوى الوطني في:

على المستوى المركزي:

[1]– عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق، جامعة وهران، 2012–2013، ص 247-248.

[2]– مريم عراب، المرجع السابق، ص 1228.

– المخبر المركزي للشرطة العلمية بالجزائر العاصمة: عملها يكون في مسرح الجرائم التي تستعمل فيها الأسلحة بمختلف أنواعها، جرائم التزوير، الجرائم الالكترونية، مهامها جمع وتحليل كل ما يفيد التحقيق الجنائي[1].

على المستوى الجهوي:

– المخبر الجهوي للشرطة العلمية بقسنطينة.
– المخبر الجهوي للشرطة العلمية بوهران.
– المخبر الجهوي للشرطة العلمية بتمنراست.
– المخبر الجهوي للشرطة العلمية ببشار.

تتولى دائرة الأدلة الرقمية والآثار التكنولوجية، الموجودة على مستوى كل مخبر، مهام البحث والتحقيق بشكل متخصص. بعد عام 2004، تم تعزيز هذه الدائرة بثلاثة أقسام فرعية: قسم استغلال الأدلة الرقمية المتعلقة بالحواسيب والشبكات، وقسم استغلال الأدلة المتعلقة بالهواتف النقالة، بالإضافة إلى قسم تحليل الأصوات. تتألف الدائرة من ثمانية أعضاء محققين، يتمتع أربعة منهم بصفة ضابط شرطة قضائية، حيث يتمتعون بخبرة في تخصص الأعمال الجنائية ويحملون شهادات جامعية في الاعلام الآلي، بالإضافة إلى معرفتهم بالجانب القانوني، ويتابعون بانتظام دورات تدريبية لتحديث معرفتهم بآخر التطورات التقنية والقانونية في مجال المعلومات[2].

من مهام هذه الدائرة دعم مختلف أجهزة الشرطة والقضاء من خلال توفير الدعم التقني في مجال التحقيقات الإلكترونية، من خلال البحث عن البيانات والمعلومات الرقمية المشبوهة مثل الصور، الرسائل الالكترونية...، وذلك باستخدام أدوات وبرامج مخصصة تستطيع استعادة البيانات المحذوفة وفحص محتوى وسائط التخزين الإلكترونية بشمولية تامة[3].

[1]– مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة –وثيقة صادرة عن نيابة– مديرية الشرطة العلمية والمديرية العامة للأمن الوطني– ص 2-3.

[2]– نعيم سعيداني، آليات البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2012–2013، ص 180.

[3]– مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية – وثيقة خاصة صادرة عن مديرية الشرطة القضائية– المديرية العامة للأمن الوطني– ص 46.

أثناء مرحلة البحث والتحري، يستجيب أفراد الدائرة عادةً للطلبات التي تقدمها عناصر الشرطة المتخصصة في مكافحة الجرائم المعلوماتية، التابعة لمديريات الأمن الوطني، وكذلك لطلبات وكيل الجمهورية أو قاضي التحقيق عن طريق إنابات قضائية يقدمون الدعم والمساعدة خلال مرحلة معاينة مسرح الجريمة، ويشاركون في حجز الأدلة المتاحة.

أما في مرحلة التحقيق القضائي، فإن دور أفراد الدائرة يتحول إلى دور الخبراء، حيث يُعدون تقارير الخبرة بناءً على طلبات وكيل الجمهورية وخاصة قاضي التحقيق. يقومون بتحليل الأدلة المحجوزة واستخراج الأدلة الإلكترونية منها، مثل تحليل محتوى أقراص الحاسوب المستخدمة في الجريمة أو التي تنتمي للضحايا، بالإضافة إلى جميع وسائل التخزين الإلكترونية بأنواعها المختلفة. يستهدفون هذه الأدلة لتحديد المواقع التي تم استخدامها وعناوين الجناة، ويعتمدون على استخدام وسائل مادية متطورة وذات جودة عالية في أداء مهامهم[1].

على المستوى المحلي:

لتعزيز القدرات الوقائية والتحقيقية في مجال مكافحة الجرائم المعلوماتية، أسست المديرية العامة للأمن الوطني في عام 2016 حوالي 48 فرقة مختصة في مجال مكافحة الجرائم المعلوماتية، موزعة على مختلف ولايات البلاد. تتمثل مهمتها في استقبال الشكاوى والبحث في الجرائم المعلوماتية والتحقيق فيها، بالإضافة إلى تعزيز التواصل بين الإدارة والمواطنين في هذا الصدد[2].

ثانيا: الوحدات التابعة للدرك الوطني: تقوم قيادة الدرك الوطني بتنفيذ مهامها في مجال الحفاظ على الأمن والنظام العام ومكافحة الجريمة بجميع أشكالها، من خلال تشكيل وحدات متعددة ومتنوعة سواء على مستوى القيادة العامة أو على مستوى القيادات الجهوية والمحلية . تسعى مؤسسة الدرك الوطني بجدية إلى مواجهة التحديات المتعلقة بالجرائم على الإنترنت، من خلال تسهيل عمليات البحث والمعاينة والتفتيش في أنظمة الحواسيب، ومراقبة شبكات الإنترنت.

[1]– نعيم سعيداني، المرجع السابق، ص 181.

[2]– عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة استكمالا لمتطلبات شهادة الماستر المهني، تخصص إدارة التحقيقات الاقتصادية والمالية، قسم علوم التسيير، جامعة قاصدي مرباح، ورقلة، 2018–2019، ص 40.

ولتحقيق هذه الأهداف، تم تنظيم مصالح الشرطة القضائية التابعة للدرك الوطني وذلك وفقا للاختصاصات والصلاحيات وطبيعة الجرائم.

- ✓ على المستوى المركزي:
- ✓ مديرية الأمن العمومي والإستغلال: تعد هيئة مسؤولة عن تنسيق الجهود بين الوحدات الإقليمية والمركز التقني العلمي في مجال البحث والتحري في الجرائم الالكترونية.
- ✓ المصلحة المركزية للتحريات الجنائية: تعتبر هيئة ذات الاختصاص الوطني، ومن بين مهامها الرئيسية مكافحة الجريمة المتعلقة بتكنولوجيا المعلومات والاتصالات.
- ✓ المعهد الوطني للأدلة الجنائية وعلم الإجرام: تم بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 2004/06/26، تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام. هو مؤسسة عمومية ذات طابع إداري، وهو جزء من عملية تحديث قطاع الدرك الوطني. يعد المعهد مركزا حديثا يجمع بين التجارب التطبيقية والتحاليل الحديثة، ويستفيد من التقنيات الحديثة لتقديم خدماته بكفاءة. يشكل المعهد جهة متخصصة في إجراء الخبرات والمعاينات في مجالات متنوعة، بما في ذلك دائرة الإعلام الآلي والإلكترونيات، حيث يتولى تحليل الأدلة المرتبطة بالجرائم الالكترونية. من بين الخدمات الرئيسية التي يقدمها المعهد في هذا السياق: توظيف الخبرات والتحليلات استجابة لطلبات القضاة والمحققين والسلطات المؤهلة.
- ✓ تقديم الدعم التقني للوحدات أثناء التحقيقات المعقدة.
- ✓ تصميم بنوك البيانات وتنفيذها وفقا للقوانين.
- ✓ المشاركة في الدراسات والأبحاث ذات الصلة بالوقاية والتقليل من جميع أشكال الجريمة.
- ✓ المساهمة في تحديد سياسات جنائية مثلى لمكافحة الجريمة.
- ✓ المبادرة بالأبحاث ذات الصلة بالجريمة وتنفيذها باستخدام التكنولوجيا المتقدمة.
- ✓ تعزيز البحث التطبيقي وأساليب التحقيق المثبتة فعاليتها في مجالات علم الجريمة والأدلة الجنائية على المستويين الوطني والدولي.
- ✓ تنظيم دورات لتحسين المستوى والتدريب المتقدم في تخصصات علوم الجنائية[1].

[1]– الموقع الرسمي لقيادة الدرك الوطني، تاريخ الإطلاع: 31 ماي 2024 الساعة 16:34 الرابط الموقع : http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined.

- ✓ مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: يسعى مركز الوقاية من جرائم الإعلام الآلي إلى تقديم المساعدة التقنية من خلال توفير أسماء خبراء متخصصين ينتمون للمعهد الوطني للأدلة الجنائية وعلم الإجرام. يتم ذلك عن طريق تزويد جميع المحاكم والمجالس القضائية بقائمة بهم، لتمكين القضاة من الاستفادة من خبراتهم في مجال الإعلام الآلي والإنترنت. هذا يسهل فهم الأدلة التقنية المرتبطة بالجرائم الإلكترونية ويسهل العمل القضائي[1].

الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أنشأ المشرع الجزائري في ظل مكافحة الجرائم الالكترونية، هيئة وطنية مختصة بالوقاية من هذه الجرائم ومكافحتها، وذلك وفقا لأحكام القانون رقم 04/09، حيث تنص المادة 13 منه على ذلك.

أولا: تعريف الهيئة: أنشأ المشرع، على مستوى محكمة مقر مجلس قضاء الجزائر، قطبا جزائيا متخصصا في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والجرائم المرتبطة بها وتكون تشكل جنحا. تعتبر الجرائم المتصلة بتكنولوجيا الإعلام والاتصال أي جريمة ترتكب أو يسهل ارتكابها باستخدام منظومة أو نظام للاتصالات الإلكترونية أو وسيلة أخرى، أو آلية ذات صلة بتكنولوجيا الإعلام والاتصال[2]. وتعتبر هذه الجرائم أكثر تعقيدا بتعدد الشركاء والمتضررين أو آثار جسيمة تخلفها الجريمة وقد تكون منظمة عابرة للحدود أو تمس بأمن الدولة وتتطلب استخدام وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى التعامل القضائي الدولي[3].

تتمتع بالشخصية المعنوية، الاستقلال المالي وتوضع تحت سلطة رئيس الجمهورية.

[1]– مريم عراب، المرجع السابق، 1228-1229.

[2]– أنظر المادة 211 مكرر 22 من قانون الاجراءات الجزائية المعدل والمتمم.

[3]– أنظر المادة 211 مكرر 25 من قانون الاجراءات الجزائية المعدل والمتمم.

الذمة المالية: تتحمل الهيئة الوطنية للوقاية من الجرائم الإلكترونية، بصفتها كيانا قانونيا، مسؤولية ذمتها المالية، مع كل التبعات القانونية المترتبة عن ذلك، حيث تشكل الذمة المالية مجموعة مترابطة تتضمن عناصر إيجابية وسلبية[1].

الأهلية: يحظى هذا الكيان القانوني بحقوق التملك والتصرف، بما في ذلك الحق في إبرام العقود واستخدام الصلاحيات الممنوحة له بموجب القوانين واللوائح والدستور والنظام الأساسي الخاص به[2]، مع مراعاة التوجيهات والضوابط الصادرة عن المكتب الوطني لمنع الجرائم الإلكترونية والاتصالات. تعتبر الهيئة ككيانات قانونية متمتعة بالشخصية الاعتبارية، وتتمتع بالأهلية الكاملة في الحدود المنصوص عليها بموجب القانون، بما يتيح لها الحق في التعاقد وقبول الهبات ومزاولة باقي الصلاحيات المخولة لها بموجب القانون.

الموطن: يقع مقر الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال في العاصمة بمدينة الجزائر[3]. ويتجلى أهمية الموطن القانوني في تحديد الاختصاص الجغرافي للسلطات الفاصلة في المنازعات المتعلقة بنشاطات الهيئة، مما يؤدي إلى تحديد الجهات المختصة في التعامل مع المسائل القانونية والفنية المرتبطة بتكنولوجيا المعلومات والاتصالات على الصعيدين الوطني والدولي.

حق التقاضي: القانون الإجرائي الخاص بالأجهزة والوحدات الإدارية يعتبر مستقلاً عن القانون الإجرائي الذي يطبق على الدولة، حيث يمكن مقاضاتها من قبل ممثليها. تمتلك الهيئات والوحدات التي تتمتع بالشخصية المعنوية القدرة على رفع الدعاوى أو التعامل كمدعى عليها، وفي هذا السياق، يحق للهيئة أن تقاضي أو تقاضى، ويمثلها رئيسها أمام القضاء بصفته المخولة.

تحمل المسؤولية عن الأضرار التي تسببها للغير: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال هي كيان معنوي مستقل، فهي تعمل بذاتها ولا تتأثر بإرادة الأفراد

---

[1]– بعلي محمد الصغير، القانون الإداري: التنظيم الإداري، النشاط الإداري، دار العلوم للنشر والتوزيع، عنابة، 2004، ص 40.

[2]– المرجع نفسه، ص 41.

[3]– المادة 03 من مرسوم رئاسي رقم 19–172 مؤرخ في 06 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر عدد 37 الصادر في 09 يونيو 2019.

الذين يشكلونها، ومن هذا فهي تتحمل المسؤولية الكاملة عن أي ضرر يلحق بالآخرين سواء كان ذلك الضرر ماديا أو معنويا[1].

ثانيا: تشكيل الهيئة.

حددت تشكيلته بموجب المرسوم الرئاسي 15-261 في المادة 04:

لجنة مديرة.

مديرية عامة.

مديرية المراقبة الوقائية واليقظة الالكترونية.

مديرية التنسيق التقني.

مركز العمليات لتقنية[2].

و تم تقليص تشكيلته بموجب قانون 21- 439 وأصبحت تشكيلة الهيئة كما يلي:

مجلس التوجيه والمديرية العامة، ويوضعان تحت سلطة رئيس الجمهورية ويقدمان تقريرا عن كل دورة أو نشاط [3].

– مجلس التوجيه: وفقا للمادة 8 من المرسوم الرئاسي رقم 21–439، يعقد المجلس اجتماعاته في دورة عادية في السنة، بدعوة من رئيسه. كما يمكن عقد جلسة غير منتظمة عند الضرورة، بدعوة من رئيس المجلس أو بناء على طلب من أحد أعضائه أو من المدير العام للهيئة[4]. يرأس المجلس الأمين العام لرئاسة الجمهورية ويمكنه تعيين ممثلين له. ويتكون المجلس من:

---

[1]– سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجرائم الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 02، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2022، ص 565.

[2]– أنظر المادة 04 من مرسوم الرئاسي رقم 15–261 مؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 53 الصادر في 08 أكتوبر 2015.

[3]– المادة 05 من مرسوم رئاسي رقم 21– 439 مؤرخ في 07 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر عدد 86 الصادر في 11 نوفمبر سنة 2021.

[4]– المادة 08 من مرسوم رئاسي 21– 439 .

-الأمين العام لوزارة الشؤون الخارجية- الأمين العام لوزارة الداخلية والجماعات المحلية - الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية- المدير العام للأمن الداخلي- قائد الدرك الوطني- المدير العام للأمن الوطن- المدير المركزي لأمن الجيش الوطني الشعبي- رئيس مصلحة الدفاع السبرياني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي- ممثل عن رئاسة الجمهورية.

يتولى مدير العام للهيئة أمانة مجلس التوجيه[1].

مهامها:

1. دراسة كل مسألة تندرج ضمن اختصاصها، خاصة فيما يتعلق بشروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية كما جاء في المادة 04 من القانون رقم 09-04 .

2. مناقشة الاستراتيجية الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال ومكافحتها.

3. التداول حول قضايا التطوير والتعاون مع المؤسسات والهيئات الوطنية والدولية ذات الصلة بالجرائم المتعلقة بتكنولوجيا المعلومات والاتصال.

4. تقييم حالة التهديدات بشكل دوري في مجال الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال لتحديد العمليات والأهداف بدقة.

5. اقتراح الأنشطة المتعلقة بالبحث وتقييم العمليات المباشرة في مجال الوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال ومكافحتها.

6. إعداد واعتماد النظام الداخلي للهيئة.

7. دراسة التقارير السنوية لأنشطة الهيئة والموافقة عليها.

8. دراسة مشروع الميزانية السنوية للهيئة والموافقة عليه.

9. إبداء الرأي في كل مسألة تتعلق بمهام الهيئة.

10. تقديم الاقتراحات المتعلقة بمجال اختصاص الهيئة.

[1]- المادة 06 من مرسوم الرئاسي 21- 439.

تشمل آليات مجابهة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال:

– المساهمة في وضع المعايير القانونية ذات الصلة بمجال اختصاصها[1].

المديرية العامة: وتنقسم المديرية العامة إلى الوحدات التالية:

– مديرية للمراقبة الوقائية واليقظة الإلكترونية.

– مديرية للإدارة والوسائل.

– مصلحة للدراسات والتلخيص.

– مصلحة للتعاون واليقظة التكنولوجية

– المصلحة الجهوية[2].

يدير الهيئة العامة مدير عام يعين بموجب مرسوم رئاسي، وينتهي تكليفه بناء على نفس السبيل[3]. وتتمثل صلاحيات المدير العام، وفقا للمادة10 من المرسوم ذاته، فيما يلي:

1. إعداد مشروع الميزانية السنوية للهيئة .

2. إعداد وتنفيذ برنامج عمل الهيئة .

3. تنسيق وتنشيط جهود الوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصال ومكافحتها.

4. إعداد التقارير السنوية ورفعها إلى رئيس الجمهورية، والتقارير بصفة دورية إلى رئيس مجلس التوجيه.

6. تمثيل الهيئة لدى سلطة القضاء والمؤسسات الوطنية والدولية.

7. تحضير اجتماعات مجلس التوجيه للهيئة.

8. ضمان التسيير الإداري والمالي للهيئة.

9. التوظيف على مستوى هياكل المديرية العامة.

---

[1]– أنظر المادة 07 من مرسوم الرئاسي 21–439.

[2]– أنظر المادة 11 من مرسوم رئاسي 21–439.

[3]– أنظر المادة 09 من مرسوم رئاسي 21–439.

10. السهر على احترام السر المهني في الهيئة[1].

ثالثا: مهام الهيئة.

دورها الوقائي: تهدف التدابير الوقائية إلى توعية مستخدمي تكنولوجيا المعلومات والاتصالات بخطورة الجرائم التي يمكن أن يتعرضوا لها أثناء استخدام هذه التقنيات. ومن بين أهم هذه الجرائم:

- التجسس على الاتصالات والرسائل الإلكترونية.

- اختراق حسابات العملاء أو الاستيلاء على بطاقات الائتمان.

- اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية وغيرها[2].

دورها العلاجي:

بموجب المادة 14 من القانون رقم 09-04، فإن مهام الهيئة تتمثل في:

1. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها.

2. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحقيقات المتعلقة بالجرائم ذات الصلة بتكنولوجيا المعلومات والاتصال، وذلك من خلال جمع المعلومات والخبرات القضائية.

3. تبادل المعلومات مع الجهات المماثلة في الخارج لجمع المعطيات المفيدة في التعرف على مرتكبي الجرائم وتحديد مكان تواجدهم[3].

وفي إطار أحكام المرسوم الرئاسي رقم 21-439 الذي يعيد تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها، تضاف إلى المهام المذكورة في القانون 09-04 المهام التالية:

---

[1]- أنظر المادة 10 من مرسوم رئاسي 21-439.

[2]- أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2012-2013، ص 45.

[3]- أنظر المادة 14 من قانون 09-04.

1. تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال وتنفيذها.

2. المساهمة في تكوين المحققين المتخصصين في مجال التحقيقات التقنية ذات الصلة بتكنولوجيا المعلومات والاتصال.

3. تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها.

4. تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصادرها ومسارها للاستخدام في الإجراءات القضائية.

بالإضافة إلى ذلك، تمتلك الهيئة صلاحيات إدارية ومالية إضافية من خلال أجهزتها الداخلية[1] .

[1]- أنظر مواد الفصل الثالث تحت عنوان سير الهيئة من قانون 21-439 .

المبحث الثاني

طرق الإثبات في جريمة الابتزاز والتهديد عبر الانترنت

الإثبات هو كل ما يسهم في كشف الحقيقة، سواء في الاستخدام العام أو القانوني، حيث يتعين في الأخير تقديم الأدلة على وجود قاعدة قانونية ونتائجها أمام القضاء، وفق الطرق المحددة قانوناً. يعد الإثبات تحديا أساسيا يواجه سلطات التحقيق، خاصة في حالات الجرائم الإلكترونية التي تتسم بتعقيداتها وعدم ملموسيتها.

في حالات الجرائم الإلكترونية، يكون العثور على الأدلة وتحديدها أمرا صعبا، حيث تحدث الجرائم في بيئات غير تقليدية وتتمثل المعلومات بنبضات إلكترونية تنتقل عبر الشبكات، مما يسهل على المتهمين محو الأدلة. الوسائل التقليدية للإثبات لا تكون دائمًا فعالة في مواجهة هذا النوع من الجرائم، بسبب اختلاف عناصرها المادية وأساليب تنفيذها.

لذا، كان من الضروري تطوير وسائل الإثبات لمواكبة التطورات في الجرائم الإلكترونية، حيث أصبحت الأدلة الرقمية والإلكترونية ضرورية للعدالة الجنائية. هذا يتطلب تطوير أساليب جديدة ومتقدمة لجمع وتحليل الأدلة الإلكترونية، لتمكين الأجهزة القضائية من مواجهة التحديات المتزايدة في هذا المجال.

إن تحقيق العدالة في مجال الجرائم الإلكترونية يعتمد بشكل كبير على فاعلية وسائل الإثبات، التي يجب أن تتطور مع التكنولوجيا وتلتزم بمتطلبات القانون ومبادئ العدالة.

المطلب الأول

أدلة الإثبات في جريمة الابتزاز والتهديد عبر الانترنت

تشكل الأدلة الأساس لدعم وتثبيت الحقائق والمعلومات أمام القضاء. تقوم الأدلة التقليدية على استخدام الأساليب والتقنيات التقليدية مثل الشهادات أو الإعتراف، لكن مع تطور التكنولوجيا والتقنيات الرقمية، ظهرت الأدلة المستحدثة التي تعتمد على الإلكترونيات والبيانات الرقمية التي يتم استرجاعها من الأجهزة الإلكترونية. تتطلب هذه الأدلة مهارات متقدمة في التحليل الرقمي والاسترجاع الإلكتروني للبيانات لضمان جودتها وموثوقيتها أمام المحكمة.

الفرع الأول: أدلة الإثبات العامة في جريمة الابتزاز والتهديد عبر الانترنت

هي إجراءات قولية يستثنى منها الخبرة فهو إجراء تطبيقي، ذات أهمية في جرائم الانترنت كأهميتها في الجرائم التقليدية، تدرج كأدلة داعمة للإثبات في مجال العالم الرقمي، فقد قيد المشرع الجزائري الإثبات في جرائم الانترنت فقط بالأدلة بشكل الكتروني مدعمة بالوسائل التقليدية المنصوص عليها في قانون الاجراءات الجزائية[1] ، وهي على النحو التالي:

اولا/ الإقرار: يعتبر اعتراف المتهم بنفسه بارتكاب الواقعة الجنائية من أبرز وسائل الإثبات، حيث يعد الاعتراف إجراء مباشرا يتخذه المتهم، ويعتبر "سيد الأدلة". غالبا ما يتم الحصول على الاعتراف خلال استجواب المتهم في مرحلة التحقيق الابتدائي. يشير القانون الجزائري في المادة 213 من ق إ ج إلى أن قبول الاعتراف يعتمد على تقدير القاضي، ويمكن أن يكون الاعتراف كاملا أو جزئيا[2]. ورغم أن الاعتراف يعتبر سيد الأدلة، إلا أنه يخضع لاعتبارات القاضي وتقديره، حيث يمكن أحيانا أن يكون الاعتراف كاذبا نتيجة لعوامل مثل الضغط الإعلامي أو دوافع إنسانية، كما يمكن للقاضي في الجرائم الإلكترونية أن يستعين بخبير لتأكيد أو نفي صحة الاعتراف.

ثانيا/ الشهادة: وهي ما يدركه الإنسان بواسطة حواسه الخمس. عندما يطلب من الشخص أداء شهادته أمام الجهات القضائية، يجب عليه أن يقدم شهادته بحسب فهمه وادراكه بحواسه مباشرة للواقعة المعنية، وذلك بشكل يتماشى مع الوقائع الفعلية التي شهدها بنفسه، ويجب أن يقدمها شفهيا بعد أداء اليمين القانوني[3].

تقبل شهادة الشاهد وفق الشروط المنصوص عليها في ق إ ج شريطة أن يكون عاينة الجريمة أو له علاقة بالمتهم أو الضحية، لكن يختلف الأمر بالنسبة للجرائم المتعلقة بالانترنت

---

[1]– دلال مولاي ملياني، إشكاليات الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017–2018، ص 97.

[2]– قرار المحكمة العليا صادر في 1980/12/02، الغرفة الجنائية الثانية، مجموعة قرارات الغرفة الجنائية، ص 26:« الإعتراف هو إقرار من المتهم بكل أو بعض الوقائع المنسوبة إليه، وهو كغيره من أدلة الإثبات موكول لتقدير قضاة الموضوع وفقا لأحكام المادة 213 من قانون الاجراءات الجزائية».

[3]– إحمود فالح الخرابشة، الإشكاليات الاجرائية للشهادة في المسائل الجزائية دراسة مقارنة، ط 01، دار الثقافة، عمان، الأردن، 2010، ص 35.

بحيث نميز نوعان من الشهود: الأول هم من كانوا في مسرح الجريمة، والنوع الثاني من لديهم معلومات وخبرة تقنية في مجال المعلوماتية ونظام المعالجة الآلية للبيانات أو من الأشخاص لهم صلة بالانترنت ويطلق عليهم مصطلح الشاهد المعلوماتي[1]. ويشمل محل الشهادة النظام المعلوماتي بمفهومه الوسع[2] يتضمن حتى الشبكات المحلية والعالمية[3]

فئات الشاهد المعلوماتي: مشغل الحاسوب: المسؤول عن تشغيل الحاسوب والمعدات المتصلة به، بحيث يتمتع مشغلو الحاسب الآلي والانترنت بخبرة كبيرة في استخدامهما.

خبراء البرمجة: لديهم الخبرة في كتابة أوامر البرامج ، تخطيط وتعديل وتصحيح برامج وتطبيقات نظام الحاسب الآلي.

محللون النظم: تحليل ودراسة البيانات للنظام المدروس .

مهندسو الصيانة والاتصالات: وهم المسؤولين عن أمال الصيانة الحاسب الآلي والشبكات المتصلة به.

مدير النظام: المسؤول عن ادارة في النظم المعلوماتية.

مقدمي خدمة الانترنت.

تعتبر شهادة الاشخاص العادية مهمة في إثبات جرائم التكنولوجيا والاتصال، خاصة عندما يتعلق الأمر بالأنشطة الفعلية في العالم الواقع للجاني الرقمي. فعلى سبيل المثال، يمكن للسلطات تحديد مصدر الجريمة عبر الإنترنت من خلال عنوان IP[4]، الذي يمكن أن يكون لجهاز الكمبيوتر المتصل، والذي قد يكون في مقهى الإنترنت. يمكن للشهود، سواء كانوا

[1]– عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، الكتب القانونية، المجلة الكبرى، مصر، 2007، ص 157.

[2]– النظام المعلوماتي المنظومة المعلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرامج معينة.

[3]– دلال مولاي ملياني، المرجع السابق، ص 37.

[4]– رقم مكون من أربعة أجزاء في كل جزء أقل من 256، يعرف الجزء الأول من الرقم بدءا من اليسار المنطقة الجغرافية والجزء الثاني يحدد المنطقة أو الحاسوب المزود والجزء الثالث يحدد مجموعة الحسابات التي تنتمي إليها الجهاز أما الجزء الأحير فهو يحدد الجهاز.

صاحب المقهى أو موظفون آخرون، أن يقدموا شهادات مهمة في إثبات الأنشطة المشبوهة على الإنترنت[1].

ثالثا / القرائن: هي استنتاج الواقعة المطلوب اثباتها من واقعة أخرى قام عليها دليل إثبات، فالقرينة من الأدلة الغير مباشرة ترجع إلى السلطة التقديرية للقاضي، يمكن تقسيم القرائن في جرائم التكنولوجيات الاعلام والاتصال تنقسم إلى نوعان قرائن قاطعة وقرائن بسيطة، فالدليل الرقمي من فئة القرائن القضائية التي تعود إلى تقدير القاضي فمعرفة عنوان الانترنت الرقميIP يشير إلى الحاسوب الذي ارتكبت منه الجريمة ولا يؤدي إلى معرفة الفاعل الأصلي، فيضل في حاجة إلى دعمه بدليل مادي لكي يمكننا التوصل بمقتضاه إلى الإدانة[2] فالقرائن تساعد كثيرا في إثبات جرائم الانترنت لكنها تضل داعمة ولا يمكن الإعتماد عليها.

رابعا/ الخبرة: في سياق جمع الأدلة، تعتبر الخبرة خطوة حاسمة بعد إحاطة الموضوع بالمعلومات الفنية الضرورية للاستنتاج والوصول إلى الدليل المناسب. تعد الخبرة وسيلة أساسية من وسائل الإثبات، حيث تهدف إلى كشف بعض الأدلة أو تفسيرها بالاستناد إلى المعرفة العلمية. يعتمد القاضي في اتخاذ قراره المناسب بشكل كبير على الخبرة المتاحة، حيث يمثلون مصادر ثقة ومعرفة في مجالاتهم المختصة[3].

تتطلب الخبرة في مجال المعلوماتية شروطا خاصة تتماشى مع التطورات الطارئة في تكنولوجيا المعلومات والجرائم المتعلقة بها. ليكون خبيرًا قضائيا في مجال الجريمة المعلوماتية، يجب على الفرد أن يتوفر على مؤهلات ومهارات محددة، بما في ذلك حصوله على شهادات ودراسات عليا في تخصص المعلوماتية، وخضوعه لتدريب عملي وقانوني مستمر لمواكبة تطورات

[1]– دلال مولاي ملياني، شهادة الشهود في جرائم تكنولوجيا الإعلام والاتصال، مجلة البحوث القانونية والسياسية، العدد 06، جوان 2016، ص 293- 294.

[2]– محمد طارق عبد الرؤوف الحق، جريمة الإحتيال عبر الانترنت، الأحكام الموضوعية الأحكام الجزائية، منشورات الحلبي الحقوقية، لبنان ، 2011، ص 310.

[3]– عبد الناصر محمد فرغلي، محمد عبيد سيف المسماري، الإثبات بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 12-14نوفمبر 2007، ص 24.

أساليب المجرم المعلوماتي، بالإضافة إلى معرفته المستمرة بالجوانب الفنية والتقنية المتعلقة بمجاله[1].

الخبرة التقنية في جرائم الابتزاز والتهديد عبر الإنترنت تعتبر أحد أهم وسائل الإثبات، حيث تلعب دورا بارزا في مراحل التحقيق الأولية والنهائية. تعرف في الفقه المقارن بمصطلح المعلوماتية الشرعية، والتي تشير إلى استخدام الطرق العلمية في جمع وتحليل وتفسير الدليل الرقمي. تقوم الخبرة المعلوماتية الشرعية بدور مماثل لتشريح الجثة في الطب الشرعي، حيث تسهم في إعادة بناء مجريات القضية وتوضيحها أمام المحكمة[2].

الفرع الثاني: أدلة الإثبات المستحدثة في جريمة الابتزاز والتهديد عبر الانترنت

الدليل الذي يجد له أساسا في العالم الفعلي هو الذي يقود إلى الاعتقاد بأن الجريمة قد وقعت، وهو تلك المعلومات التي يقبلها المنطق والعقل، ويعتمدها العلم، ويتم الحصول عليها بإجراءات قانونية وعلمية. ومن بين هذه الأدلة، يأتي الدليل الرقمي الذي يستند إلى تحليل البيانات الحسابية المخزنة في أجهزة الحاسوب وشبكات الاتصال. يمكن استخدام هذا الدليل في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة ما أو المجني عليه.

اولا/ تعريف الدليل الرقمي: الدليل الرقمي هو الدليل المأخوذ من أجهزة الكمبيوتر في شكل موجات ونبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها بواسطة برامج وتطبيقات وتقنيات خاصة. يعتبر هذا الدليل تشكيلًا رقميًا لمعلومات متنوعة مثل النصوص المكتوبة، أو الصور، أو الأصوات، أو الرسوم، ويستخدم أمام أجهزة تطبيق القانون لتقديم الأدلة[3].

[1]– عبد الناصر محمد فرغلي، محمد عبيد سيف الغافري، المرجع السابق، ص 26.

[2]– مريم عراب، المرجع السابق، ص 1219.

[3]– نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جامعة باتنة، جوان 2017، ص 911.

ثانيا/ شروط صحة الدليل الرقمي:

الدليل الرقمي غير قابل للشك: الدليل الرقمي يجب أن يكون يقينيا وغير قابل للشك، ويصل القاضي إلى اليقين بعد تحليل الأدلة الرقمية، وتحديد قوتها في إثبات نسبة الجريمة لشخص معين[1].

الدليل الرقمي متحصل عليه بطريقة مشروعة: المشروعية هي الامتثال لأحكام القانون ومضمونه العام، بهدف حماية الحقوق الشخصية والحريات من تعسف السلطة. تضمن القاضي أن يستند في قراراته إلى أدلة مشروعة فقط، مع استبعاد أي دليل ناتج عن إجراءات غير قانونية أو معيبة، حتى لو كانت تستند إلى أدلة أخرى مشروعة[2].

الدليل الرقمي غير قابلا للمناقشة: القاضي يجب أن يعتمد فقط على الأدلة التي تم مناقشتها وجاهيا وعلنيا في معرض المرافعة، ويتم عرضها أمام القاضي وأطراف الدعوى. لذا، يجب أن تعرض الأدلة المتعلقة بجرائم الحاسوب والإنترنت مباشرة أمام القاضي الجزائي في جلسة المرافعة، ولا يمكن الاعتماد عليها إذا لم تكن قد تمت مناقشتها وتقديمها للخصوم في هذه الجلسة[3].

ثالثا/ حجية الدليل الرقمي: مرحلة الحكم في الدعوى الجنائية هي المرحلة الحاسمة التي تهدف إلى الوصول إلى حكم قاطع ينهي الدعوى. تقدير الأدلة، بما في ذلك الأدلة الرقمية في حال الجرائم الإلكترونية، يشكل جوهر هذا الحكم[4]. التشريع الجزائري يعتمد على مبدأ حرية الإثبات، ولم يفرد بقواعد خاصة للأدلة الرقمية. القاضي يحتاج إلى خبرة خاصة لتقدير قيمة الأدلة العلمية، بما في ذلك الأدلة الرقمية، ويمكنه الاعتماد على رأي الخبراء في حال الشك في مصداقيتها. ومع ذلك، يظل للقاضي سلطة تقديرية محددة ومسيطرة في الحكم، ويمكنه استبعاد الأدلة التي تم الحصول عليها بطرق غير مشروعة. يتمثل دور القاضي في الرقابة القانونية

---

[1]– ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 125.

[2]– أنظر المادة 212 من قانون الاجراءات الجزائية المعدل والمتمم.

[3]– عزيزة رابحي، المرجع السابق، ص 296.

[4]– مبارك بن طيبي، محمد رحموني، شروط قبول الدليل الرقمي كدليل إثبات في الجرائم الالكترونية، مجلة القانون والعلوم السياسية، المجلد 05، العدد 02، جامعة أحمد دراية، أدرار، 2019، ص 28.

على التقارير الفنية، ويجب عليه مراعاة مبدأ الاقتناع الشخصي في تقدير الأدلة، بما في ذلك تقارير الخبراء[1]. التشريع الجزائري لا يضمن قواعد خاصة بالأدلة الرقمية، سواء في قانون الإجراءات الجزائية أو في قانون 09-04[2].

المطلب الثاني

صعوبات الإثبات في جريمة الابتزاز والتهديد عبر الانترنت

إن الإثبات الجنائي هو عملية متكاملة تهدف إلى جمع الأدلة الجنائية التي تثبت حدوث الجريمة، بما في ذلك ظروف وأسباب ارتكابها وتنفيذها من قبل المتهمين، بهدف تقديمهم أمام العدالة. الجرائم الإلكترونية تواجه تحديات كبيرة في هذا السياق، حيث تؤثر صعوبات إثباتها على الأدلة التي يتم جمعها من مثل هذه الجرائم.

تفتقر وسائل الإثبات الجنائي العامة إلى الفعالية فهي بمثابة دعائم للدليل الرقمي في الجرائم الإلكترونية، مما أدى إلى ظهور الظاهرة الرقمية، والتي تعتمد على التقنيات الحاسوبية والإنترنت لجمع ما يُعرف بالأدلة الإلكترونية أو الرقمية. هذه الأدلة تُستخدم لإثبات وقوع الجرائم الإلكترونية وتوجيهها للأفراد المسؤولين عنها.

فالإثبات الجنائي في الجرائم الالكترونية عموما وجريمة الابتزاز والتهديد عبر الانترنت، تحفوه مجموعة من الصعوبات منها ما تخص الدليل الرقمي منها صعوبات تواجه المحققين.

فقسمنا هذا المطلب إلى صعوبات الإثبات في جريمة الابتزاز والتهديد التي تواجه المحققين (الفرع الأول)، وصعوبات الإثبات في جريمة الابتزاز والتهديد عبر الانترنت المتعلقة بالدليل الرقمي (الفرع الثاني).

الفرع الأول: الصعوبات التي تواجه المحققين في إثبات جريمة الابتزاز والتهديد عبر الانترنت

أولا: نقص الخبرة: من التحديات الرئيسية التي تواجه عملية الحصول على الدليل الرقمي في جرائم الابتزاز والتهديد عبر الإنترنت هو نقص الخبرة. يعد هذا الأمر ذا أهمية بالغة، خصوصا

[1]– سهيلة بن قدوم، ليدية بسام، الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبر الرحمان ميرة، بجاية، 2017–2018، ص 83.

[2]– مبارك بن طيبي، محمد رحموني، المرجع السابق، ص 28-29.

إذا نظرنا إلى تطور هذه الجرائم وتقنياتها العالية. يتطلب الأمر من القائمين على البحث والتحقيق إتقانا تقنيا في مجال جرائم التكنولوجيا والاتصالات ونظم المعلومات والبيانات، بجانب المعرفة القانونية. ومع ذلك، قد يكون التوجه القانوني وحده غير كاف، فقد يشجع ذلك بدوره المرتكبين على ارتكاب مزيد من الجرائم. هذه التحديات تعتبر أحد المشاكل التي تواجه أجهزة الأمن والعدالة الجنائية في مواجهة جرائم الإنترنت[1].

ثانيا: صعوبة تحديد الجاني: إحدى أبرز التحديات التي تواجه السلطات في مكافحة الجرائم الإلكترونية هي قدرة المجرمين الإلكترونيين على إخفاء هوياتهم بذكاء، مما يجعل من الصعب على السلطات تتبعهم وكشف هوياتهم[2]. يعمل هؤلاء المجرمون أيضا على استخدام فيروسات تدميرية لمنع أي محاولات لتعقب الآثار الإلكترونية لهم أو لأجهزتهم الأصلية.

الفرع الثاني: الصعوبات المتعلقة لالدليل الرقمي في جريمة الابتزاز والتهديد عبر الانترنت

وهناك عدة صعوبات متعلقة بالدليل الرقمي في مرحلة الاثبات، وهي:

اولا/ سهولة حذف الدليل: بعد ارتكاب جريمة الابتزاز والتهديد، يبذل الجناة قصارى جهدهم لمسح أي أثر يشير إلى الجريمة، مما يجعل من الصعب بل وفي بعض الأحيان المستحيل الوصول إلى الأدلة[3].

ثانيا/ صعوبة التعرف على هوية الجاني من خلال الدليل الرقمي: في جريمة الابتزاز والتهديد عبر الإنترنت، تحدث الجريمة في بيئة افتراضية تسيطر عليها الرموز والبيانات، بدون وجود عنف ظاهر أو آثار مادية كالجرائم التقليدية. هذا يصعب العثور على أدلة مادية مثل بصمات الأصابع، مما يجعل تحديد الجاني أمرًا معقدا ومليئا بالعقبات[4].

---

[1]– عبد الفتاح بيومي حجازي، المرجع السابق، ص 122.

[2]– عماد بلغيث، يوسف جغلولي، صعوبات التحقيق في الجرائم الالكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 06، العدد 03، مخبر سوسيولوجية جودة الخدمة العمومية، جامعة محمد بوضياف المسيلة، سبتمبر 2021، ص 81.

[3]– نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 02، دار الثقافة للنشر والتوزيع، الأردن، 2004، ص 54.

[4]– غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016، ص 45.

ثالثا/ صعوبة الوصول للدليل: الجاني قد يضع عقبات فنية لتعقيد كشف جريمته، من خلال تشفير الملفات الرقمية لمنع تداول المعلومات وحجبها عن الوصول، وبالتالي يعوق وصول المحققين إلى مصدر الإرسال وكشف الجريمة[1].

[1]– المرجع ذاته، ص 46.

خاتمة

خاتمة:

نتيجة للتطورات التكنولوجيا التي شهدها العالم فقد ظهرت وسائل إتصال جديدة والتي ساهمت في توسيع العلاقات الاجتماعية بين أفراد المجتمع، وترتب على الاستخدام السيئ لها ظهور الجرائم الالكترونية التي يمكن أن ترتكب بأشكال متنوعة ومن ذلك جريمة الابتزاز والتهديد عبر الانترنت، إذ تعتبر هذه الجريمة من الجرائم المستحدثة والتي تتشابه بقدر كبير مع جريمة الابتزاز والتهديد التقليدية. غير أن طبيعة ارتكابها والذي يكون في عالم افتراضي مليء بالرموز والشفرات والشبكات المعلومات والأجهزة الحديثة جعل منها جريمة مستحدثة تختلف نوعا ما عن سابقاتها.

أصبح الابتزاز والتهديد الالكتروني مشكلة خطيرة تواجه العديد من الدول ومن بينها الجزائر فقد يتسبب هذا النوع من الجرائم بحدوث جرائم بعدها كالقتل، الاعتداء، أخذ أموال الغير دون وجه حق... وغيرها، لذا لابد من نشر الوعي داخل المجتمع بأخطار هذه الجريمة وتشجيع من يتعرض للابتزاز والتهديد بالإبلاغ عنها.

تتعامل المحاكم مع مرتكبي جرائم الانترنت وفقا لقانون العقوبات الجزائري وقانون الاجراءات الجزائية أي تخضع لإجراءات روتينية في الجريمة التقليدية، غير أنه في ظل التطور التقني ظهرت الحاجة لتجديد النصوص التشريعية، فقد استجاب المشرع لهذه التطورات وبما فيها جريمة الابتزاز والتهديد لاتصالها بالجرائم الالكترونية، فأصدر قانون 04-15 وكذا قانون 09-04 إضافة إلى قانون 18-07. غير أنه تجدر الإشارة إلى أن جريمة الابتزاز والتهديد الالكتروني لم تنل حضها بنص تشريعي خاص بها، وبالتالي كان لزاما على القاضي مواجهة الجريمة بالنصوص التجريمية القديمة وهي المواد من 284 إلى 287، 371، 303مكرر إلى 303 مكرر2 من قانون العقوبات .

وفي الأخير نخلص هذه الدراسة إلى النتائج والتوصيات

خاتمة:

النتائج:

- ✓ جريمة الابتزاز والتهديد عبر الانترنت جريمة مستحدثة تختلف عن الجريمة الابتزاز والتهديد التقليدي من خلال الوسائل المستخدمة فيها كالهواتف النقالة، الحاسب الآلي، باستعمال شبكة الاتصال واستخدام أحد المنصات التي تتيحها كمواقع التواصل الإجتماعي.
- ✓ تعتبر هذه الجريمة اعتداء على حرمة الحياة الخاصة والتي كفلها المشرع وحماها من خلال الدستور وكذا قانون العقوبات.
- ✓ جريمة الابتزاز والتهديد قد تتسبب في جرائم بعدها وذلك تحت التهديد والإكراه .
- ✓ جريمة الابتزاز والتهديد عبر النت صعبة الإثبات، حيث أنه من السهل محو آثارها فتحتاج لخبرة فنية وتقنية لإثباتها.
- ✓ الدليل الرقمي أهم أدلة الإثبات في جريمة الابتزاز والتهديد عبر الانترنت إلا أن التعامل معه يحتاج لكوادر متدربة على استعمال الوسائل الالكترونية.
- ✓ أساليب التحري الخاصة لا يتم اللجوء إليها إلا إذا اقتضت ضرورات التحري ذلك .
- ✓ إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، بينما هذه الهيئة ذات اختصاص اقليمي فقرب المشرع الإدارة للمواطن باستحداث وحدات خاصة تابعة للأمن والدرك الوطني محاولتا لتشجيع على الإبلاغ.
- ✓ قسور النصوص التجريمية.

التوصيات:

- ✓ ضرورة إصدار قانون خاص يجرم الابتزاز والتهديد عبر الانترنت بكل أنواعه ويشدد العقوبة خاصة اذا كان المتضرر مراهق أو حدث، وهذا ليكون الردع بشقيه العام والخاص ذا فاعلية أكبر.
- ✓ ضرورة إقامة ندوات ودراسات خاصة بهذه الجريمة لزيادة الوعي لدى الضحايا بضرورة التبليغ عن المجرمين فور وقوع الجريمة .
- ✓ إنشاء وحدات أو مكاتب لمعالجة جرائم الابتزاز والتهديد عبر الانترنت في الجهات الأمنية لاستقبال بلاغات الابتزاز وتتبع أثر المبتزين بحرفية عالية.

- ✓ وجوب الاهتمام بتدريب الخبراء والمحققين والقضاء مع التعامل مع هذا النوع من الجرائم الالكترونية.
- ✓ وأخيرا ضرورة التعاون الدولي لمكافحة هذه الجرائم من خلال إنشاء وحدات متخصصة على المستوى الدولي والعربي تهتم بالتنسيق الأمني بين الدول في مجال المتابعة ومحاكمة مرتكبي الجرائم الالكترونية.

تمت بحمد الله

الملاحق

مراسيم تنظيميّة

مرسوم رئاسي رقم 21-439 مؤرّخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إنّ رئيس الجمهورية،

– بناء على الدستور لا سيما المادتان 91-7 و141 (الفقرة الأولى) منه،

– وبمقتضى القانون العضوي رقم 04-11 المؤرخ في 21 رجب عام 1425 الموافق 6 سبتمبر سنة 2004 والمتضمن القانون الأساسي للقضاء،

– وبمقتضى الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدل والمتمم،

– وبمقتضى الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم،

– وبمقتضى الأمر رقم 71-28 المؤرخ في 26 صفر عام 1391 الموافق 22 أبريل سنة 1971 والمتضمن قانون القضاء العسكري، المعدل والمتمم،

– وبمقتضى القانون رقم 90-21 المؤرخ في 18 صفر عام 1411 الموافق 15 غشت سنة 1990 والمتعلق بالمحاسبة العمومية، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-02 المؤرخ في 29 محرم عام 1427 الموافق 28 فبراير سنة 2006 والمتضمن القانون الأساسي العام للمستخدمين العسكريين، المعدل والمتمم،

– وبمقتضى الأمر رقم 06-03 المؤرخ في 19 جمادى الثانية عام 1427 الموافق 15 يوليو سنة 2006 والمتضمن القانون الأساسي العام للوظيفة العمومية،

– وبمقتضى القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– وبمقتضى القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية،

– وبمقتضى الأمر رقم 21-09 المؤرخ في 27 شوال عام 1442 الموافق 8 يونيو سنة 2021 والمتعلق بحماية المعلومات والوثائق الإدارية،

– وبمقتضى المرسوم رقم 74-60 المؤرخ في 27 محرم عام 1394 الموافق 20 فبراير سنة 1974 والمتضمن إنشاء إطار من الموظفين المدنيين الشبيهين بالموظفين العسكريين في وزارة الدفاع الوطني وتحديد قواعد القانون الأساسي المطبق على الشبيهين الدائمين بالعسكريين، المتمم،

– وبمقتضى المرسوم الرئاسي رقم 20-39 المؤرخ في 8 جمادى الثانية عام 1441 الموافق 2 فبراير سنة 2020 والمتعلق بالتعيين في الوظائف المدنية والعسكرية للدولة، المتمم،

– وبمقتضى المرسوم الرئاسي رقم 20-183 المؤرّخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

يرسم ما يأتي :

الفصل الأول
أحكام عامة

المادّة الأولى : يهدف هذا المرسوم إلى إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص "الهيئة".

المادّة 2 : الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى رئيس الجمهورية.

المادّة 3 : يحدد مقر الهيئة بمدينة الجزائر.

ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي.

المادّة 4 : تمارس الهيئة المهام المنوطة بها، تحت رقابة السلطة القضائية، طبقا لأحكام قانون الإجراءات الجزائية، والقانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وبهذه الصفة، تكلف الهيئة، على الخصوص، ما يأتي :

– تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ،

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– ضمان المراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة.

كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الإلكترونية عندما يتعلق الأمر بأمن الجيش، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول.

– تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية،

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال،

– المساهمة في تحيين المعايير القانونية في مجال اختصاصها،

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية،

– تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، وفقا لأحكام المادتين 17 و18 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

الفصل الثاني

تشكيلة الهيئة وتنظيمها

المادّة 5 : تتكون الهيئة من مجلس توجيه ومديرية عامة، يُوضَعان تحت سلطة رئيس الجمهورية، ويُقدمان له عرضًا عن نشاطاتهما.

القسم الأول

مجلس التوجيه

المادّة 6 : يتولى الأمين العام لرئاسة الجمهورية رئاسة مجلس التوجيه الذي يتشكل من الأعضاء الآتي ذكرهم :

– الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج،

– الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية،

– الأمين العام لوزارة العدل،

– الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية،

– قائد الدرك الوطني،

– المدير العام للأمن الداخلي،

– المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي،

– المدير العام للأمن الوطني،

– رئيس مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي،

– ممثل عن رئاسة الجمهورية، يعينه رئيس الجمهورية.

يتولى المدير العام للهيئة أمانة مجلس التوجيه.

المادّة 7 : يكلف مجلس التوجيه على الخصوص، بما يأتي :

– توجيه عمل الهيئة والإشراف عليه ومراقبته،

– دراسة كل مسألة تخضع لمجال اختصاص الهيئة، والبتّ فيها، لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه،

– المداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مخطط عمل الهيئة والموافقة عليه،

– القيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة، بدقة،

– اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– دراسة مشروع ميزانية الهيئة والموافقة عليه،

– المداولة حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– دراسة مشروع النظام الداخلي للهيئة والموافقة عليه،

– تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة وإبداء رأيه في كل مسألة تتصل بمهامها،

– دراسة التقرير السنوي لنشاطات الهيئة والموافقة عليه.

المادّة 8 : يجتمع مجلس التوجيه في دورة عادية مرة واحدة في السنة، بناء على استدعاء من رئيسه.

ويمكنه أن يجتمع في دورة غير عادية، كلّما كان ذلك ضروريا، بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

يعد مجلس التوجيه تقريرا بعد كل دورة.

القسم الثاني

المديرية العامة

المادّة 9 : يدير المديرية العامة مدير عام يعيّن بموجب مرسوم رئاسي، وتنهى مهامه حسب الأشكال نفسها.

تعد وظيفة المدير العام وظيفة عليا في الدولة.

المادّة 10 : يسهر المدير العام على حسن سير الهيئة، ويتولى في هذا المجال :

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والسهر على تنفيذها،

– إعداد مشروع ميزانية الهيئة،

– اقتراح مخطط عمل الهيئة والسهر على تنفيذه،

– تنشيط أعمال هياكل الهيئة وتنسيقها ومتابعتها ومراقبتها،

– تحضير اجتماعات مجلس توجيه الهيئة،

– تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية،

– تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية،

– ممارسة السلطة السلّمية على مستخدمي الهيئة،

– السهر على احترام قواعد حماية السرّ المهني في الهيئة،

– السهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعنيين في الهيئة،

– إعداد التقرير السنوي لنشاطات الهيئة، ورفعه إلى رئيس الجمهورية،

– إعداد التقارير الدورية لنشاطات الهيئة ورفعها إلى رئيس مجلس التوجيه،

– ضمان التسيير الإداري والمالي للهيئة،

– إعداد مشروع النظام الداخلي للهيئة،

– المساهمة في تحيين المعايير القانونية في مجال اختصاصه،

– التوظيف على مستوى هياكل المديرية العامة،

– تعيين المستخدمين الذين لم تتحدد كيفيات أخرى لتعيينهم.

يخطر المدير العام للهيئة رئيس الجمهورية، فورا، عن كل حادثة من شأنها المساس بأمن الدولة أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضا رئيس أركان الجيش الوطني الشعبي عندما يتعلق الأمر بمسائل تخص الدفاع الوطني.

المادّة 11 : تضم المديرية العامة :

– مديرية المراقبة الوقائية واليقظة الإلكترونية،

– مديرية الإدارة والوسائل،

– مصلحة للدراسات والتلخيص،

– مصلحة للتعاون واليقظة التكنولوجية،

– ملحقات جهوية.

المادّة 12 : تعدّ كل من وظائف مدير المراقبة الوقائية واليقظة الإلكترونية، ومدير الإدارة والوسائل، ونواب المديرين، ورئيس مصلحة الدراسات والتلخيص، ورئيس مصلحة التعاون واليقظة التكنولوجية، ورؤساء الملحقات الجهوية، وظائف عليا في الدولة.

يتم التعيين في هذه الوظائف بموجب مرسوم رئاسي بناء على اقتراح من المدير العام للهيئة، وتنهى المهام فيها حسب الأشكال نفسها.

المادّة 13 : يحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار من الأمين العام لرئاسة الجمهورية، بناء على اقتراح من المدير العام للهيئة.

الفرع الأول

مديرية المراقبة الوقائية واليقظة الإلكترونية

المادّة 14 : تكلف مديرية المراقبة الوقائية واليقظة الإلكترونية بما يأتي :

– تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول،

– تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات المفيدة في تحديد مكان تواجد مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتعرف عليهم،

– جمع ومركزة واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وحفظها،

– تزويد السلطات القضائية ومصالح الشرطة القضائية، تلقائيا أو بناء على طلبها، بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

– القيام بالتدقيق والتفتيش في أي مكان أو هيكل أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية، باستثناء تلك التابعة لوزارة الدفاع الوطني،

– تنشيط عمل الملحقات الجهوية تحت إشراف المدير العام،

– تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها،

– تطبيق قواعد الحفاظ على السرّ المهني في نشاطاتها،

– السهر على إنجاز مهام اليقظة الإلكترونية.

المادّة 15 : تضع مديرية المراقبة الوقائية واليقظة الإلكترونية، على مستوى المنشآت القاعدية لمتعاملي ومقدمي خدمات الاتصالات الالكترونية، التجهيزات والوسائل والأجهزة التقنية الضرورية لتنفيذ مهامها طبقا للتشريع الساري المفعول.

يلزم المتعاملون ومقدمو الخدمات بتقديم المساعدة الضرورية لهذه المديرية من أجل ممارسة مهامها.

تمارس هذه المديرية مهامها المرتبطة بالشرطة القضائية طبقا لأحكام قانون الإجراءات الجزائية.

تنظم مديرية المراقبة الوقائية واليقظة الإلكترونية في مديريات فرعية.

الفرع الثاني

مديرية الإدارة والوسائل

المادّة 16 : تكلف مديرية الإدارة والوسائل، على الخصوص، بما يأتي :

– تسيير الموارد البشرية والوسائل المادية والمالية للهيئة،

– الإسناد التمويني والإسناد التقني للهيئة،

– صيانة العتاد والوسائل والمنشآت،

– إعداد احتياجات الهيئة في إطار تحضير تقديرات الميزانية.

تنظم مديرية الإدارة والوسائل في مديريات فرعية.

الفرع الثالث

مصلحة الدراسات والتلخيص

المادّة 17 : تكلف مصلحة الدراسات والتلخيص، على الخصوص، بما يأتي :

– إعداد مشروع مخطط عمل الهيئة بالتشاور مع الهياكل الأخرى للهيئة،

– القيام بتلخيص الوثائق المتعلقة بنشاطات الهيئة،

– القيام بكل دراسة وبحث تتعلق بنشاطات الهيئة،

– إعداد التقارير والحصائل السنوية لنشاطات الهيئة،

– مركزة ومراقبة الإجراءات المتعلقة بالطلبات القضائية، طبقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية،

– حفظ الوثائق والأرشيف.

الفرع الرابع

مصلحة التعاون واليقظة التكنولوجية

المادّة 18 : تكلف مصلحة التعاون واليقظة التكنولوجية، على الخصوص، بما يأتي :

– التعاون مع الشركاء فيما يخص تنفيذ عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

– اليقظة الدائمة في متابعة تكنولوجيات الإعلام والاتصال المتعلقة بنشاطات الهيئة.

الفرع الخامس

الملحقات الجهوية

المادّة 19 : تكلف الملحقة الجهوية بتنفيذ عمليات المراقبة الوقائية للاتصالات الالكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول.

يتم وضع الملحقات الجهوية قيد الخدمة والتشغيل من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية.

الفصل الثالث

سير الهيئة

المادّة 20 : لسير الهيئة، يلحق بها :

– قضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول،

– ضباط وأعوان للشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والأمن الوطني، الذين يحدد

عددهم بموجب قرارات مشتركة بين وزير الدفاع الوطني والوزير المكلف بالداخلية والأمين العام لرئاسة الجمهورية،

– مستخدمو الدعم التقني والإداري للمصالح العسكرية للأمن المختصة والدرك الوطني والأمن الوطني.

المادّة 21 : يمكن للهيئة أن توظف فئات أخرى من المستخدمين، حسب الحاجة.

المادّة 22 : يؤدي مستخدمو الهيئة الذين يدعون إلى الاطلاع على المعلومات السرّية، اليمين الآتي نصها أمام المجلس القضائي المختص إقليميا، قبل تنصيبهم :

"أقسم بالله العلي العظيم أن أقوم بعملي أحسن قيام، وأن أخلص في تأدية مهنتي، وأن أكتم الأسرار والمعلومات أيّا كانت التي اطلع عليها أثناء قيامي بعملي أو بمناسبته، وأن أسلك في كل الظروف سلوكا شريفا".

المادّة 23 : يلزم مستخدمو الهيئة بالسرّ المهني وبواجب التحفظ.

ويلزم مستخدمو مقدمي الخدمات في علاقاتهم مع الهيئة، أيضا، بواجب التحفظ.

ويخضع المستخدمون المدعوون إلى الاطلاع على معلومات سرّية، إلى إجراءات التأهيل.

المادّة 24 : في إطار التعاون، يمكن للهيئة أن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضروريتين لإنجاز المهام المسندة إليها.

المادّة 25 : قصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها، تكلف الهيئة حصريا، في مجال اختصاصها، بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاضٍ لدى الهيئة، وفقا للأحكام المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، على أن تخضع إجراءات التفتيش والحجز لأحكام قانون الإجراءات الجزائية.

المادّة 26 : يمكن الهيئة، لتنفيذ عملية مراقبة الاتصالات الإلكترونية، أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

يتولى الأعوان المؤهلون في الهيئة ووحداتها المكلفة بالمراقبة، لصالح ضباط الشرطة القضائية، الجوانب التقنية للعمليات المنصوص عليها في قانون الإجراءات الجزائية تحت إدارة ومراقبة قاضٍ لدى الهيئة، وبمساعدة ضابط من الشرطة القضائية أو أكثر ينتمي للهيئة.

تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلّمة من السلطة القضائية.

وتدوّن أشغالها في محاضر تعد طبقا لأحكام قانون الإجراءات الجزائية.

المادّة 27 : تحفظ المعلومات المستقاة أثناء عمليات المراقبة، خلال حيازتها من طرف الهيئة، وفقا للقواعد المطبقة على حماية المعلومات المصنفة.

المادّة 28 : تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية.

وفي هذه الحالة، تسلّم التسجيلات والمحررات محل الطلب، إلى السلطات القضائية وإلى مصالح الشرطة القضائية المختصة وتحتفظ السلطات القضائية، دون سواها بهذه المعطيات أثناء المدة القانونية المنصوص عليها في التشريع الساري المفعول.

المادّة 29 : يجب، تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع الساري المفعول، ألاّ تستخدم الاتصالات الإلكترونية والمعلومات والمعطيات التي تستلمها أو تجمعها الهيئة، لأغراض أخرى غير تلك المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وذلك وفقا للأحكام المنصوص عليها في القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه.

المادّة 30 : يمكن أن يقوم القضاة وضباط الشرطة القضائية التابعون للهيئة، أثناء ممارستهم لوظائفهم أو بمناسبتها، طبقا للشروط والكيفيات المنصوص عليها في التشريع الساري المفعول، ولا سيما قانون الإجراءات الجزائية، بتفتيش أي مكان أو هيكل أو جهاز بلغ إلى علمهم أنه يحوز و/أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية.

وفي حالة معاينة أفعال يمكن وصفها جزائيا، تخطر الهيئة وكيل الجمهورية المختص للقيام بالمتابعات المحتملة.

لا تشمل أحكام هذه المادة المنشآت التابعة لوزارة الدفاع الوطني.

المادّة 31 : تضمن المديرية العامة للاستعلام التقني الإسناد المتعدد الأشكال للهيئة.

المادّة 32 : يمكن أن تطلب الهيئة مساعدة موظفين مختصين من الوزارات المعنية في مجال تكنولوجيات الإعلام والاتصال، طبقا للشروط والكيفيات المحددة في التنظيم الساري المفعول.

كما يمكنها أن تستعين بأي خبير أو أي شخص يمكن أن يساعدها في أعمالها.

المادّة 33 : لا يمكن أن تستورد أو تقتني أو تحوز أو تستعمل الوسائل والتجهيزات التقنية لمراقبة الاتصالات الإلكترونية إلاّ الهيئة في إطار اختصاصها.

الفصل الرابع

أحكام مالية

المادّة 34 : تسجل ميزانية الهيئة في الميزانية العامة للدولة، وتلحق ضمن ميزانية رئاسة الجمهورية، طبقا للتشريع والتنظيم الساريي المفعول.

ويكون المدير العام هو الآمر بصرف ميزانية الهيئة.

المادّة 35 : تشتمل ميزانية الهيئة على باب للإيرادات وباب للنفقات.

في باب الإيرادات :

– إعانات الدولة،

– المساهمات المتعلقة بالنشاطات المرتبطة بموضوعها.

في باب النفقات :

– نفقات التسيير،

– نفقات التجهيز،

– كل النفقات الأخرى الضرورية لإنجاز هدفها.

المادّة 36 : تمسك محاسبة الهيئة وفق قواعد المحاسبة العمومية.

يتولى مسك المحاسبة عون محاسب يعيّنه أو يعتمده الوزير المكلف بالمالية.

المادّة 37 : يمارس المراقبة المالية للهيئة مراقب مالي يعيّنه الوزير المكلف بالمالية.

الفصل الخامس

أحكام قانونية أساسية

المادّة 38 : يبقى القضاة وضباط وأعوان الشرطة القضائية وكذا المستخدمون التابعون للوزارات المعنية والممارسون وظائفهم في الهيئة، خاضعين للأحكام التشريعية والتنظيمية والقانونية الأساسية المطبقة عليهم.

المادّة 39 : يستفيد مستخدمو الهيئة، طبقا للتشريع الساري المفعول، من حماية الدولة من التهديدات أو الضغوطات أو الإهانات، مهما تكن طبيعتها، التي قد يتعرضون لها بسبب أو بمناسبة قيامهم بمهامهم.

المادّة 40 : تحدد طريقة صرف النظام التعويضي المطبق على مستخدمي الهيئة بموجب نص خاص.

الفصل السادس

أحكام خاصة وختامية

المادّة 41 : تلغى جميع الأحكام المخالفة لهذا المرسوم لا سيما المرسوم الرئاسي رقم 20-183 المؤرّخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020 والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المادّة 42 : ينشر هذا المرسوم في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021.

عبد المجيد تبون

★

مرسوم رئاسي رقم 21-440 مؤرّخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يعدّل ويتمّم المرسوم الرئاسي رقم 02-479 المؤرّخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة وتحديد صلاحياته وتنظيمه وعمله.

إنّ رئيس الجمهورية،

– بناء على تقرير وزير السياحة والصناعة التقليدية،

– وبناء على الدستور، لا سيما المادتان 91-7 و141 (الفقرة الأولى) منه،

– وبمقتضى المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة ويحدد صلاحياته وتنظيمه وعمله،

– وبمقتضى المرسوم الرئاسي رقم 21-275 المؤرخ في 19 ذي القعدة عام 1442 الموافق 30 يونيو سنة 2021 والمتضمن تعيين الوزير الأول،

– وبمقتضى المرسوم الرئاسي رقم 21-281 المؤرخ في 26 ذي القعدة عام 1442 الموافق 7 يوليو سنة 2021 والمتضمن تعيين أعضاء الحكومة،

يرسم ما يأتي :

المادّة الأولى : يعدّل هذا المرسوم ويتمّم بعض أحكام المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمتضمن إنشاء المجلس الوطني للسياحة، وتحديد صلاحياته وتنظيمه وعمله.

المادّة 2 : تعدل وتتمم أحكام المواد 2 و3 و5 من المرسوم الرئاسي رقم 02-479 المؤرخ في 27 شوّال عام 1423 الموافق 31 ديسمبر سنة 2002 والمذكور أعلاه، وتحرر كما يأتي :

قائمة المصادر والمراجع

أ/ قائمة المصادر:

1. القرآن الكريم.
2. أبو الفضل جمال الدين محمد بكر (ابن منظور)، معجم لسان العرب، دار صابر،لبنان.
3. أحمد بن فارس بن زكرياء القزويني الرازي، كتاب مجمل اللغة معجم لغوي من الأصول، حققه أبو الحسن عمرو شهاب الدين، دار الفكر، لبنان، 1994.
4. محب الدين أبي فيض الزبيدي، تاج العروس من جواهر القاموس، دار الفكر، بيروت، 2005.

ب / قائمة المراجع بالعربية :

- **الكتب:**

1. الراغب الأصفهاني أبي القاسم الحسين بن محمد المعروف، المفردات في غريب القرآن، الطبعة 01، المؤسس الإعلامي للمطبوعات، 2009.
2. الحسني عباس عمار، التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات -دراسة مقارنة- ، الطبعة 01، المركز العربي للنشر والتوزيع، مصر، 2017.
3. الدرة ماهر عبد الشويش، شرح قانون العقوبات القسم الخاص، الطبعة 02، شركة العاتك لصناعة الكتاب، القاهرة، 2009.
4. احسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة 10، دار هومة، الجزائر، 2018.
5. احمد عبد الإله هلالي، الجوانب الموضوعية والاجرائية لجرائم المعلوماتية، الطبعة 01، دار النهضة العربية، القاهرة، 2003.
6. ابراهيم خالد ممدوح، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة 02، دار الفكر الجامعي، الإسكندرية، 2010.
7. إحمود فالح الخرابشة، إشكاليات الاجرائية للشهادة في المسائل الجزائية -دراسة مقارنة- ، الطبعة 01، دار الثقافة، عمان الأردن، 2010.
8. بعلي محمد الصغير، القانون الإداري: التنظيم الإداري، النشاط الإداري، دار العلوم للنشر والتوزيع، عنابة، 2004.

9. حسام الدين الأهوائي، الحق في احترام الحياة الخاصة(الحق في الخصوصية)-دراسة مقارنة-، الطبعة 02، دار النهضة العربية، القاهرة، 2014.
10. حسن صادق المصرفاوي، شرح قانون العقوبات القسم الخاص، منشأة المعارف، الإسكندرية، 1975.
11. خالد الحمد مسره، الدليل الرقمي ومعايير جودته في الإثبات الجنائي، الطبعة 01، المركز الكتاب الأكاديمي، الأردن، 2014.
12. خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسوب الآلي في ضوء حماية الملكية الفكرية، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
13. شحاتة غريب شلقامي، الحق الأدبي لمؤلف برامج الحاسوب الآلي، دار النهضة العربية، القاهرة، 2004.
14. عبد الله الحسين على حموده، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة 01، دار النهضة العربية، القاهرة، 2001.
15. عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، الكتب القانونية، المجلة الكبرى، مصر، 2011.
16. عبد المهين سالم بكر، الوسيط في شرح قانون الجزاء الكويتي القسم الخاص، مطبوعات جامعة الكويت، الكويت، 1979.
17. عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، الطبعة 01، دار النهضة العربية، مصر، 2005.
18. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون -دراسة مقارنة- ، الطبعة 02، منشورات الحلبي الحقوقية، بيروت لبنان، 2007.
19. على حسن طوالبة، التفتيش الجنائي على النظم الحاسوب والانترنت، عالم الكتب الحديثة، الأردن، 2004.
20. غنية باطلي، الجريمة الالكترونية -دراسة مقارنة- ، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016.

21. محمد أمين شوابكة، جرائم الحاسوب والأنترنت، الطبعة 01، دار الثقافة للنشر والتوسيع، الأردن، 2000.
22. محمد طارق عبد الرؤوف الحق، جريمة الإحتيال عبر الانترنت، الأحكام الموضوعية الاحكام الجزائية، منشورات الحلبي الحقوقية، لبنان، 2011.
23. محمود نجيب حسني، شرح قانون العقوبات القسم الخاص جرائم الإعتداء على الأشخاص، دار النهضة العربية، القاهرة، 1978.
24. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.
25. نجم محمد صبحي، الجرائم الواقعة على الأشخاص، الطبعة 01، دار الثقافة، القاهرة، 1994.
26. نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 02، دار الثقافة للنشر والتوزيع، الأردن، 2010.

- **الرسائل والمذكرات الجامعية:**

أولا: أطروحات الدكتوراه:

1. دلال مولاي ملياني، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان، 2017-2018.
2. صبرينة بن سعيد، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا الإعلام والاتصال، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية تخصص قانون دستوري، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2014-2015.
3. عبد الرحمن هيان الرشيد غازي، الحماية القانونية من الجرائم المعلوماتية، (الحاسب والانترنت)، أطروحة أعدت لنيل درجة الدكتوراه في القانون، كلية الحقوق، الجامعة الإسلامية في لبنان، لبنان، 2004.

4. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق، فرع قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر (01)، 2010-2011.
5. يحيى التومي، جرائم الإعتداء على الأشخاص باستخدام تكنولوجيا الإعلام والاتصال، أطروحة من أجل نيل شهادة الدكتوراه تخصص قانون، كلية الحقوق، جامعة الجزائر(01)، 2017-2018.

ثانيا: مذكرات الماجستير:

1. أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة، 2007.
2. أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء قانون رقم 09-04، مذكرة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح،ورقلة، 2012-2013.
3. طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الانترنت -دراسة مقارنة-، مذكرة لنيل شهادة الماجستير قانون جنائي، قسم الحقوق، فرع الماجستير قانون جنائي، جامعة محمد خيضر، بسكرة، 2006-2007.
4. عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير تخصص قانون جنائي، كلية الحقوق، جامعة وهران، 2012-2013.
5. محسن بن سلمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، مذكرة لنيل درجة الماجستير تاشريع الجنائي الإسلامي، كلية الدراسات العليا قسم العدالة الجنائية، أكادمية نايف العربية للعلوم الأمنية، 1423-1424.
6. محمد بن المحسن بن شلهوب،جريمة الابتزاز الالكتروني -دراسة مقارنة-، بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، المعهد العالي للقضاء ، قسم السياسة الشرعية شعبة الأنظمة، جامعة الإمام محمد بن سعود الإسلامية، 2011.
7. محمد بن نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والاترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

8. ممدوح بن يحيى الخليوي، دور التواصل الاجتماعي في زيادة جريمة الابتزاز ضد المرأة من وجهة نظر طالبات الجامعات السعوديات،رسالة مقدمة إستكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، قسم الدراسات الأمنية ، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، 2014.
9. نعيم سعيداني، آليات البحث والتحري في الجرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم القانونية، جتمعة الحاج لخضر، باتنة، 2012-2013.
10. يوسف صغير، الجريمة المرتكبة عبر الانترنت،مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية مدرسة الدكتوراه« قانون أساسي والعلوم السياسية» جامعة مولود معمري، تيزي وزو، 2013.

ثالثا: مذكرات الماستر:

1. أشواق بلباي، فطيمة أعراج، تفاعلية التطبيقات الالكترونية في الهواتف الذكية - اليوتيوب نموذجا-، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في الإعلام تخصص سمعي بصري، شعبة العلوم والاتصال، كلية العلوم الإجتماعية والإنسانية، جامعة الشهيد حمه لخضر، الوادي، 2019- 2020.
2. أمال برحال، جريمة الابتزاز عبر الوسائط الالكترونية، مذكرة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2019-2020.
3. زهية معيش، نسيمة غانم، الإبات الجنائي في الجرائم المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2012-2013.
4. سهيلة قدوم، ليدية بسام، الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر في القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية ، جامعة عبد الرحمان ميرة، بجاية
5. عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لاستكمال متطلبات شهادة الماستر المهني تخصص إدارة التحقيقات الاقتصادية والمالية، قسم علوم التسيير، جامعة قاصدي مرباح، ورقلة، 2018-2019.

- **المقالات:**

1. المطلق نورة بنت عبد الله بن محمد، ابتزاز الفتيات أحكامه في الفقه الإسلامي، جامعة الإمام محمد بن سعود الإسلامية، الرياض.
2. دلال مولاي ملياني، شهادة الشهود في جرائم تكنولوجيا الإعلام والاتصال، مجلة البحوث القانونية والسياسية، العدد 06، جوان 2016.
3. رامي احمد الغالبي، جريمة الابتزاز الالكتروني وآلية مكافحته في جمهورية العراق، مجلة ثقافتنا الأمنية، الإصدار الثاني، وزارة الداخلية العراقية مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019.
4. سامي حمدان رواشده، الأدلة المتحصلة من مواقع التواصل الاجتماعي ودورها في الإثبات الجنائي، دراسة في القانونين الإنجليزي والأمريكي، المجلة الدولية للقانون، جامعة قطر، جانفي 2017.
5. سعيد سالم المزروعي،عبد الرحمان عزمان، اجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقا للتشريع الإماراتي، مجلة العلوم الاقتصادية والادارية والقانونية، المجلد 02، العدد 13، أكتوبر، 2018.
6. سماح محمودي، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية، العدد 08، الجزء 01، المركز الجامعي، بريكة، جوان 2017.
7. سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الالكترونية ومكافحة الجريمة الالكترونية، المجلة النقدية للقانون والعلوم السياسية، المجلد 17، العدد 02، كلية الحقوق والعلوم السياسية جامعة تيزي وزو، 2022.
8. سيهام عكوش، الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري، المجلة السياسية العالمية، المجلد 06، العدد 02، جامعة امحمد بوقرة بومرداس، 2022.
9. عادل فاضل عبد الطائي، التشهير الإعلامي حقيقته وآثاره، دراسة مقارنة بين الشريعة الاسلامية والقانون، مجلة المفكر، جامعة بسكرة، ص 17.

10. عبد الرحمان بن عبد الله السند، جرائم النظم المعلومات مطابع أكادمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2000.
11. عبد القادر فلاح، آية عبد المالك نادية، التحقيق الجنائي للجرائم الالكترونية إثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، جامعة الجلالي بونعامة، خميس مليانة، 2019.
12. عبد العزيز النويري، المخاطر القانونية للانترنت على حرية التعبير والحياة الخاصة، مجلة التواصل، العدد 26، جامعة الحاج لخضر، باتنة، 2010.
13. عز الدين عثماني، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد 04، جانفي 2018.
14. عماد بلغيث، يوسف جغلولي، صعوبات التحقيق في الجرائم الالكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 06، العدد 03، مخبر سوسيولوجية جودة الخدمة العمومية، جامعة محمد بوضياف المسيلة، سبتمبر 2021.
15. فاطمة العرفي، الحماية القانونية للحق في الخصوصية للأطفال من جريمة التشهير عبر مواقع التواصل الاجتماعي في القانون الجزائري، مجلة الاجتهاد القضائي، مخبر اثر الإجتهاد القضائي على حركة التشريع ،المجلد 12، العدد 02، جامعة محمد خيضر، بسكرة، أكتوبر 2020.
16. مبارك بن طيبي، محمد رحموني، شروط قبول الدليل الرقمي كدليل إثبات في الجرائم الالكترونية، مجلة القانون والعلوم السياسية، المجلد 05، العدد 05، جامعة أحمد درارية، أدرار، 2019.
17. محمد هشام فريجة، النظام القانوني للجريمة المعلوماتية وصعوبات تحقيق الأمن الالكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد 24، كلية الحقوق والعلوم السياسية، جامعة المسيلة، جوان 2018.
18. مريم عراب، جريمة الابتزاز والتهديد الالكتروني، مجلة الدراسات القانونية، المجلد 07، العدد 01، جامعة احمد بن بلة، وهران، 2021.

19. مصطفى عليان ربحي، البريد الالكتروني، مجلة الأمن والحياة، العدد 224، المملكة العربية السعودية، 2000.
20. ممدوح رشيد مشرف العنزي، الحماية الجنائية للمجني عليه من الابتزاز الالكتروني، مجلة العربية للدراسات الأمنية، المجلد 33، العدد 70، الرياض، 2017.
21. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكادمية، العدد 11، جامعة باتنة، جوان 2017.

- **المداخلات:**

1. الحمين عبد العزيز بن الحمين بن أحمد، الابتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم، الأسباب، العلاج)، جامعة الملك سعود، 2011.
2. أحمد آيت طالب، العلاقة بين الإرهاب المعلوماتي والجريمة المنظمة، الدورة التدريبية في مكافحة الجرائم الإرهابية المعلوماتية، كلية التدريب، قسم البرامج التدريبية، القنطيرة، المملكة المغربية 9-2006/04/13.
3. حسني عوض، أثر مواقع التواصل الاجتماعي في تنمية المسؤولية الاجتماعية لدى الشباب، برنامج التنمية الاجتماعية والأسرية، جامعة القدس، فلسطين.
4. علي محمود علي حموده، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، منظم المؤتمر أكادمية شرطة دبي، مركز البحوث والدراسات، العدد01- الإمارات العربية المتحدة- 26-28 نيسان 2003.
5. عبد الناصر محمد فرغلي، محمد سيف المسماري، الإثبات بالأدلة الرقمية من الناحيتين القانونية والفنية-دراسة تطبيقية مقارنة- المؤتمر الأول للعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، -الرياض- 12-14 نوفمبر 2007.

- **محاضرات:**

1. ناصر حمودي، الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة ،محاضرات في القانون الجنائي العام ،موجهة لطلبة السنة الثانية جذع مشترك .ليسونس.كلية الحقوق والعلوم السياسية ،جامعة العقيد أكلي محند اولحاج ،البويرة.

- **النصوص القانونية:**

أولا: الدستور:

1. المرسوم الرئاسي 20-442 المؤرخ في 30 ديسمبر 2020 يتعلق بإصدار التعديل الدستور، جريدة الرسمية 82 لسنة 2020.

القوانين:

1. أمر 66-155 مؤرخ في 08 جوان 1966 الموافق ل18صفر 1386 المتضمن قانون الاجراءات الجزائية الجزائري، المعدل والمتمم، ج ر عدد 51، سنة 1966.
2. أمر 66-156 مؤرخ في 08 جوان 1966 ، المتضمن قانون العقوبات، لمعدل والمتمم، ج ر عدد 49، سنة 1966.
3. الأمر رقم 58-75 مؤرخ في 20 رمضان عام 1395 الموافق ل26 سبتمبر 1975، المتضمن قانون المدني المعدل والمتمم، ج ر عدد 78، سنة 1975م
4. قانون رقم 06-01 مؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته، ج ر عدد 14 صادر في 08 مارس 2006.
5. قانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق5غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

النصوص التنظيمية:

1. المرسوم الرئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، جريدة الرسمية عدد 53 صادر في 08 أكتوبر 2005.
2. المرسوم الرئاسي رقم 19-172 مؤرخ في 06 يونيو 2019،يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وكيفيات سيرها، جريدة الرسمية عدد 37 صادر في 09 يونيو 2019.
3. المرسوم الرئاسي 21-439 مؤرخ في 07 نوفمبر 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية عدد 86 صادر في 11 نوفمبر 2021.

- **الأحكام القضائية:**

1. قرار المحكمة العليا صادر في 02 ديسمبر 1980، الغرفة الجنائية الثانية، مجموعة قرارات الغرفة الجنائية، المجلة القضائية، العدد 01 1983.

- **المطويات:**

1. مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية – وثيقة خاصة صادرة عن مديرية الشرطة القضائية– المديرية العامة للأمن الوطني.
2. مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق–وثيقة خاصة صادرة عن مخبر الجهوي للشرطة العلمية–وهران– نيابة مديرية الشرطة العلمية والتقنية –المديرية الشرطة القضائية– المديرية العامة للأمن الوطني .

- **المواقع الالكترونية:**

1. تهاني السبيت، ماهو البريد الالكتروني، مقال منشور في موقع الالكتروني، رابط الموقع: www.C4arab.com .
2. حسين بن سعيد الغافري، جهود السلطنة في مواجهة جرائم الانترنت، مقال منشور في موقع الكتروني، رابط الموقع: http://www.eastlaws.com.
3. رماح الدلقموني، وسائل التواصل حقائق وأرقام، مقال منشور في موقع الكتروني، رابط الموقع: www.aljazeera.net .
4. مات أليغري، إحصائيات واتجاهات وسائل التواصل الاجتماعي[تحديث 2024] تم تحريره والتحقق من صحته بواسطة فريق WSR، 8 مايو 2024، مقال منشور على موقع الكتروني ،رابط الموقع: WWW.Websiterating.com .
5. الموقع الرسمي لقيادة الدرك الوطني الرابط الموقع : http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined.

1-المؤلفات باللغة الأجنبية:

1. Roagna Lvana.La protection du droit au respect de la vie prive et familiale par la convention empennée des droits de l′homme.sérié des précis droit l′homme du conseil de l′europe.1eréEdition.strasboueg .

الفهرس

فهرس المحتويات