وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة –
كليّة الحقوق والعلوم السياسية
قسم القانون العام

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر
تخصص: جريمة وامن عمومي
بعنوان:

الابتزاز عبر مواقع التواصل الاجتماعي

إعداد الطالبة:
نصير هدى

إشراف الدكتورة:
أحمد بومعزة نبيلة

اللجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
خالدي خديجة	أستاذ محاضر – أ–	رئيسا
أحمد بومعزة نبيلة	أستاذ محاضر – أ–	مشرفا ومقررا
عثماني عز الدين	أستاذ تعليم عالي	مناقشا

السنـــة الجامعيـــة: 2023-2024

وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة –
كليّة الحقوق والعلوم السياسية
قسم القانون العام

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر
تخصص: جريمة وامن عمومي
بعنوان:

الابتزاز عبر مواقع التواصل الاجتماعي

إعداد الطالبة:
نصير هدى

إشراف الدكتورة:
أحمد بومعزة نبيلة

اللجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
خالدي خديجة	أستاذ محاضر – أ–	رئيسا
أحمد بومعزة نبيلة	أستاذ محاضر – أ–	مشرفا ومقررا
عثماني عز الدين	أستاذ تعليم عالي	مناقشا

السنـــة الجامعيـــة: 2023-2024

الكلية لا تتحمل أي مسؤولية على ما

يرد في هذه المذكرة من آراء

"وَلَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالإِثْمِ وَأَنتُمْ تَعْلَمُونَ""

سورة البقرة، الآية 188

شكر و عرفان

الحمد الله الذي بنعمته تتم الصالحات ، الحمد الله اولا و آخرا ، و الصلاة و السلام على خير الأنام و قوله الكريم :

«من لا يشكر الناس، لا يشكر الله»

كما لا يسعني ان اتقدم بجزيل الشكر الى الأستاذة الفاضلة " أحمد بومعزة نبيلة " لقبولها الإشراف على مذكرتي، و الإهتمام الخاص من خلاص النصائح و التوجيهات، و إرشادي منذ بداية العمل الى نهايته، و أشكرها على صبرها و حسن معاملتها، فلها فائق الاحترام و التقدير.

كما أتقدم بجزيل الشكر والامتنان الى أعضاء اللجنة المناقشة القديرين الدكتورة " خالدي خديجة" والأستاذ الدكتور " عثماني عز الدين" لتحملهما عبء تقييم هذه المذكرة.

كما أتوجه إلى أساتذتي الكرام بكلية الحقوق والعلوم السياسية وبالخصوص قسم القانون العام على كل ما قدموه لنا من معلومات طيلة المسار الدراسي لهم مني جزيل الشكر والتقدير والعرفان.

فجزى الله كل هؤلاء خيرا، وعافاهم وكفاهم و كافأفهم الجنة.

الإهداء

إلهي لا تطيب اللحظات إلا بذكرك وشكرك ولا تطيب الآخرة إلا بعفوك ولا تطيب الجنة الا برؤيتك

أهدى ثمرة جهد تخرجي الى

من هو جزء من القلب والفؤاد إلى أجمل وأروع إنسان الى قدوتي وخير مثال الى من أحمل اسمه بكل فخر وعزة وشرف الى أبي الغالي " رحمة الله عليه.

الى من جعل المولى الجنة تحت قدميها إلى روحي ونبع الرحمان وفيض الايمان إلى أمي الحبيبة أطال الله من عمرها.

إلا من كانوا لي السند والعون في مسيرتي الدراسية وحياتي العملية إخوتي وأخواتي أخصهم كل باسمه ومقامه على رأسهم أخي الغالي "جمال"

والى الأستاذ القدير" حميدان عبد الرزاق"

الى كل من عرف هدى واحترمها إلى كل من ساندني في إنجاز عملي من قريب أو بعيد.

قائمة المختصرات

ق.ع.ج	قانون العقوبات الجزائري
ق.إ.ج	قانون الإجراءات الجزائية
د.ط	دون طبعة
د.ن	دون سنة
ج.ر.ج	جريدة رسمية جزائرية
ص	صفحة

مقدمة

مقدمة

الجريمة ظاهرة قديمة عرفتها المجتمعات البشرية منذ القدم وظهرت في هذه المجتمعات السلطة الحاكمة انطلاقا من رب الأسرة إلى شيخ القبيلة حيث وضعت بعض القيود على تصرفات الأفراد لاستتباب الأمن لدى الفرد والمجتمع، واعتبرت أن كل فعل يمس الجماعة أو حياة الفرد أو ماله وسلامته الجسدية فعل مجرم يستحق العقاب عليه.

لكن بعد ظهور فكرة الدورة تولت بنفسها سلطة تجريم الأفعال والعقاب عليها حيث أصدرت تشريعات منها ما هو موضوعي "قانون العقوبات" الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي "قانون الإجراءات الجزائية" الذي يحدد الإجراءات الواجب اتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان.

غير أنه يتطور الإنسان في شتى الميادين خصوصا في مجال التقنية، إذ ظهر الحاسب الآلي وشبكة الإنترنت، وغزت هذه الوسيلتين جميع المجالات نظرا لما تتسم به من الدقة والسرعة وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم ونوع جديد من المجرمين وهو الانعكاس السلبي لهذه الثورة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية، فهذه التقنية تسمح بنقل المعلومات صوتا وصورة عبر الإنترنت وفي أي مكان في العالم، مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم، وهذا يعتبر خطر يهدد المجتمع والعالم ككل.

فهذه الجرائم إما تقع عبر الكمبيوتر أو بواسطته حيث يصبح أداة في يد الجناة يستخدمونها لتحقيق مآربهم الإجرامية مستغلين بذلك تلك التقنيات المستحدثة والتي أصبحت فيما بعد محللا لتلك الجرائم أو وسيلة لارتكابها، فأصبح الوسط الذي ترتكب في الجريمة الإلكترونية ومضادات كهربائية أو مغناطيسية ورموز وشفرات ولم يعد مسرح الجريمة إلا مسرحا افتراضيا.

إن بعض مجرمي الإنترنت التقليديين قد عزفوا عن جريمة سرقة بطاقات الائتمان ومعلومات التعريف الشخصي واتجهوا إلى أسلوب أسهل ألا وهو الابتزاز الإلكتروني وهو التهديد والتعدي على حقوق الأفراد في الخصوصية، حيث يستخدمون التهديدات التي تحتوي على صور شخصية وأفلام رقمية للضحية للمطالبة بأموال بدلا من سرقتها.

حيث أصبحت جريمة الابتزاز الإلكتروني ظاهرة تخترق المجتمع وتهدد دعائمه و.... في مقتل أهم أهداف أي مجتمع متحضر في تحقيق الأمن للأفراد، ولعل جوهر تجريم الابتزاز الإلكتروني هو التعدي على الحياة الخاصة وحقوق الفرد واستغلالهم على غير وجه حق والضغط

الذي تمارس على الضحية بكشف أسرار من شأنها أن تضره، مما يضطره للانصياع والإذعان برغبة الجاني وتحقيق مطالبه تحت الإكراه والخوف من الفضيحة وهو ما دعى المشرعين في العديد من الدول إلى سن قوانين تجرم السلوك الإجرامي الذي يتمثل في جريمة الابتزاز الإلكتروني، واهتم شراح القانون بتغييره وشرحه وبيان أركان الجريمة التي تقوم عليها وكذلك طرق التحقيق والاثبات فيها، كما أن للدليل الرقمي أسس وقواعد مختلفة في التعامل معه بسبب خطورة هذه الجريمة وهو ما حذا حذوه المشرع الجزائري على وجه الخصوص.

ولكون جريمة الابتزاز عبر مواقع التواصل الاجتماعي من الجرائم المستجدة على المجتمع ولما لها من آثار مترتبة عنها فإن للبحث محل الدراسة **أهمية علمية وعملية.**

فمن الناحية العلمية لفت انتباه الباحثين لدراسة الموضوع وتسليط الضوء على مختلف جوانبه كذلك لفت انتباه المشرع إلى إعادة النظر إلى النصوص القانونية لمكافحة هذه الجريمة.

أما من الناحية العملية تبرز أهمية البحث في معرفة مدى كفاية النصوص الجبائية الواردة في قانون العقوبات إلى الحد من ارتكاب هذه الجريمة وردع مرتكبيها للتعليل من آثارها وزيادة الوعي لدى مستخدمي الأجهزة الحديثة لمخاطر هذه الجريمة وضرورة توخي الحيطة والحذر في استخدامها.

أما عن **أسباب اختيار الموضوع** فهي ذاتية تتمثل في الرغبة في دراسة هذه الظاهرة المستجدة لكونها غير معروفة في القانون الجبائي سابقا وزيادة إنتشارها باتخاذها أبعادا إجرامية خطيرة على الفرد والمجتمع على حد السواء وتأثير وسائل التواصل الاجتماعي على كليها بالطريقة السلبية تسليط الضوء على الثقافة الدخيلة على المجتمع الجزائري وعاداته وأعرافه التي تتحفظ على كل ما يتعرض للسمعة والشرف خصوصا أن هذه الجريمة أغلب ضحاياها نساء. أما الأسباب الموضوعية فتكمن في إثراء المكتبة وساد النقص في المراجع المتخصصة في هذا المجال ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها.

ومما سبق نطرح الإشكالية التالية: هل نجحت الجهود الوطنية والدولية في مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي؟

اذ ارتكزت الدراسة على **المنهج** الوصفي لوصف الجريمة من خلال تعريفها وآثارها ووسائل ارتكابها والمنهج التحليلي معتمدين على تحليل نصوص وقوانين من خلال المواد التي تتضمنها وتنص على الجريمة محل البحث كقانون العقوبات وقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وبيان موقفها من الجريمة المتمثلة في الابتزاز عبر مواقع التواصل الاجتماعي.

و يكمن **الهدف** من هذه الدراسة في النقاط التالية:

- التعرف على جريمة الابتزاز عبر مواقع التواصل الاجتماعي.
- التعرف على طرق ارتكابها ودوافعها ودراسة أركانها.
- تسليط الضوء على هذا النوع من الإجرام في التعرف على كيفية التحقيق فيها وإثباتها وعلاقة الدليل الرقمي بهذه الجريمة

ونظرا لتزايد نسبة ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرا لخصوصيتها ووسائل وطرق تنفيذها أدى إلى انعكاس هذه الخصوصية على مضمون القانون حتى يتماشى وطبيعة الجريمة.

يعد الابتزاز عبر مواقع التواصل الاجتماعي من المواضيع التي تم تسليط الضوء عليها من دراسات سبقتنا في تناوله إلا أن **الدراسات السابقة** عالجت هذا النوع من الإجرام وفق دراسات مقارنة منها **دراسة الباحثين** باقر غازي حنون و الأستاذ الدكتور حماد حميد "**جريمة الابتزاز الالكتروني**" دراسة مقارنة و قسم الدراسة الى فصلين الفصل الأول: في التشريع العراقي اما الفصل الثاني: في التشريعات الأخرى وأما دراستنا ارتكزت على القانون الجزائري كظاهرة تؤرق المجتمع الجزائري أسوت عن بقية الدول .

من خلال دراستي للموضوع واجهتني بعض الصعوبات في إنجازه تمثلت في ضيق الوقت ونقص المراجع في هذا الموضوع باعتباره جزئية من جرائم أخرى بالإضافة إلى أن هذا النوع من الجرائم له علاقة بالجانب التقني وهذا ما يستدعي التخصص لدراسة بعض الجزيئات بدقة.

ولدراسة هذا الموضوع ارتأينا تقسيم البحث إلى فصلين، الأول بعنوان الأحكام الموضوعية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي وقد تناولت في المبحث الأول منه ماهية الابتزاز عبر مواقع التواصل الاجتماعي أما المبحث الثاني التنظيم القانوني لجريمة الابتزاز عبر مواقع التواصل الاجتماعي والعقوبات المقررة لها، أما الفصل الثاني فقد كان بعنوان القواعد الإجرائية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي الذي يحتوي بدوره أيضا على مبحثين الأول بعنوان إجراءات التحقيق للحصول على الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي أما الثاني فكان تحت عنوان إثبات جريمة الابتزاز عبر مواقع التواصل الاجتماعي وآليات مكافحتها.

الفصل الأول:

الأحكام الموضوعية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي

تعتبر ظاهرة الابتزاز عبر مواقع التواصل الاجتماعي من الظواهر المستجدة والمستحدثة التي ظهرت بظهور التقنيات الحديثة من مجال الاتصالات والتي تعنى بها في ورقتنا البحثية ظهور شبكة الأنترنت، حيث أصبحت هذه الوسائل الحديثة هي محرك العالم بأكمله سواء بصورتها الإيجابية أو بصورتها السلبية وهي محل بحثنا و المتجسدة في الابتزاز عبر وسائل التواصل الاجتماعي بجميع صورة فايسوك ، واتساب. تيك توك، انستغرام، تلغرام، الايمايل، الفيبر...وغيرها من الوسائل.

فالانفتاح التقني الذي شهدته الجزائر من أواخر التسعينات وما صاحب هذا الانفتاح من قفزة نوعية في الاتصالات عامة وفي مجال الانترنت خاصة أوجد عدة مظاهر سلبية نجمت عنه سوء استخدامها لأنها تعد من الجرائم السلسة التي تخلو من العنف فالابتزاز الالكتروني هو الصورة المقابلة لجريمة الابتزاز التقليدي التي ترتكب في مسرح الجريمة باعتبار الابتزاز عبر مواقع التواصل الاجتماعي يتم في عالم افتراضي بتقنيات ورموز وبيانات خاصة الذي سنتطرق من خلال هذا الفصل إلى ماهية الابتزاز عبر مواقع التواصل الاجتماعي من خلال المبحث الأول.
أما المبحث الثاني: سنعرج إلى تحريم هذه الجريمة والعقوبات المقررة لها.

المبحث الأول: ماهية الابتزاز عبر مواقع التواصل الاجتماعي

إن تعريف جريمة الابتزاز عبر مواقع التواصل الاجتماعي يعتريه غموض من بداية ارتكابها إلى غاية صدور الحكم فيها وتنفيذه، فهذه الجريمة في حد ذاتها تعد تحديا كبيرا أمام الجهات القضائية لعدم وجود تعريف جامع مانع لها.

رغم اختلاف التعريفات التي صاحبت هذه الجريمة لكنها اتفقت على أن استخدام التقنيات الحديثة والواقع الافتراضي هو مسرح الجريمة إضافة إلى المهارات والذكاء الفائق لمرتكب الجريمة الذي يميز المجرم التقليدي على هذا المجرم.

لذا ارتأينا من خلال هذا المبحث إلى تقسيمه إلى مطلبين:

المطلب الأول: سنتطرق إلى مفهوم الابتزاز عبر مواقع التواصل الاجتماعي أما فيما يخص **المطلب الثاني:** سنعالج تحريم جريمة الابتزاز عبر مواقع التواصل الاجتماعي والعقوبات المقررة لذلك.

المطلب الأول: مفهوم الابتزاز عبر مواقع التواصل الاجتماعي

يعتبر الابتزاز عبر مواقع التواصل الاجتماعي هو نتاج الاستخدام السلبي للتقنيات الحديثة والأنترنت التي واكبها العالم حديثا وهي من الأثار الغير مرغوب فيها للكثيرين باعتبارها تجعل المجرم يستتر خلق شاشة ما، ويمارس عمله الإجرامي ويعتدي على مصلحة مكفلة قانونيا للضحية، حيث تتم هذه الجريمة عن طريق الضغط على المجني عليه بتهديده تارة والوعيد تارة أخرى بنشر معلومات أو صور أو تسجيلات لا يرغب هذا الأخير في إظهارها. فالابتزاز عبر وسائل التواصل الاجتماعي هو أسلوب من أساليب الضغط والإكراه على المجني عليه لتحقيق مقاصده الإجرامية والوصول إلى هدفه الإجرامي سواء ماديا أو معنويا.

ومن خلال هذا المطلب سيتم التطرق إلى تعريف الإنذار عبر مواقع التواصل الاجتماعي من خلال الفرع الأول، أما في الفرع الثاني سنتناول أسبابه وصوره.

الفرع الأول: تعريفه

أولا: تعريف الابتزاز

أ- التعريف اللغوي:

- ابتزّ يبتزز/ ابتز، ابتزازا فهو مبتز والمفعول مبتزّ.
- ابتزّ المال من الناس: ابتزهم، سلبهم إياه، نزعه منهم بجفاء وقهر.
- ابتز قرنيه: سلبه تكسب منه بطرق غير شرعية محتال يبتز جيرانه.

يرجع أصل كلمة ابتزاز إلى الفعل الثلاثي بز بتشديد الزاي، فيقال بزّ الشيء يبزّه بزّا بمعنى اغتصبه، والبزّ هو السلب، وابتززت الشيء استلبته ومن ذلك جاء المثل (من عزيز) معنى ذلك من غلب سلب. [1]

التعريف الاصطلاحي:

1- هو عملية تهديد وترهيب للضحية نشر صور أو مواد فيلمية أو تسجيلات صوتية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير شرعية أو غير مشروعة لصالح المبتزين كالإفصاح أو تبيان معلومات سرية خاصة بجهة العمل أو غيرها من الأعمال الغير قانونية.

وعادة ما يتم تصيد الضحايا عن طريق البريد الالكتروني أو وسائل التواصل الاجتماعي المختلفة كالفايسبوك، تويتر، انستغرام وغيرها من وسائل التواصل الاجتماعي نظرا لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع وتزايد عمليات الابتزاز الالكتروني في ظل تنامي عدد مستخدمي وسائل التواصل الاجتماعي، الشارع المتهود في إعداد برامج المحادثات المختلفة:[2]

2- محاولة الإكراه وسلب الإرادة والحرية لإيقاع الأذى الجسدي أو المعنوي على الضحايا عن طريق وسائل أو مواقع التواصل الاجتماعي يتفنن الجاني قد استخدامها لتحقيق جرائمه الأخلاقية أو المادية أوكلاهما معا.[3]

3- محاولة تحصيل مكاسب مادية أو معنوية من شخص (طبيعي أو اعتباري بالإكراه بالتهديد بفضح سر وقع عليه المبتز).

4- استغلال القوة مقابل ضعف إنسان أخر سواء كان موقتا، أو دائما أما الابتزاز الالكتروني فهو مصطلح مكون من كلمتين:

الأول: الابتزاز وقد تم التطرق له سابقا.

الثاني: أي يكون الابتزاز عن طريق الوسائل أو التقنيات المستحدثة وعن طريق الشبكة المعلوماتية، إذ أن هناك الكثير من المواقع المعدة خصيصا لذلك مثل مواقع التواصل الاجتماعي أو عن طريق الأجهزة الالكترونية كالحاسوب وما يشبهه مثل الهواتف النقالة والذكية.

---

[1] أحمد مختار عبد الحميد عمر، معجم اللغة العربية المعاصرة، ط1، ج1، دار عالم الكتب، الرياض، 2008، ص 2000.

[2] بلال حناجرة: الانترنت والابتزاز الالكتروني WWW.NOOR BOOK.COM تم الاطلاع بتاريخ 09-02-2024 على الساعة 22:05.

[3] المرجع نفسه، ص 14.

ولهذا يمكن القول أن الابتزاز الالكتروني هو التهديد والضغوطات التي تتم باستخدام الوسائل التكنولوجية الحديثة والمستجدة لاستغلال من وقع عليه الابتزاز ألا وهو الضحية ماديا، جسديًا أو معنويا.

ب- **التعريف الفقهي:** تعددت التعريفات الفقهية حول الابتزاز فقد عرفه جانب من الفقه على أنه وسيلة ضغط يباشرها شخص ما على إرادة شخص آخر ليجره على ارتكاب جريمة معنية.

وقد عرفه البعض الآخر على أنه فعل يقوم به شخصا لتهديد شخص أخر بأي طريقة ولا يهم نوع أو أسلوب التهديد مادام المهدى من ذلك هو التأثير على إرادة ونفسية المجني عليه بتخويفه أو إزعاجه من خطر لم يتحقق بعد قد يلحق الضحية أو نفسه أو أي شخص له صلة بالمجني عليه.

وقد عرفه على أنه "القيام بتهديد شخص بفضح أمره مالم يستجب المهدد إلى تنفيذ طلبات الجاني وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعة كمس **الشرف** أو تتعلق بحرمة الحياة الخاصة للشخص الذى تم ابتزازه".[1]

وفي تعريف أخر فقد عرف الابتزاز عبر مواقع التواصل الاجتماعي " بأنه الحصول على وثائق وصور، ومعلومات عن الضحية من خلال وسائل الكترونية، أو التهديد بالتشهير بمعلومات ووثائق خاصة عن طريق استخدام الوسائل الالكترونية لتحقيق أهداف يسعى لها المبتز".[2]

من خلال ما سبق من التعريفات الفقهية الابتزاز يخير أنها لا تخرج على اعتبار الابتزاز هو وسيلة ضغط أو تهديد بممارسة المبتز يضغط على إرادة المجني عليه بهدف الوصول إلى تحقيق مراده ومبتغاه لأن الابتزاز مرتبط و متصل اتصال مباشر و وثيق بالتهديد فدونه لا يتحقق الابتزاز.

كما تستطيع القول أن الابتزاز الالكتروني يمثل ويجسد السلوك الغير مشروع أو غير أخلاقي باعتباره يقع عن طريق الشبكة المعلوماتية وبوسائل وتقنيات حديثة.

فتحية التطور التكنولوجي الذي شهده العالم والحركة التسارعية لوسائل التواصل الاجتماعي هناك الكثير من المواقع الاجتماعية الخاصة والمخصصة لممارسة الابتزاز مثل (الفايسوك) وأكثرها

[1] ممدوح رشيد مشرف الرشيد العنزي، الحماية الجبائية للمجني عليه من الابتزاز (مقال منشور على شركة الأنترنات) المحلية العربية للدراسات الأمنية، مجلد -33- العدد 70، الرياض، 2017، ص 199.

[2] المرجع نفسه، ص 199.

انتشارا أخيرا أو عن طريق الأجهزة الالكترونية الأخرى كالهواتف الذكية والأجهزة المحمولة الأخرى كالحواسيب، الأيباد، الساعات الذكية... وغيرها.

جريمة الابتزاز عبر الوسائل الاجتماعية لا تخرج عادة عن نطاق الجرائم العادية لكنها ترتكب بوسيلة معينة والقانون بصفة عامة لا نقيمه بوسيلة اقتراف الجريمة.

فقد سوى كقاعدة عامة من الوسائل يرغم تعريفات ظاهرة الابتزاز الالكتروني المتعددة إلا أنها تقف جميعًا في عنصر التهديد الذي يستخدمه الجاني وينتهي بعمل غير قانوني أو عنف مرتكب على الشخص إن لم يستجب لمطلب المبتز، وإذا نظرنا لتعريف جريمة الابتزاز عبر مواقع التواصل الاجتماعي نجد أنها جريمة ما تتعلق بالحصول على أموال أو ممتلكات أو خدمات من فرد أو مؤسسة أي إذا كان شخص طبيعي أو شخص معنوي عن طريق التهديد باستخدام طرق عدم مشروعة قانونيا كاختراق حاسوب، أو التقاط صور، أو فيديوهات لشخص أو قد يكون من سلمها إلى المبتز إما الطريقة التي تم الحصول بها على هذه الوسائل المستخدمة في الابتزاز طواعية أو غير طواعية دون علم الضحية بذلك هنا يتم استخدامها من المبتز بغرض طلب الأموال.

إذا قمنا بتحليل التعريفات تستنتج:

1- إن تهديد شخص ما أو إكراهه أو القيام بأمر معين أو خدمة أو تنازل عن ممتلكاته فهذا يعد اعتداء صريح على حق الملكية المتمثل في الأموال والممتلكات فبذلك يعد أيضا إعتداء على الحق الفردي من خلال استخدام عنصر التهديد والذي من المفروض أن يكون الشخص آمن على حياته وممتلكاته الخاصة من الاعتداء عليها فهو حق مكفول قانونيا و دستوريا.

2- إن اختراق الحواسيب والهواتف الذكية أو ما شبهها ذلك من الوسائل والحصول على المراسلات الخاصة للأفراد وتهديد الشخص فيه انتهاك لسرية المراسلات، واعتداء على حرمة الحياة الخاصة التي كفلتها الدساتير والقوانين.[1]

- لا خلاف في الفقه أن تعريف مجال الحياة الخاصة أمر عسير وصعب وذلك لاختلاف مضمون هذه الحياة واختلاف نطاق الخصوصية من فرد إلى آخر.[2]

[1] الشحات ابراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية تحت فقه مقارن، ط1، دار الفكر الجامعي، الاسكندرية، ص 80

[2] المرجع نفسه، ص 81.

– الخلاف في محور حول نطاق الحياة الخاصة لكن لا بد إلى الحق في الخصوصية فهو حقيقة مؤكدة لدى جميع الأفراد والأشخاص وفي كل المجتمعات فهي تعنى الحق في الحياة الأسرية والشخصية والداخلية والروحية لكل شخص عندما يمشي وراء بابه أو في نطاقه الخاص.[1]

– إن اندراج نظام المعالجة الآلية للمعلومات قلب الكثير من الأوضاع وأصبح له الأثر البالغ على المجتمع خاصة في مجال الحياة الخاصة، فأصبح بذلك بنك المعلومات وهو جزء من النظام الآلي ومستودع كبير للكثير من الأسرار المتعلقة بالحياة الخاصة للأفراد مما يسمح بالحصول على هذه الأسرار والاطلاع عليها بكل سهولة وسرعة خارقة وغير مسبوقة وبكميات هائلة ونقلها من مكان إلى آخر عن طريق أجهزة الاتصال التي تعمل عن بعد في أماكن مختلفة.

– إن الحق في الحياة الخاصة يتطلب أن يربط بمحاور الحماية الجزائية وتفعيل الشروع في هذه الجرائم بذلك أصبحت أعظم حاجة وأكبر إلحاح خصوصاً وقد تجلب الأفكار الآنية والمتأنية المجرمين التقنين في اتباع وسائل و طرق مستحدثة لتحقيق الاعتداء على الحياة الخاصة للأفراد عن طريق الابتزاز عبر وسائل التواصل الاجتماعي.

الفرع الثاني: أسبابه وصوره

أولا: أسباب جريمة الابتزاز عبر مواقع التواصل الاجتماعي: أرجع بعض المختصين أسباب الابتزاز الالكتروني إلى الضحية نفسها كما ذكر البعض من الخبراء أنه لولا تجاوب بعض الضحايا من النساء أو الفتيات أو حتى الرجال الذين يقومون بإرسال أو تسليم أو منع المبتز الصور إما بإرسال أو تسليم هذه الصور أو مقاطع الفيديو وتحوها لما استطاع المبتز أن يجد وسيلة الابتزاز ففي الشائع تستجيب الضحية لبداية التواصل والاتصالات طمعا أو رغبة في إقامة العلاقات والجاني عادة لا يبتز الضحية ويهددها إلا شيء قد تم الحصول عليه بطريقة أو بأخرى كأن تقوم الضحية بتسليم الجاني موادا تمكنه أو تمنحه من الابتزاز تحت حالة من الثقة المصطنعة لتكوين علاقة ما مشروع أو غير مشروعة، فالمبتز مجرم لكونه باشر بابتزاز الضحية بالمواد التي وصلت إليه طوعًا أوكرها[2]، فهي التي سلمته ما يبتزها به عن طريق المكالمات الهاتفية التي قام بتسجيلها أو بصورة هي قامت تسليمه إياه أو بمقاطع فيديو قامت هي بتصويرها وعرضها على قناتها أو موقعها أو قامت هي شخصيا تسليمه إياها.

[1] مهد علي قطب: الجرائم المستحدثة وطرق مواجهتها، قراءة فن المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية، ط1، دار الفجر للنشر والتوزيع، ص 90.

[2] سلمان في عبد الرزاق الغديان، خطاطبة يحي بن مبارك النهيمي عز الديب عبد الله عواد، جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين و رجال الهيئة والمستشارين النفسيين مجلة البحوث الأمنية المجلد 27 العدد 69، 2018، ص 175.

من أسباب هذه الجريمة ضعف الوازع الديني، فقدم استشعار مراقبة الله عز وجل للإنسان يجعله يقدم على هذه الأفعال المحرمة والمجرمة، بل ربما يفتخر بارتكابها ويشكر ضعف الوازع الديني والتربية غير القويمة أو التسوية وعدم مراقبة الآباء للأبناء وعدم الاطلاع على أحوالهم ونصحهم وضعف أدوات الرقابة الذاتية وضعف مؤسسات التوجيه الديني والأخلاقي وعجزها عن أداء دورها مما شجع ضعاف النفوس وضعاف الإيمان على ارتكاب مثل هذه الجرائم.[1]

دخول وسائل الاتصال المدينة بصورة كبيرة من حياة الأسر خصوصا الفضائيات وشبكية الأنترنت التي ألغت الحواجز والساتر التي كانت تحفظ الفتيات من الاختلاط بالآخرين من غير محارمها. لقد وفرت التقنيات الحديثة والأنترنت فرصا عن مسبوقة لانتشار الابتزاز إذ تلعب البيئة دورا كبيرا في إنتاج الجريمة والخروج عن القواعد الاجتماعية فوقت الانحراف عن قواعد الامتثال ليلاً ونهاراً وفي أي مكان وعدم وجود رقابة وقد تشكل المعلومات هدفا سهل المنال ويحقق المنفعة السريعة فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف فيها ضئيلة إذ أصبح ضعاف النفوس يصفونهما من أماكن حساسة ومن ثم استغلال محتوياتها للابتزاز.[2]

إن الجهل بسلبيات التعامل مع تقنية المعلومات والاتصالات، يعد سببا للتعرف للابتزاز الإلكتروني فالجهل بالأمور وعدم معرفة الحقائق والمعلومات الكاملة والصحيحة عن مواضيع حساسة مثل الأنترنت والهواتف النقالة يعرض الضحية للابتزاز الالكتروني.[3]

أصبحت التقنيات والبرامج الحديثة قادرة على اختراق العديد من الهواتف الذكية والحواسيب الإلكترونية وحتى الشخصية منها وهذا ما يتعرض له البعض، ولاسيما من الفتيات اللاتي يقمن بتصوير أنفسهن أو غيرهن من هذه الأجهزة، فقد أصبحت البرمجيات الحديثة قادرة على استعادة الصور حتى لو تم حذفها من الأجهزة ولاسيما عند من يقومون بصيانة وإصلاح هذه الأجهزة أي ذوي الخيرة أو الهاكر الذين يستطيعون التحول إلى أماكن تخزين هذه الصور من الاستيلاء عليها بهدف ابتزازها مستقبلا.

حقق الرقابة الأسرية وتقصيرها في توجيه الأبناء وعدم مراقبتهم والجهل ببعض الأمور والحرمان من المحبة والتودد والتعامل الحسن يجعل الضحية عرضة أكثر للانحراف وتكون محل جريمة الابتزاز من طرف أصحاب الترصد لهذه الفئات ذات النفوس الضعيفة.[4]

[1] جريمة الابتزاز الالكتروني وعقوباتها في القانون https://ethna tanay TV تاريخ الاطلاع يوم 07-02-2024، 23:04 .

[2] نفس المرجع https://ethna tanay TV يوم 07-02-2024، 23:04

[3] سليمان بن عبد الرزاق الغديان خطاطية يحي مبارك النعيمي، عز الدين عبد الله العواد المرجع السابق، ص175

[4] المرجع السابق موقع على الانترنت https://ethna tanay TV

إن سوء التنشئة الاجتماعية وضعف الضبط الاجتماعي وعدم تأدية كل فرد من الأسرة واجباته التي خلقه الله له مثل الأب لكسب العيش وتوجيه الأبناء بالحب والعطف وأن يزرع في داخلهم القدوة الحسنة يحسن تصرفاته في حياته مع الجميع، وأكدت دراسة أن سوء الضبط الاجتماعي يسهم بشكل كبير في تعرض الضحية للابتزاز الالكتروني، إن تقصير الأسرة في القيام بواجباتها بتوجيه الأبناء.

حيث يفشل الآباء في مراقبة سلوك الطفل وإهمال معاقبة الطفل عندما يرتكب سلوك منحرف وضبط الذات الذي يؤثر على أداء الأفراد في المؤسسات مثل المدرسة والعمل والزواج.[1]

كما أن الثقة بالعلاقات القائمة عبر مواقع التواصل الاجتماعي يعد سببا في تعرض الضحية للابتزاز الالكتروني وافق انتشار وسائل ومنصات التواصل الاجتماعي انتشار العدد الهائل لمستخدمي هذه المنصات ونحن أمام هذا الكم الهائل الذي يتم غالبا التواصل عن بعد ومن دون معرفة حقيقة بالطرف، هذا كله سهل التخفي واستغلال التمويه والتزوير في الشخصيات والادعاءات الكاذبة من بعضهم حيث تقوم أغلب هذه العلاقات على الخداع والتزييف في الصفات، ففي العديد منها مثلا يقدم بعضهم نفسه على أنه أنثى في حين يكون رجلاً، أو أنه ذو منصب اجتماعي أو سياسي رفيع ويكون الهدف الأساسي لهذا الشخص هو التعرف على الضحايا ومحاولة الحصول منهم على أي ملفات على شكل صور أو ملفات صوتية أو ملفات فيديو، تحت مسمى الصداقة أو البحث عن الزواج ويكون في الحقيقة إما بهدف التسلية أحيانا أو يهدف الابتزاز الالكتروني في أحيان أخرى. [2]

ثانيا: صور الابتزاز عبر وسائل التواصل الاجتماعي : تنطلق العلاقة بين طرفي الابتزاز عن طريق الثقة المزيفة أو الوهمية المتبادلة والأساليب الملتوية والمخادعة والوعود الكاذبة ثم تتطور هذه العلاقة حتى يكون باستطاعة المبتز الحصول على بعض أسرار الضحية ويحتفظ بها ومن ثم تبدأ عملية المساومة والابتزاز تتعدد أسباب ودوافع الابتزاز يحسب شخصية الهدف ومدى قابلية للدخول في هذه الدائرة ولكن في أغلب الأحوال هو الخلل السلوكي لدى الطرفين المبتز أو الضحية.

تعتبر المرأة الضحية الأبرز في هذه الجريمة بصفة عامة والفتيات بصفة خاصة ويرجع ذلك إلى التعاون الأسري في عملية الرقابة على أبنائهم وإعطائهم الحرية دون ضوابط صحيحة،

[1] جريمة الابتزاز الالكتروني وعقوباتها في القانون المصري –نفس المرجع متوفرة موقع على الانترنت https://ethna tanay TV تاريخ الاطلاع: 08-02-2024 الساعة 08:00.

[2] المرجع نفسه، نفس تاريخ الاطلاع.

كما يلعب الفقر والحرمان بالكثير من الأفراد في مختلف المجتمعات في القيام بممارسات تضل في كثير من الأحيان إلى حد الانحراف وارتكاب الجرائم كما أن استخدام التقنية والاتصالات بشكل سلبي مثل البريد الالكتروني العشوائي والايميلات المجهولة والمواقع الالكترونية العامة والخاصة ومواقع التعارف بين الجنسين ومواقع الألعاب والمنتديات الالكترونية ومواقع الدردشة والإعلانات المضللة في المواقع الالكترونية فهي من أكبر الوسائل التي يتم استخدامها لأغراض الابتزاز كما أنها أصبحت في متناول الجميع.

أما من حيث أساليب الابتزاز التي يمارسها المبتز على الضحية فيعتمد على أسلوب التهديد سواء كان التهديد بالتشهير، أو التهديد بإبلاغ ذوي الضحية، الأمر الذى يجعل الضحية يقع تحت وطأة ضغوط المبتز ليجيرها على مجاراته في تحقيق غاياته.

كما يعد استخدام الشبكة العنكبوتية استخدام سلبي عاملا مهما في الانتشار السريع لهذه الجريمة التي يستغلها المبتز كوسيلة ضغط فتعد جرائم ابتزاز النساء أكثر أنواع الابتزاز انتشارا وشهرة، حيث أن جرائم الابتزاز الالكتروني للنساء والفتيات تعتبر النموذج المثالي للجريمة لاسيما إذا كان المبتز رجلا والضحية مرأة.

وتعد هذه الجرائم من الجرائم المتشعبة حيث أن هذه الصور تتنوع تارة بالنظر إلى الهدف المرتقب من الجريمة، أو المنفعة التي تعود على المبتز.

1-الابتزاز عبر مواقع التواصل الاجتماعي بالنظر لشخصية الضحية:

ويتم تقسيم الابتزاز من هذه الناحية إلى:

أ- **الشخصيات الاعتبارية:** قد تكون الفئة المستهدفة من جرائم الابتزاز عبر مواقع التواصل الاجتماعي هي أشخاص اعتبارية كالحكومات، والشركات والمؤسسات وذلك عن طريق الحصول على معلومات سرية خاصة بها.[1]

ثم يقوم المبتز بالتهديد بالإفصاح عنها وإفشائها والإفصاح عنها ونشرها الأخرين.

تبدأ أو تنطلق الجريمة بمتطفل أو دخيل على مواقع أو بيانات مهمة أو بالسطو على هذه المواقع للشخص الاعتباري وخاصة أن المجرم لديه يقين من تشبع الذمة المالية للضحية وبأنه لن يعاني من كونه معسر.

ب- **الأحداث:** اختلقت التشريعات في تعريفها للأحداث، ويرجع ذلك إلى اختلاف تحديد بين التمييز وسن الرشد بسبب العوامل الثقافية الخاصة بكل مجتمع، وتكثر جرائم الابتزاز

[1] المسند صالح بن محمد، المهني عبد الرحمن بن راشد جرائم الحاسب الآلي، الخطر الحقيقي في عصر المعلومات المحلية العربية للدراسات الأمنية والتدريب، المجلد 15 العدد 29، الرياض 2015 ص 181.

الالكتروني للأحداث بالضغط على الحدث أو القاصر بتهديده بنشر صوره، أو تسجيل مرئي أو محادثات على مواقع الدردشة أو أية مادة عن واقعة من شأنها تحقير الضحية عند أهله والمجتمع المحيط به ككل عامة.[1]

عادة الهدف من ابتزاز هذه الفئة يكون من أجل مطامع جنسه، أو تسريب معلومات عن الأهل فيستغل المجرم المبتز جهل الطفل في التصرف ويمارس جريمته بعد التسلل إلى عقل الطفل الحدث لأن الحدث أو الأحداث هم أكثر الفئات اتصالا بالتكنولوجيا ووسائل التواصل الاجتماعي وأكثر ولعا وتعلقا بها حيث باتت تشكل حيزا كبيرا من يومهم مما يسهل انزلاقهم في الجريمة.

ج- **النساء:** يعد ابتزاز النساء هو النموذج الأكثر شهرة وانتشارا خاصة إذا كان الجاني رجل والضحية امرأة ويعود ذلك أنه غالبا ما تكون تهديد المبتز للمرأة بصور أو محادثات خادشة بالحياء أو عرضا مرئيا لعلاقة غير شرعية جمعت بين الطرفين أو شخص آخر.

قد يكون المبتز خطط لجريمته مسبقًا، أو قد زرع الفكرة من رأسه بعد أن وطد العلاقة مع ضحيته، فقد تكون المرأة تحت سن الرشد ومن فئة الأحداث والتي غالبا ما تتجاوب مع الابتزاز خوفا من الفضيحة أو العار إذا لم تنصاع أو ترضخ إلى طلبات المبتز، خاصة إذا كان ما تحرص على إخفائه علاقة عند مشروعة ينظر لها الدين والمجتمع بالتحريم والرقص والاستهجان.

ليس شرط أن يكون الابتزاز نتيجة فضح علاقة غير شرعية قد تكون الضحية تبتز لأسباب لا علاقة لها بجنسها أو سبب علاقة محرمة شرعًا وقانونا، فقد تهدد المرأة بطبيعة عملها كونها سيدة أعمال تهدد بفضح أسرار نشاطها التجاري مثلا. [2]

د- **الرجال:** وكما يمتلك الابتزاز الالكتروني الأثر على النساء بإمكانه أن يؤثر أيضا على الرجال فلا شك يخشلى الرجال التهديد ببث صور ومقاطع ومحتويات يمكنها المساس بشخصيته أو شرفه أو كرامته أو سمعته أو وضعه الاجتماعي أو وظيفته.

كما أنه لا يسمح قطعا بكشف أسرار عمله أو عائلته وعند استشعار اقتراب خطر مماثل يبدأ في طرح سؤال كيف أبلغ عن شخص يبتزني في الجزائر وخارجها وعادة ما يتم استخدام المقاطع والصور في تهديد الرجال لإخافته بفقد مكانة ووظيفة أو زلزلة مركزه الاجتماعي واعتباره أو تسريب معلومات شخصية تمس أسرته أو شرفه أو سمعته أو بيانات سرية متعلقة بالعمل.

---

[1] الزريق خليفة بن على بن محمد ، استقرار الأحداث وعقوبته في النظام السعودي (دراسة تأصيلية مقارنة تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015، ص ص 72-73.

[2] الحميد عبد العزيز بن دمين بن أحمد، الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم، الأسباب والعلاج) جامعة الملك سعود، 2014، ص 61.

2- **بالنظر إلى الهدف المرجو من المجني عليه:** تتطرق هذه الجزئية إلى الهدف المرجو من الابتزاز عبر مواقع التواصل الاجتماعي والذي ينقسم بدوره إلى هدف مادي (مالي)، هدف نفعي، هدف انتقامي، هدف غير أخلاقي (جنسي).

أ- **هدف مادي (مالي):** لا يختلف الابتزاز المادي كثيرا عن الابتزاز الجنسي فهو من أنواع الابتزاز الالكتروني الخطيرة والتي يتم فيها ابتزاز الفتيات وابتزاز الشباب أيضا وجميع الفئات فمن منا لا يحتفظ بالعديد من المعلومات الخاصة أو بيانات حسابية.

قد تكون هذه البيانات عبارة عن صور وفيديوهات أو معلومات هامة تخص الحسابات البنكية وغيرها من المعلومات السرية، لذلك يستهدف الجاني أو المبتز الحصول على هذا المحتوى السري وبالتالي التهديد به.[1]

- وهناك عدة أشكال من الابتزاز المادي:
- ابتزاز بالصور.
- ابتزاز بالفيديوهات والمقاطع السيئة.
- ابتزاز بالحصول على بيانات ومعلومات قد تدين الضحية في أمرها.
- أما عن حدوث الجريمة فهي عبارة عن سرقة المعلومات والبيانات والمحتوى من الهاتف أو الكمبيوتر الشخصي عبر الدخول غير مشروع أو سرقة الجهاز ثم التواصل مع الضحية والقيام بابتزازه ماديا عبر تهديده بنشر الصور والفيديوهات مقابل دفع أموال.
- في الغالب تخضع الضحية وذلك يدفع أموال خوفا من نشر هذه الأسرار على الملأ ولكن لا تدري الضحية سواء كان الابتزاز للشباب أو الفتيات بأن هذه البداية فقط، حيث يبدأ الجاني في اختلاف تهديد آخر مقابل أموال أخرى، لذلك يجب معالجة الابتزاز الذي من هذا النوع في أسرع وقت بسبب نتائجه الخطيرة على الضحية.

ب- **هدف نفعي:** يتحقق هذا النوع بقيام المبتز بتهديد الضحية بإفشاء أسراره ونشرها للعامية والملأ وذلك إذا لم يلبي طلباته أو لم يحقق مصلحة للمبتز أو ترويج مخدرات أو يكون عمل مشروع كالتوسط لدى شخص لإتمام عمل، طالما كان العمل ضد إرادة المجني عليه فقد تحققت جريمة الابتزاز الالكتروني.[2]

[1] عراب مريم، جريمة التهديد والابتزاز الالكتروني، المجلد 7، العدد 1، مجلة الدراسات القانونية المقارنة، تاريخ الاطلاع 08-02-2024 الساعة 20:45 ص 1211.

[2] المرجع نفسه، 1211.

ج- هدف انتقامي: يعد العامل النفسي العنصر الأساسي في عملية الابتزاز الالكتروني وذلك باعتبار أن المجني عليه يعيش صراعا داخليا نتيجة أن الجاني سيقوم بتنفيذ تهديداته ضده في أي وقت شاء ما ينفعه إلى تلبية طلبات الجاني تجنبا للفضيحة، حيث سيتمتع الجاني بأذية المجني عليه واستماعه لتوسلاته وما يزيد الأمر سوءا أن يقوم الجاني بتصوير المجني عليه ويطلب منه ذكر أي بيانات تتعلق به كما يكون الدافع لدى الجاني هو الانتقام من المجني عليه عن طريق إلحاق الأذى به و إساءة سمعته بنشر صوره عن طريق شبكة الانترنت.[1]

هـ- هدف غير أخلاقي (جنسي): يبدو هذا الهدف أكثر وضوحا في حال كان الضحية امرأة ويتحقق هدف المبتز المستهدف من جرائم الابتزاز الالكتروني عندما ينجح في إقناع الضحية بتصوير مقاطع أو التقاط صور في أوضاع إباحية.

- ويتم اقتراف جريمة الابتزاز الالكتروني بدافع جنسي عندما يسعى المجرم المبتز إلى حيازة معلومات وصور أو بيانات تخص الضحية ويبدأ في تهديده بكشفها ما لم يشبع رغبته الجنسية عن طريق تصوير مقاطع أو أخذ صور جنسية في أوضاع معينة في مقابل التزامه الصمت وتسليمه ما تخصه والامتناع عن نشره وتداوله.[2]

المطلب الثاني: وسائل الابتزاز عبر مواقع التوصل الاجتماعي والآثار المترتبة عنه

تعتبر ظاهرة الابتزاز الالكتروني من الظواهر الجديدة نسبيا حيث أنها لم تظهر إلا بظهور وتوسيع شبكة الانترنت ومع ظهور وسائل الاتصال الشهيرة تزايدت هذه الظاهرة وأصبحت تؤثر على فئات المجتمع الجزائري بدون استثناء وباتت تخلق مصائب مجتمعية في وقت أصبح قراصنة يسعون بشتى الطرق للانتقام من خصومهم والنيل منهم من خلال استعمال منصات التواصل الاجتماعي لتصفية حساباتهم بمجرد الضغط على زر المفاتيح والاختباء خلف الشاشة.

- لهذا فالابتزاز الالكتروني بعد أي طريقة تستخدم بواسطة وسائل الاتصال التكنولوجية الحديثة حيث تستدرج الضحية:

- عبر مواقع التواصل الاجتماعي Social Media
- بعض تطبيقات الهواتف الذكية Smart mobile apps

لإغرائهم بالظهور في أوضاع مخلة وتصويرهم دون علمهم، وتهديدهم أو ابتزازهم بنشرها مقابل الحصول على مبالغ مالية وللقيام بما يسبب خطرا على الضحية. مما يضع المختصين في مجال

[1] عراب مريم، المرجع نفسه، ص 1211.

[2] المرجع نفسه، ص 1211.

مكافحة الجريمة المقصود جريمة الابتزاز الالكتروني عدة خصائص وملامح لعملية الابتزاز الالكتروني فهي:

- نوع من أنواع الجرائم الالكترونية الحديثة.
- تعد من الجرائم الأكثر انتشارا خاصة بين أوساط الشباب.
- قد تصدر من شخص مبتدأ أو متمرس.
- جريمة في غاية الخطورة.
- سهلة الارتكاب ويصعب اكتشافها.
- يصعب تقدير حجم أضرارها التقنية والمادية.

يتنزع المجرمين اعتبارا لعدة معايير منها الخبرة، علاقة المبتز بالضحية أو من حيث المعرفة التقنية، أو كونهم مجرمين فرديين أو ينتمون إلى عصابات منظمة.

بالإضافة إلى اختلاف كل نوع إلا عدة حالات فمن حيث الخبرة نجد المتمرس والمبتدأ إما من ناحية العلاقة نجد المعلوم أو المجهول للهوية وهناك جرائم متمكنين من التقنيات وآخرين يستخدمون التأثر والتلاعب بالمشاعر إضافة إلى المجرم الفردي والذي ضمن عصابات.

فهذا التنوع يؤدي إلى تنوع الوسائل والآثار المترتبة عن جريمة الابتزاز عبر مواقع التواصل الاجتماعي فهذا ما سيتم التطرق إليه من خلال فرعين الأول تتناول فيه الوسائل والثاني الآثار المترتبة عن هذه الجريمة.

الفرع الأول: وسائل الابتزاز عبر مواقع التواصل الاجتماعي

يتم استدراج ضحايا الابتزاز عبر مواقع التواصل الاجتماعي بشكل عام عن طريق الحاسب الآلي، وتوابعه وبرامجه وعن طريق شبكة الانترنت (مواقع التواصل الاجتماعي، أو بعض تطبيقات الهواتف الذكية) ومن أشهر مواقع التواصل الاجتماعي استخداما لتصيد الضحايا: facebook, instagram, twitter, snapchat, youtube, tiktok

ومن أشهر تطبيقات الهواتف الذكية Skype, Viber, Whatsapp أسوة عن البريد الالكتروني وأية وسيلة الكترونية أخرى يمكن من خلالها الوصول إلى معلومات سرية أو حساسة عن الضحية.[1]

أولا: الحاسب الآلي: الحاسب الآلي أو الحاسوب عبارة جهاز يقوم بتنفيذ العمليات الحسابة والمنطقية ومعالجة البيانات المدخلة من وحدات الإدخال ضمن وحدة المعالجة المركزية ومن ثم

[1] عراب مريم، المرجع السابق، ص 1211.

تحويلها وإخراجها على شكل معلومات عبر وحدات الإخراج، كما يمكن تعريف الحاسوب على أنه جهاز الكتروني حديث قادر على تخزين البيانات ضمن وحدات التخزين المتعددة أو مجموعة من الوحدات الالكترونية لتقديم العديد من الخدمات في شتى المجالات الطبية والعلمية والهندسية والتكنولوجية بالإضافة لتلبية الاحتياجات الشخصية مثل كتابة وتحرير المستندات وتصفح الانترنت وعرض الصور ومقاطع الفيديو وغيرها، وجميع هذه العمليات التي يقوم بها الحاسب مبنية على نظام التشغيل operating system الذي يشكل أساسا عمل الحاسوب.[1]

– وقد عرف الفقهاء والدارسون جرائم الكمبيوتر بعدة تعاريف تتعدد لموضوع العلم المنتمي إليها وتبعا لمعيار التعريف ذاته.

– فهذه التعريفات تختلف بحسب ما إذا كانت منتمية للقانون الجنائي أو متصلة بالحياة الخاصة أو متعلقة بحقوق الملكية الفكرية أي حق التأليف البرمجي.

– حسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الانترنت "أي جريمة تفاعلها معرفة فنية تقنية الحاسبات تمكنها من ارتكابها".

وحسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الانترنت "هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات ونقلها".

يعتمد التعريف على معيارين:

1– وصف السلوك.

2– اتصال السلوك بالمعالجة الآلية للبيانات وتحليلها.

1– تقسيم الجرائم تبعا لدور الحاسب الآلي في الجريمة:

قد يكون الهدف الاعتداء استهداف معطيات المعالجة المخزنة أو المتبادلة بواسطة الحاسب الآلي هذا ما يعبر عنه بالمفهوم الضيق [2] (جرائم الكمبيوتر) وقد يكون وسيلة لارتكاب جريمة أخرى في إطار (الجرائم المرتبطة بالكمبيوتر) فقد يكون هذا الأخير بيئة لجريمة أو وسطها مخزنا للمادة الإجرامية وفي هذا النطاق هناك معلومات يجري الخلط بينهما يعبران على هذا الدور.

الأول: جرائم التخزين، ويقصد بها تخزين المواد الإجرامية أو المستخدمة في ارتكاب الجريمة أو الناشئة منها.

[1] موقع على الانترنت www. Arageek.com تاريخ الاطلاع: 15–02–2024 الساعة 14:36.

[2] محمود أحمد عبانية، جرائم الحاسوب وأبعادها الدولية، ط 1، الإصدار الأول 2004، الطبعة 2، الإصدار 2، 2009، دار الثقافة للنشر والتوزيع، عمان، ص 70.

الثاني: جرائم المحتوى أو ما يعبر عن بالمحتوى غير مشروع أو غير القانوني والمصطلح الأخير استخدم في ضوء تطور أشكال الجريمة مع استخدام الإنترنت.

والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وكوسيلة لارتكابها في نفس الوقت وهذا التقسيم الشائع وهو تقسيم الجرائم إلى جرائم هدف وجرائم وسيلة لدى الفقه المصري، أما تقسيمات كجرائم هدف ووسيلة ومحتوى فإنه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في أوربا تحديدا و أفضل ما يعكس هذا التقييم الاتفاقية الأوربية الكمبيوتر والانترنت 2001.

2-تقسيم الجرائم حسب مساسها بالأشخاص والمرتبطة بالحاسب الآلي: تخرج هذه الجرائم عن الجرائم التي تستهدف الأموال فتتصل بجرائم الاختراق وإنشاء كلمة سر الغير والحيازة غير المشروعة للمعلومات وإساءة استخدام المعلومات ونقل معلومات خاطئة أما الجرائم الماسة بالأشخاص المرتبطة بالكمبيوتر فتظم طائفتين رئيسيتين هما:

الجرائم غير جنسية التي تستهدف الأشخاص وهي تضم التهديد عبر الوسائل المؤمنة والأحداث المتعمد للضرر العاطفي والملاحقة عبر الوسائل التقنية وأنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية وبث المعلومات المظللة الزائفة والانتهاك الشخصي لحرمة الكمبيوتر الدخول غير المصرح به وطائفة الجرائم الجنسية.[1]

مثال: كمثال على استخدام الكمبيوتر أو الحاسب الآلي في ارتكاب جريمة الابتزاز الإلكتروني فيقوم أحد الموظفين بالدخول إلى الحاسب الآلي التابع للشركة ثم يقوم بالدخول إلى المستندات الخاصة بالمعلومات والبيانات المتعلقة بالموظفين خاصة السرية ثم يقوم بتهديدهم أو ابتزازهم.

ثانيا: برامج الحاسب الآلي : يتضمن الحاسب الآلي العديد من البرامج الأساسية الهامة التي تساعد في إتمام العمليات الحسابية وإدراج الصور والتصميمات وكذلك حفظ المعلومات إذ يجب أن يحتوي الكمبيوتر على برامج التشغيل والبرامج المكتبية لأنها من أسس التعامل على جهاز الحاسوب بسلاسة وسوف نعرض أهم برامج الحاسب الآلي فيما يلي:

- **أهم برامج الحاسب الآلي:** هناك العديد من برامج الحاسب الآلي المهمة التي تستخدم في مجموعة متنوعة من المجالات التي تتمثل في برامج التصميم وتحرير الصور منها:

-أنظمة التشغيل opérating system تدير وتشغل الحاسب الآلي.

-البرامج المكتبية office suits تشمل هذه البرامج معالجة النصوص.

[1] محمود أحمد عبانية، المرجع السابق، ص 72

-برامج تحرير الصور والرسومات: مثل Adobe photoshop تستخدم لتحرير الصور وإنشاء الرسومات والتلاعب بها.

-برنامج التصميم والنمذجة ثلاثية الأبعاد: مثل الرسوم المعمارية الصناعية وغيرها.

-برنامج تطوير البرمجيات: تتضمن محرر النصوص وترجمة اللغات.

هذه البرامج و غيرها من البرامج فهي على سبيل المثال ومنها أيضا برامج قواعد اللسانيات، برامج التصفح والانترنت هذه البرامج لها عدة استخدامات ووظائف حسب الغرض المستخدم لها هناك استخدام إيجابي لتطوير وتسهيل العمل على المستخدم ولها استخدامات سلبية من بينها ابتزاز الغير اذا ما تم استخدامها من قبل المبتز لمواجهة الضحية.

ورد تعريف لبرامج الحاسب الآلى في نظام مكافحة الجرائم المعلوماتية السعودي بأنه "مجموعة من الأوامر والبيانات التي تتضمن توجيهات وتطبيقات حين تشغيلها في الحاسب الآلي أو شبكات الحاسب الآلي، تقوم بأداء الوظيفة المطلوبة".

فبرامج الحاسب الآلي يعرف أيضا باسم تطبيق أو كيان برمجي هو عبارة عن مجموعة أو سلسلة من الأوامر تعطى للحاسوب لتنفيذ مهمة معينة في إطار زمني.[1]

ثالثا: الإنترنت: من الطبيعي أن تخلق الإنترنت أنماطا إجرامية مستحبة ومستحدثة أو تؤثر بالآلية التي ترتكب فيها جرائم الحاسب الآلي ذاتها بعد أن تحقق شبابيك الحواسيب معاني نطاق شبكات محلية واقليمية وعالمية، وقد ساد مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحاسوب ووسائل الاتصال (الشبكات).

وفي نطاق هذا المعيار يجري التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر ذاته خلال مرحلة المعالجة والتخزين، والاسترجاع وبين الشبكات ذاتها أو المعلومات المنقولة عبرها وطبعا الأنشطة التي تستهدف مواقع الإنترنت وحادمها من نظم الكمبيوتر العملاقة أو تستهدف تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات الإلكترونية.

عرفت الجريمة بصفة عامة على "أنها كل فعل غير مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدابير احترازية وتعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت على المعلومة بشكل رئيسي، هذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم ".[2]

[1] أنواع برامج الكمبوتر متوفرة على الموقع: presstetouan.com : //https تاريخ الاطلاع: 2024/02/18 الساعة: 09:00.

[2] صغيري يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجيتير في القانون، كلية الحقوق والعلوم السياسية/ مدرسة القانون الأساسي والعلوم السياسية ، جامعة مولود معمري، تيزيوزو، تاريخ المناقشة: 2013/03/06، ص 08.

وقد عرف بعض الفقه الجريمة المرتكبة عبر الإنترنت "هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية والحاسوب الآلي الرقمي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف".[1]

– هذه الجرائم المستهدفة التي أتى بها التطور العلمي في مجال الاتصالات فهي تختلف عن الجرائم التقليدية والتي ترتكب في العالم المادي حيث أن الجريمة المرتكبة عبر الإنترنت هي أسرع تطورا للتطور التكنولوجي الهائل، والمشارع لشبكة الإنترنت كما تتم عن طريق مجرم محترف في التعامل مع الشبكة لكي يقوم بالتجسس والتغريد بالقصر واختراق خصوصيات الغير دون عنف أو أثر مادي خارجي.

– تتم عملية الابتزاز عبر مواقع التواصل الاجتماعي كصورة من صور الجرائم المرتكبة عن طريق الانترنت بواسطة البريد الإلكتروني، المواقع الإجتماعية المختلفة والهواتف الذكية وملحقاتها وبرامجها.

1–البريد الإلكتروني: يعرف الايميل أو البريد الإلكتروني بأنه خدمة تمكنك من إرسال واستقبال الرسائل الإلكترونية عبر الإنترنت.[2]

يعرف جانب آخر من الفقه البريد الإلكتروني بأنه "مستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم شرط تأمين هذا الصندوق بعدم الدخول إليه وذلك بطرق التأمين المعروفة ومنها التشفير وكلمة المرور وغيرها من تقنيات الحماية الفنية.[3]

أما تعريفه قانونيا فقد تباينت التشريعات في تعريفه:

فقد عرفه القانون الأمريكي المتعلق بخصوصية الاتصالات الإلكترونية الصادر عام 1986 إذ جاء فيه "البريد الإلكتروني وسيلة يتم بواستطها نقل المراسلات الخاصة عبر شبكة خطوط تلفونية خاصة أو عامة وغالبا ما يتم كتابة الرسائل على جهاز الكمبيوتر ثم يتم إرسالها الكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه إذ يتم إرسالها عبر نظام خطوط التلفون إلى الكمبيوتر المرسل إليه".[4]

---

[1] صغيري يوسف، المرجع السابق، ص 08.

[2] طريقة تبادل الرسائل بشكل رقمي موقع على الانترنت، https : ar.n.wikipedia.og/wiki تاريخ الاطلاع: 2024/02/21 الساعة: 02:45.

[3] الطالب علي باسم، جريمة انتهاك مراسلات البريد الالكتروني (الجريمة الالكرتونية) بحث مقدم الى مجلس كلية القانون كجزء من متطلبات لنيل شهادة البكالوريوس في القانون، سنة 2018، ص 06.

[4] عدي جابر هادي، الحماية الجزائية للبريد الإلكتروني، دراسة مقارنة، بحث مقدم بمجلة رسائل الحقوق، سنة الثانية، عد 03، كلية القانون، جامعة القادسية ، 2010، ص 156.

أما غب التشريع الفرنسي في القانون الخاص بالثقة في الاقتصاد الرقمي الصادر في يوليو 2004 إذ جاء فيه "البريد الإلكتروني هو كل وسيلة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات ويتم إرسالها عبر شبكة اتصالات عامة وتخزين عند أحد خوادم تلك الشبكة أو في المعدات الصوفية للمرسل إليه ليتمكن هذا الأخير من استعادتها".

في حين نجد التشريعات العربية لا تزال بعيدة عن معالجة التطور الحاصل في مجال التقنية بدليل أن كل القوانين العربية لم تعرف البريد الإلكتروني.

من خلال ما تم ذكره عن البريد الإلكتروني فإنه يحتاج لحماية قانونية خاصة الحماية الجزائية وذلك لعدة اعتبارات أهمها: حماية الحقوق، خاصة الحق في الخصوصية التي بها وجهاز متلازمان وهما حرية الحياة الخاصة وسرية الحياة الخاصة.

فعلى الرغم من انتشار الكثير من الصور التقنية للبريد الإلكتروني من تشفير، كلمة مرور لكن هذا لم يمنع المتطفلين أو قراصنة المعلومات من ارتكاب جرائم بواسطة البريد الإلكتروني.

في أغلب حالات الابتزاز عبر مواقع التواصل الاجتماعي يكون بدخول غير مشروع لهذه المواقع أو البريد الإلكتروني رغم انتشار التقنيات لحماية هذه المواقع الا أنه يتم اختراقها فعادة يكون الدخول دون علم الضحية مما يشكل صعوبة لمكان وصول الجرائم إلى علم السلطات خوفا من السمعة.

وفي بعض الأحيان تعرف الجريمة ولكن الجاني مجهول، لأنه لا يستخدم اسمه الحقيقي بل يستخدم اسما مستعارا أو وهمي عند إرسال الرسالة في البريد الإلكتروني كما لا يستخدم حاسوبه الخاص وإنما يرتاد مقاهي الإنترنت، وقد تتوفر الخبرة التقنية ومع ذلك لا يمكن التوصل للجاني.

كما أن هناك صعوبات قانونية تحول بين الجاني والضحية لحمايته من هذه الجرائم ومنها:

- قد يكون الجاني في دولة والضحية في دولة أخرى كذلك مسألة تنازع القوانين الجزائية وكذلك اختلاف الأحكام بين قوانين الدول.
- قد يكون الفعل المجرم في دولة مباحا في دولة أخرى.

2-مواقع التواصل الاجتماعي: هي تلك المنظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به ومن ثم ربطه من خلال نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم الاهتمامات والهوايات تعتدها أو جمعه مع أصدقاء يعرفهم واقعيا، فتعد شبكات التواصل الاجتماعي مثل فايسبوك، تويتر أو تطبيقات مثل السكايب أو واتساب من أفضل الوسائل التي ربما ميزت العصر الحديث وأسهمت في إحداث طفرة حقيقية في التواصل المباشر بين المسلمين وغير المسلمين وبين مختلف الجنسيات والديانات. فقد أصبحت هذه المواقع تعرف بالإعلام

الاجتماعي الجديد الذي يشهد حركة ديناميكية من التطور والانتظار فقد كان في بدايته مجتمعا افتراضيا على نطاق ضيق ومحدود، ثم ما لبث أن ازداد مع الوقت لاتحول من أداة اعلامية نصية مكتوبة إلى أداة اعلامية سمعية بصرية تؤصر في قرارات المتأثرين واستجاباتهم.

إن لمواقع وبرامج التواصل الاجتماعي أهمية كبيرة وبصفة خاصة في الجزائر فقد أصبحت شهرتها واسعة وكثر التعامل معها بين الناس حيث يتواصلون عبر هذه المواقع للتعرف على بعضهم ومعرفة أخبار بعضهم البعض وإرسال رسائل وتلقي الأخبار والموضوع وكل ما هو جديد في الساحة.

– فقد تباينت التعريفات حول مواقع التواصل الاجتماعي فنجد:

تعريف المشروع الفرنسي للتواصل الاجتماعي عبر شبكة الأنترنت : في المادة 04 من القانون رقم 575_2004 الصادر بتاريخ 21 يونيو 2004 بأنه "بروتوكول اتصال مفتوح أو ربط بيانات وتبادلها بأي شكل يصل إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية".[1]

تعريف القانون الإماراتي رقم 05 لسنة 2012 المواقع الإلكترونية هي مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات.

- أما مواقع التواصل الاجتماعي يمكن تعريفها على أنها "تلك الوسائل التقنية الحديثة التي يستخدمها الأشخاص في ما بينهم لتحقيق التواصل الاجتماعي المشاع عبر شبكة الإنترنت كالفايسبوك، تويتر، اليوتيوب وغيره.[2]

السؤال الذي يطرح نفسه هنا:

كيف يتم اصطياد واستدراج الضحايا عبر مواقع التواصل الاجتماعي؟

يتم استدراج وجذب الضحية عن طريق النقر على رابط وهمي من شأنه أن يثير فضول واهتمام أي شخص فيطلب منه معلومات عن الهوية وبعض المعلومات الشخصية كرقم بطاقات الائتمان أو رقم الضمان الاجتماعي وقد يظن البعض أنه من السهل اكتشاف أن هذه العملية مجرد احتيال ولكن للأسف حتى أكثر المستخدمين للمواقع وفائقي الذكاء قد وقعوا ضحايا لهذه

[1] دنيا عبد العزيز فهمي، المسؤولية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، دراسة مقارنة، بحث مقدم في مجلة الشارقة، دورية علمية، محكمة، المجلد 16، العدد 01، يونيو 2016، ص 373.

[2] المرجع نفسه، ص ص 373 – 374.

الاحتيالات نظرا لتنوع الوسائل والأساليب التي يستخدمها المجرمون وهي أساليب غير مشروعة بغرض الحصول على المعلومات.

يرتكب مجرمو الإنترنت جريمة الابتزاز الإلكتروني فيجعل من مواقع التواصل الاجتماعي أداة ووسيلة للوصول إلى غايتهم باستدراج ضحاياهم فيستجيب الضحايا للابتزاز خوفا من التشهير، حيث يعد الابتزاز عن طريق مواقع التواصل الاجتماعي جريمة تتم من خلال التهديد بالكشف عن بيانات محرجة أو ضارة عن شخص في الجمهور أو العائلة أو الزملاء ما لم يشير هذا الأخير ضمن المبتز في بعض الدول يعتبر الابتزاز الإلكتروني عبر الفيسبوك التهديد الرئيسي المرتبط بانتهاك الخصوصية.

ضبط الخصوصية على الحسابات الإلكترونية لا يعني أن الحساب آمن وخاص كما أن كثيرا من المستخدمين لا يقومون بتعيين الإعدادات المتعلقة بالخصوصية لحفظ حساباتهم ويعود إلى صعوبة القيام بذلك أو ليس لديهم فكرة كافية عن وجود هذه الإعدادات ونظرا لكون التواصل الاجتماعي أصبح جزءا مهما من حياتنا اليومية، فتعد هذه التقنية بيئة خصبة لارتكاب الجرائم الإلكترونية خاصة جريمة الابتزاز الإلكتروني أو عبر مواقع التواصل الاجتماعي.

مقدم استخدام الهوية الشخصية في هذه المواقع تعد فرصة لاستغلالها من قبل المجرمين كثغرة لسرقة البيانات واستخدامها كوسيلة للابتزاز.

وتتعدد بذلك الأفعال المجرمة من طرف أصحاب مواقع التواصل الاجتماعي ومن أكثر الجرائم ارتكابا تلك الماسة بالأشخاص والخصوصية وتعد جريمة الابتزاز الإلكتروني أكثر الجرائم ارتكابا حيث تتزايد معدلاتها بشكل يدعو للقلق حيث تتزايد عمليات الابتزاز الإلكتروني مع عدد مستخدمي وسائل التواصل الاجتماعي والتسارع المشهود في إعداد برامج المحادثات المختلفة.

رابعا: الهاتف النقال : قدمت التكنولوجيا للإنسان عدة امتيازات جعلت من حياته أكثر سهولة ورفاهية، إلا أن هذا الأسلوب الجديد في الحياة صاحب العديد من المشكلات والأضرار التي في الغالب تكون مصاحبة للاستعمال السلبي لهذه الأدوات سواء من قبل صانعيها أو حتى من قبل مستخدميها، فمن هذه الوسائل الحديثة الهاتف النقال.

يعتبر الهاتف النقال وسيلة اتصال لاسلكية تعمل من خلال شبكة أبراج البث المباشر على تغطية مساحات معينة وتترابط فيما بينها بواسطة خطوط ثابتة وأقمار صناعية وهو ما يعرف بشبكة التغطية.[1]

[1] طريقة تبادل الرسائل بشكل رقمي، المرجع السابق، تاريخ الاطلاع: 2024/03/08، الساعة: 12:09.

ومع تطور أجهزة الهاتف النقال أو الخلوي أصبحت الأجهزة أكثر مجرد وسيلة للاتصال الصوتي حيث أصبحت تستخدم كأجهزة كمبيوتر وتصفح الإنترنت والأجهزة الحديثة نفس خصائص ودقة وضوح الكاميرات الرقمية.

نظرا لخطورة هذه الوسيلة عملت بعض التشريعات الغربية على وضع قوانين تجرم الأفعال التي توصف بأنها جرائم ترتكب بواسطة الهاتف النقال وذلك من خلال إضافة مواد عقابية تجرم هذا النوع من الجرائم على غرار التشريع الفرنسي، الانجليزي والأمريكي ولكن أغلب التشريعات العربية لم تقم بتجريم توظيف الهاتف النقال من ارتكاب جريمة بإستثناء المشرع السعودي والاماراتي.

– بينما المشرع الجزائري لن يقم بتحريم الأفعال المرتكبة بواسطة الهاتف النقال إلا في جرائم محددة تمس الإساءة لرسول الله صلى الله عليه وسلم أو المعلوم من الدين أو الإساءة لشخص الرئيس رئيس الجمهورية.

– واكب الجانب الإجرائي هذا التطور من خلال الاستعانة بالهاتف النقال أو غير من الوسائط الإلكترونية كوسيلة للكشف عن الجرائم ومرتكبيها وهو ما يتجلى في قانون الإجراءات الجنائية الجزائري والقانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الذي حدد فيه المشرع جميع الإجراءات التي يجب على السلطات التحري والتحقيق والعمل بها في جريمة ذات طابع إلكتروني كما أن المشرع الجزائري بموجب هذا القانون قد عمل على تأسيس هيئة وطنية لمكافحة الجريمة الإلكترونية بجميع صورها.[1]

تنقسم برامج التشغيل للحاسب الآلي أو الهاتف النقال الذكي إلى برامج أساسية فيظهر في شكل برامج تطبيقية تهدف للقيام بمهام محددة ومن أمثلة ذلك الماسنجر، الفيسبوك.

– أما البرامج غير الأساسية وهي المعلومات التي تتميز بها الهواتف الذكية وتظهر في شكل وسيط أو أداة تغطي خدمة معينة كرسائل البريد الإلكتروني والبريد النصي والصور الرقمية ومقاطع الفيديو المخزنة قد تتعلق المعلومات بشخص المستخدم أو تتعلق بوظيفته، وقد تتضمن أسرارا قد تشكل خطرا على المصلحة العامة أو تهديدا لها.

– نكون هذه المعلومات محلا لجريمة الابتزاز الإلكتروني أو عبر مواقع التواصل الإجتماعي وذلك عندما يقوم المجرم الإلكتروني باستخدام الإنترنت في برامج التواصل الاجتماعي أو المعلومات

[1] التوجي محمد، الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال، رسالة مقدمة لنيل شهادة دكتوراه، في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة احمد دراية، ادرار، 2019، ص 03.

الموجودة بالهاتف النقال الموجه للتجسس على الآخرين وانتهاك حرمة حياتهم الخاصة أو عن طريق الاستخدام غير المشروع لملحقات الهاتف الذكي، الكاميرا والبلوتوث أو آلات التسجيل.[1]

الفرع الثاني: الآثار المترتبة عن ذلك

تخلف ظاهرة الابتزاز عبر مواقع التواصل الاجتماعي آثار خطيرة نتناولها فيما يلي

أولا: الآثار الإجتماعية : تشكل ظاهرة الابتزاز عبر مواقع التواصل الاجتماعي خطرا فعليا على الفرد والمجتمع والعائلة على حد سواء حيث أن أغلب ضحاياه نساء مما أدى بهم إلى الانفصال عن أزواجهم كما أم أغلب الفتيات اللائي تعرضن إلى الابتزاز لا يقدمون شكوى في المحاكم خوفا من المشاكل الناجمة كأن يفرق الناس من التقدم للزواج منهن خاصة المحيط القريب منهن، فقد ترفض الفتاة الزواج نتيجة تاريخها السابق، وقد يؤدي الابتزاز إلى هدم بين الزوجين بالطلاق فهو أثر مباشر للابتزاز.

- يخلق بدورة الابتزاز عدة آثار خاصة للفتاة باعتباره أكثر فئة معرضة للابتزاز وأكثر فئة يلاحقها العار إذا ما تم نشر صور أو فيديوهات لها، ففي أغلب حالات الابتزاز تنصاع الفتاة لطلبات المبتز خوفا من الفضيحة فقد يصل إلى اغتصاب الفتاة وحملها والاجهاض أو التخلي عن الطفل إلى الملاحق أو الشارع وهذا كله نتيجة لحظة تهور من الفتاة بدخولها في علاقة وهمية مع المبتز أو نتيجة إختراق المواقع والحصول عفى البيانات فالصور كمادة دسمة لابتزاز الفتاة بالحصول على غرضه المجرم.[2]

ثانيا: الآثار النفسية: أما بالنسبة للآثار النفسية فهي فقدان الثقة بالنفس وبالمحيطين، الشعور بالقلق والخوف والتوتر والاكتئاب ولوم الذات والشعور بالخجل والندم، وقد يعاني من اضطرابات نفسية يتطلب تدخل علاج طبي متخصص وينخفض مستوى أداءه في الدراسة أو العمل وقد يفكر في الإقدام على الانتحار، مما يزيد من الآثار النفسية على الضحية عدم قدرة هذه الأخيرة على طلب المساعدة بسبب الإحراج أو الجهل بأساليب الوقاية أو أن هناك من يستطيع تقديم يد العون والتهوين عليه.

– نجد عند فئة المراهقين والقصر لا يفهم أهلهم مشكلتهم فقد يميلون للوحدة والعزلة كما أنهم يتغيبون على الدراسة أو العمل والدخول في حالة من الكآبة والحزن والتوتر والعدوانية تجاه

[1] التوجي محمد، المرجع السابق، ص 03.

[2] شريق محمد السويدي، مصطفى نوفل، أسباب الابتزاز الالكتروني والآثار الاجتماعية والنفسية المرتبطة به (دراسة كيفية) جامعة الشارقة/ مجلة الأدب، العدد 146، سنة 2022، ص 618.

الآخرين نتيجة الضغوطات النفسية ويتفاقم الوضع مع مرور الوقت ودخول الضحية في حالة هستيرية من البكاء والصراخ.

– كما قد يتحول الضحية إلى مجرم مبتز أيضا إبتزاز جنسي نتيجة لما حدث له أو ردة فعل لما أصابه.[1]

ثالثا: آثار الحماية : يعد الابتزاز من الأساليب التي تهدد المجتمع في أمنه وحمايته للفرد مما يؤدي إلى تفشي الفساد وانهيار القيم والأخلاق في المجتمع فلا يؤمن الفرد على عرضه وشرفه، فإذا كان الغرض مز الابتزاز هو غرض مالي فهذا يؤدي إلى تفاقم وانتشار جرائم النصب والسرقة خاصة إذا كان الضحية معسر ولا يملك ما يقدمه للمبتز مقابل صمته.[2]

- أما إذا كان الغرض منه جنسي غير أخلاقي فهذه الجريمة لا تكون منفردة بل تصاحبها جرائم أخرى كالإغتصاب، السكر ، الزنا، السرقة ، القتل، وغيرها من الجرائم فقد يقدم الضحية على قتل المبتز يعد ارتكاب الفاحشة وتصويره لها ، فإذا ما تم تداول صور الجريمة يقوم أهل الضحية بقتل المبتز المعتدى والانتقام منه خاصة في بعض المجتمعات التي لا ترى غسل العار إلا بسفك الدم.
- تعد ظاهرة الابتزاز من الظواهر سريعة الإنتشار لسرعة انتشار الصور والفيديوهات بكبسة زر تنشر على أوسع نطاق وهذا ما يهدد الفرد في استقرار حياته الخاصة رغم التشديد التشريعي والأمني لذلك.

[1] شريق محمد السويدي، زيزيت مصطفى نوفل، المرجع السابق، ص ص 618-619.

[2] محمد بن عبد المحسن بن شلهوب، جريمة الابتزاز الالكتروني دراسة مقارنة بحث تكميلي لنيل درجة الماستر في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الأنظمة جامعة الإمام محمد بن سعود الإسلامي، ص 59.

المبحث الثاني: التنظيم القانوني لجريمة الابتزاز عبر مواقع التواصل الاجتماعي والعقوبات المقررة لها

تعد جريمة الابتزاز عبر مواقع التواصل الاجتماعي من الممارسات البغيضة، كونها تؤرق الضحية وتحول حياته من حياة هادئة إلى حياة يعمرها الخوف والاكتئاب والاضطراب، مما يجعله رهينة في يد المبتز، إذ يصبح ممتثلا لأوامره وملبيا لرغباته بصرف النظر عن مضمون التهديد سواء كان متعلقا بالشرف والسمعة والاعتبار، أم كان يتعلق بالنفس أو المال، وبالتالي يعد الابتزاز الإلكتروني من أبشع الجرائم لكونه قد يتصل بالإنسان لدرجة الرق والعبودية فهو تهديد الآخرين بشتى الوسائل لاستشعارهم بالخطر المحدق بهم، مما يجعلهم يخضعون لرغبات الحياة ويكونون تحت تصرفهم.

لذا فالابتزاز هو جريمة غير أخلاقية تعج بها المجتمعات كافة ولا سيما مع التطور التقني الذي أثر في طبيعة الجريمة بشكل عام، والوسائل المستخدمة في ارتكابها، إذ انتقلت وسائل ارتكاب جريمة الابتزاز من الأدوات التقليدية إلى الأدوات المتطورة التي تعتمد على الوسائل الإلكترونية وتأسيسا على ما تقدم يسعى هذا المبحث بيان التنظيم القانوني للابتزاز الإلكتروني من خلال مطلبين نتناول في الأول أركان جريمة الابتزاز عبر مواقع التواصل الاجتماعي ونبين في المطلب الثاني العقوبات المقررة لها في التشريع الجزائري.

المطلب الأول: أركان جريمة الابتزاز عبر مواقع التواصل الاجتماعي

من أجل اعتبار السلوك الإنساني جريمة بمفهومها الجنائي ينبغي توافر عناصر وشروط معنية وهي العناصر والشروط اللازمة لقيام الجريمة والتي تسمى بالمفهوم القانوني أركان الجريمة.

لذا سنقوم في هذا المطلب إلى فرعين نخصص الأول لمناقشة الركن الشرعي أما من خلال الفرع الثاني سنبين عناصر الركن المادي بجريمة الابتزاز عبر مواقع التواصل الاجتماعي أما الفرع الثالث نبين الركن المعنوي لها من خلال إبراز عناصره.

الفرع الأول: الركن الشرعي

من المتعارف عليه أن في كل دولة جهاز قضائي وآخر تنفيذي قانوني يلاحق المجرمين ويصدر القوانين التي تعاقب هذه الفئة المبتزة من المجتمع حيث نجد الدولة هي الجهة الوحيدة المسؤولة عن محاسبة المجرم وهي التي تفرض العقوبات على جميع المجرمين حيث ما يراه المشرع من خصوصية للحياة الشخصية وكذا الأنظمة. [1]

لهذا لا يمكن أن تعاقب أنت بنفسك المبتز أو ابتكار الحيل لإيذاء المبتز فلا يمكن علاج الخطأ بالخطأ وإنما اللجوء إلى الفريق الشرطي والدولة هو الأفضل حل وأفضل خيار لعقاب وتتبع

[1] نعيمي أسماء (سلمى): الابتزاز والتشهير الالكتروني وعقوبته في القانون الجزائري تفاقم جنح التهديد بالابتزاز والتشهير في ظل الرقمية والالكترونيات، 1 فبراير 2024 آخر تنقيح الصدور في 14 أكتوبر 2016، تاريخ الاطلاع 08-03-2024، الساعة 13:35 www.ech.chaab.com

هذا المجرم المبتز، لهذا كل من تعرض إلى جريمة التهديد بالابتزاز والتشهير به، التوجه إلى الجهات المختصة في الدولة، سواء دوائر الأمن الوقائي أو البحث الجنائي أو الهيئات المخصصة لمكافحة الجريمة الإلكترونية وتقديم عريضة الشكوى.

أولا: جريمة مصنفة ضمن الجرائم الخطيرة: وبكل تأكيد فإن أغلب القوانين العربية والعالمية تعاقب على جنح التهديد بالابتزاز والتشهير كونها من الجرائم الخطرة التي تلحق بالضاحية الكثير من الضرر سواء عن عمله أو سمعته أو تدمر نفسية الضحية وحياته الخاصة، لهذا الكثير من القوانين تنظر إلى جريمة الابتزاز كجريمة مصنفة ضمن الجرائم الخطرة والتي تحدثت معظم القوانين عنها بصراحة وعالجت أغلب وقائعها لا بل فرضت عقوبات قاسية على المجرم تصل إلى الحبس لسنوات وغرامات مالية عالية، ويشار أن هذه الجرائم تتعامل معها على الأغلب الأجهزة الشرطية في الدولة بكل سرية وبكل وحرفية على أيدي أناس مدربين سواء خبراء في عالم التقنيات أو خبراء في القبض على المجرم المتخفي، وفعلا القوانين تعاقب على هذا النوع من الجرائم لكن الصعوبة تكمن في كيفية إثباتها وكيفية الوصول إلى المجرم في وضع التلبس وهي مسألة صعبة ومعقدة وبحاجة إلى خبرة واسعة في هذا المجال، إذن في الملخص هي جريمة خطرة لمالها من أبعاد من وقعت عليه.[1]

ثانيا: يخطر أي عنف بدني أو معنوي أو أي مساس بالكرامة: فهذه الجريمة في أغلب الدول تكون قاسية وتصل إلى الحبس لسنوات وغرامات مالية كبيرة فالإعلان العالمي لحقوق الإنسان يقر في مادته صراحة المادة 12 "يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"، كما اهتم الدستور الجزائري المؤرخ في 30-12-2020 هو الآخر بهذا الموضوع في مادته 30 "تضمن الدولة عدم انتهاك حرمة الإنسان، بخطر أي عنف بدني أو معنوي أو أي مساس بالكرامة.

يعاقب القانون على التعذيب وعلى المعاملات القاسية واللاإنسانية أو المهنية والإتجار بالبشر."[2]

ثالثا: المواد المخصصة لتجريم الابتزاز عبر مواقع التواصل الاجتماعي : الركن الشرعي في الجريمة هو نص التحريم والعقاب فهو النص الذي نستند إليه لتجريم فعل معني والعقاب عليه وأن

[1] نعيمي أسماء، المرجع السابق.

[2] المادة 40 سابقا من دستور 2016.

يكون هذا النص ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة "لا جريمة ولا جزاء ولا إجراء ولا تنفيذ للعقوبة إلا بقانون".

– تطبيقا لمبدأ الشرعية فالرجوع لبعض القوانين العربية نجد أنها قد نصت على هذه الجريمة وحددت العقوبات اللازمة لها أما في البعض الآخر من الدول العربية فلم ينص المشرع صراحة على تجريم الابتزاز الإلكتروني فلا وجود لقواعد قانونية تخص تلك الجرائم بالذات إلا أن القضاء حاول جاهدا معالجة هذه الجرائم وفق تكييفها القانوني من خلال تطوير القواعد القانونية الموجودة في قوانينها العقابية.

– أما بالنسبة للمشرع الجزائري قد أولى أهمية بالغة للخصوصية الشخصية للأفراد واعتبر الاعتداء عليها جريمة تصيب مركز المجني عليه حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه جريمة الابتزاز الإلكتروني أو عبر مواقع التواصل الاجتماعي المختلفة في المجتمع الجزائري، الذي طالما اعتز بمبادئه وقيمه الفاضلة فمثل هذه الجريمة كفيلة بهدم حياة المجني عليه وتفقد عائلته كرامتها وانتمائها للمجتمع وقد تطرق المشرع لتلك الحماية لحرمة الحياة الخاصة في الدستور في مص المادة 39 منه سالفة الذكر.

– حسب م 02 من القانون 09-04 المؤرخ في 5 أوت 2009 حيث يعرف الجريمة المتصلة بتكنولوجيات الإعلام والاتصال بأنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".

– نص التجريم في المادة 303 مكرر القانون 06-23.[1]

"يعاقب بالحبس من ستة (6)أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

- يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية جدا للمتابعة الجزائية.

[1] القانون 06-23 الصادر بتاريخ 20 ديسمبر 2006 المعدل والمتمم لقانون لعقوبات الجزائري.

-المادة 303 مكرر 1 من ق العقوبات.[1]

-حيث تضمنت المواد سالفة الذكر 303 مكرر، 303 مكرر 1 ثلاث صور للتجريم وهي تسجيل ونقل والتقاط الأحاديث الخاصة والسرية المتعلقة بالأشخاص دون موافقتهم على ذلك بالإضافة إلى جريمة التقاط وتسجيل أو نقل صورة لشخص في مكان خاص دون رضا أو إذن صاحبها وكذا جريمة الاحتفاظ والوضع في متناول الجمهور أو الغير أو الاستخدام لتلك المكالمات أو الأحاديث أو الصور المحصل عليها بإحدى تلك الطرق.

1- مجال الحياة الخاصة: حسب ما ورد في قانون العقوبات الجزائري فقد حصر المشروع الحياة الخاصة بمفهومها الضيق في عنصرين هما الحق في سرية المكالمات والمحادثات الخاصة والحق في سرية الصور عند التواجد في مكان خاص.

2- المقصود بالمكالمات والأحاديث الخاصة والسرية: هي تلك الأحاديث التي يتفوه بها المرء إما مباشرة دون استخدام وسيلة معينة للاتصال وهي الصورة التي يكون فيها المتحدث وجها لوجه مع المتحدث معه، وإما أن يكون بطريقة غير مباشرة في حالة بعد المسافة مما يقتضي الأمر لإيصال الصوت استعمال جهاز الهاتف أو الحاسوب وتسمى بذلك مكالمة.

والكلام المتفوه به يعني الحديث الذي يتلفظ به الشخص وتكون به دلالة ولا يشترط في هذه الدلالة أن يكون مفهومه لدى عامة الناس وإنما يكفي أن يكون مفهوم لدى فئة محددة منه، بل قد يصدر الكلام من شخص مع نفسه لأن المشرع استعمل مصطلح الأحاديث وليس المحادثات كما أن المفهوم الضيق لعبارة المكالمات والأحاديث عن أنه يجب أن يصدر كلام معني فلا تدخل الأصوات فيه نطاق تطبيق النص.[2]

أما بالنسبة لمضمون الحديث الخاص والسري يعني أنه يتضمن الكلام مسائل عائلية مرتبطة بالعلاقة الزوجية أو العلاقات الشخصية أو حتى الكلام المتعلق بالحالة الصحية ولا عبرة بالمكان الذي صدر فيه الحديث أما الأحاديث التي قيلت في أماكن عمومية وتضم المسائل المتعلقة بالحياة الخاصة قاعدتها تدخل في نطاق الأحاديث الواردة في المادة 303 مكرر.

3- **المقصود بالحق في سرية الصورة في المكان الخاص:** هي تلك الوضعية التي يظهر بها الشخص في مكان خاص لا يريد أن يراه فيها إلا الأشخاص الذين يحددهم بنفسه، هنا التحريم يكون متعلق بانتهاك حرمة الصورة وارتباطها ارتباطا وثيقا بطبيعة المكان الذي

[1] انظر المادة 303 مكرر قانون العقوبات الجزائري.

[2] زواوي سنية، الحماية القانونية للحق في جريمة المحادثات الهاتفية، كلية الحقوق والعلوم السياسية، مخبر المرافق العامة والتنمية، جامعة جيلالي سيدي بلعباس الجزائر، العدد 19، جوان 2018، ص 659.

يجب أن يتم فيه التصوير وهو المكان الذي لا يتم الدخول له إلا بإذن وهذا ما يضيق من مجال التجريم مقارنة مع المساس بحرمة المكالمات والأحاديث[1].

– أما التصوير في مكان عمومي سواء كان عمومي بطبعه أو بالتخصيص أو المصادفة لا يدخل في نطاق التحريم[2].

– ويتصرف مفهوم المكان الخاص إلى كل حيز مكاني ثابت أو منقول لا يمكن دون استنزاف أو تسجيل أو نقل، أو استماع ما يدور بداخله وإن أمكن مشاهدة من بداخله ولا يجوز دخوله إلا بموجب موافقة مالكه أو حائزه أو ممن تربطهم رابطة وظيفية أو مهنية .

ومن ثم أحكام الحماية الجزائرية على الحديث الذي يتم من هذا المكان ويتناول أمورا عامة ليست لها صفة الخصوصية[3].

الفرع الثاني: الركن المادي

نعني به السلوك المادي الخارجي الذي ينص التشريع على تجريمه أي كل ما يدخل في إطار جريمة الابتزاز عبر مواقع التواصل الاجتماعي وتكون له طبيعة مادية ملموسة وهو ضروري لقيام الركن المادي إذ لا يعرف القانون الجرائم دونه.

يتكون الركن المادي بدوره إلى ثلاثة عناصر وهي السلوك الإجرامي، النتيجة الإجرامية والعلاقة السببية.

أولا: السلوك الإجرامي لجريمة الابتزاز عبر مواقع التواصل الاجتماعي : يتمثل السلوك الإجرامي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي بالتهديد المقترن بطلب إذ يشترط فيه أن يكون بالإيذاء وأن يترك أثرا في نفس المجني عليه يدفعه إلى تنفيذ مطالب المبتز من دون إرادته كأن يطلب الجاني مبالغ مالية أو إقامة علاقات جنسية محرمة وفي حالة عدم الاستجابة فإنه سيقوم بتنفيذ تهديده .

–وفي الواقع أن السلوك الإجرامي في جريمة الابتزاز الإلكتروني صورتين الأولى التهديد بالأذى المادي والصورة الثانية التهديد بالأذى المعنوي كالآتي :

1– **التهديد بالإيذاء المادي:** الإيذاء المادي هو الإيذاء الذي يكون محله الجسد أو المال كالتهديد بإحداث إصابة بدنية مثل القتل والضرب... الخ وبالتالي يعد ابتزازا إذ هدد شخص امرأة بقتلها أو

[1] عز الدين طباش، شرح القسم الخاص من قانون العقوبات، جرائم ضد الأشخاص والأموال، د ط، دار بلقيس، دار البيضاء الجزائر،د.ن، ص 125.

[2] المرجع نفسه، ص 126.

[3] نبيل صقر، الوسيط في جرائم الأشخاص، دار الهدى، عين مليلة–الجزائر، د.ط، 2009، ص 174.

تدمير ممتلكاتها ذات القيمة المادية كالتحف غالية الثمن أو ذات قيمة خاصة لديها كالصور والمقتنيات الخاصة إذا ما توقفت عن الاستمرار بالعلاقة الجنسية معه.

أ- **التهديد الذي يكون محله الجسد:** يشمل كل صور التهديد بالعنف ضد الجسد، سواء أكان موجها للضحية أو لشخص آخر يهمه أمره، ومن التطبيقات القضائية عن التهديد بالإيذاء ضد الجسد ما جاء في قرار محكمة التمييز في العراق، بأنه إذا كان تهديد المشتكية بالقتل بالمسدس مصحوبا بطلب التنازل عن المهر المعجل والمؤجل قاعدته هذا الفعل ينطبق على المادة 430 من قانون العقوبات ر س م 431[1].

ب- **التهديد الذي يكون محله المال:** فيشمل كل صور التهديد الموجه للمال، بصرف النظر عما إذا كانت ملكية تعود للمجني عليه أو لشخص آخر عزيز عليه، مادام التهديد أنتج أثر في إرادة الضحية وجعله منصاعا لأوامر المبتز ويكون فحوى هذا التهديد وضع المال موضع الخطر، مما يدخل الرعب والخوف في نفس المجني عليه وبالتالي جعل إرادته مشلولة وغير حرة وبالنتيجة ينصاع وراس رغبات الجاني وينفذ له طلباته خشية من بطشه وتنفيذ تهديده بارتكاب فعل ضار يقع على المال[2].

مثال: مثال عن ذلك تهديد الجاني للضحية بأنه في حال عدم إعطائه مبلغا من المال أو أن يترك وظيفته فإنه سيقوم بحرق المنزل العائد له.

2- **التهديد بالإيذاء المعنوي:** الإيذاء المعنوي هو الإيذاء الذي يكون محله الشرف أو السمعة أو الاعتبار كالتهديد بالتشهير بما يمس سمعة شخص أو تمس شرفه أو توجيه اتهام له، وتتعدد صور التهديد بالإيذاء المعنوي منها التهديد بإفشاء أو إسناد أمور شائعة أو توجيهها لشخص معين، أو توجيه اتهام له وأيضا التهديد باتخاذ إجراءات قانونية تنال من سمعته أو مكانته الإجتماعية أو مركزه الوظيفي أو تضعه في مواجهة القانون.

أ-**التهديد بافشاء أو إسناد أمور مخدشة بالشرف** : هو إفشاء أو نسبة أمور إلى المجني عليه تمس سمعته وشرفه واعتباره أي أن يكون مدلول هذه الأمور الخادشة للشرف مطابقة لمدلول نفسه الذي تفرضه جريمة القذف، وهي الأمور التي لو كانت صادقة لأوجبت عقابا لمن أسندت إليه أو احتقاره عند أهله ووطنه.

[1] باقر غازي-حسن حماد حميد، جريمة الابتزاز الالكتروني (دراسة مقارنة)، كلية القانون جامعة البصرة، مجلة دراسات البصرة، ملحق العدد 42، 2021، ص 63.

[2] باقر غازي-حسن حماد حميد، المرجع السابق، ص 63.

-ومن الأمور الشائنة على سبيل المثال من يسند لآخر أنه يتردد على محلات الدعارة أو أنه فر من مستشفى الأمراض العقلية[1].

ب- بالنسبة للتهديد باتخاذ الإجراءات القانونية ضد الضحية : ففي الواقع أن جريمة الابتزاز الإلكتروني لا تشترط أن يكون التهديد بأمر غير مشروع إذ يمكن أن يقع التهديد بأمر مشروع كمن يهدد آخر باللجوء إلى المحكمة إن لم يلبي له طلباته التي ليس له حق فيها أو أن يهدده بتأخير ترقية المستحقة، أو الإساءة لمركزه الوظيفي أو الاجتماعي، فالتهديد في جريمة الابتزاز الإلكتروني يتحقق عندما يكون القصد شرا حتى ولو لم يشكل جريمة.

كما تقوم جريمة الابتزاز الإلكتروني عندما يتضمن التهديد توجيه اتهامات لشخص إن لم يحقق الجاني ما يريد، كما يقوم موظف بتهديد موظفة بالتبليغ عن ارتكابها لجريمة اختلاس مال عام إن لم تمارس معه الفعل الجنسي، إذ يشكل ذلك ابتزازا سواء أكانت الموظفة قد ارتكبت فعلا تلك الجريمة أم لا. لأن الغرض من التهديد لم يكن تحقيق العدالة أو المساهمة في اكتشاف الجريمة وإنما ابتزاز مرتكبيها[2].

ثانيا: النتيجة الإجرامية : النتيجة الإجرامية هي الأثر المترتب عن السلوك الذي يقصده القانون بالعقاب فهي الحقيقة المادية إلى كيان ملموس عن العالم الخارجي أو أنها الحقيقة القانونية.

وفي جريمة الابتزاز الإلكتروني تقع النتيجة الجرمية لمجرد قيام المبتز بتهديد الضحية بإفشاء سر من أسرارها التي تعتبره أمرا لا يجب الاطلاع عليه أمام الملأ وكان تهديدا بأمر غير مشروع. طالما يسبب ذلك الخوف والهلع والتأثير على إرادة نفسية الضحية بأن يلقي في نفسها قلقا من قيام المبتز بتنفيذ تهديده.

فإن سعي الجاني بالتهديد إلى مجرد ترهيب الضحية أو طلب منفعة أو أن يحمل المجني عليه على أداء عمل أو الامتناع عن عمل فهنا تقع النتيجة سواء فعل المجني عليه ما طلب منه أم لم يفعل[3].

ثالثا: العلاقة السببية: تعد العلاقة السببية العنصر الثالث من عناصر الركن المادي للجريمة فهي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الجرمية، وتعرف العلاقة السببية بأنها الصلة بين السلوك الذي يعترف به القانون سببا والأثر الذي يعترف به القانون نتيجة[4].

---

[1] باقر غازي-حسن حماد حميد، المرجع السابق، ص 64.

[2] المرجع نفسه، ص 65.

[3] محمد عبد المحسن بن شلهوب، المرجع السابق، ص 91.

[4] راسي أحمد غالبي: جريمة الابتزاز الالكتروني وآلية مكافحتها في جمهورية العراق، مقال منشور في مجلة ثقافتان الامنية، الإصدار الثاني وزارة الداخلية العراقية دار الكتب والوثائق بغداد، 2019، ص 45.

–ولقيام الركن المادي لا بد من أن تنتسب النتيجة الإجرامية إلى الفعل أو الامتناع المؤثر الصادر عن الجاني معنى أن تحدث النتيجة الجرمية بسبب فعل الجاني أي لولا حصول الفعل لم تحدث تلك النتيجة[1].

– وفي جرائم الابتزاز عبر مواقع التواصل الاجتماعي لو أن النتيجة تحققت بإفشاء أسرار المجني عليه ولكن بفعل شخص آخر لم يكن هو المبتز أو سبب ضياع هذه الوثائق أو الصور أو الأفلام وانتشارها بمحض الصدفة فلا مسؤولية على الفاعل حيث أن علاقة السببية انتهت، فقد يسأل عن جريمة أخرى بحسب التكييف القانوني للفعل.

– حيث توجد علاقة السببية بين الابتزاز والتسليم في حال كان الباعث للجاني هو الحصول على المال إن لم يلزم أن يكون تسليم المال نتيجة ما أحدثته في نفس المجني عليه من خوف فإذا لم يحدث التهديد هذا الأثر وجرى تسليم المال لاعتبارات أخرى انقطعت علاقة السببية.

– أما إذا كان الابتزاز للقيام بعمل أو الامتناع عن أداء عمل فإن النتيجة هنا وقوع الضرر وهو الخوف في نفس المجني عليه وتكون علاقة السببية بينه وبين الابتزاز هو أن يكون الابتزاز سببا في امتهان كرامة المعتدى عليه واحتقاره وتعريضه لبعض أهله والناس واذا امتنع الضحية من أداء عمل ليس على سبيل الخوف من المبتز وإنما لرغبته في الالتزام القانوني فهنا لا تقع جريمة الابتزاز وذلك لانتفاء علاقة السببية في الجريمة[2].

الفرع الثالث: الركن المعنوي

إن الجريمة ليست كيانا ماديا خالصا قوامه الفعل وآثاره ولكنها أيضا كيانا نفسيا وقد استقر في القانون الجبائي الحديث ذلك المبرر الذي يقضي بأن ماديات الجريمة لا تنشئ مسؤولية ولا توجب عقابا ما لم يتوافر إلى جانبها العناصر النفسية التي يتطلبها كيان الجريمة وتجتمع هذه العناصر النفسية في ركن يختص بها يحمل مسمى الركن المعنوي .

أولا: القصد العام: يشتغل القصد العام في جريمة الابتزاز عبر مواقع التواصل الاجتماعي على عنصرين هما العلم، الإرادة .

1- **العلم:** العلم هو تصور لحقيقة الشيء، أي إدراك الأمور على نحو يطابق الواقع أو صفة يتضح بها الشيء ويظهر على ما هو عليه فالعلم بالشيء هو عكس الجهل به، والذي هو انعدام العلم بشكل كلي أو جزئي.

[1] راسي أحمد غالبي، المرجع السابق، ص 41.

[2] المرجع نفسه، ص 41.

–وفي الجريمة محل الدراسة "يجب أن يعلم الجاني" وقت يشترط أن يحيط الجاني علما بكل العناصر التي تسهم في ارتكاب جريمة الابتزاز عبر مواقع التواصل الاجتماعي أي يجب أن يعلم الجاني وقت متعارفه فعله أن من شأن فعله إرغام الضحية عليه على تنفيذ أمر رغما عن إرادته، كما يجب أن يعلم بأن المنفعة التي حصل عليها إنما هي ثمرة التهديد الذي صدر منه، وأنه ليس له الحق فيما يلزم المجني عليه بتنفيذه فإن كان يجهل ذلك كأن يعتقد بحسن نية أنه يسترد مالا مملوكا له أو أنه يستوفي دنيا له في ذمة المجني عليه، أو أن المجني عليه قد سلمه المال عطفا عليه أو مراعاة لقرابة أو صداقة ما بينهما[1].

– فلا تقوم جريمة الابتزاز الإلكتروني لانتفاء أحد عناصر القصد الجرمي وهو العلم بانتفاء القصد الجرمي لا تتحقق جريمة الابتزاز عبر المواقع لأنها لا تقوم إلا عمرية مع ملاحظة أن عدم المراقبة على جريمة الابتزاز الإلكتروني لا يمنع في بعض الأحوال من المعاقبة على جريمة أخرى كالتهديد مثلا أو غيرها من الجرائم إن توافرت شروطها.

2– الإرادة : هو الإرادة في تحقيق نتيجة غير مشروعة نحو المساس بحق أو مصلحة يحميها القانون ومن ثم ينبغي أن تتجه إرادة المبتز إلى تحقيق النتيجة الإجرامية المتمثلة في ابتزاز المجني عليه فلا يقف الأمر عند علم الجاني ما يترتب على ذلك من آثار نفسية تلحق بالمجني عليه بل يتعمد قصد الجاني التهديدي إلى تخويف أو حمل المجني عليه على القيام بعمل أو الامتناع عنه دون النظر إلى تنفيذ العمل أو عدم تنفيذه فتتوقع حدوث النتيجة يكفي لرغبة الجاني في حدوثها عند مباشرة نشاطه الإجرامي .

–وبما أن الابتزاز الإلكتروني يعد من الجرائم الشكلية التب تتطلب نصيحة معنية فإن المنظم السعودي والقانون الإماراتي والعماني قد حددوا تلك النتيجة بحمل المجني عليه على القيام أو الامتناع عنه[2].

– تنقسم الإرادة إلى قسمين إرادة الفعل و إرادة النتيجة :

لكي تقوم المسؤولية يجب إثبات أن إرادة الفعل اتجهت إلى القيام بهذا الفعل وذلك دون أن تقع الإرادة في عيب من عيوب الإرادة كأن يكون مختارا ومدركا، أنه يحصل على صور سرية وخاصة بالضحية فإذا كان مكرها فلا يوجد قصد جنائي ولا تقوم المسؤولية الجزائية للفاعل المكره.

- أما إرادة النتيجة فلا بد أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية بالحصول على المنفعة المادية أو النفعية اللاأخلاقية كما أنه لا أثر للباعث في توافر القصد الجنائي طبقا

[1] ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 212.

[2] المرجع نفسه، ص 212.

للقاعدة العامة فالباعث لا عبرة له في الجريمة فيستوي في الابتزاز عبر مواقع التواصل الاجتماعي أن يكون الباعث شريفا أو وضعيا كانتقامه من المجني عليه أم لتحقيق مصلحة معينة[1].

2- **القصد الخاص:** بما أن جريمة الابتزاز الإلكتروني هي من الجرائم التي تحتاج إلى معرفة خاصة وعالية بتكنولوجيا المعلومات من أجل تنفيذها فلا يمكن تصور حصولها من دون قصد فهي من الجرائم العمدية التي يكتفي فيها بالقصد العام ولا يشترط أن يكون القصد الخاص[2].

المطلب الثاني: العقوبات المقررة لها

إن الصياغة التشريعية لنصوص التجريم والعقاب هي ليست مجرد إفراغ للنصوص في قوالب شكلية، إنما هي أولا وقبل كل شيء فكر قانوني يرد النصوص لضوابطها القانونية، التزاما بالأصول المنطقية ومن ثم يدخل فيها التثبت من إتفاق النصوص مع الفعل المجرم.

لذلك تعد النصوص القانونية عبارة عن جدار يحمي الإنسان ويحيطه بمزيد من الحماية والأمن والخصوصية، وبالتالي فإن أي شخص يحاول كسر هذه الحواجز أو اختراق هذا الجدار فهو مدان ويستحق العقاب المقرر لفعله .

– وتختلف الأنظمة والقوانين المجرمة في كل دولة وذلك باختلاف كل سياسة جنائية يتخذها المشرع في التخفيف و التشديد في العقوبة وقد عمد المشرع إلى وضع قواعد قانونية رادعة كما يخص جريمة الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي حيث جرم هذا السلوك بكل صوره وتعدياته فوضعت لها عقوبات تناسب مع الجريمة فتنوعت بين عقوبات أصلية وعقوبات تكميلية كما وضع أحكام تخص الشروع في هذه الجرائم .

– وتأسيسا على ما تقدم سنحاول من خلال هذا المطلب تبيان العقوبات المقررة لجريمة الابتزاز عبر مواقع التواصل الاجتماعي من خلال ثلاث فروع، في الفرع الأول سنسلط الضوء على الشروع في جريمة الابتزاز عبر مواقع التواصل الاجتماعي أما في الفرع الثاني سنتناول العقوبات الأصلية التكميلية لذلك وفي الفرع الثالث سنحاول شرح ظروف التشديد والتخفيف لهذه الجريمة .

الفرع الأول: عقوبة الشروع والاشتراك في جريمة الابتزاز عبر مواقع التواصل الاجتماعي

أولا: عقوبة الشروع في جريمة الابتزاز عبر مواقع التواصل الاجتماعي: توجب كلمة الشروع بصورة عامة إلى المحاولة المترافقة بالعزم مع وجود ما يظهر ذلك العزم من وقائع في العالم

[1] محمد عبد المحسن شلهوب، المرجع السابق، ص 107.

[2] المرجع نفسه، ص 104.

الخارجي، فهو مرحلة لاحقة على النية أو العزم على اتيان الأمر المشروع فيه، غير أن الشروع لا يقتصر على معنى ثابت ومحدد وإنما له عدة دلالات مختلفة بحسب الأساس الذي ينظر إليه منه[1]، فالشروع في الجريمة هو البدء في تنفيذ سلوك إجرامي مؤدي إلى ارتكاب جناية أو جنحة تنتهي دون تحقق النتيجة الإجرامية لأسباب لا دخل لإرادة الجاني فيها.

-فالشروع بدوره كسلوك ينقسم إلى نوعين الشروع الناقص، الشروع التام.

1- الشروع الناقص : هو أن يأتي الفاعل بعضا من الأفعال التنفيذية اللازمة لإتمام الجريمة وبهذا لا يكون السلوك الإجرامي قد تم كاملا، فالنتيجة لم تتحقق لأن الفعل قد أوقف بعد البدء فيه وقبل نهايته.

- ومن الخصائص المميزة للشروع الناقص تعطيل التصرف الجرمي أو إيقافه حيث يكون في هذه الحالة حدث أجنبي لا دخل لإرادة الجاني فيه ويتحقق معه حالات التوقف الجبري عن التنفيذ.

- وفي بعض الأحيان يكون راجعا لإرادة الجاني واختياره الحر، وهو العدول التلقائي الذي يرجع لأسباب نفسية خالصة أو يصدر عن الإرادة الحرة للجاني الذي من شأنه عدم استمراره في تنفيذ الجريمة، وهذا النوع من العدول قد يؤدي إلى عدم معاقبة الجاني أو تخفيف عقوبة الشروع في الجريمة.

- أما الخاصية الثانية للشروع الناقص فهي عدم استنفاذ التعرف الجرمي حيث أن هذا الشروع يقوم عند حدوث طارئ ما عطل، أو أوقف هذا التعرف الجرمي قبل اكتماله، وبالتالي لم يستنفذ من قبل الجاني، وأنه لا يزال هناك جزء من هذا التصرف يتطلبه لحدوث النتيجة الجرمية التي أرادها، ولا يهم بعد ذلك قدر ما تم من ذلك التعرف الجرمي، وما يتبقى منه.

- ومع ذلك ينبغي أن يرتبط عدم حدوث النتيجة الجرمية بعدم اكتمال التصرف الذي أوقف وأنه لولا هذا التوقف لكانت قد تحققت الجريمة[2].

2- الشروع التام : هو أن يأتي الفاعل كل الأفعال اللازمة لإتمام الجريمة ومع ذلك فإن النتيجة الإجرامية لا تتحقق وتسمى الجريمة في هذا الشروع إما بالجريمة الخائبة أو الجريمة المستحيلة، حيث تتحقق الجريمة الخائبة عندما يقوم الفاعل على تنفيذ مشروعه الإجرامي بأن يقوم بكل الأفعال التنفيذية التي تحقق الجرم إلا أنه يصل إلى الهدف الذي قصده لسبب خارج عن إرادته

[1] بن عودة صليحة، الشروع في الجرائم المعلوماتية بين الوقاية والردع، المجلد 1، العدد 2، سنة 2021، ص 73.

[2] المرجع نفسه، ص 75.

وتلحق هذه الجريمة بالمحاولة في الجريمة وتراقب بذات العقوبة للمحاولة وقد نص عليها المشرع الجزائري[12].

ويوجد شرطان لذلك هما :

– يجب أن يكون الفاعل قد استنفذ جميع الأعمال التي يتوقف عليها ارتكاب الجريمة.

– يجب أن لا يحدث عدول اختياري كأن يضع الجاني دواء في طعام زوجته بقصد إجهاضها ثم يسقط الصحن فلا تتناوله أو أن يأكل ذلك الطعام وان ما.

– **الشروع حسب القانون الجزائري** : حسب القانون الجزائري يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في م 303 مكرر بالعقوبات المقررة للجريمة التامة.

- ولذا نص المادة 303 مكرر 1 الشروع في جريمة الابتزاز الإلكتروني يتحقق بالتهديد بإفشاء معلومات أو صور أو مقاطع فيلمية أو أي بيانات خاصة للمجني عليه، حتى وإن تراجع المبتز عن إكمال جريمته لسبب خارجي طالما أن التهديد بنشر الأسرار قد صدر منه ووقع في نفس المجني عليه موضع التأثير والرهبة التي جعلته يعتقد أن المبتز سينفذ تهديده لا محالة وهي الهدف الذي تحقق بإلقاء الرعب في قلب المجني عليه، والشروع في الجريمة هنا يتحقق طالما كان الركن المادي فيها قد شرع في تنفيذه وتوافر القصد الجنائي .

ثانيا: عقوبة الاشتراك في جريمة الابتزاز عبر مواقع التواصل الاجتماعي : قد يقوم بجريمة الابتزاز عبر مواقع التواصل الاجتماعي شخص واحد فنكون أمام ارتكاب جريمة من قبل شخص واحد فهو فاعلها أو مبرزها إلى حيز الوجود وقد يرتكب هذه الجريمة عدة أشخاص فنكون أمام جريمة متعددة الأشخاص وهذا التعدد فق الأشخاص يتطلب منا بيان دول كل شخص في ارتكاب الجريمة وهذه هي نظرية المساهمة في الجريمة.

– والمساهمة الجنائية هنا تعني تعدد الحياة الذين يقومون معا بارتكاب جريمة الابتزاز الإلكتروني أي أن هذه الجريمة ثمرة نشاط عدد من الأشخاص لكل منهم دور فيها، وترتب على هذا النشاط المتعدد نتيجة إجرامية واحدة .

– وتفترض المساهمة أن فعل التهديد المكون لجريمة الابتزاز الإلكتروني ارتكب بواسطة أكثر من شخص، فلا يكفي أن يتواجد شخص وسط جماعة ترتكب جريمة للقول يتوافر المساهمة وبمسؤوليته عن الجريمة التي ارتكبت، بل لا بد أن يكون له دور مادي ومعنوي فيها، أي يسهم في ارتكابها بأعمال مادية وإرادة إجرامية.

[1] بن عودة صليحة، المرجع السابق، ص 76.

[2] انظر المادة 30 من ق.ع.ج.

– وتعدد الجناة في الجريمة الواحدة هو ما يميز المساهمة الجنائية عن غيرها من النظم القانونية مثل تعدد الجرائم والعود.

– فالابتزاز الإلكتروني الذي يتم عبر مواقع التواصل الاجتماعي يكون نتيجة مساهمة أكثر من شخص لكل منهم دوره المادي وإرادته الإجرامية بحيث يعتبر فعل كل حياتي مكملا للآخر في تحقيق العناصر المكونة للجريمة، ويكون الجميع أصحاب مشروع إجرامي واحد يساهمون فيه بنسب مختلفة وتتحدد مسؤولية كل مساهم حسب الدور الذي قام به في تكوين الجريمة.

– وينبغي لاعتبار جريمة الابتزاز الإلكتروني واحدة رغم وقوعها من عدة أشخاص أن يكون بين الجناة قصد جنائي مشترك يجمع بينهم وهذا القصد المشترك يفترض اتجاه إرادة كل مساهم نحو تحقيق نتيجة واحدة[1].

شروط قيام المساهمة في جريمة الابتزاز عبر مواقع التواصل الاجتماعي

لقيام هذه الجريمة يشترط ما يلي:

1- **تعدد الجناة** : يتحقق تعدد الجناة عندما لا ينفرد شخص واحد في ارتكاب الجريمة بل يشترك عدة أشخاص في ارتكابها، بأن يقوم كل منهم بدور المساهمة فيها وهنا تكون أدوارهم متماثلة في الأهمية وقد تكون مختلفة.

- وتعدد الجناة الواجب لتحقيق الاشتراك الأصلي الجريمي في الابتزاز الإلكتروني هو ذلك التعدد الاحتمالي للجناة الذي يمكن أن تقوم به جريمة الابتزاز الإلكتروني فقد تقع من قبل جاني واحد فقط أو يشترك فيها عدة جناة كالقتل والسرقة[2].

مثلا أن تقبل هذه الجرائم أن ترتكب من قبل فاعل واحد بطبيعتها كما يمكن أن تقع من قبل جانب عدة أشخاص يشتركون فيها بأدوار مختلفة فإذا وقعت جريمة الابتزاز الإلكتروني من قبل شخص غير الذي نفذها بمساعدة آخر كنا بصدد اشتراك جرمي وذلك لأن تعدد المشتركين في جريمة الابتزاز عبر مواقع التواصل الاجتماعي أمر احتمالي وقابل للتحقيق كما أن احتمال وقوع القتل من قبل شخص واحد أمر وارد.

2- **وحدة الجريمة بأركانها الثلاث:** يراد بوحدة الجريمة وجود رابطة تضامن أو مشاركة أو مساهمة في الحياة فلا يكفي لتحقيق المساهمة في الجريمة تعدد الجناة إنما لا بد ذلك أيضا من أن تكون جريمة الابتزاز عبر مواقع التواصل الاجتماعي المرتكبة نتيجة لها

[1] المساهمة الجنائية في جريمة الابتزاز الالكتروني، متوفرة على الموقع الالكتروني https :mail.almerja.com تاريخ الإطلاع 08-03-2024 على الساعة 17:59

[2] نفس المرجع بنفس التاريخ.

اشتراك والتعاون بين الجناة هي جريمة واحدة، وتتحقق هذه النتيجة فيما لو جمعت بين عناصرها وحدة الجانب المادي ووحدة الجانب المعنوي، ولذا نفترض المساهمة الجنائية أن يصدر عن كل جاني نشاط معين يسعى من خلاله للاشتراك في الجريمة وهذه النشاطات تغطي في نهاية المطاف إلى تحقيق نتيجة جرمية واحدة وقد تكون النتيجة الواحدة التي حققها الجناة بفعل مؤدي لواحد أو عدة أفعال جنائية.

– ومن ثم تحتفظ الجريمة بوحدتها عندما تجمع بين عناصرها وحدة مادية ووحدة معنوية، أي كان ركنها المادي محتفظة بوحدته وكان ركنها المعنوي محتفظة بوحدته المعنوية.

– وتتحقق الوحدة المادية أو وحدة الركن المادي لجريمة الابتزاز الإلكتروني إذا ارتبطت أفعال المساهمين فيها برباط سببي بالجريمة التي وقعت أي يجب أن تتوافر علاقة سببية مادية بين فعل كل مساهم والجريمة بدون هذه العلاقة يفقد الركن المادي وحدته وتفقد المساهمة الجرمية أحد أركانها وتنتفي تبعا لذلك .

– لا يكفي لكي تتحقق وحدة جريمة الابتزاز الإلكتروني أن يكون الركن المادي قد احتفظ بوحدته وإنما يجب علاوة على ذلك أن يحتفظ الركن المعنوي بوحدته أيضا وهو ما يتحقق بتوافر أو قيم رابطة ذهنية تجمع بين المساهمين في الجريمة[1].

الفرع الثاني: العقوبات الأصلية والتكميلية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي

أولا: العقوبات الأصلية : أقرت جل التشريعات عقوبات لمرتكب جرائم الابتزاز عبر مواقع التواصل الاجتماعي باعتبارها جريمة تمس بشكل مباشر بالجانب المادي والمعنوي للأشخاص ونظرا لخطورتها على الحياة الخاصة للأفراد ومن بين هذه التشريعات نذكر على سبيل المثال لا الحصر التشريع السعودي والإماراتي والعماني والجزائري.

– نص المشرع السعودي في المادة 3 من نظام مكافحة الجرائم المعلوماتية على توقيع عقوبة السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 500.000 ريال أو بإحداهما على كل شخص يرتكب أي من الجرائم المعلوماتية التالية :

– تهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا.

– تعد المساس بالحياة الخاصة للأشخاص عن طريق الهواتف النقالة عالية الدقة والمزودة بكاميرات وما في حكمها هي سلاح المعتدي الأسهل والأكثر انتشارا.

[1] نفس المرجع https :mail.almerja.com تاريخ الإطلاع 08-03-2024 على الساعة 18:03

– أما المادة 16 من القانون الاتحادي الإماراتي نصت في مضمونها على معاقبة كل مبتز أو من يهدد شخص لقيامه بعمل أو الامتناع عنه باستخدام شبكة معلوماتية أو أي وسيلة تقنية بعقوبة الحبس لمدة لا تزيد عن سنتين والغرامة لا تقل عن 250.000 درهم.

– وتكون العقوبة بالسجن لمدة لا تزيد عن 10 سنوات إذا كان التهديد أو الابتزاز بارتكاب جناية أو إسناد أمور خادشة للشرف أو الاعتبار[1].

– أما القانون العماني فقد حدد عقوبة الابتزاز بمدة لا تزيد عن 3 سنوات ولا تقل عن سنة وبغرامة لا تقل عن 1000 ريال عماني ولا تزيد عن 5000 ريال عماني، فالملاحظ أن المشرع العماني وضع حد أدنى وأقصى بالنسبة للعقوبات السالبة للحرية والعقوبات المالية أيضا .

– أما بعض التشريعات العربية فقد شددت من العقوبات بالنسبة لهذه الجرائم مثل التشريع المصري إذ جعل عقوبتها السجن لمدة لا تزيد عن 5 سنوات ولم يحدد الحد الأدنى للعقوبة .

– في حين نجد أن هناك تشريعات بها فراغ في ما يتعلق بعقوبة هذه الجرائم ألا وهي جرائم الابتزاز عبر مواقع التواصل الاجتماعي مثل القانون العراقي وعليه كان للقضاء دور هام في تحديد عقوبات لهذه الجريمة من خلال تطويع النصوص الحالية والخاصة بجرائم التهديد في حالة ارتكابها بطريق الإنترنت .

بالنسبة للمشرع الجزائري: فلقد حددت المواد 303 مكرر و 303 مكرر 1، 303 مكرر 2 العقوبات الخاصة بهذه الجنحة وهي كالآتي :

المادة 303 مكرر

العقوبة الواردة في نص المادة وفي فحواها كانت الحبس من 6 أشهر إلى 3 سنوات هذا فيما يتعلق بالعقوبة السالبة للحرية، أما العقوبة المالية فقد حددها المشرع بغرامة مالية من 50 الف دج إلى 300 ألف د ج وهذا لكل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت .

المادة 303 مكرر 1

....المشرع العقوبة المتعلقة بالشروع في ارتكاب الجنح المنصوص عليها في هذه المادة بالعقوبات المقدرة للجريمة الثانية.

–ويتغيب دائما الحكم لمصادرة الأشياء التي استعملت لارتكاب الجريمة[2] .

[1] ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 213.

[2] إذا تم اعتبار التهديد نفسه الابتزاز في التشريع الجزائري فإنه تنطبق على هذه الجريمة أحكام المادة 371 ق.ع.ج أيضا.

ثانيا: العقوبات التكميلية : العقوبات التكميلية اسمها دال عليها فهي تلك التي تصيب الجاني بناء على الحكم بالعقوبة الأصلية فهي مكملة لها لكن تختلف العقوبة التبعية التي تصيب الجاني بناء على الحكم بالعقوبة الأصلية دون الحاجة إلى إصدار حكم تبعي فهو مرتبط ارتباطا مباشرا ووثيقا بالعقوبة الأصلية[1].

– ففي جريمة الابتزاز عبر مواقع التواصل الاجتماعي نجد المشرع الجزائري أوجب الحكم بالمصادرة من خلال نص المادة 303 مكرر وذلك فيما يتعلق بالأشياء المستعملة في ارتكاب الجريمة كما أن المادة 303 مكرر 2 أحالت إلى المادة 09 مكرر 1 و 18 من ق العقوبات باعتباره الشريعة العامة.

– حيث يجوز للقاضي الحكم بإحدى هذه العقوبات أو أكثر حسب طبيعة الجريمة المنصوص عليها في المادة 303 مكرر و 303 مكرر 1.

1– يمنعه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 من ق ع.ج لمدة لا تتجاوز 5 سنوات.

- كما يجوز للمحكم نشر حكم الإدانة طبقا لما ورد في المادة 18 ق.ع.ج.

الملاحظ من خلال نصوص المواد سالفة الذكر أن المصادرة تكون بعد صدور الحكم القضائي بالإدانة وباعتبار أن هذه الأخيرة عقوبة تكميلية كأصل عام حسب نص المواد 9 مكرر 1 و 18 من ق.ع.ج إلا أن طبيعة هذه الجرائم تكون إلزامية بالنسبة للقاضي للحكم بها وهنا لا يتغير لكيفها القانوني بأنها عقوبة تكميلية إلا أنها تأخذ حكم العقوبة الأصلية باعتبارها مصبوغة بصبغة الإلزامية ومرجع ذلك إلى خطورة هذه الجرائم والوسائل المستعملة فيها.

الفرع الثالث: ظروف التشديد والإعفاء لجريمة الابتزاز عبر مواقع التواصل الاجتماعي

تعد جريمة الابتزاز من الجرائم الخبيثة داخل الوسط أو المجتمعات باعتبارها جرائم ناعمة لا تستخدم العنف واستخدام المبتز أسلوب الحيل في استدراج ضحيته على هذا الأساس تكاثفت الجهود في خلال التشريعات المحلية للحد من هذه الجرائم عن طريق الردع المجسد في النصوص القانونية بتوقيع العقوبات على المبتزين خاصة عبر مواقع التواصل الاجتماعي المختلفة، فهناك حالات تتشدد فيها العقوبة في جريمة الابتزاز عبر مواقع التواصل الاجتماعي عند تحقق شروط معينة .

[1] راجع المواد 09 مكرر 1 – 18 ق.ع.ج.

– والمقصود بتشديد العقوبة أن يرفع القاضي العقوبة إلى الحد الأقصى الذي تحدده القاعدة أو النص القانوني للجريمة محل العفوية والمسموح به قانونا أو يحكم بعقوبتي الحبس والغرامة معا.

– فقد اختلفت التشريعات بالنسبة لظروف التشديد فيما يتعلق بجرائم الابتزاز عبر مواقع التواصل الاجتماعي نجد على سبيل المثال:

– المشرع السعودي: لم يحدد الحد الأدنى للعقوبة المقررة لجريمة الابتزاز عبر مواقع التواصل الاجتماعي واكتفى بوضع الحد الأقصى لا يجوز تجاوزه ومع ذلك جعل المشرع حالات تقع فيها جريمة الابتزاز عن طريق التقنية تشدد فيها بالعقاب بحيث لا تقل عن النصف و .... السلطة التقديرية للقاضي في تحديد مدة السجن وتحديد الغرامة المالية التي يدفعها الجاني بشرط أن لا تتجاوز الحد الأعلى المقررة كعقوبة للجريمة محل النص القانوني ألا وهي الابتزاز الإلكتروني .

– **المشرع الإماراتي:** من خلال نص المادة 16 من قانون مكافحة جرائم تقنية المعلومات الإماراتي تشدد المشرع العقوبة بما يتعلق بالابتزاز الإلكتروني إلا أنه من خلال النص لم يتبين لنا إذا كانت متفردة أو يجمعها مع الغرامة المحددة في الحد الأعلى ب 500.000 درهم من هنا نلاحظ أن المشرع الإماراتي شدد في العقوبة المتعلقة بالتهديد بارتكاب خيانة أو إسناد أمور تمس بالشرف في حالة ما اذا كان هذا الاستناد متعلق بالابتزاز .

في القانون المغربي: يعمل القانون المغربي على تشديد العقوبة على الشخص الذي يرتكب جريمة الابتزاز بأي طريقة ومن بينها الابتزاز عن طريق مواقع التواصل الاجتماعي فحدد المشرع المغربي عقوبات رادعة بالنسبة لكل مبتز والتي تصل إلى 5 سنوات كحد أقصى ولا تقل عن سنة كحد أدنى بالإضافة إلى الغرامة المالية ووردت العقوبات أيضا في نص المادة 447 المتعلقة باستخدام الأنظمة المعلوماتية في التشريع الجزائري بالرجوع إلى قانون العقوبات الجزائري نلاحظ أن المشرع في .... المادتين 303 مكرر، 303 مكرر 1 أن المشرع حدد الحد ٨١الأدنى والاقصى فيما يتعلق بعقوبة الابتزاز عبر وسائل التواصل أو الجريمة المعلوماتية سواء فيما تعلق بالعقوبة السالبة للحرية والتي تتراوح بين 6 أشهر و 3 سنوات أو العقوبة المالية التي تتراوح بين 50 ألف إلى 300.000 دج.[1]

ثانيا: الظروف المعفية من العقاب لجريمة الابتزاز عبر مواقع التواصل الاجتماعي

الإعفاء من العقوبة هو نظام يقوم على الرغم من قيام الجريمة بحيث يمحو المسؤولية القانونية عن الجاني على الرغم من ثبوت إدانته.

[1] بالنسبة للمشرع الجزائري أغفل تحديد ظروف التشديد فيما يتعلق بهذه الجريمة لعدم وجود نص صريح لها أو بنص على الابتزاز بصورة واضحة فهذا يعد تقصير من المشرع فيما يتعلق بهذه الجريمة وفيما يتعلق بظروف التشديد.

- **حالات الإعفاء:** بالرجوع إلى الشريعة العامة الا وهو قانون العقوبات نجد أن حالات الإعفاء واردة على سبيل الحصر فهي 3: عذر المبلغ، عذر القرابة العائلية، عذر التوبة.
- **عذر المبلغ:** يتعلق المبلغ هنا بمن ساهم في مشروع جريمة ثم يقدم خدمة للمجتمع بأن يبلغ العدالة عنها أو عن هوية المتورطين فيها، ولقد قرر المشرع أن يكافئ المبلغ لقاء هذه الخدمة وذلك بالإعفاء من العقوبة في طائفة من الجرائم لا سيما تلك التي يصعب الكشف عنها.
- مثل الجرائم المتعلقة بأمن الدولة.
- المبلغ عن جمعية أشرار.[1]

والمتعلقة بالنقود المزورة[2] وتم الكشف عن هوية الجناة، والمتعلقة أيضا بأختام الدولة[3] وتقليدها.[4]

يتولد عن الجرائم المرتكبة السالفة الذكر مثلا إذا كانت عن طريق الوسائل التقنية الحديثة وكانت بجريمة الابتزاز الإعفاء من العقوبة إذا تم التبليغ عنها من قبل المساهمين والكشف عن رؤوس الإجرام.

عذر القرابة: عادة ما تكون درجة القرابة هي عائق تحول دون استفادة الضحية من معاقبة الجاني نتيجة أعراف أو نتيجة الخوف من الفضيحة خاصة إذا تعلق الأمر بعلاقات مشبوهة أو علاقات غير قانونية أو غير شرعية ففي هذه الحالات حتى وإن وقع الضحية نتيجة ابتزاز بوسائل التواصل الاجتماعي إما نتيجة جهل بمخاطرها أو نتيجة تأثير من المبتز بالحصول على معلومات أو صور تكون وسيلة ضغط على الضحية من أجل الحصول على ممارسات جنسية أو مبالغ مالية.

عادة ما تكون هذه الممارسات أو التهديدات بين الأقارب والأصهار وخوف من الفضيحة يمنع الضحية من التبليغ عن المبتز.[5]

عذر التوبة: وهو مقرر لمن أنبه ضميره فصحا بعد الجريمة وانصرف إلى محو آثارها بأن أبلغ السلطات العمومية المختصة أو استجاب لطلبها قبل نفاذ الجريمة ففي هذه الحالة يقصى التائب من العقاب باعتبار أن جرائم الابتزاز من الجرائم الماسة بالشرف وتهديم الكيان الأسري وقد عمل المشرع في حالات التوبة إلى التشجيع عن الحد من هذه الظاهرة ومنع تفتيشها في المجتمع والوسط الشبابي خاصة.[6]

---

[1] خالد صو عبد الرحمان سنوسي، الاعذار القانونية و ةالضروف المخففة للعقوبة في قانون العقوبات الجزائري، مجلة العلوم القانونية والسياسية، المجلد 12، العدد01، الجزائر، افريل 2021، ص 45

– أنظر المادة 179 ق.ع.ج

[2] المادة 199 ق.ع.

[3] المادة 205 ق.ع.ج.

[4] المادة 197، 198 ق.ع.ج.

[5] خالد ضو عبد الرحمان السنوسي، المرجع السابق، ص 46.

[6] المرجع نفسه، ص 47.

ملخص الفصل الأول:

تناولنا في الفصل الأول من الدراسة إلى الأحكام الموضوعية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي كصورة من صور الجرائم الالكترونية فتم من خلال هذا الفصل التطرق إلى ماهية الابتزاز عبر مواقع التواصل الاجتماعي بتعريفه لغويا واصطلاحا وفقهيا وتبيان أسبابه وصوره كما تم التطرق إلى وسائل الابتزاز عبر مواقع التواصل الاجتماعي بالنظر إلى الحاسب الآلي وبرامج الانترنت وبالتطرق إلى الهاتف النقال وما في حكمه أيضا.

كما تم التطرق إلى التنظيم القانوني لجريمة الابتزاز عبر مواقع التواصل الاجتماعي من خلال التعرض إلى أركانها الشرعي، المادي والمعنوي.

وفي الأخير تم دراسة العقوبات المقررة لذلك في بعض التشريعات العربية سواء منها العقوبات الأصلية والتكميلية وعقوبة الشروع والمساهمة فيها كما تم تسليط الضوء على ظروف التشديد والإعفاء عنها.

الفصل الثاني:

القواعد الإجرائية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي

إن التطور السريع و الهائل في التكنولوجيا والاتصال أدى إلى إنتاج وسائل حديثة في التواصل الاجتماعي وإحداث تغيرات جذرية مست الحياة الخاصة للناس في كل مجالاتها، فالمعلوماتية أدت إلى انتقال الجريمة من الفضاء المادي إلى الفضاء الافتراضي مما جعل لهذه الجرائم طابع خاص و إجراءات خاصة للكشف عنها، فإذن طبيعة الجرائم الإلكترونية بصفة عامة والجرائم عبر مواقع التواصل الاجتماعي ووسائل ارتكابها دفع بالمشرع الجزائري إلى إعادة النظر في الكثير من المسائل الجزائية خاصة فيما يتعلق بمسألة الإثبات ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من طبيعة إلكترونية وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة مما يشكل صعوبات أمام هذه الجهات فيما يتعلق في إثبات هذه الجرائم من عدمها، فكل هذا وذلك يستدعي تكاتف الجهود الدولية والوطنية لمحاربتها لذا تم تقسيم هذا الفصل إلى مبحثين:

المبحث الأول: تحت عنوان إجراءات التحقيق للحصول على الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي

المبحث الثاني: فيتمثل في: إثبات جريمة الابتزاز عبر مواقع التواصل الاجتماعي وآليات مكافحتها.

المبحث الأول: إجراءات التحقيق للحصول على الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي

إن التطور التقني الذي لحق نظام المعالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير الكثير من المفاهيم السائرة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقيم منهج بعض الإجراءات التقليدية من قانون الإجراءات الجزائية فضلا عن استحداث قواعد إسرائيل أخرى تتلائم مع طبيعة البيئة التقنية، فطور الآليات ووسائله أمر في غايا الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهو الأمر الذي سوف نعالجه من حيث بحث القواعد الإجرائية التقليدية والحديثة وإلى أي مدى يمكن الاستناد عليها في الحصول على الدليل الرقمي في المطلب الأول ثم تتعرض إلى الصعوبات التي تواجه الجهات القضائية في جريمة الابتزاز الإلكتروني وعبر مواقع التواصل الاجتماعي في المطلب الثاني.

المطلب الأول: القواعد الإجرائية التقليدية والحديثة في الحصول على الدليل الرقمي

تعتبر مواقع التواصل الاجتماعي ميدان خصب للجريمة المعلوماتية لأنها تمثل قلب الثورة المعلوماتية والهياج الإلكتروني وتأثيره على جمهور عريض من مستخدمي شبكة الإنترنت متمثلا في جرائم الإنترنت وشبكات التواصل الاجتماعي في العالم عامة والجزائر خاصة، وقد انتشرت هذه الجرائم بشكل نسبي وترتبت عن هذه المخالفة أضرار بالغة عن حق الفرد والمؤسسات بل و الدول ذاتية فطبيعتها وطبيعة المجرم المرتكب لها باستخدام أغراض غير مشروعة لابتزاز الضحية من أجل الحصول على غرضه مما يستدعي منا التطرق من خلال هذا المطلب إلى تسليط الضوء على الهيئات الوطنية المكلفة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في الفرع الأول، أما الفرع الثاني سنتطرق إجراءات وقواعد تحصيل الدليل الرقمي بطريقة تقليدية، أما في الفرع الثالث سنعرج إلى القواعد الإجرائية الحديثة في الحصول على الدليل الإلكتروني.

الفرع الأول: القواعد الإجرائية التقليدية في الحصول على الدليل الرقمي لإثبات جريمة الابتزاز عبر مواقع التواصل الاجتماعي

أولا: المعاينة

أ- دور المعاينة في استخلاص الدليل الإلكتروني في الجرائم المرتكبة بواسطة مواقع التواصل الاجتماعي: تعد المعاينة خطوة هامة في الكشف عن الجريمة التقليدية إلا أن دورها يتضائل في الكشف عن جرائم بالدليل الرقمي وذلك بسبب الجرائم التي تقع على الشبكات أو بواستطها نادرا ما يترك آثار مادية.

– الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة الإلكترونية خلال المدة الزمنية ما بين ارتكاب الجريمة والكشف عنها التي في الغالب لن تكون قصيرة نسبيا وهذا ما يتيح فرصة لحدوث تغيير بآثار الجريمة ومحوها وذلك عن بعد. [1]

– لذلك جاء المشرع الجزائري في المادة 43 من ق.إ.ج بنصها "يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم بإجراء أي تغيير على حالة الأماكن التي قد وقعت فيها الجريمة..." وبالرغم من أن هذه المادة تعالج الجريمة التقليدية فإنه يمكن تطبيقها على الجريمة المعلوماتية.

ب– مسرح المعاينة في الجرائم المرتكبة عبر مواقع التواصل الاجتماعي: وهو المسرح الافتراضي أي الرقمي التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكاته في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، وفي هذه الحالة يجب أن تتم المعاينة إلا على يد متخصص في المعلوماتية.[2]

وعند إجراء المعاينة يجب مراعاة الضوابط التالية:

– تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

– إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتى يستعد من الناحية الفنية والعملية.

– إعداد خطة العمل أو المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل .

– العناية بالطريقة التي تم بها إعداد النظام.

– ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يتمكن إجراء عمليات التحليل.

– عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الحاسب في أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.[3]

ثانيا: التفتيش

أ– **التفتيش وضبط الأدلة: التفتيش:** يقصد بالتفتيش أنه إجراء من إجراءات التحقيق الابتدائي التي تهدف إلى البحث عن الأدلة المادية لجناية أو جنحة تتحقق وقوعها بهدف إثبات ارتكابها.[1]

---

[1] آيت حمودة كاهنة: البحث والتحري الجنائي في مسرح الجريمة الالكترونية، مجلة الفكر القانوني والسياسي، المجلد 7، العدد 1، جامعة حسيبة بن بوعلي، الشلف 2023، ص 186.

[2] المرجع نفسه، ص 187.

[3] عبد الناصر محمد محمود فرغلي، عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي المنعقد بالرياض 12–14 نوفمبر 2008، ص13.

– يعتبر التفتيش من إجراءات التحقيق بمعناه الفني والقانوني هو ذلك التفتيش الذي يقوم به ضابط الشرطة القضائية لإثبات الجريمة أو نفيها سواء كان التفتيش متعلقا بشخص أو مكان أو شيء حسب طبيعته لضبط الأدلة ويعتبر هذا الإجراء من أهم الإجراءات لأنه يمس حق الإنسان في احترام شخصيته وكفالة حياته الخاصة.[2]

– والهدف منه في الجريمة الإلكترونية هو ما يحتويه الحاسب الآلي من أشياء مادية ومعنوية تساعد في اكتشاف الحقيقة وتمكن القضاء من إدانة المشتبه به ويكون محل التفتيش هذا الحاسب الآلي وأنظمة المعالجة، فإذا كان التفتيش في الجريمة العادية هو البحث عن الأدلة المادية فإن مجال التفتيش في الجريمة الإلكترونية هو مكونات الحاسب الآلي وهذا الحاسب الآلي يكون من مكونات مادية وهي عبارة عن الجسم المادي الحاسوب المتكون من وحدة الإدخال ووحدة المعالجة المركزية وغيرها من الوحدات أما المكونات المعنوية فهي التي تشكل خصوصية في تفتيشها وتعد من قبيل هذه الأخيرة المعلومات والبيانات والبرمجيات والتطبيقات.[3]

أ1– الكمبيوتر محل التفتيش الإلكتروني: مما سبق ذكره أنه يكون الحاسوب محل التفتيش الإلكتروني وفي هذا الأخير يتكون من مكونات مادية ومكونات معنوية.

– **تفتيش المكونات المادية:** إن تفتيش المكونات المادية للحاسوب لا يثير أي صعوبة ويرجع ذلك إلى أن مسرح الجريمة هنا يحتوي على الأدلة المادية التي تدل بصورة واضحة على وقوع الجريمة الإلكترونية وإمكانية نسبها لشخص معين وتعتبر متاحة بشكل كبير.[4]

– **تفتيش المكونات المعنوية:** في هذه الحالة قد يثار جدل فقهي كبير حول صلاحية المكونات المعنوية لأن تكون محلا للتفتيش باعتبار البيانات الإلكترونية أو البرامج في ذاتها تفتقر إلى مظهر ملموس ففي هذا الصدد نقسم الفقه إلى فريقين: فريق يؤيد ذلك وفريق معارض لها، أما عن المشرع الجزائري فقد أجاز ذلك من خلال نص المادة 5 من ق 04–09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[5]

– في هذا الصدد جاء المشرع الجزائري في الفقرة 3 من نفس المادة من ق 09–04 حالة تخزين المعلومات خارج الإقليم الوطني[6]، إذ يكون الحصول على هذه المعطيات بمساعدة من السلطات

---

[1] آية حمودة كاهنة، المرجع السابق، ص 187.

[2] المرجع نفسه، ص 187.

[3] المرجع نفسه، ص 187.

[4] المرجع نفسه، ص 188.

[5] راجع نص المادة 5 من ق 09–04.

[6] راجع المادة 5 الفقرة 3 من ق 09–04 انظر المادة 18 ق 09–04

الأجنبية طبقا للقواعد المقررة في الاتفاقيات والمعاهدات الدولية التي تؤكد على ضرورة التعاون الدولي في مجال مكافحة الجرائم المعلوماتية والوقاية منها.[1]

أ 2- القواعد الموضوعية لتفتيش الحاسوب: تتلخص هذه القواعد فيما يلي:

- وقوع جريمة إلكترونية.

- توافر أدلة إلكترونية قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الجريمة.

- أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.[2]

- القواعد الشكلية لتفتيش الحاسوب:

تتضمن عدة قواعد نذكر منها:

- أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش.

- أن يكون التفتيش مسبقا.

تكوين فريق تفتيش يتضمن خبراء وتقنيين ومتخصصين بالحاسوب والأنظمة الإلكترونية.[3]

- يتمثل الضبط في العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها ويعتبر الضبط هو الهدف من التفتيش والنتيجة المباشرة والمستهدفة ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط.

- ويختلف الضبط في الجريمة المعلوماتية عن ضبط الجرائم الأخرى من حيث المحل لأن الجريمة الإلكترونية يرد فيها الضبط على الأشياء ذات طبيعة معنوية من حيث البيانات والمراسلات والاتصالات الإلكترونية وعلى الأشياء ذات الطبيعة المادية كالكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرنة.[4]

ثالثا: الخبرة الفنية

- **الخبرة وتدريب الكوادر:** تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاء وسلطات التحقيق على حد سواء وذلك ما استعصى عليهم الأمر ومن بين هذه المجالات التي

[1] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال على ضوء ق 09-04، مذكرة لنيل شهادة ماجستير كلية الحقوق جامعة ورقلة 2013، ص 92.

[2] عبد بلعابد، المرجع السابق، ص 143.

[3] المرجع نفسه، ص 143.

[4] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكتروني، دار الفكر الجامعي، الاسكندرية، 2010، ص 221.

تستدعي اللجوء إلى الخبرة نجد الجريمة الالكترونية حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الالكترونيان.

أما تدريب الكوادر فهو آلية من آليات مكافحة الجريمة الالكترونية، فيخضع الكوادر إلى دورات تدريب لتبادل الخبرات على المستوى الإقليمي والدولي كآلية من آليات التعاون.

فالكوادر قد يستعينون بالخبراء وبعد تدريبهم في المجال المعلوماتي يصبحون خبراء في عملهم.

1- **الخبرة الفنية:** الخبرة هي وسيلة لتحديد التفسير الفني والتقني بالاستعانة بالمعلومات العلمية فهي مستقلة عن الدليل القولي أو المادي وإنما هي تقسيم لهذا الدليل[1]، وقد تعتمد الخبرة من أجل كشف الجريمة المعلوماتية ولا بد أن تتماشى هذه الخبرة مع خصوصية الجريمة الإلكترونية أو المعلوماتية.

- وعلى الخبير أن يتمتع بمؤهلات عالية وفنية في تركيب الكمبيوتر وشبكة الإنترنت والتعامل مع الجريمة التي خلفتها التقنية الحديثة، وكيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.

- المشرع الجزائري أجاز للمحقق الاستعانة بالخبرة ومنه بطلب خبير في اي وقت إلى أن ينتهي التحقيق وهو أمر وجوبي في مجال الجرائم المعلوماتية التي تتطلب خبرة فنية بحتة لا يكشف غموضها الا المتخصصين.

- **أهمية الخبرة في البحث عن الدليل الإلكتروني:** تكون أهمية الخبرة في الأدلة التي تقدمها لجهة التحقيق والقضاء ولسائر السلطات المعنية أو المختصة بالدعوى الجزائية لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد 143 إلى 156 من قانون الإجراءات الجزائية واعتبرها من إجراءات البحث عن الدليل حين نص 143 [2]على أنه من حق جهات التحقيق أو النيابة العامة أو الخصوم من طلب خبرة إذا تعلق الأمر بالجريمة المعلوماتية.

- كما أشار المشرع الجزائري في المادة 5 [3]من ق 09-04 على إجازة للسلطات المكلفة بالتفتيش إلى الاستعانة بأهل الخبرة في الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال والجريمة الإلكترونية.

- والجدير بالذكر أن المشرع الجزائري قدر الحماية اللازمة للخبير إذا ما سبب له المعلومات التي أفاد بها للقضاء أي خطر حول حياته أو سلامته الجسدية أو سلامة أفراد عائلته أو أقاربه أو مصالحه الأساسية وذلك بموجب الأمر 12/15 المعدل والمتمم لقانون الإجراءات الجزائية بموجب المواد 65 مكرر إلى 65 مكرر 28.

---

[1] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص جامعة أبو بكر بلعايد، تلمسان 2018، ص 271.

[2] انظر المادة 143 قانون إجراءات جزائية.

[3] انظر المادة 5 من ق 09-04.

2-تدريب الكوادر: طبيعة الجرائم الواقعة على الأسرار المعلوماتية تقتضي معرفة بنظم المعلوماتية وكيفية تشغيلها من قبل مستخدميها ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري والتحقيق في مجال الجرائم المعلوماتية.

- ففي الجزائر وعلى مستوى جهاز الشرطة أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة ومخبرين جهويين في كل من قسنطينة، وهران، أما على مستوى الدرك الوطني للأدلة الجنائية وعلم الإجرام قسم الإعلام والالكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.[1]

- كما تسعى الأجهزة الأمنية المعنية بالتحقيق في استقطاب المتخصصين والكفاءات في المجال المعلوماتي لضمهم إليها ليكونوا ضمن كوادرهم والاستفادة منهم.

والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول وأجهزة العدالة لديها، فمثلا يتم إرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى، والهيئات الدولية بهدف الاطلاع على أحدث الأنظمة المقارنة من خلال عقد ندوات ومؤتمرات وورشات عمل جماعي متخصصة في مواجهة تلك الجرائم، تعقد على المستوى الدولي أو الإقليمي.

- حيث نسلط الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال مناقشة أبعادها، أخطارها ووسائل الوقاية بأساليب ووسائل تفوق تلك التي يستعملها مرتكبوها، فالتعاون الدولي في مجال تدريب الكوادر العاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولى والإقليمي يستهدف توحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة.[2]

الفرع الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الإلكتروني

أولا: التسرب الإلكتروني : لقد تطرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 06/22 التي تنص على "يقصد بالتسرب قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضباط الشرطة القضائية المكلفة بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا

[1] رابحي عزيزة، المرجع السابق، ص 273.

[2] المرجع نفسه، ص 274.

الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 69 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم".[1]

– فالتسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه في أنهم ارتكبوا الجريمة بإظهار أنه ساهم معهم أو شريك ويستعمل الضابط أو العون هوية مستعارة إذا ما ارتبط بأحد هذه الجرائم.

– جرائم المخدرات.

– الجريمة المنظمة العابرة للحدود.

– الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

– جرائم تبييض الأموال.

– الجرائم الموصوفة بأعمال إرهابية.

– الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.[2]

ثانيا: اعتراض المراسلات والمراقبة الإلكترونية

1– **اعتراض المراسلات:** استحدث بموجب المادة 66 مكرر إلى 65 مكرر 10 من ق.إ.ج إمكانية قاضي التحقيق أن يأمر ضباط الشرطة القضائية بترخيص كتابي وتحت إشراف مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط وتثبيت وتسجيل وبحث في سرية وفي أي مكان عام عن طريق وسائل الاتصال السلكية واللاسلكية ووضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط الصور وتثبيت وبحث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة.[3]

ولم تشر المادة المذكورة أعلاه لطبيعة هذه المراسلات مما يفتح المجال للمراسلات المكتوبة مهما كان شكلها (كتابة، رموز، أشكال، صور) و.... أن تكون ورقية أو رقمية، وسواء كانت بالفاكس أو تلغرام أو لاسلكية مثل البريد الإلكتروني والهاتف النقال.

وعلى ذلك فإن عملية الاعتراض أو المراقبة تتم عن طريق ترتيبات تقنية سرية يتم وضعها دون موافقة الأشخاص المعنيين المشتبه فيهم، بغرض التنصت والتقاط وتثبيت وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه في أماكن عامة أو خاصة من أجل استعمالها كدليل لمواجهته.

---

[1] المادة 65 مكرر 5 من قانون الإجراءات الجزائية أمر رقم 66–156 مؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84 معدل ومتمم وفقا للقانون 06–é2 المؤرخ في 20 جويلية 2006ز

[2] فلاح عبد القادر– آيت عبد المالك نادية، مرجع سابق، ص 1698.

[3] المادة 65 مكرر ق.إ.ج.

– كما تعد المراسلات عبر البريد الإلكتروني مجالا خصبا للربط والاتصال الإلكتروني بين الأشخاص في مختلف أنحاء العالم وبوقت قياسي، ومن ثم يمكن إخضاعها لعملية الاعتراض والمراقبة للكشف عن الجرائم الإلكترونية.[1]

– **الشروط المطلوبة في المراسلات محل الاعتراض:** يشترط في المراسلات التي يمكن أن تكون محلا لإجراء الاعتراض أو المراقبة أن تتسم بالسرية والخصوصية ولا شك أن ذلك لا يتحقق إلا في ظل توافر عنصرين هما:

– فحو الرسالة والتي تنص على معلومات أو أفكار سرية وشخصية.

– تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة.

– مع الإشارة أن المشرع الجزائري لم يتبنى إجراء المراقبة الإلكترونية كإجراء للتحقيق القضائي وكذلك التحري بموجب القانون رقم 04/09 بل أعطى تصريح للجهات القضائية باستعمال الاعتراض بهدف الوقاية من بعض الجرائم التي تشكل خطرا على أمن الدولة.[2]

– الشروط القانونية لاعتراض المراسلات:

تبقى عملية الاعتراض أو مراقبة المراسلات مرهونة على توافر الشروط التالية:

– توافر إذن مكتوب من الجهات القضائية المختصة: أي من طرف وكيل الجمهورية بمرحلة التحقيق الابتدائي أو من طرف قاضي التحقيق القضائي تحت طائلة بطلان الإجراءات القضائية ولا شك أن اشتراط الإذن هو إجراء حتمي من منطلق أسلوب اعتراض المراسلات السلكية واللاسلكية يتم دون علم المعنيين لأنه ورغم نجاعته في الكشف عن الجرائم المعلوماتية إلا أنه يشكل اعتداء على سرية المراسلات والاتصالات ومساس بحرمة الحياة الخاصة التي كفلها الدستور[3] ويشترط أن يتضمن الإذن طبيعة الجريمة التي تبرر الإجراء مع ضرورة أن تكون من الجرائم التي يجوز منح الإذن فيها بالإضافة إلى تحديد المراسلات المراد اعتراضها وتسجيلها وتحديد الأماكن المقصود سواء كانت أماكن عامة أو خاصة مع تحديد مدة الاعتراض والتي لا تتجاوز 4 أشهر قابلة للتجديد.[4]

التسبيب: أي تبيان دواعي اللجوء إلى الاعتراض ومراقبة المراسلات وتبيان مدى جدية تلك الدواعي ودورها لإظهار الجريمة والجناة.[5]

---

[1] مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية مجلة البحوث القانونية والاقتصادية، المجلد 6، العدد 3، مغنية الجزائر، ص 202.

[2] المرجع نفسه، ص 203

[3] المرسوم الرئاسي 20–442 الصادر في 30 ديسمبر 2020 ح.ل 82 لسنة 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020.

[4] فلاح عبد القادر – آيت عبد المالك نادية، المرجع السابق، ص 1699.

[5] المرجع نفسه، ص 1699.

– **تحديد الجرائم محل الاعتراض والمراقبة:** والتي يتوجب أن لا تخرج عن ما هو مقرر قانونا مع مراعاة سرية الإجراءات وكتمان السر المهني.[1]

2– **المراقبة الإلكترونية:** تعد الرقابة على الاتصالات الإلكترونية أو كما يطلق علبها بمصطلح الرقابة الإلكترونية للاتصالات من أهم مصادر التحري التي يستعان بها في التقصي على مختلف الجرائم بما في ذلك الجرائم المتصلة بالتكنولوجيات الحديثة خاصة في ظل لجوء الجناة إلى الوسائل التقنية الحديثة للاتصال في تنفيذ مخططاتهم الإجرامية، والتواصل فيما بينهم، كما تعد مراقبة الاتصالات الإلكترونية مصدرا للأدلة الرقمية.[2]

– نجد أن المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الإلكترونية لكن بعض التشريعات قد قامت بتعريفها مثل التشريع الأمريكي الذي عرفها على أساس أنها "عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر.

– إلا أنه يمكن أن تعرفها على أساس أنها إجراء تحقيق يباشر خلسة وتنتهك فيه سرية الأحاديث الخاصة، تأمر السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة المعلوماتية ويتضمن من ناحية استراق السمع في الأحاديث ومن ناحية أخرى حفظه بواسطة أجهزة متخصصة في ذلك.[3]

بينما في القانون 09–04 السالف الذكر وفي مادته 03 منه قد حدد كيفية مراقبة الاتصالات[4] وبالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء وفي الحالات المحددة حصريا في المادة 04 من القانون 09–04.

3– **تسجيل الأصوات والتقاط الصور:** يقصد به مراقبة الأحاديث وتسجيلها وكل الاتصالات التي تتم عن طريق سلكي أو لاسلكي أي أن عمليات المراقبة تشمل كل أدوات الاتصال سواء سلكية أو لاسلكية وتتمثل في وضع تقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص.[5]

[1] فلاح عبد القادر– آيت عبد المالك نادية، المرجع السابق، ص 1699.

[2] عبيدة بلعايد، مرجع سابق، ص 145.

[3] بوشعرة أمينة، اوي سهام، الإطار القانوني للجريمة الالكترونية مذكرة ماستر جامعة عبد الرحمان ميرة بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2017–2018، ص 82.

[4] انظر نص المادة 03 من ق 09–04.

[5] انظر المواد 65 مكرر 5 و65 مكرر 10 ق.إ.ج تعديل 2006.

– أما عن التقاط الصور هي تلك العملية التقنية التي يتم بواستطها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، وتتسم هذه الإجراءات بالسرية التامة لأنها بها مساس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.[1]

ثالثا: الكشف عن الجريمة المعلوماتية عن طريق المعطيات

1– **الحفظ والإفشاء العاجلان للمعطيات الإلكترونية:** يعد الحفظ والإفشاء من الإجراءات المستحدثة للكشف عن الجريمة المعلوماتية والوصول إلى الدليل الرقمي ونصت عليها المادة 10 من القانون 09–04 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها.

– ومن ثم فإنه يقوم بهذا مقدمي خدمات الانترنت أين يقومون بالحفظ عن طريق الحيازة بالأرشيف بهدف حماية المعطيات التي سبق وجودها في شكل مخزن مما يحول دون تلقيها أو تجريدها من صفتها أو حتى حالتها الأصلية وفق النماذج التي تراها ملائمة لوضع عملية الحفظ وموقع التنفيذ، ومن ثم هناك نوع من المعطيات يمكن أن تكون محل تحفظ مع مراعاة جملة من الضوابط يتم التطرق إليها فيما يلي:

أ– **المعطيات محل التحفظ:** حددت المادة 11 من القانون 09–04 سابق الإشارة إليه معطيات المرور التي يتعين على مقدم الخدمات التحفظ عليها بناء على طلب من السلطات القضائية المختصة والتي تتجسد فيما يلي:

– المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

– المعطيات المتعلقة بالتجهيزات المستعملة بالاتصال ومن ذلك الإشارة إلى الرقم التسلسلي للجهاز وكذلك نوعه وطرق تشغيله.

– المعطيات التي تسمح بالتعرف على المرسل إليهم ومن ذلك أرقام الهواتف أو عناوينهم.

– الخصائص التقنية وكذلك تاريخ ووقت ومدة الاتصال.

– المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المعلومة المستعملة ومقدميها.[2]

ب–الضوابط الواجب مراعاتها خلال عملية حفظ المعطيات: نظرا لكون عملية حفظ المعطيات تمس الحق في الخصوصية فقد حدد المشرع الجزائري ضوابط يتوجب على مقدم خدمات الانترنت التقيد بها كالآتي:

– احترام المدة الزمنية المقررة لعملية الحفظ والتي حددها المشرع الجزائري بموجب المادة 11 من القانون 09–04 نسبة واحدة ابتداء من تاريخ التسجيل وبعد انقضاء المدة المقررة للحفظ يتوجب على

[1] انظر المادة 11 من ق 09–04 في فقرته ه التي عرفت أيضا مراقبة الاتصالات الالكترونية.

[2] مجدوب نوال، المرجع السابق، ص 204–205.

مزود الخدمة السحب الفوري للمعطيات المخزنة من خلال اتخاذ التدابير التي نفيد عدم إمكانية الاطلاع عليها.

– مراعاة سرية التحفظ إذ يلتزم مقدمو الخدمات بالحفاظ على سرية كل الإجراءات والتدابير التي تفرضها العملية طيلة الفترة المقررة وتبقى الحكمة من هذا الالتزام في مراعاة الحق في الخصوصية وتفادي تغيير البيانات ومحوها من طرف أشخاص.

– الإفشاء العاجل لمعطيات السير على النحو المنصوص عليه بموجب المادة 10 من قانون 09-04.

– ونشير في هذا السياق إلى عملية أخرى فعالة في التحقيق والكشف عن الجريمة المعلوماتية والمستجدة في إنتاج البيانات المعلوماتية فهو إجراء حديث يتماشى وطابع الدليل المعلوماتي.[1] إلا أن المشرع الجزائري لم ينص على هذا الإجراء كإجراء يمكن الاعتماد عليه في سبيل التحري وهو ما يتطلب معه وعلى وجه الضرورة أن يتدارك المشرع الجزائري هذا السهو.

2- تجميع معطيات المرور بوقتها الفعلي: يتم جمع المعلومات المساعدة في عملية التحري من طرف مقدم خدمة الإنترنت ويعرف هذا الأخير على أنه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات أو هو أي كيان يقوم بمعالجة أو تخزين معطيات لفائدة خدمة الاتصال..»

وبالتالي فإنه يقع على عاتق مقدم خدمة الإنترنت التعاون مع جهات البحث والتحري بهدف الوصول إلى الدليل الرقمي وذلك من خلال قيامه بما يلي:

– حفظ المعطيات التي تسمح بالتعرف على مستعمل الخدمة وكذلك الخصائص التقنية ومدة الاتصال بالإضافة إلى المعطيات التي تسمح بالتعرف على المرسل إليهم وعناوينهم والمواقع التي تم الاطلاع عليها.

– مراعاة أن يكون حفظ المعطيات لمدة سنة واحدة ابتداء من تاريخ التسجيل وتقديمها لجهات التحقيق في طلبها.

– التدخل الفوري لسجل المحتويات التي يسهل الاطلاع عليها بمجرد علمهم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين مع تخزينها أو جعل الدخول إليها غير ممكن.

– وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة أو إخبار المشتركين لديهم بوجودها.[2]

[1] مجدوب نوال، المرجع السابق، ص 205.

[2] المرجع نفسه، ص 206.

– ونشير في هذا السياق أن امتناع مقدم خدمات الانترنت على التعاون مع السلطات من شأنه تعريضه للعقوبة الإدارية وللمسائلة الجنائية حسب ق 09-04.

– ومع بروز القانون 20-05 [1]المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحتهما والذي يصبو لوضع حد لكل تمييز وخطاب الكراهية بغض النظر عن الوسيلة المستعملة سواء كانت تقليدية أو إلكترونية نجد أن المشرع الجزائري بموجب المادة p2 منه من أجاز للجهات القضائية المختصة بمناسبة التحقيق في هذه الجرائم أن نأمر مقدمي خدمات الانترنت أو أي شخص آخر بتسليمها المعلومات والمعطيات المخزنة باستعمال وسائل تكنولوجيات الإعلام والاتصال.

– كما يمكنها إصدار أمر إلى مقدمي خدمات الانترنت بالتحفظ الفوري للمعطيات المرتبطة بهذا النوع من الجرائم نظرا لخطورتها.

الجدير بالذكر أن الإجراءات المتبعة في جريمة الابتزاز عبر مواقع التواصل الاجتماعي نفس الإجراءات المتبعة في الجريمة السبرانية بصفة عامة اعتبار أن جريمة الابتزاز الإلكتروني صورة من صور الجرائم الإلكترونية.

المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في تحصيل الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي

تتمثل الجرائم التي ترتكب عبر الإنترنت يكون محلها معلومات أو برامج معالجة آلية عبر الحواسيب أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي وغير محدود مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها، بل كذلك في الوسيلة التي ترتكب بها الأمر الذي ينجم عنه صعوبات اكتشاف الجريمة والتحقيق فيها.

فهي تتنوع بين صعوبات متعلقة بالجريمة في حد ذاتها وصعوبات مرتبطة بالجهات المتضررة وصعوبات متعلقة بالجهاز القضائي وهذا ما سيتم تناوله في هذا المطلب في ثلاثة فروع على التوالي.

الفرع الأول: صعوبات مرتبطة باكتشاف الجريمة المرتكبة عبر الإنترنت (الابتزاز عبر مواقع التواصل الاجتماعي)

يعود صعوبة اكتشاف الجريمة المرتكبة عن طريق الانترنت إلى عدة اختبارات منها ما هو متعلق بانعدام الآثار المادية للجريمة ومنها ما هو راجع لتكتم الضحية ومنها ما هو متعلق بنقض الخبرة لدى سلطات التحقيق.

[1] القانون 20-05 المؤرخ في 5 رمضان علم 1441 هـ الموافق لـ 28 أفريل سنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها الصادر في ج ر ج ج بتاريخ 06 رمضان 1441 هـ الموافق لـ 29 أبريل 2020 العدد 25.

أولا: طمس الآثار المادية للجريمة وسهولة تعديلها أو تدميرها: إذا كان من السهل على جهات التحري أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة والتتبع والمساعدة ، فإنه يصعب عليها القيام بهذا التحري وبهذه الطرق بالنسبة للجرائم التي ترتكب بالوسائل الإلكترونية، فارتباط الجريمة المعلوماتية بالبيئة التقنية انعكس على طبيعة الدليل المترتب عنها.[1]

ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية يمكن استقبالها أو إشعاعات كهرومغناطيسية يمكن التقاطها، سواء من كابلات الربط أو من خلال الأثير يمكن الجاني من فرض تدابير أمنية تمنع اكتشافها ومن ثمة تمنع الحصول على دليل ضده.[2]

– يستعمل المجرم الإلكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والستر عنها بسهولة كبيرة وذلك من خلال التوسل بتقنيات معدة لهذا الغرض مع الأخذ بعين الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الإلكترونية التي يمكن القيام بها في أزمان قياسية متناهية .....تقاس باللحظات والثواني.

– فمن خلال إدخاله لبعض التعليمات في نظام الحاسوب يتم محو البيانات بالكامل في لمح البصر. كما يمكنه وبمجرد كبسة زر خاطفة على لوحة المفاتيح أن يقوم بإلغاء الأوامر الصادرة للجهاز، على اعتبار أن الجريمة تتم في صورة أوامر تصدر إلى الجهاز وما أن يحس الجاني بأن أمره سيكشف حتى يبادر بإلغاء هذه الأوامر، الأمر الذي يجعل كشف الجريمة وتحديد مرتكبيها أمر في غاية الصعوبة بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده.

– إلى جانب ذلك يستعمل الجناة أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد البيانات والبرامج أو إدخال بيانات مختلفة مزيفة أو معرفة في نظام معلومات الحاسب أو تغيير مسار البيانات الصحيحة المدخلة دون أن يحس المجني عليه بذلك.[3]

ثانيا: إعاقة الوصول إلى الدليل الإلكتروني : لا تقف صعوبة إثبات الجرائم الإلكترونية عند تعذر الوصول إلى الأدلة التي تكفي لإثباتها وإنما تمتد هذه الصعوبة لتشمل إجراءات الحصول على هذه الأدلة، بالإضافة إلى ذلك تمتد إلى الجناة أنفسهم لأن مرتكبي هذا النوع من الجرائم قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فالمجرم المعلوماتي غالبا ما يضرب سياجا أمنيا

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماستر في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة الحاج لخضر باتنة، 2012– 2013، ص 190.

[2] بوشارب هانية، بن شهرة شول، صعوبة عملية استخلاص الدليل الالكتروني، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 1، جانفي 2023، ص 71.

[3] المرجع نفسه، ص 71.

على أفعاله غير المشروعة قبل ارتكابها فيزيد بذلك صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه.[1]

– ومن التدابير الأمنية التي من الممكن أن يستخدمها الجناة لإعاقة الوصول إليهم وبالتالي نزع كل صلة بينهم وبين فعلهم الإجرامي. إخفاء هوية المستخدم باستخدام مختلف أدوات الاتصال أمرا متاحا، ومن بين الأدوات التي تستخدم لهذا الغرض برنامج (Pasiphon) بسيفون وشبكة (Tor) تور والهدف من هذا الإجراء عرقلة تتبع عنوان بروتوكول الإنترنت (IP) لهذا المستخدم، ويزداد الأمر صعوبة عندما تكون المعلومات المحملة في IP غير حقيقية.[2]

كما يقوم المجرمين عبر الإنترنت بإخفاء هويتهم أو انتحال شخصيات أخرى حتى لا يمكن التعرف عليهم حال اكتشاف الجريمة.

ثالثا: التكتم عليها من قبل المجني عليه: غالبا ما يلجأ الضحية في هذه الجريمة إلى التكتم وغالبا ما يكون مصرفا أو مؤسسة مالية أو شركة أو مشروعا صناعيا ضخما.

ويحرض المجرمون على عدم الإبلاغ عن الجريمة التي راحت ضحيتها من أجل إخفاء أساليب ارتكابها للحيلولة دون تقليد الآخرين للجناة كذلك التستر على معلومات لا يجب الإبلاغ عنها خاصة إذا كانت الضحية شركة تأمين أو البنوك.

رابعا: نقص الخبرة لدى رجال الضبط القضائي: من الصعوبات التي قد تواجه عملية استخلاص الدليل في الجريمة الماسة بأنظمة الاتصال والمعلوماتية مسألة نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة وكذلك لدى أجهزة العدالة الجنائية متمثلة في سلطات الاتهام والتحقيق الجنائي وذلك فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها وذلك على الأقل في البلدان العربية بشكل عام، نظرا لأن تجربة الإعتماد على الحاسب الآلي وتقنياته وانتشارها في هذه البلدان جاءت متأخرة من أوروبا وكندا والولايات، كما أن أجهزة العدالة المقاومة للجرائم المرتبطة بهذه التقنية تبدأ في التكوين والشكل عقب ظهور هذه الجرائم وهو أمر يستغرق وقتا أبطأ من زقت انتشار الجريمة، لأن الجريمة الماسة بأنظمة الاتصال والمعلوماتية تتقدم بسرعة هائلة توازي سرعة تقدم التقنية ذاتها وحتى الآن فإن الحركة التشريعية أو الثقافية الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل، وهذا الفارق في التقدم أو التطور ينعكس سلبا على فئة إجراء الاستدلالات والتحقيقات في الدعوى الجنائية في

[1] سعيداني نعيم، المرجع السابق، ص 190.

[2] عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان الجزائر، ص ص 122،123.

الجريمة الماسة بأنظمة الاتصال والمعلوماتية ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات الأمن وجهات التحقيق والادعاء والحكم في شأن هذه الجرائم.[1]

الفرع الثاني: صعوبات متعلقة بالجانب القضائي والتعاون الدولي

أولا: الصعوبات المتعلقة بالجانب القضائي : يفترض الطابع الخاص لهذا النوع من الجرائم تعاون أكثر من دولة لكن هذا القصور مقارنة بتفاقم وتطور هذه الجريمة يشكل فارق شاسع بين الجريمة وبطء الإجراءات.

وقد نجم عن هذه الإشكالية أيضا صعوبات تتمثل في القانون الواجب التطبيق والمحكمة المختصة (تنازع الاختصاص) حيث ترى كل دولة أن لها الحق في ملاحقة ومتابعة مرتكب هذه الجريمة لعدة اعتبارات.

1- **عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية:** نظرا لاختلاف المفاهيم الخاصة بالجريمة واختلاف التقاليد والأعراف القانونية الدولية فإن ذلك يضعف منظومة القانون الدولى في مجال ضبط تلك الجرائم مما يسهل إفلات الحياة من المسائلة الجنائية وذلك بسبب عدم توفر تعريف موحد للجريمة فتكون محرمة في تشريع وفي تشريع آخر مباحة.[2]

فالطبيعة الدولية لهذه الجريمة تثير إشكالية تحديد القانون الواجب التطبيق هل هو قانون الدولة التي ارتكب فيها الفعل أو قانون الدولة التي ظهرت فيها الآثار المادية الضارة.

كذلك تعارض القوانين من الناحية الموضوعية والإجرائية يتطلب العمل على توحيد التشريعات المتعلقة بمكافحة هذا النوع من الجرائم إضافة إلى إبرام اتفاقيات في هذا المجال.[3]

والجديد بالذكر أن جريمة الابتزاز عبر مواقع التواصل الاجتماعي تتعرض لنفس الإشكال فيما يتعلق بالقانون الواجب التطبيق والجهة المختصة بالفصل في النزاع في حالة وقوع هذه الجريمة مما يشكل صعوبة في الحد منها.

- كما أن اختلاف النظم القانونية الإجرائية والتحقيق والمحاكمة قد تثبت فاعليتها في دولة ما وقد تكون عديمة الفائدة في دولة ما وقد لا يسمح بإجرائها كما هو الشأن بالنسبة للمراقبة الإلكترونية والتسليم المراقب وغيرها من الإجراءات.

[1] عز الدين عثماني: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، 2018، تبسة، ص 56.

[2] صغيري يوسف، المرجع السابق، ص 133.

[3] رابحي عزيزة، المرجع السابق، ص 329.

2-إشكالية القانون الواجب التطبيق والمحكمة المختصة بالجريمة: تعتبر الجرائم المعلوماتية من الجرائم التي تثير مشكلة الاختصاص القضائي على المستوى المحلي أوالدولي. وتبقى مشكلة الاختصاص المحلي في الجرائم المعلوماتية تنازع الاختصاص بين أكثر من جهة قضائية داخل إقليم الدولة، أما مشكلة الاختصاص الدولي تعني تنازع الاختصاص بين أكثر من دولة.

أ- تحديد القانون الواجب التطبيق:

أ1- المبادئ التقليدية في تحديد القانون الواجب التطبيق: تخضع الجريمة بصفة عامة إلى مبادئ تقليدية في تحديد القانون الواجب التطبيق وتتمثل في مبدأ الإقليمية ومبدأ عينية النص الجنائي ومبدأ شخصية النص الجنائي.

أ2-انقضاء المبادئ التقليدية أمام خصوصية جريمة الابتزاز عبر مواقع التواصل الاجتماعي: نظرا لعدم تبعية شبكة الإنترنت لأي جهة أو شخص محدد ونظرا لعدم وجود مقر لها في دولة محددة تخضع لرقابتها ونظرا لعدم وجود نص جبائي موحد يحكم هذه الشبكة فإن القوانين الجبائية التي تطبق عليها بتعدد الدول المرتبطة بها باعتبار أن القانون الجنائي يتعلق بسيادة الدولة.[1]

ب- تحديد المحكمة المختصة:

تنوعت المعايير الفقهية التي اعتمدت لتحديد المحكمة المختصة بنظر الجرائم المرتكبة عبر الإنترنت إلى ثلاث معايير:

- **معيار الاختصاص المكاني:** وتضبطه ثلاث ضوابط هي مكان وقوع الجريمة، محل إقامة المتهم أو مكان إلقاء القبض عليه[2] وفي حال اجتماع أكثر من ضابط تكون المحكمة المختصة بنظر الدعوى هي التي رفعت إليها الدعوى أولا.

ويقصد بمكان ارتكاب الجريمة، المكان الذي ارتكب فيه السلوك لسبب الذي تحققت فيه النتيجة.[3]

وتثار مشكلة الاختصاص القضائي بالنسبة لجرائم المعلوماتية في حالة ما إذا ارتكبت الجريمة في أكثر من نطاق اختصاص محلي داخل الإقليم الوطني للدولة بسبب طبقية الجريمة وشبكة المعلوماتية، فالجريمة في هذه الحالة سواء تمثلت بجريمة الدخول أو إتلاف بيانات الحاسب الآلي وأنظمة المعالجة الآلية للمعطيات وغيرها، وهي من الجرائم التي يمتد فيها الاختصاص بالإضافة إلى بعض الجرائم الأخرى.[4]

[1] صغيري يوسف، المرجع السابق، ص 144.

[2] انظر المواد 37-329 ق.إ.ج.

[3] رابحي عزيزة، المرجع السابق، ص 330.

[4] انظر المواد 37-47-80-329 ق.إزج.

- **معيار القانون الأكثر ملائمة:** يرى أصحاب هذا الاتجاه بأنه نظرا للطبيعة الخاصة للجرائم الإلكترونية والأضرار الناجمة عنها التي تمتد لتشمل أكثر من دولة واحدة وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى يجب التوسع في تفسير قاعدة الاختصاص (وقوع الفعل وحصول الضرر) ليجعل الاختصاص لمحكمة الدولة الأكثر تعرضا للضرر بشكل فعلي مع التركيز على مبدأ التخلي.

- **معيار الضرر المرتقب:** نظرا لكون الجريمة تتم في عالم افتراضي لا يخضع لأي سلطة إقليمية وبالتالي فالضرر الذي تسببه الجريمة المرتكبة الكترونيا يمكن أن يحدث ٤ي أي دولة متصلة بالإنترنت وهذا هو معيار الضرر الافتراضي أو المرتقب.

- فتطبيق معيار (الارتقاب) لا يمكن إيجاده إلا من خلال صلة أو علاقة للقانون المختص مع مبدأ موضوع وذلك بعيدا عن تذرع كل دولة باختصاصها المحتمل.

- وأول المعالم الموضوعية في الاختصاص هي محل تمركز الموقع الذي نشرت فيه الأقوال والمعلومات والصور والأفلام وهو أكيد يمكن التحكم فيه بخلاف مكان تلقيها الذي يبقي احتماليا.[1]

ثانيا: الصعوبات المتعلقة بالتعاون الدولي

1- **قصور التعاون القضائي الدولى في مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي:**

يعتبر التعاون الدولي في مجال الجريمة الإلكترونية عموما وجريمة الابتزاز عبر مواقع التواصل الاجتماعي من أصعب المواضيع المطروحة على هذا المستوى بسبب الاختلاف القائم في الممارسات بين الدول والتشريعات وكذلك بسبب العدد المحدود نسبيا من المعاهدات، والاتفاقيات المتاحة للدول بشأن التعاقد الدولي الذي يعد مطلبا تسعى لتحقيقه كل دولة، إلا أنه له معوقات تقف دون تحقيقه.

- إن عدم الاتصال بين الدول لجمع الأدلة والمعلومات يعيق التعاون الدولي في مجال مكافحة الجريمة، فعدم التعاون والتنسيق بين الدول فيما يخص الإجراءات وجمع الاستدلالات والتحقيق خاصة وأن الحصول على دليل في هذه الجريمة قد يكون خارج نطاق الدولة هو أمر غاية في الصعوبة.[2]

2- **التجريم المزدوج:** يجد شرط التسليم المزدوج أساسه في أن الدولة طالبة التسليم الذي تهدف به إلى متابعة من نسب إليه السلوك الإجرامي أو تنفيذ العقوبة عليه، وبالتالي لا بد أن يكون السلوك مجرما في تشريعها وإلا فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية أو تنفيذ عقوبة جزائية ومن لا يمكن معالجة الدولة المطلوب إليها التسليم إيقاع عقوبة على ارتكاب

[1] صغيري يوسف، المرجع السابق، ص 146.

[2] المرجع نفسه، ص 135.

سلوك ما هو في الأساس غير محرم وفقا لقانونها وذلك راجع لعدم وجود معاهدات ثنائية للتعاون في هذا المجال.

- مما يشكل صعوبة في ملاحقة المبتز وتسليط عليه عقوبة تتناسب والفعل المجرم المرتكب.

3-**صعوبة الانابة القضائية الدولية:** انبثقت الإنابة القضائية الدولية من الواجبات والالتزامات التي يفرضها القانون الدولي على الأمم المتحدة وبموجبها يعهد للسلطات القضائية المطلوب منها اتخاذ إجراء القيام بالتحقيق لمصلحة السلطة القضائية المختصة في الدولة الطالبة مع احترام حقوق وحريات الإنسان المعترف بها عالميا ومقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل واحترام النتائج القانونية المتوصل إليها من طرف الدولة المطلوب منها المساعدة القانونية.

توسم أعمال الإنابة القضائية بالبطئ والتعقيد مما يتعارض مع سرعة الجريمة.

المبحث الثاني: إثبات جريمة الابتزاز عبر مواقع التواصل الاجتماعي وآليات مكافحتها

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد منها، أفرز إلى حيز الوجود نوعا جديدا من الأدلة يتماشى وطبيعة جرائم الإنترنت وهو ما يعرف بالدليل الرقمي أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجة للحواسيب وشبكة الإنترنت.

وباعتبار الدليل الرقمي ذو أهمية بالغة في مجال الإثبات الجنائي للجرائم المعلوماتية فإنه يجب التعرض إليه بشيء من التفصيل.

كما أن طبيعة هذه الجرائم المستحدثة شهدت انتشار متسارع ومتطور بين معظم الدول لسرعة الوسائل المستخدمة لارتكاب الجريمة المعلوماتية مما يستدعي تدخل على المستوى الدولي والوطني لمحاربتها والحد من انتشارها عن طريق آليات قانونية لمكافحتها وهذا ما سيتم إليه في هذا المبحث من خلال مطلبين، المطلب الأول سيتم التطرق إلى الدليل الرقمي كوسيلة إثبات أما في المطلب الثاني سيتم التطرق إلى آليات مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي على المستوى الدولي والوطني.

المطلب الأول: موقع الدليل الرقمي من الأدلة الجنائية

إن تحديد موقع الدليل الرقمي من الأدلة الجنائية المختلفة يقتضي التطرق بدءا إلى تعريفه ثم أنواعه وشروط صحته كما يجب علينا تبيان مصادر الحصول علبه والصعوبات التي تعترض الدليل الرقمي لاعتباره وسيلة إثبات أمام الجهات القضائية كل هذا وذاك سيتم دراسته بشيء من التفصيل في الفروع محل الدراسة.

الفرع الأول: مفهوم الدليل الرقمي

أولا: تعريف الدليل الرقمي : لقد وردت عدة تعريفات للدليل الرقمي أو الإلكتروني تدور كلها حول مفهوم واحد منها أنه "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برنامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إتقان وتطبيق القانون.[1]

[1] إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، العدد العاشر، الجزائر، ص 186-187.

– وقد عرفه البعض الآخر على أنه "مجموعة من البيانات أو المعلومات التي تمكن من أن تثبت أن جريمة ما وقعت أو وجود صلة بين الجريمة والجاني أو علاقة بين الجريمة والمجني عليه".[1]

– ومنها ما يعرفه بأنه "الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها.[2]

– يحتاج إثبات الجرائم الإلكترونية بصفة عامة والابتزاز الإلكتروني أو عبر مواقع التواصل الاجتماعي إلى دليل رقمي كوسيلة إثبات الابتزاز فيتطلب إجراء خطوات جمع الأدلة.

ثانيا: خصائص الدليل الرقمي

1- **الدليل الإلكتروني ذو طبيعة تقنية:** إن الخاصة العلمية للدليل الإلكتروني تقتضي بالضرورة التعامل مع هذا النوع من الأدلة من قبل تقنيين في الأدلة الجنائية العلمية والبيئة الافتراضية خصوصا، لذا فالطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المستخلص وبين البيئة التي تكون فيها، لأن التقنية في حد ذاتها لا تتيح لنا سكينا يتم به اكتشاف القاتل مثلا وإنما تنتجه هو نبضات أو مجالات مغناطيسية أو كهربائية تشكل معلومات مختلفة ولا يمكن معالجتها وقراءتها إلا من طرف أخصائيين يفهمون البيئة التي نشأ فيها والقوانين الخاضعة لهذا النوع من الأدلة.[3]

2- **الدليل الإلكتروني دليل علمي:** يتطلب في استخلاص الدليل الإلكتروني وتحايله طرق غير تقليدية، بحيث يتم إجراء تجارب علمية وتقنية على جهاز الحاسب الآلي الذي استخدم في جريمة معينة.

وعليه عندما يتم البحث عن الدليل الرقمي يجب أن تكون هذه العملية في إطار جغرافيا النظام الافتراضي، الخاضعة لقوانين الإعلام الآلي أو البيئة المعلوماتية ككل.

وبناء على هذه الخاصية يمكن القول أنه لا يمكن الحصول على الدليل الرقمي أو الاطلاع عليه سوى باستخدام الوسائل والأساليب العلمية وهذا يعود إلى المنشأ الذي تكون فيه الدليل.[4]

---

[1] محمد الأمين الشري، التحقيق في الجرائم المستحدثة، ط1، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004، ص 234.

[2] ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012، ص 74.

[3] خطوى مسعود، عكوش حنان، خصوصية الدليل الالكتروني، محجلة الفكر القانوني والسياسي، المجلد 7، العدد الأول، جامعة عمار ثلجي الأغواط، الجزائر، ص 1065.

[4] المرجع نفسه، ص 1064-1065.

3- **الدليل الرقمي ذو طبيعة ثنائية:** تعتبر الطبيعة الثنائية التي يختص بها الدليل الرقمي امتداد للطبيعة والتقنية لهذا الأخير وأيضا امتداد للبيئة الافتراضية التي تكون فيها، لذا فالمعلومات والبيانات التي تشكل دليلا جزئيا رقميا تكون في الأصل شكلا ثنائيا أو رقميا، ومرد ذلك أن الحاسب الآلي أو أي جهاز آخر له نفس خصائصه يقوم باستقبال هذه البيانات والمعلومات وتحويلها إلى أرقام ثم معالجتها.

- ومنه فمضمون الطبيعة الثنائية للدليل الرقمي هو اختزال البيانات أو المعلومات كالنصوص أو الصور أو الصوت أو أي معلومة أخرى إلى رموز ثنائية، وهذه الرموز الثنائية تتكون من سلسلة من رقم الصفر (0) إلى (1) ومثال ذلك أن الحرف (أ) يقابله في البيئة الرقمية الافتراضية 11000110 وهكذا يتم من خلال طرق الترميز نقل وتمثيل البيانات المختلفة، لتكون صالحة للتعامل معها داخل الحاسب الآلي وكذا الأجهزة الرقمية، بحيث أن لغة التعامل بين الأجهزة هو النظام الثنائي الرقمي والتي تسمى في الأصل لغة الآلة.[1]

4- **الدليل الجنائي الرقمي متنوع ومتكرر:** إن مصطلح الدليل الرقمي يشمل جميع البيانات الرقمية التي يمكن تناولها رقميا، سواء كانت هذه الأدلة متعلقة بالحاسب أو غيرها من الأجهزة، أو شبكة الإنترنت أو شبكات الاتصال السلكية واللاسلكية ومنه فالآثار الرقمية المستخلصة متنوعة لما تحتويه من معلومات عن وقائع قد تشكل جريمة فتصبح أدلة براءة أو إدانة ومن بينها صفحات المواقع الإلكترونية الصور، الفيديوهات الرقمية والملفات المخزنة في الحاسب الآلي الشخصي أو المعلومات المتعلقة بمستخدم شبكة الإنترنت وغيرها.

فهذا التنوع يدل على اتساع قاعدة الدليل الجنائي الرقمي الذي يمكن أن يكون دليل براءة أو إدانة.[2]

- أما خاصية التطور فهي ناتجة عن تزايد استعمال تقنية المعلومات الرقمية لتلبية احتياجات المستخدمين الأمر الذي أدى إلى ظهور أنواع جديدة من الأدلة.

- بالإضافة إلى خصائص أخرى للدليل الرقمي منها: صعوبة طمس الأدلة الرقمية لأنه يتم إسترجاعها بعد محوها وإصلاحها بعد إتلافها مما يؤدي إلى صعوبة التخلص منها، بالإضافة إلى أن الدليل الرقمي دليل قابل للنسخ في عدة نسخ واستخدامها كدليل للإثبات الجنائي خاصة في جريمة الابتزاز الإلكتروني.

الفرع الثاني: أشكال الدليل الرقمي وشروط صحة قبوله كحجية في الإثبات

سنتطرق في هذا الفرع إلى أشكال الدليل الرقمي وشروط صحته وهو ما سنتناوله فيما يلي:

[1] خطوى مسعود، المرجع السابق، ص 1065.

[2] رابحي عزيزة، المرجع السابق، ص 270.

أولا: أشكال الدليل الرقمي

1- **الصور الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة وفي العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة الصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطورا ولكنها ليست بالصورة أفضل من الصورة التقليدية.[1]

2- **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية وتشمل المحادثات الصوتية على الإنترنت والهاتف..الخ[2]

3- **النصوص المكتوبة:** وتشمل النصوص التي تم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والهاتف النقال والبيانات المسجلة بأجهزة الحاسب الآلي...الخ[3]

ثالثا: شروط صحة الدليل الرقمي وقبوله

1- **أن يكون مشروعا:** فقواعد الإثبات الجنائي وأدلته تخضع لمبدأ المشروعية والدليل الرقمي واحد منها، مما يترتب عليه عدم قبوله إلا إذا جرت عملية البحث والحصول عليها في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها بمعنى ضرورة اتفاق الإجراء الذي تم الحصول من خلاله على الدليل الرقمي مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، فقاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا أن تراعي حقوق الإنسان والمواثيق والاتفاقيات الدولية، فقواعد النظام العام وحسن الآداب في المجتمع بالإضافة إلى المبادئ التي استقر عليها القضاء.[4]

2- **أن يكون الدليل الرقمي يقيني:** أي مبني على الجزم واليقين بعيدا عن الظن والتخمين ذلك أنه لا مجال لدحض فرضية البراءة وافتراض عكسها إلا عندما يصل القاضي إلى الجزم واليقين الذي لا يشترط أن يكون مطلقا بل بصفة نسبية يتحقق معها تكوين القاضي لعقيدته الشخصية التي يبني عليها حكمه، لكن ليس المطلوب فقط الاقتناع الشخصي للقاضي بل

[1] خطوى مسعود، عكاش حنان، المرجع السابق، ص 1067.

[2] المرجع نفسه، ص 1067.

[3] المرجع نفسه، ص 1067.

[4] إلهام شهرزاد روابح: المرجع السابق، ص ص 194-195.

اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوتها في الاقتناع.[1]

3- **أن تتم مناقشته في جلسة الحكم:** حتى يتمكن القاضي من بناء قناعته وهو ما يعبر عنه بشرط "وضعية الدليل" ما معناه أن يكون للدليل أصل ثابت في أوراق الدعوى ثم يطرح للمناقشة بعد اطلاع الخصوم عليه وهذا ما جاء النص عليه في المادة 212 من ق.إ.ج في فقرتها 2.[2]

والحكمة من ذلك هي تكوين القاضي لقناعته القائمة على مناقشة كل الأدلة.[3]

ثالثا: حجية الدليل الرقمي في الإثبات : تختلف حجية الأدلة الرقمية بحسب نظام الإثبات الجنائي الذي تعتمده الدولة وهو في الجزائر نظام الإثبات الحر[4]، وبما أن الدليل الرقمي دليل علمي يتمتع بجملة من الخصائص والتي منها دقة المعلومة وسهولة الوصول إلى مصدرها، وقيامه على نظريات حسابية مؤكدة، فإنه لا يطرح إشكال كبير من حيث اعتباره حجية خاصة إذا تم استخلاصه وفق ضمانات قانونية وفنية تضمن صحته وسلامته[5] بل هو في رأينا الخاص يأتي على قمة الأدلة الجنائية من حيث قوة الإثبات ووجب الأخذ به في المقام الأول.

– فالمشرع الجزائري لم يضع أي نصوص قانونية صريحة بهذا الخصوص حيث تم الاستناد في هذا الموضوع للمادة 212 ق.إ.ج والتي طبق من خلالها مبدأ حرية الإثبات، إلا أن المشرع أدرك أن هذا لا يكفي لوحده وليواكب التطور الحاصل فيما بعد ووضع القانون رقم 04/15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات الذي أقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وبعدها تدخل المشرع الجزائري لحماية المعاملات الرقمية حين وضع القانون 04/09.[6]

وكل ذلك راجع إلى طبيعة الدليل الرقمي وخصوصيته لذا فهو يخضع إلى طرق خاصة في تحصيله تختلف عن الدليل التقليدي كما أنه يخضع إلى أحكام وطرق خاصة في الإثبات.

---

[1] ثامر أمال: إثبات الجرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية والإجرامية، كلية الحقوق جامعة سعد دحلة البليدة، جوان 2012، ص 145.

[2] انظر المادة 212 ق.إ.ج

[3] إلهام شهرزاد روابح، المرجع السابق، ص 195.

[4] ما أكدته المادة 212 ق.إ.ج في فقرتها 1.

[5] تامر آمال، المرجع السابق، ص 151.

[6] نور الهدى محمودي، حجية الدليل الرقمي ف إثبات الجريمة المعلوماتية باحثة (دكنوراء جامعة باتنة 1) ص ص 922-923.

الفرع الثالث: مصادر تحصيل الدليل الرقمي والصعوبات التي تعترضه في ذلك

أولا: مصادر تحصيل الدليل الرقمي: تعتمد جهات التحري والتحقيق على مصادر لتحصيل الدليل الرقمي ومن المصادر التي يسمح لها القانون، إجراء الإرشاد الجنائي وإجراء الوضع تحت المراقبة الإلكترونية وتعاون مقدمي خدمات الانترنت مع السلطات القضائية.

أ- **إجراء الإرشاد الجنائي:** الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها للولوج للعالم الافتراضي وبالأخص عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستعملين صفات وهمية من أجل الكشف عن هذه الجرائم وكشف المجرمين.

فهذا الإجراء لا يتطلب جهد مادي كبير، حيث يقوم به ضباط الشرطة القضائية أو يكلف غيره من ذوي الاختصاص وهذا بعد الحصول على إذن رسمي للقيام بمهام البحث والتحري عن الجرائم وضبط مرتكبيها.

- وقد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت اسم التسرب من خلال نصوص المواد 65 مكرر إلى 65 مكرر 18 ق.إ.ج بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق تحت رقابة وكيل الجمهورية لمدة 04 أشهر قابلة للتجديد.[1]

ب- **إجراء الوضع تحت المراقبة الإلكترونية:** وهي من أهم مصادر البحث والتحري سواء في الجرائم التقليدية أو المستحدثة ويقصد بها مراقبة شبكة الجرائم المعلوماتية وتسمى بذلك المراقبة الإلكترونية.

- فهي العمل الذي بقوم به المراقب باستخدام التقنية الإلكترونية لجمع البيانات والمعلومات عن المشتبه فيه من أجل تحقيق غرض أمني أو أي غرض آخر، وهي مرتبطة بالزمن.

- وقد أجاز المشرع المراقبة الإلكترونية في الجرائم المعلوماتية عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية، كما أجاز كل الترتيبات التقنية لها دون علم المعنيين ولا موافقتهم، بغية الحصول على تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة وذلك بإذن من وكيل الجمهورية.

ج- تعاون مقدمي خدمات الانترنت مع السلطات القضائية: يقصد بمزود الخدمة كل شخص يقدم خدمة إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في آدائها على طائفة معينة من المتعاملين معه بعقد فقد عرف المشرع الجزائري مقدم الخدمة بموجب المادة 2 [2]من ق 09-04 بأنه:

[1] انظر المواد من ق.إ.ج المعدل والمتمم.

[2] انظر المادة 2 من ق 09-04.

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.

- ونظرا لضلوع الشبكة المعلوماتية في أغلب جرائم العالم الافتراضي فإن المشرع الجزائري قد فرض على مقدمي خدمات الانترنت مجموعة من الالتزامات من أجل مساعدة السلطات القضائية في أعمال التحقيق وذلك من خلال القانون رقم 09-04 في فصله الرابع تحت عنوان "التزامات مقدمي الخدمات " ومن بين الالتزامات الواردة نجد الالتزام بمساعدة السلطات والالتزام بحفظ المعطيات المتعلقة بحركة السير.

ثانيا: صعوبات التعقب لتحصيل الدليل الرقمي

1- **سهولة محو الدليل:** حيث أن الجناة بعد ارتكابهم للجريمة يحرصون على محو أي آثار للتهديد والابتزاز مما يجعل الوصول للدليل صعب وفي بعض الأحيان يكون مستحيل.[1]

2- **صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي:** تتم جريمة الابتزاز الإلكتروني في بيئة افتراضية تحكمها الرموز والبيانات وتخلو من العنف الظاهر والآثار المادية كالجريمة التقليدية مما يصعب الوصول لدليل مادي كبصمات الإصبع أو نقاط الدم مما يجعل الوصول للجاني معترض بالعقبات.

3- الصعوبات الخاصة بالمساعدات القضائية الدولية وتدريب الكوادر:

أ- **الصعوبات الخاصة بالمساعدات القضائية الدولية:** تعتبر الإنابة الدولية من أهم صور المساعدات القضائية الدولية في المجال الجنائي والتي تتم عن طريق الطرق الدبلوماسية التي تتسم بالبطئ مما لا يتناسب مع طبيعة جرائم الإنترنت التي تتسم بالسرعة.[2]

ب- **الصعوباب الخاصة بالتعاون الدولي في مجال التدريب:** تتمثل هذه الصعوبات في الفوارق الفردية بين المتدربين وتأثيرها في عملية الاكتساب للمهارات بطريقة متكافئة لدى المتدربين وتأثيرها في عملية اكتساب المهارات بطريقة متكافئة لدى المتدربين وتأثيرها في عملية اكتساب المهارات المستهدفة سيما في مجال التكنولوجيا الرقمية.

[1] نهلا عبد القادر المومني: الجرائم المعلوماتية، ط 2، دار الثقافة للنشر والتوزيع، عمان-الأردن، 2010، ص 54.

[2] رابحي عزيزة، المرجع السابق، ص 319.

المطلب الثاني: آليات مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي

حتى يتم القضاء على الصعوبات التي تواجه التعاون الدولي يجب أن تتكاثف الجهود حول محاربة كل أنواع الجرائم لأنه لم يعد يوجد مجال إلا وتلعب تكنولوجيا المعلومات دورا رئيسيا في أدائه وتطويره، ونتيجة لهذا التطور في عالم المعلوماتية نشأت ونمت أنماط جديدة من الجرائم، وبرز الاهتمام الدولي لمكافحتها لما تنطوي عليه هذه الجرائم من آثار سلبية بالغة الخطورة، الأمر الذي استوجب التصدي لهذه الجرائم وقد أصدرت العديد من الدول قوانين تحد مثل هذه الجرائم والأفعال وتعاقب عليها لكن تلك الجهود المنفردة للدول أضحت على فراغ تشريعي وحضور علمي في آليات مكافحة الجرائم.

هذا الأمر يبدو طبيعيا بالنظر لخصوصية جرائم المعلومات وتخطيها الحدود الجغرافية من جهة ومن جهة أخرى تميزها بالتطور التسارع تقنيا والانتشار الكبير في جميع جوانب الحياة هذا على الصعيد الدولي أما على الصعيد المحلي فإن التطور الذي عرفه المجتمع الجزائري في استخدام تكنولوجيا المعلوماتية على غرار ما في المجتمعات جهله يعرف أنواع من الجرائم المستحدثة وعلى رأسها الجريمة الإلكترونية في أحد صورها ألا وهو الابتزاز عبر مواقع التواصل الاجتماعي، فكان لزاما على المشرع الجزائري التدخل عبر عديد النصوص القانونية الموضوعية والإجرائية لمواجهة الجريمة الإلكترونية والمجرم الإلكتروني وهذا ما سيتم التطرق له من خلال هذا المطلب في شكل فرعين الأول يعالج آليات المكافحة الدولية لجريمة الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي باعتباره صورة من صور الجريمة السيرانية والفرع الثاني سنتطرق إلى جهود المشرع في محاربة هذه الآية.

الفرع الأول: الجهود الدولية لمكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي .

أولا: التعاون القضائي: إن إجراءات التحقيق والملاحقة القضائية في جرائم الإنترنت تقتضي تتبع النشاط الإجرامي الأمر الذي يستوجب تقصي الآثار الجرمية من مصدرها إلى غاية تنفيذها وتحديد مواقع الأضرار التي مستها وبما أن هذه العناصر وقعت في بلدان مختلفة فإنه يتعين لملاحقة مرتكبي هذه الجريمة وجود نوع من التعاون بين السلطات القضائية لهذه البلدان قصد تمديد الولاية القضائية.[1]

أ- **التعاون الأمني:** إنه من البديهي أن تقف الحدود الجغرافية ومشكلة الاختصاص الإقليمي حجر عثرة أمام الإجراءات الجنائية لملاحقة مرتكبي الجرائم لا سيما في جريمة الإنترنت عامة والابتزاز الإلكتروني خاصة التي تتميز بكونها جريمة عابرة للحدود فقد يكون مرتكب الهجوم يحمل جنسية دولة ما وينفذ جريمته من أجهزة دولة أخرى وتقع آثار هذه الجريمة في دولة ثالثة ولهذا تبرز الحاجة الملحة لتوحيد الجهود فيما يتعلق يتبادل المعطيات المتعلقة بالحريمة

[1] قردان مصطفى، زرقين عبد القادر: الآليات الدولية لمكافحة الجريمة الإلكتررونية، مجلة صوت القانون، المجلد 8، العدد 02، الجزائر، ص1225.

والمعلومات التي تسمح بكشف هوية المجرمين. مادام انه يستحيل على الدولة بمفردها القضاء على هذه الجريمة، فأجهزة الشرطة لا يمكنها تعقب مركتبي الجرائم وملاحقتهم إلا من نطاق حدودها أي أنه متى فر المجرم خارج حدود الدولة فإنه يبقى في مأمن من المتابعة.[1]

- ونجد في هذا الإطار أن هناك ثلاثة أوجه لإقامة هذا التعاون:

1- إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي جرائم الإنترنت ونشرها.

2- التعاون في إطار المنظمة الدولة للشرطة الجنائية "الأنتربول".

3- القيام بعمليات أمنية مشتركة.

د- المساعدة القضائية الدولية: تعرف المساعدة القضائية الدولية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة من دولة أخرى بصدد جريمة من الجرائم".

-ويمكن استنباط المبادئ العامة التي تحكم الالتزام بالمساعدة القضائية المتبادلة في الفقرة 1 من م 25 من اتفاقية بوداست للإجرام الإلكتروني والالتزام بالمساعدة يجب أن يتوفر لأقصى حد ممكن وأن تكون المساعدة شاملة وممتدة كما يجب تقليل المعوقات.[2]

وتتخذ المساعدة القانونية صورا عديدة منها:

1- **تبادل المعلومات:** يتم عن طريق تبادل البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، حركت الدعوى فيها ضد أحد رعاياها أو رعاية دولة أخرى مما يتضمن تبادل السوابق القضائية للمتابعين لمثل هذه الجرائم ونجد لهذه الصورة عدة تطبيقات منها ما ورد في الفقرتين 6، 7 من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية.[3]

2- نقل الإجراءات: ويقصد به قيام دولة ما بموجب اتفاقية أو معاهدة باتخاذ جملة من الإجراءات الجنائية بصدد جريمة ارتكبت في إقليم دولة أخرى لمصلحة هذه الدولة وذلك بناء على توفر جملة من الشروط من أهمها التجريم المزدوج ويقصد به أن يكون الفعل مجرم في كل من الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات بالإضافة إلى مشروعية الإجراءات المطلوبة اتخاذها أي أن توافق قانون الدولة المطلوب منها اتخاذ الإجراءات فضلا أن تكون الإجراءات المطلوبة اتخاذها جدية أي أن تكون ذات أهمية بالقدر الذي يمكن أن يسهم في الوصول إلى حقائق فاصلة في ملابسات الجريمة، وقد أقرت العديد من الاتفاقيات والمعاهدات ذلك منها:

---

[1] قردان مصطفى، المرجع السابق، ص ص 1225-1226.

[2] أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، 2011، مكتبة الوفالي القانونية، الاسكندرية، ص 426.

[3] المرجع نفسه، ص 429.

– معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية.

– اتفاقية الأمم المتحدة في مكافحة الجريمة المنظمة عبر الوطنية في مادتها 21 والمادة 23 من اتفاقية بوداست للإجرام المعلوماتي.[1]

3– **الإنابة القضائية:** ويقصد بها اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية لأثره المباشر من أجل الفصل في مسألة معروضة على السلطة القضائية تعذر على الدولة التي تقدمت بطلب الإنابة القيام به بنفسها.[2]

– وتهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يضمن إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة تجاوزا لعقبة السيادة الإقليمية التي تحظر على الدول الأجنبية ممارسة الأعمال القضائية داخل إقليم الدول الأخرى بإجراءات التحقيق والمعاينة والتفتيش أو سماع الشهود كما تم التطرق إليه سابقا.

– **تسليم المجرمين كآلية دولية في مجال مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي:**

لقد أتت هذه الصورة كنتيجة حتمية للتطور الهائل الذي شهدته كافة المجالات وبوجه أخص مجال الاتصالات والمعلوماتية فقد يبدأ المجرم بالتحضير في دولة ويبدأ بالتنفيذ في دولة أخرى، فالجريمة المعلوماتية أصبح لها طابع دولي، حيث أن أجهزة العدالة لا تستطيع تجاوز الحدود الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين واتخاذ كل الإجراءات في مواجهتهم ..... لا يفر المجرم من العقاب تم الاعتماد على تسليم المجرمين كآلية من أجل تعاون دولي لمحاربة الجريمة المعلوماتية إذ يأخذ هذا التسليم صور إما تسليم إداري أو تسليم مختلط أو قضائي وحتى يتم بصورة صحيحة يجب أن يشتمل على الشروط المتطلب فيه وهي:

عدم تسليم الرعايا، التحريم المزدوج، درجة حيازة الجريمة، عدم جواز تسليم اللاجئين السياسيين، عدم جواز تسليم المحاكمين على ذات الجريمة.

– **التعاون الدولي في مجال التدريب لمكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي:** يعد التدريب عنصرا حيويا لبناء الخبرات والمهارات وقطاع العدالة والأجهزة الأمنية ليست في منأى منه فيجب أن تتوفر لدى رجال العدالة الأرضية القانونية والخبرة الفنية اللازمة في مجال الجريمة المعلوماتية وهذه الخبرة لا تأتي دون تدريب متخصص يشمل كل ما يتعلق بتكنولوجيا المعلوماتية ونظرا للطبيعة الخاصة للجريمة المعلوماتية فيستحيل على الدولة بمفردها محاربة هذا النوع من الجرائم دون تعاون أو تنسيق مع غيرها من الدول، ويتفحص الاتفاقيات والمعاهدات الدولية والإقليمية نجد

[1] أمير فرج يوسف، المرجع السابق، ص 430.

[2] المرجع نفسه، ص 430.

أنها تؤكد على ضرورة التعاون بين الدول في مجال التدريب ونقل الخبرات والدليل على ذلك ما ورد في المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود.

– التعاون الدولي قد يأخذ أشكال عدة لا يمكن حصرها فقد يتحقق من خلال عقد مؤتمرات أو ندوات أو ورشات عمل متخصصة في مواجهة لكل الجرائم على الصعيدين الدولي والإقليمي ويتحقق هذا التعاون عن طريق تنظيم تربصات دورية أو إقامة دورات تدريبية للعاملين في أجهزة العدالة والأجهزة الأمنية من تبادل الخبرات والاستفادة من المساعدة التقنية الضرورية والتعرف على أحدث التقنيات في مواجهة أو التصدي لهذه الجرائم، الأمر الذي ينعكس إيجابا على قدرة القائمين على مكافحة جريمة المعلوماتية بصفة عامة والابتزاز الإلكتروني بصفة خاصة.[1]

الفرع الثاني: الجهود الوطنية لمكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي

أولا: آليات مكافحة الجرائم الإلكترونية في إطار القواعد العامة: تدارك المشرع الجزائري الفراغ القانوني الذي عرفه مجال الإجرام الإلكتروني خلال السنوات الأخيرة فقام بتعديل قانون العقوبات بموجب قانون رقم 04-15.[2]

مستحدثا فيه جملة من النصوص حرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله وإلى حانب ذلك قام بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى والطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22.

أ- القواعد الموضوعية المقرر في قانون العقوبات لمكافحة الجريمة الإلكترونية:

- تجريم الاعتداء على نظام المعالجة الآلية للمعطيات:

أ1- الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات: - الدخول غير مصرح به l'intrusion يقصد بفعل الدخول هنا وهو الركن المادي للجريمة الاعتداء على نظام المعالجة الآلية للمعطيات كذلك الدخول المعنوي أو الإلكتروني باستعمال الوسائل الفنية أو التقنية إلى النظام المعلوماتي، ولا يعد نظام الدخول بحد ذاته سلوكا غير مشروع وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[3]، وهو ما يستشف من م 304 مكرر من ق.ع.[4]

---

[1] أمير فرج يوسف، المرجع السابق، ص 430.

[2] قانون رقم 4-15 مؤرخ في 10-11-2004 قانون عدل وتمم الأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71، صدر بتاريخ 10-11-2004 معدل ومتمم.

[3] راضية عيمور، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، جامعة الأغواط الجزائر، ص99.

[4] راجع المادة 394 مكرر من ق.ع.

– ويلاحظ من خلال هذه المادة أن المشرع الجزائري اعتبر جريمة الدخول غير مصرح به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها تحقق مجرد الدخول إلى نظام المعالجة الآلية للمعطيات بأكمله أو إلى جزء منه فقط، شرط أن يكون فعل الدخول بدون ترخيص مقصودا وليس صدفة أو بالخطأ، كما لا تشترط المادة أن يكون هذا النظام محميا بالتشفير أو غير بل جاءت عامة ومطلقة أي تحمي كل الأنظمة المعلوماتية وهو ما أكدته المادة 2 في الفقرة من ق.ع 09-04.

– البقاء غير المرخص: .....la maintien

يقصد به استمرارية التواجد داخل نظام المعالجة دون إذن من صاحبه أو من له السيطرة عليه، بمعنى آخر هو بقاء شخص داخل نظام المعالجة ملك للغير بعد الدخول إليه خطأ أو صدفة رغم علمه بأن بقاءه غير مرخص.

– اعتبر المشرع الجزائري على غرار المشرع الفرنسي فعل البقاء غير المرخص به في نظام المعالجة الآلية للمعطيات جريمة مثلها مثل جريمة الدخول الغير مرخص به وذلك حسب م 394 مكرر ق.ع حيث حدد لهاتين الجريمتين نفس العقوبة.

ويظهر الركن المادي في صورتين:

1-يتمثل في تحقق فعل البقاء غير المرخص بها داخل نظام المعالجة الآلية للمعطيات منفصلا عن فعل الدخول.

2-تتمثل في تحقيق فعل البقاء غير المرخص به مجتمعا مع فعل الدخول.[1]

أ2- الصورة المشددة للاعتداء على نظام المعالجة الآلية للمعطيات: تتحقق عندما يترتب عن فعل الدخول أو البقاء نتائج غير مشروعة ضد معطيات النظام قد نص المادة 394 مكرر في فقرتها 2 ذلك بمضاعفة العقوبة حسب المادة وما ورد فيها.[2]

– نلاحظ من خلال نص المادة بأن المشرع الجزائري أورد طرفين لتشديد عقوبة الدخول والبقاء بدون ترخيص في نظام المعالجة الآلية للمعطيات بحيث يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام.

ويتحقق الثاني حينما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته.

– وتتجسد صورة التشديد في نظام المعالجة الآلية والتلاعب به في جريمة الابتزاز عبر مواقع التواصل الاجتماعي إذ أن المبتز تكون غايته الوصول إلى صورة أو رسائل أو تصوير فيديو من

[1] راضية عيمور، المرجع السابق، ص 100-101.

[2] راجع نص المادة 394 مكرر ق.ع.

أجل عملية الابتزاز للضحية الذي يعمد إلى التلاعب في نظام المعالجة الآلية لفك الحماية المطبقة على المواقع الخاصة للضحية.

وحتى يتحقق أركان الجريمة في الدخول والبقاء يجب أن يتحقق االنتيجة والعلاقة السببية بين الفعل و النتيجة.

– فمتى تحققت أركان جريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات في صورتها المشددة عوقب الجاني بالحبس من 6 أشهر إلى سنتين وبغرامة من 50.000 إلى 150.000 دج.

– ولعل الغاية من هذا التشديد هو الحد من تفاقم الإجرام المعلوماتي في صورة من صوره ألا وهي الابتزاز عبر مواقع التواصل الاجتماعي وما يصاحبه من أضرار بالغة وتحقيق الائتمان في المعاملات الإلكترونية إضافة إلى تجريم الاعتداء على معطيات نظام المعالجة الآلية والمحددة على سبيل الحصر في المادة 394 مكرر 1 ق.ع.

ب– القواعد الإجرائية المقررة في قانون الإجراءات الجزائية لمكافحة الجريمة الإلكترونية:

جريمة الابتزاز عبر مواقع التواصل الاجتماعي : قد أدرك المشرع الجزائري حبذا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية والتي من شأنها أن تتفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها وهو ما استدركه المشرع بتضمين القانون رقم 06–22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها والتسرب.

ثانيا: آليات مكافحة الجرائم الإلكترونية في إطار القوانين الخاصة (جريمة الابتزاز عبر مواقع التواصل الاجتماعي كصورة من صور الجريمة الإلكترونية)

تقتضي المواجهة الفعالة للجريمة الإلكترونية بمختلف أنواعها محاصرتها بنصوص خاصة إلى جانب القواعد العامة، فلما كان مجال الملكية الفكرية والأدبية حقل خصب في مثل هذه الجرائم جعل المشرع الجزائري يسارع إلى إحاطته بحماية جبائية وذلك من خلال تجريم الأفعال التي تشكل اعتداء على حقوق المؤلف ولتعزيز جهوده في مكافحة الإجرام الإلكتروني عمد إلى وضع قواعد أكثر ملائمة مع خصوصيات الجرائم المتعلقة بوسائل الإعلام والاتصال وذلك من خلال القوانين الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

1–**تقرير حماية جزائية لمعطيات الحاسب في قانون الملكية الفنية والأدبية:** الهدف من وضع قوانين الملكية الفكرية هو حماية حق الإنسان في التفكير والإبداع والابتكار الذي يعد بمثابة العامل الأساسي لتقييم المجتمعات وتطورها، ولما كانت المكونات المنطقية للحاسب الآلي

"برامجه وبياناته" ثمرة جهد فكري للإنسان، كان لزوما على المشرع اشتمال هذه المكونات المنطقية بالحماية المقررة في قانون الملكية الفنية والأدبية وذلك بتجريم الأفعال التي تشكل اعتداء عليها وإقرار ما يقابلها من عقوبات جزائية.

– اتجه المشرع الجزائري على غرار معظم التشريعات الغربية إلى الإقرار بالحماية القانونية لبرامج الحاسب الآلي من خلال إخضاعها لقوانين حماية حقوق المؤلف بحيث اعترف صراحة في الأمر 03-05 المؤرخ في 19-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة بوصف المصنف المحمي لمصنفات الإعلام الآلي.[1]

– ترتب عن جعل المشرع الجزائري برامج وبيانات الحاسب مصنفا فكريا دمجها ضمن المضفات الأصلية واعتبار أي اعتداء على الحق المالي والأدبي لمؤلف البرامج والبيانات يشكل فعل من أفعال التقليد المنصوص عليها في المادة 151 من الأمر 03-05 المذكور سلفا ويترتب عليها العقوبات الجزائية المقررة في المواد 158،157،156،153 من نفس الأمر وتنقسم جنح التقليد التي تمس مصنف برامج وبيانات الحاسب الآلي إلى ثلاثة أنواع هي:

–الجنح المرتبطة بالحق المعنوي للمؤلف وهي محددة في المادة 01/151 من الأمر 03-05.

– الجنح المرتبطة بالحق الأدبي للمؤلف.

– الجنح المرتبطة بالمصنف المقلد.

2- استحداث تدابير جديدة في قانون 09-04:

أ- **التدابير الوقائية المستحدثة:** لقد جاء في القانون 09-04 بمجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر وهي كالتالي:

– مراقبة الاتصالات الإلكترونية حسب نص م 4 من ق 09-04.

– إقحام مزودي خدمات الاتصالات الإلكترونية في مسار الوقاية من الجرائم المعلوماتية وذلك من خلال فرض مجموعة من الالتزامات المذكورة في المواد 12،11،10 من نفس القانون أعلاه.[2]

ب- التدابير الإجرائية: إضافة إلى التدابير الوقائية السالفة الذكر تبنى المسرع في القانون 09-04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجيا الإعلام والاتصال تتلخص فيما يلي:

[1] راضية عمور، المرجع السابق، ص 103.

[2] المرجع نفسه، ص 104-105.

– السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد للمنظومة المعلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها.

– إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى الذي يمكن الدخول إليها بواسطة المنظومة الأصلية بشرط إخطار السلطة المختصة مسبقا.

– إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزن في منظومة معلوماتية موجودة خارج إقليم الوطن وذلك وفق الاتفاقيات الدولية ومبدأ المعاملة بالمثل.[1]

في الأخير يتضح أن قانون 09-04 جاءت أحكامه عامة ومطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال ويطبق على كافة التكنولوجيات القديمة والجديدة بما فيها شبكة الإنترنت وعلى أي تقنية يمكن أن تظهر مستقبلا، وهو الأمر الذي يجعله قانونا فعالا ويساير التطور التكنولوجي السريع.

– وفي هذا الصدد يكون القانون قد وضع أحكام رادعة فيما يتعلق بجرائم الإعلام والاتصال عامة وجريمة الابتزاز على وجه الخصوص فقد شمله القانون سواء في قانون العقوبات باعتباره الشريعة العامة أو في القوانين الخاصة.

[1] راضية عمور، المرجع السابق، ص 105.

ملخص الفصل الثاني:

يعالج هذا الفصل القواعد الإجرائية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي وذلك بتسليط الضوء على الإجراءات التقليدية والحديثة وكذا الاشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية التحقيق من خلال التطرق إلى صعوبات اكتشاف الجريمة المرتكبة عبر مواقع التواصل الاجتماعي والصعوبات المتعلقة بالجانب القضائي والتعاون الدولي وكما تعرضنا إلى القيمة الثبوتية للدليل الرقمي كوسيلة إثبات في هذه الجرائم وهو الدليل الرقمي وذلك من خلال التطرق إلى مفهومه وشروط صحته وأهم أشكاله والخصائص التي يتميز بها عن بقية أدلة الإثبات أو وسائل الإثبات كما تم تسليط الضوء على مصادر الحصول عليه والصعوبات التي تعترض جهات التدقيق في تحصيله.

وحتى يتم الحد من هذه الجريمة يجب التطرق إلى الجهود الدولية والوطنية في مكافحتها وهذا ما تم التطرق له في ختام دراستنا.

خاتمة

خاتمة:

جريمة الابتزاز عبر مواقع التواصل الاجتماعي تعد من الجرائم المستحدثة الدخيلة على المجتمع فيطلق عليها الجرائم الصامتة أو الناعمة لأنها تخلو من استخدام العنف عكس الجرائم العادية، فجريمة الابتزاز عبر مواقع التواصل الاجتماعي هي إحدى صور الجريمة الإلكترونية وهي الوجه الآخر للابتزاز التقليدي الذي ينشأ بدوره ويولد ويرتكب في عالم مادي ملموس حيث يترك فيه الجاني أثر أما الابتزاز عبر مواقع التواصل الاجتماعي فيتم في عالم افتراضي مليء بالرموز والتشفير والحماية.

فقد أصبحت هذه الجريمة تشكل هاجسا لدى مستخدمي التقنيات الحديثة بعد التطور السريع الذي شهدته هذه التقنيات، وأمام هذه الثورة المتسارعة حاولت الدول تطوير تشريعاتها لتلاحق هذه الجرائم المستحدثة من بينها التشريع الجزائري الذي ينبه الشارع إلى إفراد هذا النوع من الجرائم بنصوص خاصة تجرم الفعل وتحدد العقوبات المقررة لها في حالة تم ارتكابها.

وبعد الإنتهاء من دراسة موضوع بحثنا (الابتزاز عبر مواقع التواصل الاجتماعي) الذي استعرضنا من خلال الإطار الموضوعي لهذه الجريمة من خلال تبيان ماهيته وتجريمه. كما تطرقنا إلى الجانب الإجرائي تسليط الضوء على التحقيق في الجريمة وإثباتها كما عالجنا آلية مكافحتها نصل في الأخير إلى أهم النتائج والمقترحات.

النتائج:

1- جريمة الابتزاز عبر مواقع التواصل الاجتماعي هي صورة من أحد صور الجريمة السبرانية إذا تتم باستخدام التقنيات الحديثة والمتطورة.

2- أن جريمة الابتزاز عبر مواقع التواصل الاجتماعي تخضع لإجراءات خاصة في التحقيق إذ لا تشترط فريق عمل من المختصين أو المؤطرين أو المؤهلين لذلك مع استيعاب التطورات الراهنة حول الوسائل الحديثة وذكاء المجرم إذ يتميز مرتكب هذا النوع من الجرائم بصفات تختلف عن المجرم العادي أو التقليدي.

3- يستخدم المبتز إلكترونيا وسائل وطرق تختلف عن المرتكبة في الابتزاز التقليدي كهاتف نقال مزود بآلات متطورة للاعتداء والتدخل في الحياة الخاصة عن طريق التقاط الصور أو نشر أخبار وتسجيلات صوتية أو تسجيلات مرئية ولو كانت صحيحة وتتصل بها.

4- جريمة الابتزاز عبر مواقع التواصل الاجتماعي تتحقق باستخدام الجاني إما سلوك واحد أو عدة سلوكيات فلا عبرة بالطريقة التي لجأ لها الجاني لتهديد الضحية، فقد تتم إما عن طريق البريد الالكتروني أو وسائل التواصل المختلفة أو أي طريقة أخرى تهدف إلى حمل المجني عليه على إحداث نتيجة معينة تتمثل في إما القيام بالفعل أو الامتناع عنه.

5- قد ينتج عن جريمة الابتزاز عبر مواقع التواصل الاجتماعي جرائم أخرى كالزنا، القتل، سرقة، الخطف، العنف.

6- جريمة الابتزاز عبر مواقع التواصل الاجتماعي من الجرائم العابرة للحدود الوطنية فقد يكون المجرم في دولة والضحية في دولة أخرى.

7- تعد هذه الجريمة من الجرائم صعبة الإثبات فهي من الجرائم التي يسهل محو آثارها بسهولة وسرعة عكس الجريمة التقليدية فهي تحتاج أيضا إلى جهود وعمل شاق كي يتم إثباتها.

8- في جريمة الابتزاز عبر مواقع التواصل الاجتماعي يعد الدليل الرقمي أهم أدلة الإثبات فيها في حين أن التعامل معه يحتاج إلى خبرات معينة وأجهزة مختصة وفريق عمل متكامل.

9- اختلاف التشريعات من حيث العقوبة المقررة إلى مثل هذا النوع من الجرائم ويعود ذلك إلى طبيعة المنطقة وخصوصية كل مجتمع حسب العادات والتقاليد السائدة به.

10- إصدار أحكام خاصة تتعلق بالتشديد أو الإعفاء أو التخفيض في العقوبات المقررة إما التشريعات المقارنة أو التشريع الجزائري الذي كان محل المعالجة أو بصدد المعالجة.

11- أن جريمة الابتزاز عبر مواقع التواصل الاجتماعي من الجرائم التي لا تستطيع الدولة الواحدة مكافحتها بل يجب تكاثف الجهود الدولية لمحاربتها باعتبارها جريمة عابرة للحدود.

المقترحات:

1- إصدار قانون خاص بجريمة الابتزاز عبر مواقع التواصل الاجتماعي في الدول التي لا يوجد في تشريعها نص ليكون العام والخاص ذا فاعلية أكبر.

2- لا بد من تكاثف جهود المؤسسات التربوية والتعليم العالي والمساجد لإقامة ندوات حول مخاطر هذه الجريمة الدخيلة على المجتمعات العربية والإسلامية.

3- تدريب وتأهيل المحققين والعاملين بجهات القضاء بأساليب التحقيق الحديثة والتعامل مع الدليل الرقمي حتى لا يفلت المجرم من بين سيد رجال التحقيق بسبب قلة الخبرة في التعامل والمحافظة على الدليل الرقمي.

4- الإعتماد على الجانب النفسي والاجتماعي لمن وقع ضحية الابتزاز عبر مواقع التواصل الاجتماعي مهما كان جنس الضحية وسنه وذلك تبعين أخصائيين لهذه الظاهرة والجرائم.

5- إنشاء مكاتب ووحدات خاصة بهذا النوع من الجرائم داخل الوحدات الأمنية لاستقبال البلاغات وتتبع المبتزين وأثرهم بحرفية عالية.

6- تكثيف التعاون الدولي بوضع آليات موحدة تجرم الابتزاز عبر مواقع التواصل الاجتماعي كي لا يفلت المجرم من العقاب نتيجة تساهل بعض الأنظمة وتشدد الأخرى مما يجعل المجرم في مأمن في الدول التي تسهل هذا النوع من الجرائم بالتالي يتفاقم الوضع بها.

الملاحق

الملحق الأول: إحصائيات قضايا الابتزاز الالكتروني على المستوى الوطني المعالجة من وحدات الدرك الوطني:

سنة 2020..... 940 قضية

سنة 2021..... 1054 قضية

سنة 2022 .....1233 قضية

سنة 2023 .....1446 قضية

سنة 2024 إلى غاية تاريخ 15 ماي .....تم تسجيل 381 قضية

أنواع الابتزاز الالكتروني المعالج من طرف المصالح المختصة في مكافحة الإجرام السيبراني بقيادة الدرك الوطني

1. **ابتزاز أشخاص طبيعيين:** خاصة الإناث من خلال التهديد بنشر صورهم الخاصة.
2. **ابتزاز أشخاص معنويين** (شركات، مؤسسات ..الخ)**:** من خلال اختراق وتعطيل أنظمتهم المعلوماتية وطلب فدية من أجل ذلك.

دور الدرك الوطني:

المصالح المختصة في مكافحة الإجرام السيبراني بقيادة الدرك الوطني تعمل من خلال محققي تكنولوجيات الإعلام والاتصال، وهم دركيين تلقوا تكوينا خاصا في التحقيق في الجرائم الالكترونية على تحديد هوية المشتبه فيهم الضالعين في القضايا أو الجرائم الالكترونية وتقديمهم أمام السلطات القضائية.

الملحق الثاني:

وزارة الداخلية،الجماعات المحلية
و التهيئة العمرانية
المديرية العامة للأمن الوطني
أمن ولاية تبسة
خلية الاتصال و العلاقات العامة

الجمهورية الجزائرية الديمقراطية الشعبية

تبسة في:2024/05/12

تعهد شرفي

إنه في يوم: الأحد الموافق لـ **12 ماي 2024.**

- أنا الممضية أسفله الطالبة: **نصير هدى** المولودة بتاريخ 1985/05/24 بالشريعة ولاية تبسة طالبة جامعية في طور الماستر تخصص حقوق بجامعة الشيخ العربي التبسي –تبسة - .

- أتعهد بشرفي أن استعمل الاحصائيات الرقمية المطلوبة الخاصة حول "**معلومات إحصائية حول الابتزاز عبر مواقع التواصل الإجتماعي خلال ثلاث سنوات الأخيرة** حسب الجدول الآتي :

السنة	عدد القضايا
2023	03
2022	03
2021	05

لغرض اعداد مذكرة التخرج ، لا غير مع عدم نشرها في أي صحيفة كانت مكتوبة أو إلكترونية أو التصريح بها لأي وسيلة إعلامية مهما كان نوعها .

المعنية بالأمر

الختم والتوقيع

ضابط شرطة رئيسي
تيقاني توفيق

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر:

التشريع الأساسي:

1. المرسوم الرئاسي 20-442 الصادر في 30 ديسمبر 2020 ح.ل 82 لسنة 2020 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020.

القوانين:

1. القانون 20-05 المؤرخ في 5 رمضان علم 1441 هـ الموافق لـ 28 أفريل سنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها الصادر في ج ر ج ج بتاريخ 06 رمضان 1441 هـ الموافق لـ 29 أبريل 2020 العدد 25.
2. من ق 09-04 في فقرته هـ التي عرفت أيضا مراقبة الاتصالات الالكترونية.
3. قانون رقم 4-15 مؤرخ في 10-11-2004 قانون عدل وتمم الأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71، صدر بتاريخ 10-11-2004 معدل ومتمم.

الأوامر:

1. أمر رقم 66-156 مؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84 معدل ومتمم وفقا للقانون 06-02 المؤرخ في 20 جويلية 2006.

المراسيم:

1. المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 53 بتاريخ 8 أكتوبر 2015.

ثانيا: المراجع

I) الكتب:

1. أحمد مختار عبد الحميد عمر، معجم اللغة العربية المعاصرة، ط1، ج1، دار عالم الكتب، الرياض، 2008.
2. أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الأولى، 2011، مكتبة الوفالي القانونية، الإسكندرية.
3. خالد ممدوح ابراهيم، الجرائم المعلوماتية الطبعة الاولى، دار الفكر الجامعي، الاسكندرية، 2009.
4. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكتروني، دار الفكر الجامعي، الاسكندرية، 2010.

5. الشحات ابراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية تحت فقه مقارن، ط1، دار الفكر الجامعي، الإسكندرية.
6. عز الدين طباش، شرح القسم الخاص من قانون العقوبات، جرائم ضد الأشخاص والأموال، د ط، دار بلقيس، دار البيضاء الجزائر.
7. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان الجزائر.
8. محمد الأمين الشري، التحقيق في الجرائم المستحدثة، ط1، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004.
9. محمود أحمد عبانية، جرائم الحاسوب وأبعادها الدولية، ط 1، الإصدار الأول 2004، الطبعة 2، الإصدار 2، 2009، دار الثقافة للنشر والتوزيع، عمان.
10. مهد علي قطب: الجرائم المستحدثة وطرق مواجهتها، قراءة فن المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية، ط1، دار الفجر للنشر والتوزيع.
11. نبيل صقر، الوسيط في جرائم الأشخاص، دار الهدى، عين مليلة–الجزائر، 2009.
12. نهلا عبد القادر المومني: الجرائم المعلوماتية، ط 2، دار الثقافة للنشر والتوزيع، عمان–الأردن، 2010.

II) المجلات:

1. إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، العدد العاشر، الجزائر.
2. آيت حمودة كاهنة: البحث والتحري الجنائي في مسرح الجريمة الالكترونية، مجلة الفكر القانوني والسياسي، المجلد 7، العدد 1، جامعة حسيبة بن بوعلي، الشلف 2023.
3. باقر غازي–حسن حماد حميد، جريمة الابتزاز الالكتروني (دراسة مقارنة)، كلية القانون جامعة البصرة، مجلة دراسات البصرة، ملحق العدد 42، 2021.
4. بن عودة صليحة، الشروع في الجرائم المعلوماتية بين الوقاية والردع، المجلد 1، العدد 2، سنة 2021.
5. بوشارب هانية، بن شهرة شول، صعوبة عملية استخلاص الدليل الالكتروني، مجلة الدراسات القانونية والسياسية، المجلد 9، العدد 1، جانفي 2023.
6. بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية، جامعة المسيلة، العدد 11، 2018.
7. خطوى مسعود، عكوش حنان، خصوصية الدليل الالكتروني، مجلة الفكر القانوني والسياسي، المجلد 7، العدد الأول، جامعة عمار ثلجي الأغواط، الجزائر.

8. راسي أحمد غالي: جريمة الابتزاز الالكتروني وآلية مكافحتها في جمهورية العراق، مقال منشور في مجلة ثقافتان الامنية، الإصدار الثاني وزارة الداخلية العراقية دار الكتب والوثائق بغداد، 2019.
9. راضية عيمور، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد السادس، العدد الأول، جامعة الأغواط الجزائر.
10. زواوي الحماية القانونية للحق في جريمة المحادثات الهاتفية، كلية الحقوق والعلوم السياسية، مخبر المرافق العامة والتنمية، جامعة جيلالي سيدي بلعباس الجزائر، العدد 19، جوان 2018.
11. سلمان في عبد الرزاق الغديان، خطاطبة يحي بن مبارك النهيمي عز الديب عبد الله عواد، جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين و رجال الهيئة والمستشارين النفسيين مجلة البحوث الأمنية المجلد 27 العدد 69، 2018.
12. شريق محمد السويدي، ...مصطفى نوفل، أسباب الابتزاز الالكتروني والآثار الاجتماعية والنفسية المرتبطة به (دراسة كيفية) جامعة الشارقة/ مجلة الأدب، العدد 146، سنة 2022.
13. عبد الناصر محمد محمود فرغلي، عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، ورقة بحثية مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي المنعقد بالرياض 12-14 نوفمبر 2008.
14. عراب مريم، جريمة التهديد والابتزاز الالكتروني، المجلد 7، العدد 1، مجلة الدراسات القانونية المقارنة.
15. عز الدين عثماني: إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع، 2018، تبسة.
16. عيدة بلعايد، خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية جامعة مولاي الطاهر، سكيكدة، العدد 06، 2011.
17. فلاح عبد القادر-آيت عبد الله نادية التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة حميس مليانة، مجلد 04، العدد 02، 2019.
18. قردان مصطفى، زرقين عبد القادر: الآليات الدولية لمكافحة الجريمة الإلكتررونية، مجلة صوت القانون، المجلد 8، العدد 02، الجزائر.
19. قلات سومية، حاجة عبد العالي مقتضات المعاينة المعلوماتية في التشريع الجزائري، مجلة الحقوق والحريات، المجلد 11، العدد 1، كلية الحقوق والعلوم السياسية جامعة بسكرة، 2023.
20. مجدوب نوال، الآليات الإجرائية للكشف عن الجريمة المعلوماتية مجلة البحوث القانونية والاقتصادية، المجلد 6، العدد 3، مغنية الجزائر.

21. المسند صالح بن محمد، المهني عبد الرحمن بن راشد جرائم الحاسب الآلي، الخطر الحقيقي في عصر المعلومات المحلية العربية للدراسات الأمنية والتدريب، المجلد 15 العدد 29، الرياض 2015.
22. ممدوح رشيد مشرف الرشيد العنزي، الحماية الجبائية للمجني عليه من الابتزاز (مقال منشور على شركة الأنترنات) المحلية العربية للدراسات الأمنية، مجلد –33– العدد 70، الرياض، 2017.
23. مولاي ابراهيم عبد الحكيم، الجرائم الالكترونية مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشو الجلفة الجزائر، العدد 23، المجلد 2.
24. نعيمي أسماء (سلمى): مقال حول الابتزاز والتشهير الالكتروني وعقوبته في القانون الجزائري تفاقم جنح التهديد بالابتزاز والتشهير في ظل الرقمية والالكترونيات، 1 فبراير 2024 آخر تنقيح الصدور في 14 أكتوبر 2016.

III) الرسائل والمذكرات:

1. أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال على ضوء ق 09–04، مذكرة لنيل شهادة ماجستير كلية الحقوق جامعة ورقلة 2013.
2. بوشعرة أمينة، اوي سهام، الإطار القانوني للجريمة الالكترونية مذكرة ماستر جامعة عبد الرحمان ميرة بجاية، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، 2017–2018.
3. ثامر أمال: إثبات الجرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية والإجرامية، كلية الحقوق جامعة سعد دجلة البليدة، جوان 2012.
4. ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونننية دراسة تأصيلية تطبيقية، رسالة ماجستير جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.
5. الحميد عبد العزيز بن دمين بن أحمد، الابتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الابتزاز (المفهوم، الأسباب والعلاج) جامعة الملك سعود، 2014.
6. حور الهدى محمودي، حجية الدليل الرقمي ف إثبات الجريمة المعلوماتية باحثة (كنوراء جامعة باتنة 1).
7. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص جامعة أبو بكر بلعايد، تلمسان 2018.
8. الزريق خليفة بن على بن محمد، استقرار الأحداث وعقوبته في النظام السعودي (دراسة تأصيلية مقارنة تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015.
9. سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012.

10.سعيداني نعيم، آليات البحث والتحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماستر في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة الحاج لخضر باتنة، 2012- 2013.

11.سيد محمد الشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية –دراسة تحليلية تطبيقية– رسالة ماجستير، جامعة نايق العربية للعلوم الأمنية السعودية، 2010.

12.صغير يوسف، الجريمة الالكترونية المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولود معمري تيزي وزو، 2013.

13.محمد بن عبد المحسن بن شلهوب، جريمة الابتزاز الالكتروني دراسة مقارنة بحث تكميلي لنيل درجة الماستر في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الأنظمة جامعة الإمام محمد بن سعود الإسلامي.

IV) المراجع الأجنبية:

1. Steve Bunting and william Wei, Enease computer farenxic, writey publishing (inc) United states of America 2006, page 371

V) المواقع الالكترونية:

1. ***WWW.NOOR BOOK.COM***
2. ***https://ethna tanay TV***
3. ***https://ethna tanay TV***
4. ***www.searint.sa/extortion.types***
5. ***www.searint.sa/extortion.types***
6. ***www. Arageek.com***
7. ***www.ech.chaab.com***
8. ***https :mail.almerja.com***

فهرس المحتويات

فهرس المحتويات

العنوان	الصفحة
بسملة	/
شكر والعرفان	/
مقدمة	01
الفصل الأول: الأحكام الموضوعية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي	
المبحث الأول: ماهية الابتزاز عبر مواقع التواصل الاجتماعي	06
المطلب الأول: مفهوم الابتزاز عبر مواقع التواصل الاجتماعي	06
الفرع الأول: تعريفه	06
الفرع الثاني: أسبابه وصوره	10
المطلب الثاني: وسائل الابتزاز عبر مواقع التواصل الاجتماعي والآثار المترتبة عنه	16
الفرع الأول: وسائل الابتزاز عبر مواقع التواصل الاجتماعي	17
الفرع الثاني: الآثار المترتبة عنه	26
المبحث الثاني: التنظيم القانوني لجريمة الابتزاز عبر مواقع التواصل الاجتماعي والعقوبات المقررة لها	28
المطلب الأول: أركان جريمة الابتزاز عبر مواقع التواصل الاجتماعي	28
الفرع الأول: الركن الشرعي	28
الفرع الثاني: الركن المادي	32
الفرع الثالث: الركن المعنوي	35
المطلب الثاني: العقوبات المقررة لها	37
الفرع الأول: عقوبة الشروع والاشتراك في جريمة الابتزاز عبر مواقع التواصل الاجتماعي	37
الفرع الثاني: العقوبات الأصلية والتكميلية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي	41
الفرع الثالث: عقوبات التشديد والإعفاء من جريمة الابتزاز عبر مواقع التواصل الاجتماعي	43
ملخص الفصل الأول	46
الفصل الثاني: القواعد الإجرائية لجريمة الابتزاز عبر مواقع التواصل الاجتماعي	
المبحث الأول: إجراءات التحقيق للحصول على الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي	49
المطلب الأول: القواعد الإجرائية التقليدية والحديثة في الحصول على الدليل الرقمي	49
الفرع الأول: القواعد الإجرائية التقليدية في الحصول على الدليل الرقمي لجريمة الابتزاز عبر مواقع التواصل الاجتماعي	54

الفرع الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الإلكتروني	54
المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في تحصيل الدليل الرقمي في جريمة الابتزاز عبر مواقع التواصل الاجتماعي	60
الفرع الأول: صعوبات مرتبطة باكتشاف الجريمة المرتكبة عبر الانترنت	60
الفرع الثاني: صعوبات متعلقة بالجانب القضائي والتعاون الدولي	63
المبحث الثاني: إثبات جريمة الابتزاز عبر مواقع التواصل الاجتماعي وآليات مكافحتها	67
المطلب الأول: موقع الدليل الرقمي من الأدلة الجنائية	67
الفرع الأول: مفهوم الدليل الرقمي	67
الفرع الثاني: أشكال الدليل الرقمي وشروط صحة قبوله كحجية في الإثبات	69
الفرع الثالث: مصادر تحصيل الدليل الرقمي والصعوبات التي تعترضه في ذلك	72
المطلب الثاني: آليات مكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي	74
الفرع الأول: الجهود الدولية لمكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي	74
الفرع الثاني: الجهود الوطنية لمكافحة جريمة الابتزاز عبر مواقع التواصل الاجتماعي	77
ملخص الفصل الثاني	82
خاتمة	84
قائمة المصادر والمراجع	88
ملخص	/

الملخـــــــــــص

عالجت هذه الدراسة جريمة الابتزاز عبر مواقع التواصل الاجتماعي في النظام القانوني الجزائري، وقد تطرقنا في البداية لهذه الجريمة كصورة من صور الجريمة الالكترونية بعرض تعريف لها وتبيان صورها واثارها وطرق ارتكابها والوسائل الحديثة المستخدمة في ارتكاب وتنفيذ هذه الجريمة بعرض اركانها، كما ان الدراسة سلطة الضوء الاثار المترتبة عنها

كان عرض جريمة الابتزاز بالتطرق الى الاركان مكونة لها، الركن الشرعي، الركن المادي والركن المعنوي وكذا عرض العقوبات المقررة لجريمة الابتزاز عبر مواقع التواصل الاجتماعي ولحالات التشديد والاعفاء ولعقاب الشروع والمساهمة الجنائية فيها.

تعالج الدراسة ايضا الاشكالات التي تثيرها جريمة الابتزاز عبر مواقع التواصل الاجتماعي من الناحية الاجرائية من اجراءات التحقيق وخصوصية هذه الاجراءات التي بدورها تواجهها عراقيل وصعوبات تعترض هذه الجهات في تحصيل الدليل

كما نتعرض من خلال هذه الدراسة لاهم طرق الاثبات التي تخص جريمة الابتزاز عبر الوسائل الالكترونية وهو ما نعنى به الدليل الرقمي والوقوف على ماهيته، اقسامه، شروطه وطرق تحصيله والتعامل معه كدليل للإثبات.

كما انا الدراسة لم تغفل الجهود الدولية والوطنية التي تعمل جاهدة لمحاربة هذا النوع من الاجرام الذى اصبح يهدد ويؤرق المجتمع والفرد على حد السواء

Abstract:

This research investigated the crime of blackmail via social networking sites in Algerian law. We first addressed this crime as a type of electronic crime by providing a definition, describing its forms, consequences, ways of its commission, and exhibiting the current tools used in committing and executing it. The study also gives light on the resultant repercussions.

The crime of blackmail was presented by addressing its constituent elements, the legal, material, and moral elements, as well as the penalties prescribed for blackmail via social media sites, aggravation and exemption cases, and the punishment for attempt and criminal contribution.

The research also tackles the issues created by the crime of blackmail via social networking sites from the procedural aspect of investigation procedures and the peculiarity of these procedures, which are then confronted with impediments and challenges that these parties experience in gathering evidence.

This research also examines the most important ways of proof connected to the crime of blackmail via electronic means, which we refer to as digital evidence, and determines it, its sections, conditions, and methods of collecting and dealing with it as evidence of proof.

The research also did not disregard international and national efforts to tackle this sort of crime, which has become a menace and source of concern for both society and individuals.