الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

المركز الجامعي عبد الحفيظ بوالصوف ميلة

معهد الحقوق

شعبة : حقوق

القسم: قسم الحقوق

الرقم التسلسلي: .....

الرمز: ..... التخصص: قانون جنائي

مذكرة بعنوان:

جريمة الابتزاز عبر الوسائل الالكترونية في التشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر

تخصص " قانون جنائي "

إعــداد الطالبتين:

حداد شيماء

جبلي سعيدة

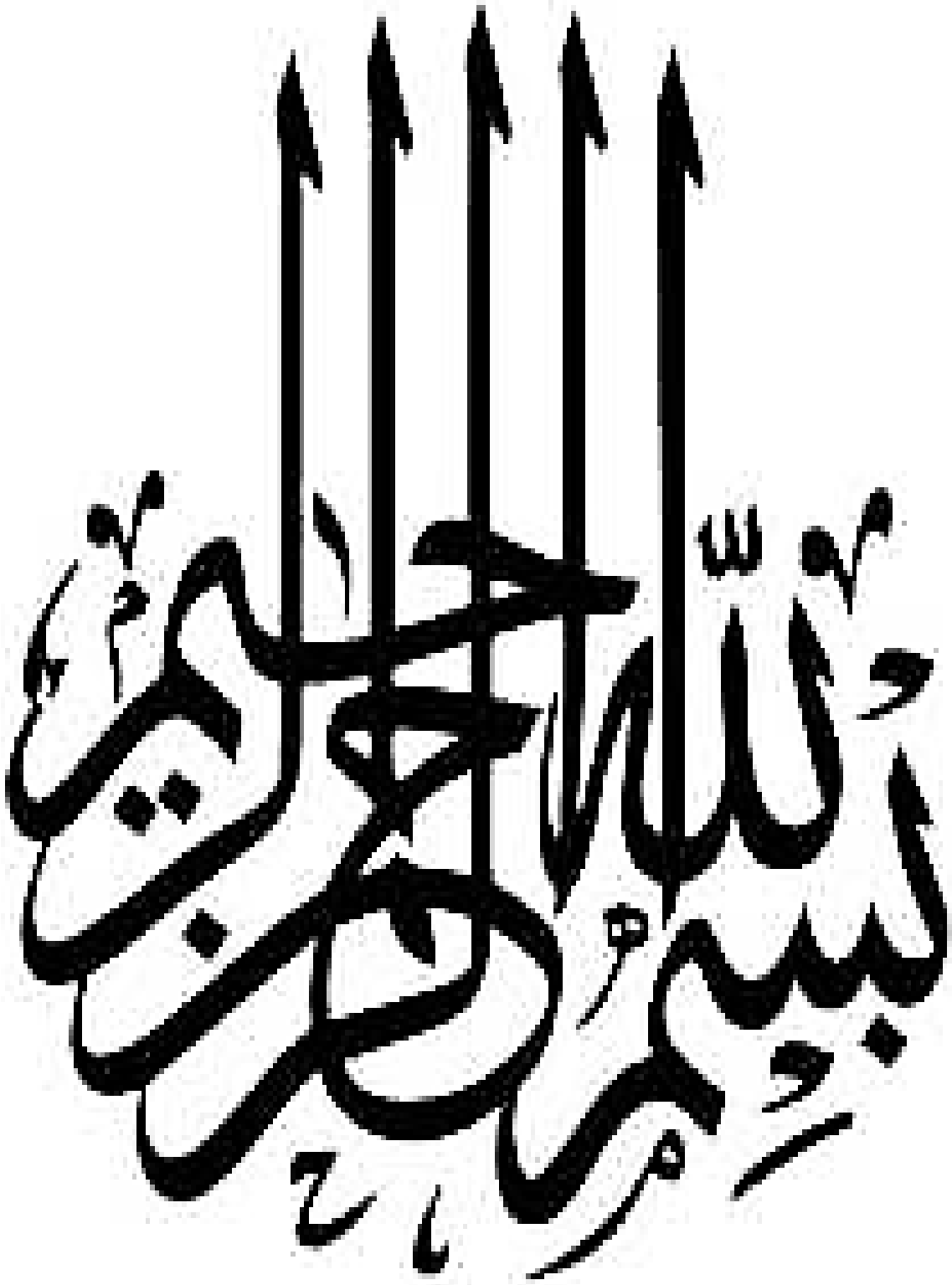
تحت إشراف:

د/ بن خدة عيسى

لجنة المناقشة

اسم ولقب الأستاذ	الجامعة	الرتبة	الصفة
أ. فضيل شريط	المركز الجامعي عبد الحفيظ بوالصوف ميلة	أستاذ محاضر	مناقشا
أ عيسى بن خدة	المركز الجامعي عبد الحفيظ بوالصوف ميلة	أستاذ محاضر	مشرفا ومقررا
أ بولعراس أحمد	المركز الجامعي عبد الحفيظ بوالصوف ميلة	أستاذ مساعد	رئيسا

السنة الجامعية 2025/2024



الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

المركز الجامعي عبد الحفيظ بوالصوف ميلة

معهد الحقوق

شعبة : حقوق

القسم: قسم الحقوق

الرقم التسلسلي: .....

الرمز: ..... التخصص: قانون جنائي

مذكرة بعنوان:

جريمة الابتزاز عبر الوسائل الالكترونية في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر

تخصص " قانون جنائي "

إعــداد الطلبة:

جبلي سعيدة

حداد شيماء

تحت إشراف:

د/ بن خدة عيسى

السنة الجامعية 2025/2024

شكر وتقدير

شكر وتقدير

الشكر الأول والأخير لله العلي العظيم الذي وفقنا لإتمام هذا العمل المتواضع نحمده كل الحمد على مدنا بالصحة والعزيمة لإتمامه رغم الظروف الصعبة... فما كان لشيء أن يجري في ملكه إلا بمشيئته جل شأنه

يشرفنا أن نتقدم بجزير الشكر ووافر الامتنان إلى الأستاذ الفاضل "بن خدة عيسى" الذي قبل الاشراف على هذه المذكرة ووجهنا لاختيار هذا الموضوع وشجعنا على البحث فيه، وبتوجيهاته السديدة والقيمة ورحابة صدره، وطول صبره، كان بحق نعم الناصح والمرشد في اتمام هذا العمل واثراءه

جزاكم الله خيرا أستاذي... وأدامكم فخرا للجامعة الجزائرية

كما نتوجه بالشكر إلى أعضاء لجنة المناقشة على تحملهم عناء قراءة وتصحيح وإثراء هذه المذكرة

كما يطيب لنا أن نتقدم بالشكر الجزيل إلى كل أسرة معهد الحقوق من أساتذة، طلبة وعمال

والشكر لكل من قدم لنا يد العون والمساعدة من قريب أو بعيد

إهـــداء

الحمد لله الذي بنعمته تتم الصالحات، وبفضله تشرق شموس العلم والمعرفة وبتوفيقه تثمر الجهود وتتكلل المساعي بالنجاح. الحمد لله عدد ما خط القلم، وعدد ما جاد الفكر، وعدد ما ترددت أصداء العلم في أروقة الزمن. إن هذا العمل بكل ما حواه من جهد، وبكل ما تطلبه من صبر، لم يكن ليرى النور لولا فضل الله وتوفيقه، ثم عطاء نفوس كريمة بذلت وأعطت، وآمنت بأن للعلم رسالة، وللمعرفة قيمة لا تضاهيها كنوز الأرض.

وإن أول ما يفرضه الوفاء، أن أزجي وافر الشكر والامتنان إلى من كان لهم الفضل الأول بعد الله في وصولي إلى هذا المقام، والدي الكريمين، اللذين كانا لي السند الذي لا يميل، والركن الذي لا ينهدم. إليكما، يا من غرستما في نفسي حب العلم والاجتهاد ويا من سقيتماني من معين العطاء بلا حساب أقدم ثمرة هذا الجهد، فمهما قلت. ومهما سطرت، ستظل حروفى عاجزة عن رد بعض فضلكما

كما أتوجه بعميق التقدير إلى إخوتي الأعزاء، **" فريد "أحمد"، مولود"، مريم"، نُزهة"، شيماء"**، وإولادهم فلذة كبدي، **"تاج الدين"، سراج" براءة"**، الذين كانوا لي عزوة وقوة، وكان دعمهم معينا لا ينضب، فكنتم المرفأ الأمن في متاهات التعب، وكنتم اليد التي ت متد لترفعني حين تضعف العزائم.

إلى من شاركني فرحة عمري، وإنتظر هذه اللحظة ليفخر بي. قوتي وسندي وشريكي في الحياة **"وحيد"**

إلى من شاركتني وتحملت معي مشقة إتمام هذه المذكرة إلى الأخت والصديقة الوفية والغالية **شيماء حداد"**

إلى كل الأهل والأقارب إلى جميع الأصدقاء والأحباب

إلى كل الذين وسعهم قلبي ولم تسعهم هذه السطور لذكرهم

وختامًا، أسأل الله العظيم أن يجعل هذا العمل نافعًا، وأن يكون لبنة تضاف إلى صرح العلم، وأن يجعله شاهدًا على جهد بذل فى سبيل المعرفة، ورمزا للإصرار والمثابرة. فإن أصبت فذلك بفضل الله ومنه، وإن أخطأت فحسب الإنسان أنه اجتهد وسعى والله ولي التوفيق، وهو نعم المولى ونعم النصير

سعيدة

إهداء

الحمد لله الذي بنعمته تتم الصالحات، وبفضله تشرق شموس العلم والمعرفة وبتوفيقه تثمر الجهود وتتكلل المساعي بالنجاح. الحمد لله عدد ما خط القلم، وعدد ما جاد الفكر، وعدد ما ترددت أصداء العلم في أروقة الزمن. إن هذا العمل بكل ما حواه من جهد، وبكل ما تطلبه من صبر، لم يكن ليرى النور لولا فضل الله وتوفيقه، ثم عطاء نفوس كريمة بذلت وأعطت، وآمنت بأن للعلم رسالة، وللمعرفة قيمة لا تضاهيها كنوز الأرض.

الى أمي الراحلة من حياتي، الحاضرة في قلبي، وفي لحظة طالما حلمتِ أن تريها، إلى من كانت سندي، ودعائي، ونبض قلبي، إلى من علمتني كيف أؤمن بنفسي وأسعى لما أُريد، فأنت السبب وانتِ الفخر، وإنتِ الأمل الذي لا يغيب، رحمكِ الله.

إلى من علمني الصبر ومعنى التحدي وغرس في نفسي وقلبي الأمل والثقة والدي العزيز أطال الله عمره وحفظه من كل شر

كما أتوجه بعميق التقدير إلى إخوتي الأعزاء عزيز، خولة، منار، داود ومصباح المنزل آية، الذين كانوا لي عزوة وقوة، وكان دعمهم معينا لا ينضب، فكنتم المرفأ الأمن في متاهات التعب، وكنتم اليد التي تمتد لترفعني حين تضعف العزائم.

إلى من شاركتني وتحملت معي مشقة إتمام هذه المذكرة إلى الأخت والصديقة الوفية والغالية "سعيدة جبلي"

إلى كل الأهل والأقارب إلى جميع الأصدقاء والأحباب

إلى كل الذين وسعهم قلبي ولم تسعهم هذه السطور لذكرهم

وختامًا، أسأل الله العظيم أن يجعل هذا العمل نافعًا، وأن يكون لبنة تضاف إلى صرح العلم، وأن يجعله شاهدًا على جهد بذل فى سبيل المعرفة، ورمزا للإصرار والمثابرة. فإن أصبت فذلك بفضل الله ومنه، وإن أخطأت فحسب الإنسان أنه اجتهد وسعى والله ولي التوفيق، وهو نعم المولى ونعم النصير

شيماء

قائمة المختصرات

ط	الطبعـة
ب س	بدون سنة
ق إ ج	قانون الإجراءات الجزائية
ق ع ج	قانون العقوبات الجزائري
ج ر	الجريدة الرسمية
ع	العدد
م	المجلد
ص	الصفحـة

.

المقدمة

المقدمة:

تداول البعض قولاً مفاده بأن من يملك حاسوباً أو وسيلة تقنية ذكية وخدمة أنترنت، بات يملك من النفوذ والقوة ما يعادل سلطة قائد عسكري يقود فيلقاً من مئات الجنود والمعدات في زمن الحرب العالمية الأولى، ولأول مرة في تاريخ البشرية، أصبحت المعرفة البوابة الأوسع والأسرع للوصول إلى النفوذ وكسب الأموال، سواء بطرق مشروعة عبر الاقتصاد المعرفي أو بطرق غير مشروعة من خلال الاستغلال السيء للفضاء الرقمي الذي تحول إلى منجم حقيقي مليء بالفرص الحديثة والمتنوعة وفي الوقت نفسه إلى مكب ضخم تتبعت منه روائح الجرائم الإلكترونية والانحرافات الأخلاقية والتي بات من الضروري التصدي لها والوعي بخطورتها.

وفي ظل الانفجار المعرفي والتكنولوجي الذي شهده العالم من خلال العقود الأخيرة شهد تطورات كبيرة وسريعة في استخدام الأنترنت ووسائل التواصل الاجتماعي الذي توافدت عليها جميع الفئات العمرية، هذا التطور فتح أبواب واسعة وآفاقاً للتفاعل والتواصل بين الأفراد من جميع أنحاء العالم حتى أصبح العالم كأنه ساحة واحدة يتقاسم فيها الأفراد الحديث والتبادل الثقافي بشكل مستمر دون أن تكون هناك حدوداً وقيود يفرضها الزمان والمكان في ظل الانفتاح الواسع على العالم الرقمي أصبح من الضروري التفطن للتحديات التي قد يترتب عليها بالخصوص فيما يتعلق بلامان الرقمي والخصوصية.

وكما هو الحال في أي تقدم تكنولوجي فإن التطورات لم تأتي صفر خالية من التحديات والمخاطر، فقد كان لهذه التحولات ولادة جديدة صنعت من التقنيات المتقدمة بيئة خصبة لظهور انواع جديدة من الجرائم، ومن أبرز هذه الجرائم التي ترعرعت في ظل التقدم التكنولوجي نجد الجرائم الإلكترونية بشكل عام وبشكل خاص مثل جريمة الابتزاز الإلكتروني، والتي أصبحت تشكل تهديداً للمستخدمين حول العالم.

وتعد جريمة الابتزاز الإلكتروني أو كما يطلق عليها البعض "**جريمة أصحاب الياقات البيضاء**" من الجرائم المستحدة نسبياً، حيث تقوم بها فئات معينة واستغلال تقنيات متطورة واستخدامها لتنفيذ مخططاتهم الدنيئة ضد فئات أخرى، يجعلون منها فرصة للاستغلال من خلال التهديد أو نشر صور ومقاطع فيديو يندم لها الجبين، او باختراق الحسابات الشخصية أو استخدام برامج التجسس ومراقبة الضحايا والتواصل معهم بطرق خفية وسرية.

ونجد الكثير من الأشخاص، وخصوصاً فئة الشباب والمراهقين، وينشرون معلوماتهم الشخصية وخصوصياتهم على الأنترنت بشكل مفرط ودون وعي بالمخاطر المحدقة بهم وهنا تكمن المشكلة الأكبر،

كما نرى بعض أيضا في الجانب الآخر بعض الأطفال يتعاملون مع هذا الفضاء الرقمي بكل عفوية مفرطة دون رقابة أو رعاية وتوجيه مما يجعلهم طعم سهل للاستغلال وسبب لهم أضرار نفسية ومعنوية كبيرة.

وفي ظل هذا التضخم التكنولوجي المتسارع، والانتشار الواسع لجرائم الابتزاز الإلكتروني عبر الشبكة المعلوماتية، ووسائل التواصل الاجتماعي وتزداد أهمية التصدي لهذه الظاهرة علمياً وقانونياً فالآليات القانونية المتاحة تُعني بحماية خصوصية الأفراد، من خلال ردع أفعال الابتزاز التي تهدد سلامة الضحايا وأمنهم وتدفعهم إلى القيام بأفعال قسرية.

كما تعد القوانين الجزائية رادعاً متيناً للمجرمين، وتحرمهم من تحقيق أهدافهم النتنة وتُسهم في نشر الوعي المجتمعي بمخاطر هذه الجريمة، وتساعد الإجراءات في تفطين وعي الضحايا نحو التمسك بالاستشارة القانونية المناسبة للتعامل مع حالات الابتزاز، وتعزيز سبل الوقاية والحماية في الفضاء الرقمي المظلم.

تنبع أهمية هذه الدراسة من التركيز على ظاهرة مستحدثة تُعد من أبرز التحديات في العصر الرقمي وهي جريمة الابتزاز الإلكتروني والتي مدت ظلالها بشكل متزايد وارتبطت ارتباطا وثيقاً بتكنولوجيا الشبكة المعلوماتية ووسائل التواصل الاجتماعي، وهذه الجريمة نرى خصائصها التي تختلف عن الجرائم التقليدية سواء من جانب الوسائل أو طبيعة الأفعال مما يستدعي التعامل معها بما يتناسب مع طبيعتها سواء من الناحية القانونية والتقنية.

ومن هذا المنطلق تبرز الحاجة إلى التقسيم والمراجعة للنصوص القانونية ذات الصلة بتجريم أفعال الابتزاز الإلكتروني والوقوف إلى مدى جهودها في مكافحة هذا النوع من الجرائم والتصدي له بفعالية.

وجاء اختيارنا لهذا الموضوع بدافع شخصي أولاً وعلمي ثانٍ، فمن الناحية الذاتية، فإن الانتشار المتزايد لهذه الجريمة أثار لدينا الرغبة القوية والتعمق في هذا المجال، خاصة اننا كغيرنا من أفراد المجتمع، قد نكون نحن، أو أحد أفراد عائلتنا أو أحد معارفنا عرضة للوقوع ضحية لهذه الجريمة المستترة التي تنمو في الخفاء، ومن هذا المنطلق أردنا التزود بالمعرفة القانونية والواقعية التي تمكننا من فهم جل أبعادها وكيفية الوقاية منها.

وبالرجوع إلى الناحية الموضوعية، فإن السبب اختيار هذا الموضوع يرجع إلى الواقع الاجتماعي الحساس الذي ينتمي له مجتمعنا العربين إلى بيئة محافظة تُعلي من شأن الشرف والسمعة والروابط الأسرية، وهو ما يجعل الابتزاز الإلكتروني تهديداً حقيقاً لأمن الاسرة واستقرارها.

ومن هنا جاءت هذه الدراسة كمساهمة علمية تهدف إلى تحليل الظاهرة قانونياً وتوعية المجتمع بخطورتها واستكشاف آليات الردع والتصدي لها.

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف العلمية والعملية من أبرزها:

- فهم جريمة الابتزاز الإلكتروني والوقوف على أسباب تصاعدها.
- التعرف على خطورة هذه الجريمة على الأفراد والمجتمعات وتأثيراتها.
- تحليل طرق ارتكابها والأساليب المستخدمة من طرف الجناة.
- التعرف على هوية الجناة وكيفية تتبعهم وكشفهم.
- التعرف على كيفية اكتشاف الجريمة والتحقيق فيها من قبل الجهات المختصة.
- تقييم مدى كفاية وفعالية النصوص القانونية الموضوعية والإجرائية الحالية في التصدي لجريمة الابتزاز الإلكتروني.

وتكمن الأهداف المرجوة من هذه الدراسة هي الوصول إلى الأشخاص والجهات المستخدمة للتكنولوجيا بغرض الابتزاز بكافة أشكالها ومدى خطورتها.

وبناءاً على الحاجة الملحة لوضع هذا الموضوع موضع دراسة وتحليل، ينبني ذلك على الإجابة على إشكالية الدراسة المتمثلة في: إلى أي مدى وفق المشرع الجزائري في مكافحة جريمة الابتزاز عبر الوسائل الالكترونية؟

ومن هنا تتفرع عدة مشكلات فرعية والتي تنتج عنها هذه الأسئلة الآتية:

- ما المقصود بجريمة الابتزاز الإلكتروني؟
- ما هي أركانها ومدى خطورتها؟
- ما هي أسباب جريمة الابتزاز وآثارها؟
- ما هي أنواعها وصورها؟
- ما هي طرق الابتزاز الإلكتروني؟
- ما هي الإجراءات المتعلقة بالتحقيق في جريمة الابتزاز الإلكتروني؟
- ما هي أدلة الإثبات الجنائي في جريمة الابتزاز الإلكتروني؟

وعلى هذا الأساس اعتمدنا عل المنهج الوصفي لوصف الجريمة من خلال تعريفها، وآثارها ووسائل ارتكابها، والمنهج التحليلي معتمدين على تحليل المواد التي تناولناها، ذلك لأن الدراسة تهتم بالجرائم المرتكبة في هذا العصر ووصف خطورتها وأسبابها.

وحتى نتمكن من معالجة الإشكالية المطروحة التي أدت إلى تقسيم الخطة إلى فصلين، الفصل الأول بعنوان الإطار المفاهيمي لجريمة الابتزاز الإلكتروني، وقد تناولنا في المبحث الاول منه ماهية جريمة

الابتزاز عبر الوسائل الإلكترونية، أما الفصل الثاني منه تجريم الابتزاز الإلكتروني عبر الوسائل الإلكترونية، أما الفصل الثاني فقد كان بعنوان الإجراءات المتبعة في التحقيق وأدلة الإثبات الجنائي في جريمة الابتزاز عبر الوسائل الإلكترونية ن الذي يحتوي على مبحثين الأول بعنوان التحقيق في جريمة الابتزاز الإلكتروني من الضبطية القضائية إلى المحاكمة، أما المبحث الثاني فتناول أدلة الإثبات الجنائي في جريمة الابتزاز عبر الوسائل الإلكترونية.

ولا يفوتنا القول أنه تلقينا صعوبات كثيرة في اختيار موضوع البحث في حد ذاته كونه حديث لم يسبق البحث فيه بوضوح وتعمق ولو أن هناك مشكلة في نقص المراجع والمقالات التي تناولت هذا الموضوع من كل جوانبه إضافة إلى أن هذه الجريمة محل الدراسة ترتبط بالحاسب الآلي مما يتطلب الإلمام بمكوناته وبنظام المعالجة الآلية للمعلومات.

الدراسات السابقة:

تناولت الدراسات السابقة جريمة الابتزاز الإلكتروني في الجزائر من عدة زوايا:

- دراسات عامة ركّزت على الجرائم الإلكترونية بشكل شامل، وأشارت إلى قصور التشريع الجزائري في مواجهة الجرائم الرقمية الحديثة.
- دراسات متخصصة أبرزت أن الابتزاز الإلكتروني لا يُعالج بشكل صريح في القانون، مما يخلق إشكالات في التكييف والإثبات، خاصة في جرائم الابتزاز عبر مواقع التواصل.
- دراسات مقارنة بيّنت تفوّق بعض التشريعات الأجنبية (مثل الفرنسية) في معالجة الجريمة رقمياً، ودعت إلى تحديث قانون العقوبات الجزائري.

الفصل الأول

الإطار المفاهيمي لجريمة الابتزاز عبر الوسائل الإلكترونية

الفصل الأول: الإطار المفاهيمي لجريمة الابتزازعبر الوسائل الإلكترونية

مع التطور الكبير الذي عرفه العالم في مجال التكنولوجيا والاتصالات، أصبحت حياتنا اليومية مرتبطة بشكل مباشر بمختلف الوسائل الإلكترونية، سواء في العمل أو الدراسة أو حتى في العلاقات الاجتماعية. ورغم الإيجابيات العديدة التي جاءت بها هذه الوسائل، إلا أنها فتحت المجال أيضًا لظهور نوع جديد من الجرائم، يُعرف بالجرائم الإلكترونية، والتي أصبحنا نسمع عنها كثيرًا في حياتنا اليومية من بين هذه الجرائم، تبرز جريمة الابتزاز عبر الوسائل الإلكترونية، التي أصبحت تهدد فئة كبيرة من الناس، خاصة مع الانتشار الواسع لمواقع التواصل الاجتماعي. حيث يعمد بعض الأشخاص إلى استغلال صور أو معلومات شخصية للضحايا، وتهديدهم بنشرها مقابل المال أو للحصول على خدمات معينة، وهو ما يخلف آثارًا نفسية واجتماعية خطيرة على الضحايا، هذه الجريمة، وإن كانت حديثة من حيث الوسيلة، إلا أن خطورتها دفعت المشرّع الجزائري إلى محاولة ضبطها قانونيًا، من خلال إدراج نصوص تعاقب عليها، ومحاولة مواكبة التطور التكنولوجي الحاصل..

انطلاقًا من هذا الواقع، سنحاول في هذا الفصل التمهيدي تسليط الضوء على ماهية جريمة الابتزاز عبر الوسائل الإلكترونية في المبحث الأول، ونتعرف على أركانها القانونية وكيف تناولها القانون الجزائر وذلك في المبحث الثاني الذي جاء بعنوان تجريم الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري.

المبحث الاول: ماهية جريمة الابتزاز عبر الوسائل الإلكترونية.

تعرف ظاهرة الابتزاز الإلكتروني أنها من الظواهر الجديدة التي تفرض نفسها أمام المجتمعات، حيث أن اول ظهور لها كان نتيجة التطور الإلكتروني وتوسع شبكة الأنترنت، حيث نرى رغم محاسن هذا الجانب من التطور وفائدته على المجتمعات نتج عنه افعال خدشت بأصول المجتمع كله بدون استثناء وأخدت عدة أبعاد من بينها المساس بأمن وسيادة الدولة والمساس بالحقوق الشخصية للإنسان، ونرى بأن انعكاساته السلبية تمس بالأكثر فئة النساء والأحداث.

وسنتطرق في هدا المبحث إلى وضع مفهوم لهذه الجريمة بتعريفها وأنواعها مع الإشارة إلى أساليبها والآثار المترتبة عنها.

المطلب الاول: مفهوم الابتزاز عبر الوسائل الإلكترونية.

يعرف الابتزاز بأنه الوعيد بالنشر أو زرع الخوف في النفس، وذّلك بالضغط على إرادة الإنسان من ان ضرراً ما سيتلقاه أو سيلحق أشخاصاً أو أشياء له به صلة، أو ذلك الفعل الذي يقوم به شخص بإنذار آخر بخطر يريد إيقاعه بشخصه او بماله أو بشخص أو مال غيره وهذا الإنذار سواء كان شفهياً او كتابياً لا فرق بينهما وكذلك بأي عبارة من شأنها إلقاء الرعب في نفس المجني عليه أو مجرد إزعاجه أو تخويفه من خطر قد يلحق بنفسه او ماله.[1]

وإجمالاً يمكن تعريف الابتزاز الإلكتروني بأنه كل فعل غير مشروع يستهدف منفعة غير مشروعة بأي صورة من الصور والوسائل التي يعتمد عليها الجاني، وهذا يفيد أن الجاني يطلب من الشخص المبتز دفع مبالغ مالية مقابل عدم نشر صور أو محادثات صوتية أو مرئية أو رسائل كتابية على الشبكة العنكبوتية، كما قد يطلب الجاني من الضحية إذا كانت فتاة ممارسة الفاحشة معه او مع غيره

كي لا يرسل كل ما يخصها إلى أقاربها أو التشهير بها على وسائل التواصل الاجتماعي، كم يمكن أن يطلب من الضحية القيام ببعض الأعمال الغير قانونية رغماً عن إرادته.[2]

1- م محسن عباس حميد، جريمة الابتزاز الإلكتروني، **مجلة القانون للدراسات والبحوث القانونية**، ع (الثاني والعشرون)2021، الجزائر، جامعة دي قار، ص6.

2- حورية المتوكل، جريمة الابتزاز الإلكتروني، **المجلة الإلكترونية للأبحاث القانونية**، ع (11) _2023، ص5.

الفرع الأول: تعريف الابتزاز عبر الوسائل الإلكترونية

تُعد جريمة الابتزاز الإلكتروني من أبرز الجرائم المعلوماتية المستحدثة، وتتمثل في استخدام الوسائل الإلكترونية لتهديد الضحية بنشر صور أو معلومات خاصة مقابل الحصول على منفعة مادية أو معنوية. وقد تزايدت خطورة هذه الجريمة مع انتشار الإنترنت ومواقع التواصل الاجتماعي، مما دفع المشرع الجزائري إلى تنظيمها من خلال وضع مجموعة من القوانين بهدف حماية الأفراد من المساس بحياتهم الخاصة وضمان الردع القانوني للجناة.

اولاً: التعريف اللغوي

يعرف الابتزاز لغة بأنه أخذ الشيء بجفاء وقهر.

إبتزه: سلبه، ورمى به، ولم يرده.[1]

وهو من الفعل بز يبزه بزاً، وجاء في المثل "من عز بز " ومعناه " من غلب سلب " ويقال ابتزت الشيء أي انتزعته، وبزه يبزه بمعنى غلبه.[2]

ثانياً": التعريف الاصطلاحي.

فيقصد به القيام بتهديد شخص بكشف معلومات معينة عنه عادة ما يحرص هذا الشخص على إخفائها، أو فعل شيء من شأنه المساس بشرف واعتبار الشخص المهدد ما لم يقم الأخير بالاستجابة الى طلبات مرتكب الفعل وليس ثمة تباين بين المفهومين اللغوي والاصطلاحي، فالجامع بينهما ان المراد بالابتزاز الحصول على المال او المنافع من شخص تحت التهديد بفضح بعض اسراره او المساس بشرفه أو اعتباره.[3]

ثالثاً: التعريف الفقهي.

---

1 – سليمان عبد الرزاق الغديان، **جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين**، دار المنظومة الرواد في قواعد المعلومات العربية، م (27)، مجلة البحوث الأمنية، ع (69) جانفي 2018، ص11.

2 – وفاء محمد سقر، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، **مجلة البحوث القانونية والاقتصادية**، كلية الحقوق جامعة بني سويف، مصر، م (36)، ع(2) _2024، ص13.

3 – مصطفى محمد الرواشدة، **جريمة الابتزاز الإلكتروني في القانون الأردني**، ط1، مركز الكتاب الأكاديمي عمان2020_ص22.

تعددت تعريفات الفقه للابتزاز، فقد عرفه بعض الفقه على أنه الضغط الذي يباشر شخص على إرادة شخص آخر بجملة على ارتكاب جريمة معينة.

وقد عرفه البعض الآخر على أنه فعل يقوم به شخص بتهديد شخص آخر بأي طريقة ولا يهم نوع عبارات التهديد مادام من شأنها التأثير في نفس المجني عليه بتخويفه، أو ازعاجه من خطر لم يتحقق بعد قد يلحق على المجني عليه، أو نفسه، أو أي شخص آخر له صلة بالمجني عليه وقد عرف على أنه القيام بتهديد شخص بفضح أمره ما لم يستجيب المهدد إلى تنفيذ طلبات الجاني وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف، أو الكرامة، أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي تم ابتزازه.[1]

رابعاً: الابتزاز الإلكتروني بالنسبة للمشرع الجزائري

يعد الابتزاز الإلكتروني في القانون الجنائي الجزائري نوعاً من أنواع جريمة السرقة، فهو محوره التهديد بنشر المعلومات الخاصة التي يكون المبتز سرقها من الضحية.

فانتهاك جريمة الابتزاز الإلكتروني لمفهوم الخصوصية في نطاق الرقمنة، فالحق في الخصوصية من الحقوق الدستورية الأساسية الملازمة واللصيقة للشخص الطبيعي بصفته الإنسانية كأصل ولو أن القانون الجزائري لا يحدد هذا المفهوم ومحدداته مما ينبئ عن تعقده وتشعب مراميه، بحيث يصبح الشخص معرضا للانتهاك متى تم تسجيل محتوى متعلق به في العالم الرقمي، مما يجعله غير قابل للمحو.[2]

1. تعريف الابتزاز الإلكتروني في التشريع الجزائري:

الابتزاز الإلكتروني هو استعمال وسائل تقنية حديثة مثل الإنترنت أو الهاتف المحمول لتهديد شخص أو جهة بالإفصاح عن معلومات أو بيانات خاصة أو للإضرار بسمعتهم، مقابل طلب مبالغ مالية أو تحقيق مكاسب غير مشروعة.

2. القوانين الجزائرية المتعلقة بجريمة الابتزاز الإلكتروني

- القانون رقم 18-07 المتعلق بمكافحة الجرائم الإلكترونية (2018):

هذا القانون يعالج الجرائم المرتكبة بواسطة وسائل الإعلام والاتصال الإلكترونية[3].

---

1 – ممدوح رشيد مشرف الرشيد العنزي، **الحماية الجنائية للمجني عليه من الابتزاز**، مقال منشور على الشبكة الالكترونية، **المجلة العربية للدراسات الأمنية**، م(33)، ع (70)، الرياض، 2017_ص199.

2 – فاطمة العرفي، المرجع السابق، ص494.

3 – القانون 18-07 المتعلق بمكافحة الجرائم الإلكترونية-2018.

المادة 14 منه تتعلق بجريمة الابتزاز الإلكتروني، حيث يعاقب كل من استعمل الوسائل الإلكترونية للتهديد أو الابتزاز للحصول على مكاسب غير مشروعة.

العقوبات تتضمن السجن والغرامات المالية.

- القانون رقم 06-03 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي (2006):

يحمي هذا القانون بيانات الأفراد من الاستغلال أو النشر بدون موافقة[1].

يعد نشر أو استخدام هذه البيانات في الابتزاز الإلكتروني مخالفة يعاقب عليها القانون.

الفرع الثاني: أنواع الابتزاز عبر الوسائل الإلكترونية

يعد الابتزاز من الجرائم متعددة الأنواع بحسب شخصية الضحية، فقد تكون الضحية من الشخصيات الاعتبارية وقد تكون من الأحداث وقد تكون من النساء او حتى الرجال، ويمكن عرض الأنواع وفقا لتقسيم التالي:

أولاً: الابتزاز عبر الوسائل الإلكترونية بالنظر للشخص الضحية.

- **الشخصية الاعتبارية كأحد ضحايا الابتزاز الإلكتروني:**

قد تكون الفئة المستهدفة من الابتزاز الإلكتروني هي أشخاص اعتبارية كالحكومات، والشركات والمؤسسات، وذلك عن طريق الحصول على معلومات سرية خاصة بها ثم يقوم المبتز بالتهديد بالإفصاح عنها، وافشاؤها، ونشرها للخر ين، فتبدأ الجريمة بمتطفل، أو دخيل على مواقع مهمة أو بالسطو على الموقع الإلكتروني للشخص الاعتباري، وخاصة، وأن المجرم لديه يقين من ملاءة الضحية المالية، وبأنه لن يعاني من كونه معسر.[2]

- **الأحداث كأحد ضحايا الابتزاز الإلكتروني:**

تعتبر فئة الأحداث الأكثر عرضة للابتزاز الإلكتروني ويرجع ذلك لعدة اسباب منها:

1. ان هذه الفئة قليلة الخبرة في التعامل مع وسائل تقنية المعلومات كما أنها تتميز بتطلعها للمعرفة على ما هو جديد.

---

[1] -القانون رقم 06-03 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي -2006 الجريدة الرسمية للأمانة العام للحكومة، ط 2،ق 32، 2025.

2 - ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص200.

2. سهولة التأثير على هذه الفئة طول الفترات التي يقضيها الطفل أمام وسائل الاتصال.

3. انشغال أوليائه عنه لأسباب مختلفة لذلك يجد في وسائل الاتصال الملاذ المغري، بالإضافة الى ضعف الرقابة الأسرية وتقصيرها في توجيه الأبناء وتوصيتهم.

4. التفكك الأسري والفراغ العاطفي وعرض تفاصيل الحياة الشخصية.

5. الإحجام عن الإبلاغ ورفع شكاوى ضد المجرمين خوفا من التهديدات ومن آثارها التي تكون مدمرة بحياة الضحية الاجتماعية.[1]

- **النساء كأحد ضحايا الابتزاز الإلكتروني:**

يعد ابتزاز النساء أكثر أنواع الابتزاز الإلكتروني انتشارا واشهره، ويعد هذا النوع النموذج المثالي لهذه الجريمة، خاصة إذا كان المبتز رجلاً والضحية امرأة وفي الغالب تكون أدوات هذا الابتزاز هي الصور الفاضحة والمحادثات المخلة بالآداب، او عرضاً مرئياً للضحية.

- **الرجل كأحد ضحايا الابتزاز الإلكتروني:**

ويكون الرجل ضحية لأسباب منها قد يكون ميسور الحال، فبالتالي يكون عرضة للابتزاز، من قبل النساء، وذلك يكون من خلال تهديده بنشر صوره، أو قد يكون ضحية بسبب نشره بعض

الأسرار فقي مجال عمله، أو أي معلومات أخرى يرى الشخص المبتز ان في نشرها أو الإفصاح عنها ضرراً على سمعة الضحية مما يفقده مركزه الاجتماعي.[2]

ثانياً: الابتزاز عبر الوسائل الإلكترونية بالنظر الى الهدف المرجو من المجني عليه:

- **هدف مادي**

في حال كانت دوافع الجاني في جريمة الابتزاز الإلكتروني مالية، فإن الجاني في حالة سيقوم بتهديد المجني عليه من أجل تسليم النقود له أو أشياء أخرى ذات الطابع المادي، باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات أو الجاني من الممكن أن يقوم بذلك بشكل مباشر أو غير مباشر والطريق المباشر أن يطلب الجاني المال مباشرة من المجني عليه، كأن يطلب منه تحويل مبالغ مالية بشكل مستمر به أو لغيره، أما الطريقة الغير مباشرة التي من الممكن أن يتبعها الجاني للحصول على المال من المجني عليه، فهي أن يطلب من المجني عليه تسديد مبلغ مالي كان قد اقترضه من أحد البنوك أو أن يطلب من المجني

1 – ياسين بن عمر، الابتزاز الإلكتروني للأطفال في التشريع الجزائري، **دفاتر السياسة والقانون**، م (16) ع (2)، 2024_ص173.

2 – فيصل عبد الله الرويس، الوعي الاجتماعي بظاهرة الابتزاز الالكتروني لدى الاسرة في المجتمع السعودي (دراسة ميدانية للعامل والآثار)، **مجلة كلية الآداب والعلوم الإنسانية، جامعة شقراء المملكة العربية السعودية**، ع (33) الجزء الثاني ص92_93.

عليه دفع أقساط لسيارة أو أي شيء آخر عليه أقساط مستحقة، ومن الممكن أن يحصل الجاني على المال بشكل غير مباشر في حال كان المجني عليه يعمل بإحدى الشركات كأن يطلب القيام بكشف أسرار الشركة التي يعمل لديها المجني عليه، أو ربما طلب الجاني الأرقام السرية لحسابات الشركة، كما يحصل الابتزاز عن طريق إطلاق الجاني لشائعات ونشرها في حال عدم دفعهم المبالغ المالية التي يريدها الجاني، أو عدم تلبية طلباته بهدف تركهم والابتعاد عنهم مع الوعد بعدم التعرض لهم وعدم تشويه سمعتهم.[1]

- **هدف إنتقامي:**

يؤدي الجانب النفسي دورا في عملية الابتزاز الإلكتروني، وذلك باعتبار ان المجني عليه يعيش صراعا داخليا نتيجة أن الجاني سيقوم بتنفيذ تهديداته ضده في أي وقت شاء ما يدفعه الى تلبيه طلبات الجاني تجنبا للفضيحة، حيث يستمتع 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 الحاق الأذى به واساءة سمعته بنشر صوره عن طريق شبكة الانترنت.[2]

- **هدف جنسي:**

هذا الهدف يبدو واضحاً وشائعاً حينما تكون المرأة الضحية أو حدث، أو أكثر شيوعاً حينما تجمع الضحية بين كونها امرأة أو حدث في نفس الوقت ويتحقق هدف المبتز الجنسي حينما يكون المقابل الذي يطلب بعدم إفشاء أسرار الضحية، وقد يكون الهدف تهديد المجني عليه للقيان بهذه الممارسات مع شخص آخر غير المبتز، ويكون الابتزاز بطلب المقابل مرة واحدة أو عدة مرات بحسب ظروف الجريمة، وأن أغلب ضحايا الابتزاز الجنسي من النساء.[3]

وقد نصت المادة **287** من القانون رقم "**04/82**" المؤرخ في **13 فبراير 1982م** " كل من هدد بالاعتداء أو العنف غير المنصوص عليه في المادة **284** وذلك بإحدى الطرق المنصوص عليها في المواد

---

1 – زهراء عادل سلبي، جريمة **الابتزاز الإلكتروني (دراسة مقارنة)، ط1**، شركة دار الأكاديميون للنشر والتوزيع الأردن _ 2020، ص40.

2 – ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص202.

3 – مريم عراب، جريمة التهديد والابتزاز الإلكتروني، **مجلة الدراسات القانونية المقارنة**، م (07) ع(1)، كلية الحقوق والعلوم السياسية، جامعة وهران 02_ احمد بن احمد 2021، ص1211.

من **284** إلى **286** يعاقب بالحبس من **3 أشهر** إلى **سنة (01 سنة)** وبغرامة مالية من **500** إلى **1,000 دج** إذا كان التهديد مصحوباً بأمر أو بشرط.[1]

- **هدف نفعي:**

فيتحقق هدف المبتز من جراء ارتكابه هذه الجريمة، وذلك من خلال قيامه من تهديد المجني عليه بأنه سوف ينشر له صوراً في حال لم يقم المجني عليه بتنفيذ طلباته التي طلبها منه أو تحقيق مصلحة له كأن يطلب منه المبتز بأن يروج المخدرات له أو أن يسرق شيء ما لصالحه، سواء كان هذت الأمر مشروعاً أو غير ذلك، فبمجرد كون هذا العمل رغماً عن إرادته واستغله كي يقوم له بارتكاب جرائمه فسوف يترتب عليه تحقيق وقوع هذه الجريمة.[2]

المطلب الثاني: وسائل الابتزاز عبر وسائل الإلكترونية وآثاره.

لكل جريمة خصوصية معينة وطرق مختلفة لتنفيذها، والتي تتم عن طريق اختيار الجاني طريقته المناسبة التي سيسلكها لتنفيذ جريمته، وبناءاً على هذا الأمر سنتطرق لبعض طرق ووسائل الابتزاز الإلكتروني.

الفرع الاول: وسائل الابتزاز عبر الوسائل الإلكترونية.

حيث نجد ان اغلب هذه الوسائل تختلف حسب كل مجرم وطرق تخطيطه لتطبيقها ونجد منها:

اولاً: الحاسب الآلي:

يعرف لغوياً الحاسب الآلي أو الكمبيوتر (computer) هي كلمة إنجليزية اشتقت من الفعل بحسب أو بعد (to computer) وقد استخدمت مصطلحات عربية عديدة للدلالة على الكمبيوتر الحاسب الإلكتروني، العقل الإلكتروني، الحاسوب الحاسب الآلي.

---

1 – قانون رقم "**04/82**" المؤرخ في **13 فبراير 1982**، المتضمن قانون العقوبات المعدل والمتمم، الصادر بالأمر رقم **156/66**، المؤرخ في **18 صفر 1386** الموافق ل 8 يونيو 2024، الجريدة الرسمية العدد 30 لسنة 2024.

2 – محمد سعيد عبد العاطي، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، **مجلة قطاع الشريعة والقانون**، كلية العدالة الجنائية جامعة نايف العربية العلوم الأمنية، الرياض، ع (16)، 2024، ص18.

ويعرف اصطلاحاً جهاز إلكتروني يقوم بإدخال عمليات حسابية ومنطقية ووحدة التحكم وأجهزة الدخل والإخراج الذاكرة حيث يتم استقبال المعطيات وإرسالها وخزنها ومعالجتها بأقل تدخل للعامل البشري محمد كمال شاهين الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي.[1]

ثانيا: برامج الحاسب الآلي.

برامج الحاسب الآلي هي مجموعة من الأوامر والتعليمات المكتوبة بلغة يفهمها الحاسوب، وتُستخدم لتوجيهه للقيام بمهام محددة. فهي تُعدّ الوسيط بين المستخدم والجهاز، إذ تتيح له الاستفادة من قدرات الحاسوب في مختلف المجالات، مثل الكتابة، الحساب، التصميم، التصفح، وغيرها، وبدون هذه البرامج لا يمكن للحاسوب أن يؤدي أي وظيفة، لأنه لا يعمل بذاته، بل يحتاج إلى من يوجهه وينظم عمله من خلال هذه التعليمات البرمجية.

ثالثا: الأنترنت.

هو تقنية حديثة، أحدثت ثورة في عالم الاتصالات، حيث تتيح للمستخدمين من كافة أنحاء العالم بالتواصل مع بعضهم البعض، أو الوصول للمعلومات من خلال شبكات الكمبيوتر التي تربط الأجهزة مع بعضها البعض، وقد ظهرت الإنترنت في الولايات المتحدة الأمريكية في عام 1970م، لكن لم يكن استخداما متاحاً للناس إلا في بداية التسعينات من القرن الماضي.[2]

فالأنترنت هي تلك الشبكة العنكبوتية التي تربط بين كم هائل من الحاسبات، مستعملة في عملية الربط هذه مختلف وسائل الاتصالات السلكية واللاسلكية، مثل الخطوط الهاتفية العامة أو الخطوط الخاصة أو الأقمار الصناعية، أو الكوابل والألياف البصرية، وغيرها من وسائل الاتصالات الحديثة والفائقة السرعة، وتمتد هذه الشبكة حول العالم لتؤلف شبكة دولية هائلة لتبادل المعلومات، بحيث يمكن لمستعملها الدخول إليها في أي وقت ومن أي مكان في العالم على أن يكون معه حاسوب مجهز بوسائط الاتصال بالشبكة لتلقي وإرسال البيانات عبر مزود الخدمة.[3]

---

1 – ميرفت محمد حبايبه، **مكافحة الجريمة الالكترونية**، دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري العلمية للنشر والتوزيع _2022، ص43_44.

2 – بلال جناجرة، **الانترنت والابتزاز الالكتروني**، ص2

3 – ضياء مصطفى عثمان، **السرقة الإلكترونية**، دراسة فقهية، دار النفاس للنشر والتوزيع ط1، 2011، ص25

_البريد الإلكتروني:

وهو وسيلة بسيطة وسريعة لإرسال الرسائل عبر الإنترنت، مثل التي كانت تكتب قديما على الورق وترسل عبر البريد العادي، لكن بشكل رقمي.

_خدمة الدردشة:

وهي وسيلة تواصل فورية تتيح تبادل الرسائل مع الآخرين في الوقت الحقيقي عبر الأنترنت تتم عبر الهاتف او الحاسوب.

رابعاً: الهاتف النقال:

هو الآخر من اهم وسائل تكنولوجيا الإعلام والاتصال وهو جهاز صغير الحجم ومربوط بشبكة الاتصالات اللاسلكية والرقمية تسمح ببث واستقبال الرسائل الصوتية والنصية والصور عن بعد بسرعة فائقة.[1]

يستخدم الهاتف النقال بواسطة المجرم الإلكتروني باعتباره أداة لارتكاب الجريمة، وذلك عندما يستخدم الأنترنت في برامج التواصل، كأن يقوم بالتجسس على الآخرين، بالاستعمال غي المشروع لتكنولوجيا الاتصالات والمعلومات الخاصة بالهاتف النقال والذي من شأنه الإضرار بمصلحة الغَير أو تعريضها للخطر، أما ملحقات الهاتف فهي الكاميرا والبلوتوث وآلة التسجيل، أما البرامج فهناك أيضا مجموعة من البرامج الخاصة بالهاتف المحمول[2].

الفرع الثاني: آثار الابتزاز عبر الوسائل الإلكترونية.

لا شك فيه أن جريمة الابتزاز الإلكتروني تنتج عنها آثار خطيرة على المجتمع بأسره وسنعرض بعض هذه الآثار بإيجاز:

1 – نوال مغزيلي، **تقنيات الإعلام والاتصال**، محاضرة أُلقيت على طلبة السنة ثانية ماستر، تخصص قانون جنائي، معهد الحقوق المركز الجامعي عبد الحفيظ بوالصوف، 2024_2025.

2 – عراب مريم، المرجع السابق ص1213.

اولاً: الآثار الشرعية:

هي من بين أكثر الآثار التي تؤثر على نفسية المبتز، وينقض ظهره ويؤدي إلى تعرضه لسخط الله تعالى، فقد ورد في آيات كثيرة تدل على حرمة الابتزاز بكافة صورها ومن ذلك قوله تعالى: **(وَلَقَدْ رَاوَدتُّهُ عَن نَّفْسِهِ فَاسْتَعْصَمَ ۖ وَلَئِن لَّمْ يَفْعَلْ مَا آمُرُهُ لَيُسْجَنَنَّ وَلَيَكُونًا مِّنَ الصَّاغِرِينَ).**[1]

سورة يوسف الآية: 32.

وأما من السنة فقد تواترت السنة المطهرة على حرمة الابتزاز في الكثير من الأحاديث ومنها ما روي عن النبي صلى الله عليه وسلم " صعد المنبر فنادى بصوت رفيع فقال: (يا معشرَ من أسلمَ بلسانهِ ولم يُفضِ الإيمانُ إلى قلبهِ، لا تُؤذُوا المسلمينَ ولا تُعيّروهُم ولا تَتّبعوا عوراتهِم، فإنه من يتبِعْ عورةَ أخيهِ المسلمِ تتبعَ اللهُ عورتَهُ، ومن يتبعِ اللهُ عورتهُ يفضحْه ولو في جوفِ رحلهِ).[2]

ثانيا: الآثار النفسية:

وهي تؤدي دوراً في الآثار المترتبة على الضحية فإن آثار الابتزاز الجنسي يتمثل في عدة آثار نفسية تلازم الضحية طوال حياته، وقد تتطور لتصبح استمرارية حياته أمراً مستحيلاً، مما يفقده الثقة بالآخرين وبالذات، ويجعل من الضحية شخصية مضطربة غريبة الأطوار وغير سوية وربما تصاب بالأمراض النفسية المستعصية كالاكتئاب والانهيار العصبي والقلق المزمن، ويؤثر الابتزاز الجنسي على المجني عليه بشكل خاص، وأسرته بشكل عام حيث يصابون بالأمراض والاضطرابات النفسية، وينعكس ذلك على المجتمع وعلى علاقة الأفراد مع بعضهم البعض، ويكون لديهم ردة فعل أو نتيجة الرغبة في الانتقام ويحقق لها تطورا في الأمراض النفسية ويدفعهم إلى الرغبة في الانتحار والرغبة في التخلص من الحياة.

ثالثا: الأثار الأمنية:

تؤدي الجرائم الجنسية وجرائم الابتزاز وغيرها من الجرائم إلى خلخلة الأمن في المجتمعات ويحول المجتمع إلى غابة وحشية، فلا يأمن الفرد فيه على نفسه وأهله، وكون الأمن والأمان من أهم معايير الحكم

1 – القرآن الكريم، سورة يوسف الآية 32،

2 – أخرجه الترمذي في سننه _ محمد بن عيسى بن سورة الترميذي (المتوفي 279هـ)_ت أحمد شاكر، طبعة الثانية 1395هـ_1975م _باب ما جاء في تعظيم المؤمن (4_378) برقم 2032.

على المجتمع القويم والسليم والإجرام بكل أنواعه يؤدي إلى انهيار القيم والأخلاق في المجتمع المسلم وتودي إلى فتك كيانه وزعزعته وانتشار الرذيلة فيه.[1]

رابعاً: الآثار الاجتماعية:

تعتبر جريمة الابتزاز من أخطر الجرائم تأثيرا على ضحاياها، وهذا ينعكس سلبيا على الأسرة والمجتمع، فالمرأة هي مربية الاجيال وهي التي تحافظ على كيان الاسرة وبنيانها، وهذه الجريمة تدفع المرأة لارتكاب السلوك المنحرف، كما أن لهذه الجريمة تأثير على قضايا العرض والشرف والمجتمع العربي والجزائري خصوصا من المجتمعات التي تمثل هذه الجريمة عارا اجتماعيا توصم به الاسرة والعائلة، وقد يؤدي الى القتل، كما انها تحطم بيت الضحية المتزوجة وتشوه سمعته لدى اطفالها ان كانت متزوجة، بالآثار مدمرة بمعنى الكلمة.[2]

1 – سليمان الغديان، المرجع نفسه، ص179.

2 – صالح بن عبد الله حميد، **بحوث ندوة الابتزاز**، المفهوم، الاسباب، العلاج، الرياض، ص66 منشور على موقع https://feqhup.com/uploads/145612377634481.pdf، نظر يوم 05 أفريل 2025، الساعة 16:33د.

المبحث الثاني: تجريم الابتزاز عبر الوسائل الإلكترونية.

يعد الابتزاز الإلكتروني من أفظع الجرائم المستحدثة، والتي تقوم على أفعال إجرامية يشترط فيها ويقتضي وجود شخصين هما طرفا الجريمة الأول الجاني والثاني مجني عليه.

ولقيام جريمة الابتزاز لابد من قيام ثلاث أركان كي تصبح جريمة يعاقب عليها القانون والمتمثلة في ثلاث أركان تقوم عليها مسؤولية الجاني وهو الركن الشرعي والذي يعتبر نص قانوني يحدده الفعل وقاعدته ان لا جريمة ولا عقوبة إلا بنص، بالإضافة إلى الركن المادي والمتمثل في القيام بالفعل أو الامتناع عنه إلى جانب النتيجة للفعل الإجرامي والعلاقة السببية بين الجاني والمجني عليه، بالإضافة إلى الركن المعنوي الذي يقوم على القصد الجنائي الذي يتطلب أن يكون الشخص قد مارس نشاطه بإرادته الواعية والحرة وهذا ما سيتم تناوله في هذا المبحث كما يلي:

المطلب الأول: أركان جريمة الابتزاز الإلكتروني:

أن النشاط والسلوك الإجرامي الذي يشكل جريمة وفقا للنصوص والقوانين بشكل عام يجب أن تتم النص عليها صراحة وأن القانون وحده هو الوحيد الذي يحدد تلك الأفعال المجرمة، وكما تعتبر الجريمة قائمة بإتمام اركانها وفقا للنمط الإجرامي والتشريع الجزائي وهذه الأركان الثلاثة اجتمعت في نموذج إجرامي وقعت العقوبة الجزائية المقررة وفقا للتشريع النافذ على الفاعل، وجريمة الابتزاز الإلكتروني مثلها كباقي الجرائم لا تقع إلا بإتمام أركان الجريمة حيث تتجرد الجريمة من عقوبتها مالم تتوفر فيها الشروط والأركان اللازمة لتحقيقها.[1]

الفرع الأول: الركن الشرعي:

يُعد الركن الشرعي أحد الأركان الاساسية لقيام المسؤولية الجنائية في وجود نص قانوني يُجرم الفعل المرتكب ويحدد العقوبة المقررة له.

ولقد تبنى المشرع الجزائري في تجريمه للأفعال التي تكون مسرحها إلكتروني، وذلك من خلال القانون **09_04** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما يستشف من نص المادة **02** منه التي جرمت الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيا

1 – محمد علي احمد ابو علي، جريمة **الابتزاز الإلكتروني في التشريع الفلسطيني**، (مذكرة لاستكمال متطلبات درجة الماجيستر في تخصص العلوم الجنائية، كلية الدراسات العليا، الجامعة العربية الأمريكية) _ 2022/9، ص22.

الإعلام والاتصال، فتكون جريمة الابتزاز الإلكتروني بذلك ضمنها استنادا إلى عمومية النص الذي يحيلنا بدوره إلى القواعد التقليدية المطبقة على جريمة التهديد في صورتها الكلاسيكية.

فجريمة التهديد التقليدية التي غالبا بالتشهير لم تتغير من حيث الأركان في ظل التحولات الرقمية والمعلوماتية، اذا يأبه المشرع بالوسيلة التي ترتكب بها الجريمة مدام أنها تنصرف إلى ذات تنصرف إلى ذات النتيجة الإجرامية إي المساس بالحياة الخاصة، وما الابتزاز الإلكتروني إلا صورة مستجدة للتهديد والابتزاز التقليدي المنصوص عليه في المادة **371 من قانون العقوبات الجزائري**، وإذا كانت العديد من التشريعات تعتبر الابتزاز الإلكتروني والتهديد مصطلحين لهما نفس المدلول، بيد أنه من وجهتنا نكون أمام جريمة الابتزاز إذا حصل تهديد مصحوبا بحمل الضحية للقيام بعمل أو الامتناع عنه

أما جريمة التهديد فتنصرف إلى الوعيد دون مطالبة المبتز للمجني عليه وإرغامه على القيام بعمل معين.[1]

الفرع الثاني: الركن المادي:

يمكن تعريف الركن المادي بأنه: القيام بفعل أو الامتناع عن فعل جرمه القانون بما يجعل الجريمة تبرز إلى الوجود تامة كانت أو ناقصة.

فلابد من القيام بفعل مادي محسوس أو الامتناع عن ذلك الفعل وأن يكون معاقب عليه بواسطة القانون كي نكون أمام جريمة ابتزاز، فجريمة الابتزاز الإلكتروني لا تقع بمجرد وجود النية لارتكاب الجريمة بل لابد من وقوع فعل مادي وملموس، وهذا الفعل الذي يمثل الركن المادي للجريمة، يعتبر شرطاً اساسيًا لاعتبار الجريمة تامة.

وينقسم الركن المادي في جريمة الابتزاز الإلكتروني إلى ثلاثة أقسام:

- **السلوك (النشاط الإجرامي):**

وهو ما يسمى بالفعل أيضا ويعرف النشاط الإجرامي أو السلوك على أنه: مجموعة الأفعال أو السوك على أنه مجموعة الأفعال أو الفعل الواحد الذي يقوم به الشخص وينظر القانون إلى تلك الأفعال على أنها

1 – أكرم ديب، دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني، **مجلة الحقوق والعلوم السياسية**، م(16)، ع (01)، 2023، ص404.

أفعال تشكل جريمة بحد ذاتها أو أن انتقالها إلى حيز الوجود وهو عنصر أساسي لقيام الجريمة ولا يكون هناك سلطة للمشرع العقابي دون وجود للسلوك المادي للجريمة في معظم الجرائم.[1]

- **العلاقة السببية:**

وهي الرابط بين سلوك الجاني والفعل الذي قام به والأثر المترتب والواقع جراء قيامه بفعله وهي من أهم شروط قيام المسؤولية الجنائية، فيجب أن يكون الفعل الصادر عن الجاني ذو علاقة سبب أدى بدوره إلى أثر انتقل إلى الجاني وبالنظر إلى العلاقة السببية نجد أن من السهولة تحديد علاقة السبب في الجريمة فمثلا إذا قام أحدهم بضرب آخر فقتله فإن علاقة السبب تكمن في السبب المؤدي على الوفاة وهي الضرب الذي أدى لحدوث كدمات أخلت في نظام عمل أجهزة الجسم أو اخترقت الجلد ومزقته حتى نزفت دماء الضحية ومات. [2]

- **النتيجة الإجرامية:**

لا يكفي بطبيعة الحال من أجل مساءلة الجناة عن قيامهم بالنشاط الإجرامي ووجود صلة بين نشاطهم وافعالهم الإجرامية، بل لابد من وجود القصد الجرمي لديهم النى يمكن على أساسها محاكمتهم، وتوقيع العقاب الجزاء الجنائي المنصوص عليهم ولهذا يصف بعضهم القصد الجرمي بأنه ركن المسؤولية، وعلى ذلك فالركن المعنوي يمثل العلاقة النفسية بين الفعل والفاعل، ويقضي بإن يكون الفاعل اهلاً لتحمل المسؤولية الجنائية، ولا يكون الأمر كذلك إذا تمتع بإرادة وإدراك يعتد القانون بهما وأن تنصرف هذه الإرادة إلى ماديات الجريمة.

الفرع الثالث: الركن المعنوي.

والقصد المعنوي في جريمة الابتزاز الإلكتروني يقوم على القصد العام على اعتبار هذه الجريمة من الجرائم العمدية التي لا تحتاج إلى القصد الخاص، ويتمثل هذا القصد في عنصريه العلم والإرادة.

- **العنصر الأول:**

هو العلم اذ يجب أن يعلم الجاني وهو يقوم بجريمة الابتزاز الإلكتروني أما أن يقوم به إلا من خلال حصوله على صورة فاضحة بأحد الأشخاص ثم تهديده بها مقابل الحصول على منفعة له تعتبر جريمة

1 – ريهام عاطف معروف، الابتزاز الإلكتروني، **مجلة روح القوانين، كلية الحقوق**، جامعة طنطا، عدد خاص _ المؤتمر العلمي الدولي الثامن_ التكنولوجيا والقانون ص2007.

2 – محمد علي احمد ابو علي، المرجع السابق، ص13.

يعاقب عليها القانون وخنا تتحقق عنصر علم الجاني وتكتمل أركان الجريمة، كما ينبغي أن يكون الجاني عالماً بماهية الفعل أو امتناع المجرم عليه قانونياً، ويعلم أن فعله يلحق ضرراً بالمجني عليه.

- **العنصر الثاني:**

فيمثل الإرادة وهي الرغبة في تحقيق النتيجة الغير مشروعة في الإضرار بحق أو مصلحة يسبغ عليها القانون حمايته، ومن ثم ينبغي أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية المتمثلة في ابتزاز المجني عليه أو الضحية، ولا يتوقف الأمر بعلم الجاني على ما يترتب عليه فعله من آثار نفسية قد تلحق ضرر بالضحية، لكن يمتد قصد الجاني إلى تهديده وحمل الضحية على القيام بأفعال أو الامتناع عن أفعال السوء سواء كانت مشروعة أو غير مشروعة دون النظر إلى تنفيذ العمل.

ولكي تقع مسؤولية الجاني يجب إثبات أن إرادة الفاعل قد اتجهت إلى القيام بجريمة الابتزاز الإلكتروني ودون إن تقع على إرادة الجاني عيب من العيوب التي تمنع المسؤولية، كأن يقوم الفاعل مختاراً ومدركاً أنه سيتحصل على معلومات وبيانات وصور وتسجيلات سرية وخاصة من مستودع

أسرار الضحية، فإن كان وقع عليه إكراه فلا يتحقق القصد الجنائي ولا تقع المسؤولية على الفاعل. [1]

المطلب الثاني: عقوبة جريمة الابتزاز عبر الوسائل الإلكترونية.

إن الابتزاز الإلكتروني اليوم اكتسى درجة من الخطورة وتنامت هذه الجريمة، مما جعلت العديد من الدول ومن بينها الجزائر لضمها إلى العديد من النصوص القانونية من خلال سن عدة قوانين وذلك من أجل مكافحتها والتصدي لها، وذلك فقد تم تحديده في الأفعال المجرمة والعقوبات التي تم إدراجها في فحواها ومن هذا المنطلق يهدف هذا المطلب الى دراسة عقوبة جريمة الابتزاز عبر الوسائل الإلكترونية.

الفرع الاول: العقوبات الأصلية والعقوبات التكميلية.

أولا: العقوبات الأصلية:

نستذكر أن المشرع الجزائري أولى حماية خاصة للأفراد وحياتهم الخاصة، لما يترتب عليها من أضرار تلحق بهؤلاء الأشخاص وقد تطرق لهدا في المواد **303** مكرر 1 من قانون العقوبات الجزائري **06/23** والعقوبة تتراوح بين الحبس من 6أشهر **إلى 3سنوات حبساً نافذاً** وغرامة مالية من **50 ألف دينار** إلى

1 – عاشور أميل جبار، المسؤولية الجنائية عن جريمة الابتزاز في مواقع التواصل الاجتماعي، (دراسة مقارنة)، **مجلة أبحاث ميسان** م (السادس عشر)، ع (31) _2020، ص124.

300الف دينار وهذه العقوبات تخص كل من تعمد المساس بخصوصية حياة الأشخاص، بأي تقنية كانت سواء كانت عن طريق التقاط الصور أو تسجيل أو نقل المكالمات سرية أو خاصة بغير إذن صاحبها أو رضاه.[1]

فأضاف المشرع الجزائري إلى جانب ذلك عقوبة على الشروع في الجنحة المنصوص عليها في المادة في ذات المادة بالعقوبات المقررة للجريمة تامة الأركان، فأضاف المشرع أيضا بمقتضى القانون من نفس المادة **303مكرر2 رقم 03/06 المؤرخ في 2006/12/20** والتي نصت هي أيضا على كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي اقنية كانت وذلك بالتقاط أو تسجيل أو نقل صور لشخص في مكان خاص.[2]

ثانياً: العقوبات التكميلية:

العقوبات التكميلية هي تللك العقوبات التي تصيب الجاني بناءاً على الحكم بالعقوبة الأصلية وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءاً على الحكم بالعقوبة الاصلية دون الحاجة لإصدار حكم تبعي فهو مرتبط ارتباطا مباشراً ووثيق بالعقوبة الأصلية.

نص التشريع الجزائري في العقوبات التكميلية على عقوبة المصادرة هي الأيلولة النهائية إلى الدولة لمال أو مجموعة من أموال معينة (المادة 15 من قانون العقوبات الجزائري).

وقد تكون المصادرة عامة، أي أيلولة كل أموال المحكوم عليه وإضافتها إلى ملكية الدولة. وقد تكون المصادرة خاصة أي أيلولة مال من أموال المحكوم عليه وإضافتها إلى ملكية الدولة.[3]

ولقد جاءت المادة 394 مكرر 6 من قانون العقوبات الجزائري صريحة، على ما يلي:

_ المصادرة للأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية.

_ إغلاق المواقع التي تكون محلاً للجريمة.

_ إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.[4]

---

1 – حمدان مداح، جريمة الابتزاز الإلكتروني في المدينة الجديدة، دراسة ميدانية بمدينة الكاليتوسة عنابة **مجلة العلوم الإنسانية**، م (22)، ع (2) _ جامعة باتنة_ 2021، ص132.

2 – أنظر المادة 303 مكرر 2 من قانون العقوبات الجزائري

2_ غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، ص215

4 – معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، (مذكرة لنيل شهادة الماجيستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر _باتنة) 2011_2012، ص127.

أولاً: الظروف المشددة للعقاب لجريمة الابتزاز الإلكتروني:

تُشدد العقوبة في بعض حالات الابتزاز الإلكتروني نظرًا لخطورة الفعل وضرره على المجتمع، خاصة إذا ارتُكبت الجريمة ضمن تنظيم إجرامي منظم، مما يعكس مدى استفحالها وتأثيرها العميق. كما تُغلّظ العقوبة إذا كان مرتكب الجريمة موظفًا عموميًا، إذ يُفترض فيه أن يكون محل ثقة الدولة ومثالاً للنزاهة، وليس موضع شبهة أو انحراف.

ويزداد التشديد أيضًا عندما يكون الضحية قاصرًا، باعتبارهم فئة تحتاج لحماية خاصة بموجب القانون. بالإضافة إلى ذلك، يُعتبر صدور أحكام سابقة ضد الجاني في جرائم مشابهة سببًا إضافيًا لتشديد العقوبة، وذلك انسجامًا مع مبدأ معاقبة العائدين لارتكاب الجرائم بسبب ما يشكلونه من خطورة إجرامية على المجتمع.

ثالثا: الظروف المعفية للعقاب لجريمة الابتزاز الإلكترونية.

إن الإعفاء من العقوبة ليس له علاقة بالسياسة الجنائية أو بالقواعد العامة او بالمسؤولية الجزائية لمرتكب الجريمة ففي القانون الجزائري يعتبر جريمة الابتزاز الإلكتروني يعاقب عليها بشدة كما أوضحناه في المادة **303مكرر**سالفة الذكر من قانون العقوبات الجزائري فإننا نجد أن المشرع لم ينص صراحة على حالات إعفاء خاصة بهذه الجريمة لكن مع ذلك يمكن تطبيق قواعد عامة للإعفاء من العقاب في بعض الحالات:

- ✓ **صفح الضحية:**

فصفح الضحية يضع حداً للمتابعة الجزائية التي تكون في جرائم المساس بحرمة الحياة الخاصة بما في ذلك الابتزاز الإلكتروني.

- ✓ **الإكراه:**

في حالة الإكراه إذا قام الشخص بالفعل المجرم تحت التهديد المباشر مثلا التهديد بنشر الصور أو معلومات حساسة شرط ألا يكون الشخص قد ساهم سواء عن طريق الإهمال أو التعمد الذي يسمح في خلق هذا.

- ✓ **صغر السن وفقدان الإدراك:**

قد تنتفي المسؤولية الجنائية أو تخفف إذا كان الشخص يعاني من اضطرابات نفسية أو عقلية التي تجعله غير مميز أو مدرك وأيضاً حالات صغر السن فمثلا لا تقام المسؤولية الجزائية على من لم يبلغ من **10سنوات** حيث يعتبر الطفل في هذا السن غير مميز ولا يسأل جنائيا وهذا مأخوذ من قانون الطفل في الجزائر.

✓ **التبليغ:**

في حالة إذا قام الجاني أو الشريك عن التبليغ السلطات القضائية عن هذه الجريمة قبل تنفيذها واكتشافها قد يعفي من العقوبة والتعاون مع السلطات أو تقديم أي معلومات تساعد في التحقيق في حالة ما إذا كانت الجريمة ارتكبت قد تخفف العقوبة وقد تعفي الجاني منها ويبقى تقدير الإعفاء أو التخفيف يعود إلى السلطات القضائية المختصة ويكون هذا حسب كل فعل إجرامي وظروفه.

الفرع الثالث: عقوبة جريمة الشروع والاشتراك في جريمة الابتزاز عبر وسائل الإلكتروني.

أولاً: عقوبة الشروع في جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري.

يقصد بالشروع هو الانطلاقة أو البداية في تنفيذ الجريمة والتي يذهب الجاني ويعقد على ارتكابها دون وصوله إلى مبتغاه وهنا الجريمة تكون ناقصة وغير متكاملة أركانها فالمشرع الجزائري خص عقوبات على الشروع في ارتكاب جريمة الابتزاز وذلك وفقا للمادة303 مكرر من قانون العقوبات الجزائري كما نص على ان الشروع في ارتكاب هذه الجنحة يعاقب بالعقوبات ذاتها المقررة للجريمة التامة.

إن العلة في العقاب على أية جريمة هي أنها تحقق عدوانا على المصالح محل الحماية القانونية. فتكون العلة في العقاب على الشروع بوصفه جريمة لابد أن تتمثل في تحقيق ذلك العدوان. ويأخذ العدوان في الشروع صورة الخطر الذي يهدد المصالح القانونية، حيث ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما تحدثه من قلق واضطراب في الجماعة أيضا ونظرا لأن مجال الشروع في الجنايات هو الأصل نظرا لخطورتها فإن هذا الأمر في الجنح لا يكون إلا في الخطيرة منها ويكون بنص.

ولأن المشرع رأى في جرائم المساس بأنظمة المعالجة الآلية للمعطيات خطورة كبيرة فقرر إخضاعها لنظام الشروع بعدما نص على العقاب على الاتفاق الجنائية المجسد بأعمال مادية.[1]

خلال نص المادة 394 مكرر 7، ومن خلال ترتيب المواد يتبين لنا ان المشرع الجزائري قد عاقب على الشروع في التحضير لارتكاب جريمة في إطار الاتفاق الجنائي بخلاف المشرع الفرنسي الذي استبعد الشروع في الاتفاق الجنائي لارتكاب الاعمال التحضيرية للجرائم الماسة بنظام المعالجة الآلية للمعطيات اذ ان المشرع الفرنسي اعتبر ان ذاك يدخل في إطار الشروع في الشروع.[2]

1 – غنية باطلي، المرجع السابق، ص202_203.

2 – معتوق عبد اللطيف، المرجع السابق، ص126.

ثالثاً: العقوبة المقررة للاشتراك في جريمة الابتزاز عبر الوسائل الإلكترونية:

يعرف الاشتراك بأنه المساهمة والمقاسمة والمشاركة في نفس الجريمة وتكون من قبل شخصين أو أكثر بحيث يشترك كل منهم بطريقة سواء كانت مباشرة أو غير مباشرة وتعد مشاركته سبباً في وقوع الجريمة.

وعليه قد يقوم بجريمة الابتزاز الإلكتروني شخص واحد أو أكثر وهذا التعدد يتطلب منا بأن كل شخص منهم دور مادي أو معنوي فيها بمعنى يساهم فيها بارتكاب أفعال مادية ولديه إرادة إجرامية.

وهذا ما نصت عليه المادة42 من قانون العقوبات الجزائري " يعتبر شريكاً في الجريمة من لم يشترك اشتراكاً مباشراً، ولكنه ساعد بكل الطرف أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها من علمه بذلك".[1]

ونصت المادة 41 من نفس القانون "يعتبر فاعلاً كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي ".[2]

كما تناول المشرع في المادة394 مكرر5 عقوبة الاشتراك في جريمة الابتزاز الإلكتروني وجاء في سندها "كل من شارك في مجموعة أو اتفاق تالف بغرض الإعداد لجريمة أو هذا التحضير بغرض الإعداد لجريمة او أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسداً بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها ".[3]

كما ارتأى المشرع الجزائري أن يوسع من نطاق التجريم ليشمل الأعمال التحضيرية التي تجسدت بأفعال مادية وتمت في إطار اتفاق جنائي.

ويفهم من نص المادة ان العقاب على الأعمال التحضيرية تشترط وجود اتفاق جنائي اي ان العمل التحضيري المرتكب من قبل شخص واحد غير معاقب عليه، ومن المتعارف عليه أن الأعمال التحضيرية غير معاقب عليها ما لم تكن تشكل جريمة مستقلة كحيازة برامج تسهل المساس بمنظومة المعالجة الآلية أو حيازة صور مخلة بالآداب العامة، والسبب في تجريم المشرع للأعمال التحضيرية التي تتم في إطار اتفاق جنائي هو رغبته في مكافحة الجريمة المعلوماتية وعدم السماح بتشكيل جماعات إجرامية تحترف

1 – انظر المادة 42 من قانون العقوبات الجزائري

2 – انظر المادة 41 من قانون العقوبات الجزائري

3 – انظر المادة 394 مكرر5 من قانون العقوبات الجزائري

الإجرام المعلوماتي، كما أنه اشترط ان يتجسد العمل التحضيري في افعال مادية كتجريب عدة كلمات سر أو محاولة الدخول الى منظومة معلوماتية بطريقة احتيالية.

بالإضافة إلى ذلك اشترط المشرع الجزائري أن يكون الاتفاق بغرض التحضير لارتكاب احدى جرائم المساس بمنظومة المعالجة الآلية، أي أن يكون كل فرد على علم بانه عضو في مجموعة اجرامية وان تتجه ارادة كل فرد إلى ارتكاب النشاط الاجرامي.[1]

1 – معتوق عبد اللطيف، المرجع السابق، ص126.

خلاصة الفصل:

تناول الفصل الأول من موضوع جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري الإطار العام لجريمة الابتزاز الإلكتروني وذلك من خلال تطرقنا لماهيتها وأنواعها وهذا لما أفرزه التطور التكنولوجي والانتشار الواسع لوسائل الاتصال الحديثة وإفرازه لأنماط جديدة من الجرائم والتي يعد الابتزاز الإلكتروني اليوم من ابرزها، كما أشرنا إلى الوسائل المستعملة لقيام هذه الجريمة، بالإضافة الى الآثار التي تحدثها وتشتمل هذه الآثار على آثار نفسية وأخرى اجتماعية خطيرة، خاصة الفئات الضعيفة كالأحداث والنساء، كما عالجنا في هذا الفصل أركان الجريمة التي تتكون من الركن المادي لها والركن المعنوي بالإضافة الى الركن الشرعي منها، وتناولنا في ختام هذا الفصل العقوبات المقررة من المشرع إلى مرتكبي هذه الجريمة وحالات الشروع والاشتراك فيها، ويخلص هذا الفصل إلى أن التشريع الجزائري قد خطا خطوات هامة في مواجهة ومكافحة هذه الجريمة، ونأمل أن تكون هناك تطوير آليات التحقيق الرقمية ونشر التوعية القانونية بما يواكب ويتماشى وتطور الجرائم.

وجهة نظري مبنية على المعرفة والقيم الإنسانية، أرى أن جريمة الابتزاز الإلكتروني من أخطر الجرائم المعاصرة، لأنها تستغل التطور التكنولوجي للإضرار بالناس نفسيًا، ماديًا، واجتماعيًا.

الابتزاز الإلكتروني ليس مجرد سرقة معلومات أو صور، بل هو اعتداء مباشر على كرامة الإنسان وحريته، وغالبًا ما يكون الضحية في موقف ضعف، ويشعر بالخوف والعار، خاصة عندما يتعلق الأمر بتهديدات بنشر محتوى خاص أو شخصي.

ما يجعل هذه الجريمة أكثر خسة هو أنها تُمارس في الخفاء، غالبًا من أشخاص يختبئون خلف شاشات، مستغلين خصوصية الآخرين، وقدرتهم على البقاء مجهولين.

الفصل الثانـي

الإجراءات المتبعة وأدلة الإثبات الجنائي في جريمة الابتزاز الإلكتروني.

الفصل الثاني الإجراءات المتبعة وأدلة الإثبات الجنائي في جريمة الابتزاز الإلكتروني:

جريمة الابتزاز الإلكتروني من أكثر من الجرائم التي تخضع للتحديات التي تواجهها اليوم العدالة في العصر الرقمي، ويرجع ذلك على تعقيداتها التي تتميز بالخفاء وعبوريها للحدود الوطنية، ونرى ان خطورة هذه الجريمة تكمن في، الأساليب والوسائل التي تطبق بواسطتها كل أشكال التهديدات والابتزاز ات، والنيل من الضحايا وتقييد حرياتهم الشخصية واخذ حقوقهم ونشر الرعب في أنفسهم، كل هذا نرى أن جهات التحقيق تسعى جاهدة لضبط وكشف غموض هذه الجريمة وملابساتها والتصدي لمرتكبيها وذلك بما يسمى التحقيق.

ويعتبر التحقيق على أنه نشاط إجرائي تباشره السلطة القضائية المختصة بالتحقيق والبحث والتحري في مدى صحة الاتهام، وتعتبر التحقيقات في جريمة الابتزاز الالكتروني خطوات دقيقة تقوم بناءاً على مجرى قضائي متكامل، تكون إجراءات تتطلب جمع كل الأدلة الرقمية والتعاون مع الجهات التقنية المختصة.

وسنقوم في هذا الفصل بعرض اجراءات التحقيق وأدلة الإثبات الجنائي في جريمة الابتزاز الإلكتروني في مبحثين حيت يتناول المبحث الأول التحقيق في جريمة الابتزاز الإلكتروني (من الضبطية القضائية إلى مرحلة المحاكمة) أما المبحث الثاني سيكون بعنوان أدلة الإثبات الجنائي في جريمة الابتزاز عبر الوسائل الإلكترونية.

المبحث الأول: التحقيق في جريمة الابتزاز الإلكتروني

يعرف الابتزاز الإلكتروني على أنه جريمة من الجرائم التي تنطوي على استخدام التهديد والتي تعتبر من أخطر الجرائم لما لها من تأثيرات نفسية وجسدية طويله الامد على الضحايا وتعتبر وسيلة لتحقيق أغراض غير مشروعة تمس بحقوق وحريات الأفراد وخصوصياتهم ويكون هذا الابتزاز إما ماديا أو معنويا، ونظرا لتميز هذه الجريمة بطابع النعومة والتخفي والسهولة لمحو وطمس الآثار الرقمية فقد اصبح من الضروري اللجوء الى العديد من اساليب التحقيق لمواجهة هذه الاشكال من الجرائم.

ويعد التحقيق اولى الاساليب وأداة ضرورية لكشفها وتحقيق العدالة ذلك من خلال جمع المعلومات والاستدلالات وتحديد هوية الجاني وجمع كل الأدلة ضدهم ومن هنا تبرز دور الإجراءات التي تتخذها الضبطية القضائية خلال فترة التحقيق خاصة التمهيدي منها وفي هذا السياق نطرح موضوع إجراءات التحقيق في جريمة الابتزاز الإلكتروني كذلك الإجراءات الابتدائية التي تتعلق بتكييف الجريمة إلى جانب ضوابط التفتيش والمعاينة الرقمية والاشارة في الاخير الى ما يتخلله التحقيق النهائي (مرحلة المحاكمة) فضلا عن الصعوبات والتحديات التي تعيق المكلفين بالتحقيق.

وأمام هذا الواقع يثور التساؤل حول إلى أي مدى وفقت اجراءات التحقيق في التشريع الجزائري وما مدى فعالية البحث عن الحقيقة الكفيلة بالتصدي لها واحترام حقوق وحريات الأفراد؟

وللإجابة على هذا التساؤل سنتناول هذه الإجراءات من خلال تقسيمها إلى فرعين الفرع الاول سنتطرق الى تناول إجراءات التحقيق التمهيدي(الأولي) في جريمة الابتزاز الالكتروني أما الفرع الثاني سنخصصه لشرح إجراءات التحقيق الابتدائي لجريمة الابتزاز الالكتروني اما الفرع الثالث سنشير باختصار الى اجراءات المحاكمة (التحقيق النهائي).

المطلب الأول: التحقيق في جريمة الابتزاز عبر الوسائل الالكترونية:

الفرع الأول: إجراءات التحقيق التمهيدي لجريمة الابتزاز الإلكتروني

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة من القواعد الإجرائية التي تخضع لها السلطة القضائية وأعوانها حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها.[1]

1 – عز الدين عثماني،، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية، **مجلة دائرة البحوث والدراسات القانونية والسياسية**، مخبر المؤسسات الدستورية والنظم السياسية، ع (الرابع) _ جامعة تبسة_2018، ص50_51

حيث تعد مرحلة التحقيق التمهيدي اجراء اولي سابق لإجراءات التحقيق الابتدائي، وهو من اهم المراحل في الإجراءات الجزائية يهدف الى كشف حقيقة الوقائع المبلغ عنها، ويعرف التحقيق التمهيدي على انه هو مجموعة الإجراءات التي تقوم بها الضبطية القضائية، وذلك تحت إشراف وكيل الجمهورية، بهدف جمع الأدلة حول جريمة ما والتحري وكشف هوية مرتكبيها، من أجل تحريك الدعوى العمومية، وتبدأ إجراءات التحقيق بتقديم شكوى من طرف الضحية أو من طرف المبلغ عن الجريمة.

ويعرف المبلغ هو" ذلك الشخص الذي يقوم بالإخبار والتبليغ عن الواقعة، وقد يكون المبلغ ذاته المجني عليه الذي استهدفته الجريمة، وهو الذي تضرر من وقوعها وقد يكون الشخص المبلغ على صلة بأطرافها قد يكون صديقا، او قريبا او جارا، بل قد يكون محاميا، لان اخذ اطرافها على انه في الحالة الاخيرة يتم اثبات الصلة بإثبات التوكيل ورقمه وجهه توثيقه، إذا تقدم المبلغ ببلاغ نيابة عن المجني عليه.[1]

أولاً: تحريك الدعوى العمومية.

يقوم الضحية المتعرض للابتزاز، الإلكتروني بشكوى بالطرق المناسبة، بحيث يجب ان تكون الشكوى فورية، ذلك من أجل تفادي زوال الأدلة الرقمية.

يتقدم المجني عليه بشكوى الى أقرب مركز للأمن الوطني، أو مصالح الدرك الوطني، أو بالتوجه الى الفرقة المختصة في مكافحة الجرائم المعلوماتية، أو وكيل الجمهورية، لتبدأ انطلاقة المتابعة القضائية ويكون المجني عليهم مرفقا بالأدلة، التي تثبت عملية الابتزاز عليه والتي تتضمن تفاصيل الواقعة ووسائل الأثبات.

1_ حفظ الرسائل والمحادثات المرسلة من طرف المبتز الذي تشتمل على صور وتهديدات.

2_ لقطات الشاشة (Screenshot) مأخوذة من المحادثات أو الرسائل التهديدية.

3_ حفظ اسماء الحسابات أو أرقام الهواتف والروابط التي استعملها المبتز.

1 – خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي، مصر، 2009، ص35.

ثانياً: تلقي البلاغات والشكاوى

لا يمكن لأعضاء الشرطة القضائية التعامل مع الجرائم التي تقع ضمن حدود اختصاصهم إلا بعد علمهم بها، سواء كان هذا العلم نتيجة للتحريات التي يقومون بها، أم كان نتيجة لشكوى أو بلاغ مقدم من قبل الغير.

ويعتبر تلقي الشكاوى والبلاغات الواجب الأول علي أعضاء الشرطة القضائية، سواء ما ورد منها من أفراد أو الناس، أم من الموظفين العموميين المكلفين بخدمة عامة عن جرائم وقعت أثناء تأدية عملهم أو بسببها، والتبليغ هو مجرد إيصال خبر الجريمة للسلطات العامة، وقد يكون من مجهول أو معلوم، وقد يكون شفهيا ام كتابيا وهو حق مقرر لكل إنسان مجني عليه، ذا مصلحة ويمنح قانون الإجراءات الجزائية لضابط الشرطة القضائية سلطة تلقي الشكاوى والبلاغات من المواطنين في مراكز عملهم المعتادة، ويختلف الأمر هنا بين الشكاوى والبلاغات، فالبلاغات يقوم بتقديمها أي شخص شاهد وقوع جريمة، أو أي مؤسسة عمومية أو خاصة، وقد يتم الإخبار كتابة أو شفويا أو بالهاتف وبكل وسائل الاتصال الأخرى.[1]

ثالثاً: الإجراءات السابقة على بدء التحقيق.

يعقب هذا إثبات مجمل الإجراءات السابقة على بدء مباشرة وكيل النيابة لإجراءات التحقيق من تلقي البلاغ وانتقاله، ومضمون محضر الاستدلالات إن وجد.

فيجب على المحقق ان يثبت البلاغ الذي تلقاه عن الحادث، على الصورة التي وردت إليه فكثيرا ما يستند إلى الإشارة الأولى عن الحادث للاستدلال على استناده إلى المتهم، ومما ينبغي على المحقق مراعاته وجوب إثبات ساعة وصول البلاغ اليه وتأشيره بذلك لأن الوقت الفاصل بين وقوع الحادث والتبليغ وبدء التحقيق على ما سبق ان اشرنا له أثر كبير في تقدير الدليل.[2]

الفرع الثاني: إجراءات التحقيق الابتدائي في جريمة الابتزاز الإلكتروني.

تواجه جهات التحقيق في قضايا الابتزاز الإلكتروني عدة عوائق، أبرزها صعوبة تتبّع الجناة بسبب استخدامهم لوسائل إخفاء الهوية مثل الشبكات المشفّرة أو الحسابات الوهمية، إضافة إلى نقص الأدلة الرقمية وضعف تعاون بعض المنصات أو الجهات الخارجية. كما قد يعيق التبليغ تأخر الضحايا في التواصل مع الجهات المختصة بسبب الخوف أو الحرج، مما يؤثر على سرعة وفعالية التحقيق.

---

1 – محمد شنه، **إجراءات البحث والتحري عن الجرائم في التشريع الجزائري**، ط1، ألفا لنشر والتوزيع 2024، ص73_74.

2 – خالد ممدوح إبراهيم، المرجع السابق، ص32.

يعرف التحقيق الابتدائي في جريمة الابتزاز الإلكتروني على أنه مجموعة من الإجراءات، التي تقوم بها السلطات القضائية المختصة بذلك، والتي تتكون من النيابة العامة، او الضبطية القضائية بهدف جمع الأدلة وتحديد هوية المجني عليه، الى جانب المعاينة والتفتيش، سماع الشهود الاستجواب والمحاكمة، ويمكن تلخيص هذه الإجراءات المادية في النظام الجزائري كالآتي:

أولاً: المعاينة.

إن المعاينة هي الانتقال إلى مكان الحادث لمشاهدة بعض معالم الجريمة، أو الآثار التي تفيد في إثباتها ونسبها إلى مرتكبيها، وذلك لأن الجاني مهما كان نوعه وذكاؤه قد بترك أثرا يهتدي به المحقق للوصول إلى الحقيقة. ونظرا لأهمية المعاينة فقد اعتبرها البعض عصب إجراءات التحري والتحقيق لأنها تعبر عن الواقع تعبيرا أمينا وصادقا دون كذب او خداع، فهي تعطي صفة واقعية عن الجريمة وما يتصل بها من ماديات وآثار، فتمكنهم من معرفة أسباب هذه الجريمة ودوافعها.

وهي "فحص مكان أو شخص له علاقة بالجريمة وإثبات حالته"، كمعاينة مكان الجريمة أو أداة ارتكابها أو محلها، أو معاينة جسم أو ملابس الجاني أو المجني عليه لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من تمزق أو جروح ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو استدلال.[1]

عند العلم بوقوع جريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة، لان هذا الأخير حجز الزاوية في التحقيق الجنائي، ومكمن الآثار والأدلة المادية، وينبغي التعامل في هذا الإطار مع مسرح الجريمة الإلكترونية على أنه مسرحان هما:

أ_ مسرح تقليدي:

ويقع خارج بيئة الحاسوب والأنترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة، للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون الى مسرح الجريمة التقليدية، قد يترك فيها الجاني آثار عدة كالبصمات، وبعض ملحقاته الشخصية أو وسائط تخزين رقمية.

1 – محمد شنه، المرجع السابق، ص77.

ب_ مسرح افتراضي:

تقع داخل البيئة الإلكترونية، يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب، وشبكة الانترنت الأقراص الموجودة بداخله.[1]

وكي تكون المعاينة لها فائدة في كشف الحقيقة عنها وعن مرتكبيها فإنه ينبغي مراعاة عدة قواعد وارشادات فنية أبرزها ما يلي:

1. ملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية خاصة السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج الى النظام وموقع الاتصال أو الدخول معه في حوار.

2. تصوير الحاسب والأجهزة الطرفية المتصلة به والتحديات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب الآلي وملحقاته ويراعي تسجيل الوقت وتاريخ ومكان التقاط كل صورة.

3. ملاحظة وإثبات حالة التوصيلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حيث عرض الأمر على القضاء.[2]

4. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب مع أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

5. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد من بصمات ويلاحظ أن الآثار المعلوماتية والرقمية المستخلصة من أجهزة الكمبيوتر من الممكن ان تكون ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة، والبريد الإلكتروني الفيديو الرقمي، الصوت الرقمي، غرفة الدردشة، المحادثات الملفات المخزنة في الكمبيوتر، الصور المرئية.[3]

6. المحافظة على البيانات المخزنة وذلك حتى لا تتعرض للإتلاف إثر وجود مجال مغناطيسي أو نتيجة لعدم معرفة كيفية التعامل مع مثل هذه المواد المعلوماتية.

---

1 – عائشة بن قارة مصطفى، **حجية الدليل الجنائي في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامعة الجديدة الإسكندرية_ 2010، ص84.

2 – هشام فريد رستم، الجوانب **الإجرائية للجرائم المعلوماتية**، مكتبة الآلات الحديثة، أسيوط مصر، ط1، 1994، ص59.

3 – صغير يوسف، **الجريمة المرتكبة عبر الأنترنت**، (شهادة الماجيستير كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه " القانون الأساسي والعلوم السياسية " جامعة مولود معمري _تيزي وزو) _ 2013، ص86.

7. حفظ المستندات الخاصة بالإدخال وكذا بالمخرجات مع الاخذ بعين الاعتبار آثار البصمات التي قد توجد على الأدلة المادية المرتبطة بها، ومن بينها الاقراص الممغنطة وأقراص الليزر وحتى المطبوعة على اوراق بطبيعة الحال.

8. ضرورة توفر قدر من الخبرة الفنية في مجال الحاسب الالي على ضباط وأعوان الشرطة القضائية القائمون بعملية المعاينة.[1]

قد نصت المادة 42 من قانون الاجراءات الجزائية الجزائري على وجوبية انتقال ضابط الشرطة القضائية فورا إلى مكان وقوع الجناية للقيام بالمعاينات، وجاء في نص المادة أنه «يجب على ضابط الشرطة القضائية الذي بلغ بجناية في حالة تلبس ان يخطر بها وكيل الجمهورية على الفور ثم ينتقل بدون تمهل الى مكان الجناية ويتخذ جميع التحريات اللازمة.

كما نصت المادة نفسها على ضرورة سهر ضابط الشرطة القضائية على المحافظة على الآثار التي يخشى أن تختفي، وكذا على ضرورة ضبطه لكل ما يمكن ان يؤدي إلى إظهار الحقيقة.

كما نصت المادة 64 الفقرة 3 على جواز قيام ضابط الشرطة القضائية القيام بالمعاينة في أي وقت وأي مكان إذا تعلق الأمر بواحدة من الجرائم المذكورة في المادة 47 ومنها جريمة المساس بأنظمة المعالجة الآلية للمعطيات.[2]

ثانيا: التفتيش في البيئة الإلكترونية

يعتبر التفتيش الالكتروني اجراء من الاجراءات التي تهدف الى البحث عن ملابسات الجريمة، كما يعد من اهم وأخطر إجراءات تحقيق في جرائم المعلوماتية وذلك من خلال مساس بالحريات الخاصة للأفراد المكفولة دستوريا، ولقد سن المشرع الجزائري جملة من التعديلات لمواجهة الجرائم المعلوماتية من خلال التفتيش والضبط.[3]

التفتيش إجراء من اجراء تحقيق التي تستهدف البحث عن الحقيقة في مستودع السر لذلك يعتبر من اهم اجراءات التحقيق يكفي كشف الحقيقة، لإنه غالبا ما يفسر عن ادلة مادية تؤيد نسبة الجريمة إلى المتهم والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله الى ادلة مادية،

1 – معتوق عبد اللطيف، المرجع السابق، ص109.

2 – معتوق عبد اللطيف، المرجع السابق، ص108.

3 – نجيب محمد دیابلو، **الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي**، ط1، المركز المغاربي، شرق الأدنى للدراسات الاستراتيجية، 2024، ص79.

تُسهم في بيان وظهور الحقيقة، ونتيجة لذلك يعد تفتيش نظام الحاسوب والانترنت من اخطر المراحل حال اتخاذ الاجراءات الجنائية ضد مرتكب الجريمة الإلكترونية، لكون محل التفتيش هنا وهو الحاسوب والشبكات محل جدل فقهي متزايد يوما بعد يوم.

1. مدى قابلية مكونات وشبكات الحاسوب للتفتيش.

أ- تفتيش مكونات الحاسوب المادية:

ليس هناك خلاف على ان الولوج الى المكونات المادية للكمبيوتر بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يفيد في كشف الحقيقة عنها وعن مرتكبها، يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة في تلك المكونات، وهل هو من الاماكن العامة او من الأماكن الخاصة، حيث أن لصفة المكان وطبيعتهُ أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والاجراءات المقررة قانونا في التشريعات المختلفة.[1]

مع مراعاة التمييز بين ما إذا كانت مكونات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من الكمبيوتر اخرى، ام انها متصلة بكمبيوتر اخر او بنهاية طرفية في مكان آخر كمسكن متهم مثلا، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود التي يستلزمها المشرع في تفتيش هذه المكونات اما اذا وجد شخص يحمل مكونات الكمبيوتر المادية وكان مسيطرا عليها او حائزا لها في مكان ما من الاماكن العامة وإن كانت بطبيعتها كالطرق العامة والميادين والشوارد، أم كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فان تفتيشها لا يكون إلا في الحالة التي يجوز فيها تفتيش الأشخاص وبنفس القيود المنصوص عليها في هذا المجال.[2]

ب- مدى خضوع مكونات الحاسوب المعنوية للتفتيش:

أثار تفتيش الكيانات المعنوية خلافا كبيرا في الفقه، فذهب رأي الفقه إلى جواز تفتيش وضبطت بيانات المعلوماتية بمختلف أشكالها، ويستند هذا الرأي في ذلك الى القوانين الإجرائية عندما تنص اصدار اي شيء فإن ذلك يجب تمييزه، بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير ملموسة، ولذلك فإنه يقترح اصحاب

1 – خالد ممدوح إبراهيم، المرجع السابق، ص195.

2 – عبد القادر كيحول، **التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية**، (مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور _ الجلفة) _2019، ص42.

هذا الراي على مواجهة هذا القصور التشريعي بالنص صراحة على جواز تفتيش المكونات المعنوية للكمبيوتر.[1]

2. الضوابط الموضوعية للتفتيش الإلكتروني.

مما يقصد بالضوابط الموضوعية التفتيش الالكتروني تلك الشروط اللازمة لإجراء تفتيش صحيح والتي يمكن حصرها في ثلاثة شروط أساسية تتمثل في سبب التفتيش المحل المراد تفتيشه، السلطة المختصة بالتفتيش.[2]

أ- سبب التفتيش الالكتروني:

يقصد بسبب التفتيش نحو الحصول على دليل في تحقيق قائم، من أجل الوصول إلى حقيقة الحدث والتفتيش باعتباره اجراء من اجراءات التحقيق لا يجوز اتخاذه إلا بعد ارتكاب جريمة بوصفها جناية أو جنحة واسنادها الى شخص معين سواء بصفته فاعلا أصليا أو شريكا فيها، وتوافر قرائن قوية ودلائل كافية للتصدي لحرمة مسكنه أو لحريته الشخصية، وذلك عملا بمبدأ الشرعية الجنائية الذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص، بدون وقوع جريمة وتوجيه الاتهام إلى شخص او اشخاص معينين وفقا لأدلة كافية يكون التفتيش باطلا من انتفاء السبب الذي يبرر.[3]

ب- محل التفتيش:

هو شرط من الشروط الموضوعية لصحة التفتيش، وكما بينا في العنصر السابق فهو يشمل ثلاث عناصر اساسية هي:

_ الأشخاص السابق بينهم والأماكن التي توجد فيها أجهزة وادوات الكترونية او رقمية.

_ المكونات المادية لجهاز الحاسوب وما يرتبط به من ملحقات وشبكات الاتصال.

_ المكونات المعنوية لجهاز الحاسوب وما يرتبط به من ملحقات وشبكات الاتصال.[4]

---

1 – محمود نجيب حسني، شرح **قانون العقوبات**، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية _ القاهرة 1972، ص42.

2 – عبد الفتاح بيومي حجازي، **جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي**، دار الكتب القانونية القاهرة2007، ص36.

3 – عبد القادر كيحول، المرجع السابق، ص11.

4 – سلمى مانع، التفتيش كإجراء في الجرائم المعلوماتية، **مجلة العلوم الإنسانية**_ جامعة محمد خيضر بسكرة_ع (الثاني والعشرون) ص238.

ج- **السلطة المختصة بالتفتيش:**

حرص المشرع الجزائري على إسنادها لجهة قضائية تكفل تلك الحريات والحقوق، وتضمها إلا أن هذه التشريعات الجنائية لم تسرع على نسق واحد فيما يخص تحديد الجهة التي يعهد لها بالتحقيق الابتدائي لتكون صاحبة الاختصاص الأصيل بإجراء التفتيش.

في الجزائر نرى انها اخذت بنظام الفصل بين سلطة الاتهام والتحقيق وتركت لهذا الأخير السلطة الاولى للنيابة العامة واذا كان الاصل ان يكون قاضي التحقيق والنيابة العامة إجراء التفتيش بنفسه بالضبط وهو نادر الحدوث عملا إلا انه يمكن لمأمور الضبط القضائي أن يقوم بذلك إلا في حالتين التلبس والانتداب.[1]

د- الضوابط الشكلية للتفتيش الإلكتروني.

أ_ أن يكون الأمر بالتفتيش مسبباً: يعتبر من الضمانات المقررة في التشريعات الإجرائية الجزائية تسبيب أمر التفتيش، ويقصد بالتسبيب ان الامر الصادر من الأمر الصادر لابد أن ينبني على عدة قرائن ودلائل تدل في المكان المراد أو الشخص المراد تفتيشه مايفيد في كشف الحقيقة.[2]

ب _تحرير محضر بتفتيش نظام الحاسب الآلي:

من حيث أن تفتيش في الأصل يعتبر عملا من أعمال التحقيق، فإنه ينبغي هو الحال كذلك يثبت كل ما تم من إجراءات وما أسفر عنه التفتيش من أدناه ولم يتطلب القانون شكلا خاصاً لهذا المحضر مما يعني أنه لا يشترط لصحته سوى ما يستوجب القواعد العامة في المحاضر عموما، كان يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره أو توقيعه محررة، وأن يحوي في طياته كافة الاجراءات التي اتخذها بشأن الوقائع التي بينها، وبالنسبة لمحضر تفتيش نظام الحاسب الآلي فإنه لابد بالإضافة الى سبق ذكره ان يكون عضو الادعاء العام او قاضي التحقيق محيطاً بتقنية المعلومات ومن جهة اخرى لابد أن يرافقه شخص متخصص في الكمبيوتر للاستعانة به في المسائل الفنية الضرورية.[3]

1 - عائشة بن قارة مصطفى، المرجع السابق.ص105.

2 - خالد ممدوح إبراهيم، المرجع السابق، ص195.

3 - خالد ممدوح إبراهيم، المرجع السابق، ص225.

ج_ إجراء التفتيش بحضور أشخاص يعينهم القانون:

تشترط معظم التشريعات عند القيام بالتفتيش حضور أشخاص يعينهم أثناء مباشرته كحضور المتهم أو في حال تعذره حضور من ينوب عنه وإذا تعذر ذلك أيضا حضور شاهدين وأن يكون بقدر الامكان من أقارب المتهم من بالغين أو من القاطنين معه في مسكن ويعد حضور هؤلاء من القواعد الأساسية التي يترتب عليها البطلان اعمالاً لمبدأ الحضور عند المسكن.

وذهب المشرع الجزائري إلى إعمال الحضور أيضا وهو ما نصت عليه المادة 5 من القانون 04/09 التي تحيل إلى الأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية من المادة 45 والتي تشترط لتفتيش المساكن حضور صاحب المسكن المشتبه به تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكفل بتعيين ممثل له هو إذا امتنع عن ذلك او كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.[1]

د_ الوقت الزمني لتنفيذ التفتيش:

نصت المادة 47 قانون03/82 من قانون الإجراءات الجزائية على وقت تنفيذ التفتيش بقولها " لا يجوز البدء في التفتيش للمساكن ومعاينتها قبل الساعة الخامسة (5) صباحاً ولا بعد الساعة الثامنة (8) مساءاً إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا"

وغير أنه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل قصد التحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون الإجراءات الجزائية.[2]

ثالثا: ضبط الأدلة الإلكترونية.

يختلف ضبط الأشياء في الجريمة الإلكترونية عن ضبط بجريمة التقليدية من حيث المحل، ففي هذه الأخيرة يكون المحل الأشياء مادية أما في الالكترونية تكون الأشياء ذات الطبيعة معنوية، كالبيانات والمراسلات الالكترونية وتجدر الاشارة الى ان ضبط الأشياء قد يرد على عناصر معلوماتية منفصلة، مثل الاسطوانات الممغنطة وهنا لا يطرح أي إشكال عند القيام بالضبط، لكن الصعوبة تكمن عندما يلزم ضبط

1 – مخلوف علمي، ضوابط التفتيش في الجرائم الإلكترونية، **مجلة المعيار، جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة** ع (8) 2024_ ص394_397.

2 – أنظر المادة 47 من قانون الإجراءات الجزائية.

النظام كله او الشبكة كلها لأنها تحتوي على عناصر لا يمكن فصلها، أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية:

- وحدات الإدخال (لوحة المفاتيح، الفأرة، نظام القلم الضوئي).
- ضبط وحدة الإخراج (الشاشة، الطابعة، الرسم، والمصغرات الفيلمية).
- كل ما يتم ضبطه من بيانات الكترونية يتعين تحريرها وتأمينها فني
- ويجدر الإشارة إلى الأنواع التي يمكن ضبطها والمتعلقة بالابتزاز الإلكتروني نجد:
- الورق.
- جهاز الكمبيوتر وملحقاته.
- البرمجيات software.
- وسائط التخزين المتحركة.
- المودم modem.

رابعاً: الاستجواب.

ان الاستجواب عبارة عن إجراء مهم من إجراءات التحقيق، يهدف الى الوصول الى حقيقة التهمة المنسوبة الى المتهم والتوصل الى اعتراف يدينه او ينفي التهمة عنه، وهو أحد إجراءات التحقيق وفيه يتم توجيه التهمة الى المتهم ومواجهته بالأدلة التي تدينه ثم مناقشته فيها بشكل تفصيلي ويطلب منه تنفيذها إن أنكر التهمة الموجهة اليه، ومن خلال الاستجواب يعترف المتهم بتهمة إن كان مذنبا بالفعل ويمكن القول ان الاستجواب وسيلة تمكن المحقق من الوصول الى الجاني الحقيقي كما انه طريقة تمكن المتهمين من الدفاع عن أنفسهم وتنفيذ جميع الأدلة الموجهة إليهم بالتفصيل.[1]

ويقصد به أيضا هو استجواب المتهم ومجابهته بالأدلة المختلفة القائمة قبله ومناقشته فيها مناقشة تفصيلية كي يفندها او كان منكرا للتهمة أو يعترف إذا شاء الاعتراف بارتكاب الواقعة، فالاستجواب يحقق في المرحلة الأولى من التحقيق الابتدائي، الغاية منه وهو جمع الأدلة لذا لا يجوز اجراء الاستجواب في مرحلة المحاكمة إلا اذا قبله المتهم هو محاميه، والاستجواب لا يكون إلا بتوجيه التهمة ومناقشة المتهم تفصيليا عنها ومواجهته بالأدلة القائمة ضده لاستجواب بمجرد سؤال المتهم عما هو منسوب إليه وإحاطته

1 – ايمن عبد الله فكري، الاستجواب الجنائي الإلكتروني، **مجلة البحوث الفقهية والقانونية مجلة علمية محكمة**، كلية الشريعة والقانون بدمنهور، ع (الثالث والاربعون) 2023، ص977.

علما بنتائج التحقيق إذا لم يتضمن ذلك مناقشة تفصيلية في الأدلة المستندة إليهم بمعنى أنه لابد من ان يتوافر في الاستجواب عنصرين لا قيام لهما بدونهما الأول يتمثل في توجيه، التهمة ومناقشة المتهم تفصيليا فيه والثاني يتمثل في مواجهة المتهم بالأدلة القائمة ضده ليتمكن من ممارسة حقه في الرد عليها وتنفيذها.[1]

✓ **نموذج لإجراء الاستجواب في جريمة الابتزاز عبر الوسائل الإلكترونية:**

اولاً: الأسئلة التعريفية (لكل الأطراف).

1. ما اسمك؟
2. ما هو تاريخ ميلادك ومكان الازدياد؟
3. ما هو عنوانك؟
4. ما مهنتك ومكان عملك؟
5. ما رقم الهاتف الخاص بك وعنوان بريدك الإلكتروني الحالي؟

ثانياً: الأسئلة الخاصة بالواقعة

✓ **الأسئلة الموجهة للضحية:**

1. متى وكيف بدأت العلاقة أو التواصل مع المشكو بحقه؟
2. ما طبيعة الابتزاز الذي تعرضت إليه؟
3. كيف تم التواصل بينك وبين المبتز؟ هل بالهاتف او الرسائل او البريد الالكتروني، وسائل التواصل الاجتماعي ؟
   1. هل تملك أدلة تثبت شكواك هذه (صور_ رسائل _تسجيلات_ شهود)؟

✓ **الأسئلة الموجهة إلى المتهم:**

1. هل تعرف المشتكي وما طبيعة علاقتك به؟
2. هل تواصلت معه عبر وسائل إلكترونية؟
3. هل قمت بطلب مبالغ مالية منه او خدمات مقابل عدم نشر معلومات عنه؟
4. ما تفسيرك لوجود رسائل وأدلة تدينك في هذه الجريمة؟
5. هل سبق لك ان حصلت على صور ومعلومات عن المشتكي؟ وكيف تم حصولك عليها؟

1 – خالد ممدوح إبراهيم، المرجع السابق، ص242.

6. هل سبق لك وأن قمت بالابتزاز على اشخاص آخرين بنفس الطريقة؟
7. هل قمت باستخدام حسابات مزيفة أو ارقام هواتف مجهولة في التواصل مع المشتكي؟
8. هل لديك شهود أو اية أدلة تنفي التهمة المنسوبة إليك؟

✓ **الأسئلة الموجهة للشهود إن وجدوا:**

1. ما طبيعة علاقتك بالضحية والمتهم؟
2. هل كنت حاضرا اثناء المحادثة أو التهديد بينهما؟
3. هل سبق لك أن سمعت من المتهم يتحدث عن النية في ابتزاز الضحية؟
4. هل لديك أدلة تدعم أقوالك؟

ثالثاً: الأسئلة الخاصة بالأدلة الرقمية.

✓ **أسئلة موجهة للمشتكي والمشكو بحقه:**

1. هل يمكننا الحصول على هاتفك او الجهاز الشخصي لفحص الأدلة؟
2. هل لديك نسخ احتياطية من المحادثات او الصور المرسلة؟
3. هل توجد حسابات مزيفة استخدمت للابتزاز، ؟ وهل هي مرتبطة بالمشكو منه؟

في الأخير يتم تسجيل كل الاجابات الخاصة بالأشخاص اللذين تم استجوابهم كما هي دون اضافة او تعديل ويتم تدوين الملاحظات التي تكون على المستجوب أثناء عملية الاستجواب، كما يمكن الاستعانة بخبراء في الجرائم الإلكترونية من اجل التحليل الدقيق للأدلة الرقمية.

خامساً: سماع الشهود.

تعرف الشهادة عموما بأنها الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق، أو القضاء بشأن جريمة وقعت، وتعتبر الشهادة الطريق العادي للإثبات الجنائي، مقابل ذلك فالكتابة تعتبر الطريق العادي للإثبات المدني، وللشهادة في مجال الإجراءات أهمية بالغة لأن الجريمة عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابها ويحرص على إخفائها عن الناس ولهذا فإن العثور على شاهد يعتبر مكسبا كبيرا للعدالة، ومن هنا جاءت قاعدة عدم رد الشهود.

وتختلف الشهادة الإلكترونية عن الشاهد المعلوماتي ففي حين يقصد بالشهادة الإلكترونية بأنها تلك الشهادة التي لا يكون فيها الشاهد حاضرا جلسة التحقيق بذاته وإنما تتم عبر وسائل إلكترونية، فإن الشاهد المعلوماتي هو ذلك الشخص الذي يدلي بشهادته في جلسة المحاكمة.[1]

كما نصت المادة 152 من قانون الإجراءات الجزائية "يسمع كل شاهد على انفراد في حضور او غياب الخصوم ويعرف قبل سماعه باسمه ولقبه ومهنته وسنه وموطنه وعلاقته ودرجة قرابته أو مصاهرته وتبعيته للخصوم يؤدي الشاهد اليمين بأن يقول الحقيقة وإلا كانت شهادته قابلة للإبطال يجوز معاودة سماع الشهود ومواجهة بعضهم البعض".

ان التزام الشاهد بالإعلام عن الجريمة الإلكترونية لها شروط لا بد من تحققها، وبغير هذه الشروط فإن الشاهد المعلوماتي لا يكون ملزما بالإعلام عن الجريمة، وتتلخص هذه الشروط بالآتي:

_الشرط الأول:

أن تكون بصدد جريمة إلكترونية وقعت فعلا بالفعل سواء أكانت جناية أو جنحة يجب أن تكون الجريمة الإلكترونية قد وقعت بالفعل حتى يتحقق التزام الشاهد المعلوماتي والإعلام عنها فالتزام الشاهد المعلوماتي لا يمكن أن يتحقق حسب القواعد العامة لضبط جريمة مستقبلة، حتى لو كان هناك تحقيقات جدية تأكد أن هذه الجريمة سوف تقع بالفعل.

ووقوع الجريمة بشكل فعلي لا يحقق هذا الالتزام أيضا، بل أن تكون الجريمة الواقعة فعلا تحمل وصف جناية أو جنحة ذلك أن المخالفات تستبعد لأن الآثار المترتبة عنها لا تشكل خطورة كبيرة على المجتمع.[2]

_ الشرط الثاني:

علم الشاهد ومعرفته بالمعلومات المتعلقة بالمعلومات أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة، وهذا شرطا ضروريا لقيام الالتزام بالإعلام في الجرائم الإلكترونية، ومضمون هذه المعلومات يتمثل في ثلاث عناصر:

تتضمن ثلاث عناصر هي: الكشف عن مفاتيح الشفرات، الإفصاح عن كلمات السر، طباعة الملفات الخاصة بالبيانات.

---

1 – بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية**، أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الجزائر1_2015، ص151_152.

2 – يحي الشديدي، الشهادة في الجريمة الإلكترونية، **مجلة جامعة البعث**، ع (50) _ 2016، ص45.

_الشرط الثالث:

أن تقتضي مصلحة التحقيق الحصول على المعلومات حتى يقوم الشاهد بأداء التزامه بالإعلام في الجريمة الإلكترونية، لابد أن تتطلب مصلحة التحقيق الحصول على معلومات جوهرية خاصة إذا كان الأمر يتطلب اختراق النظام المعلوماتي لأجل البحث والتنقيب عن أدلة الجريمة الكائنة في هذا النظام.[1]

- ✓ **نموذج أسئلة موجهة إلى الشاهد في جريمة الابتزاز الإلكتروني:**
- ✓ **علاقة الأطراف:**

1. ما علاقتك بالضحية أو المتهم؟

2. منذ متى تعرف الضحية او المتهم؟

- ✓ **تفاصيل حول الواقعة:**

1. ها كنت تعلم بأن الضحية تعرض للابتزاز، الإلكتروني؟ كيف ومتى؟

2. هل أعلمك الضحية بتعرضه للابتزاز؟

- ✓ **معلومات الاتصال بالضحية أثناء حدوث الجريمة:**

1. هل شاهدت الرسائل والمكالمات متعلقة بالابتزاز؟

2. بأي وسيلة تمت عملية الابتزاز (فيسبوك، إنستغرام، تويتر، بريد إلكتروني)؟

3. هل لاحظت على الضحية تغير في سلوكه وتصرفاته اثناء فترة التهديد؟

- ✓ **معلومات عن طريقة الابتزاز:**

1. هل أخبرك الضحية بهوية المبتز؟

2. حل لديك معلومات بكيفية حصول المبتز على معلومات او الصور التي استخدمها؟

3. هل تعرف أشخاصا يمكنهم الشهادة حول الواقعة؟

سادساً: مرحلة المحاكمة:

- ✓ **اختصاص المحكمة:**

ويكون ذلك بتحديد الإطار الجغرافي ودائرة الاختصاص المكاني من إقليم الدولة.

1 – رضا هميسي، **أحكام الشاهد في الجريمة المعلوماتية**، بحث مقدم في إطار أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة_ نوفمبر 2015، ص6.

✓ **الاختصاص المحلي في جريمة الابتزاز الإلكتروني:**

إن جريمة الابتزاز الإلكتروني بين التجريم والمتابعة تكون طبقاً لنص المادة 37 من القانون رقم 04/14 الذي ينص على " يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة وبمحل إقامة أحد الأشخاص المشتبه بمساهمتهم فيها أو بالمكان الذي تتم فيه دائرة القبض على هؤلاء الاشخاص حتى ولو حدث هذا القبض لسبب آخر ".[1]

يتعلق الأمر بكل من محكمة سيدي محمد بالجزائر العاصمة وكذا محكمة قسنطينة ومحكمة ورقلة وقسم محمة وهران، وفي نطاق جريمة التهديد والابتزاز فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الإتلاف عن طريق بث الفيروس وتحقيق النتيجة بتدمير المعلومات في مكان آخر فإن الاختصاص ينعقد في مكان السلوك أو في مكان تحقيق النتيجة، وتعد جريمة التهديد والابتزاز الإلكتروني اذا تمت عن طريق شبكة الأنترنت جريمة مستمرة، بحيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها ومتى كانت جريمة التهديد والابتزاز الإلكتروني أي كان نوعها فقد وسع المشرع الجزائري من اختصاص المحاكم الجزائرية بالنظر في الجرائم المعلوماتية والمتصلة بتكنولوجيات الإعلام والاتصال اذا أُرتكبت خارج الإقليم الوطني، او اذا كان مرتكبها أجنبي وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصلحة الاقتصادية الإستراتيجية للدولة وذلك في إطار التعاون الدولي.[2]

✓ **الاختصاص النوعي في جريمة الابتزاز الإلكتروني:**

يعاقب على جريمة الابتزاز بعقوبات جنحية أو جنائية حسب جسامة الفعل ووفقا للمشرع الجزائري وخاصة قانون الإجراءات الجزائية فأنه

1_ إذا كانت العقوبة المقررة للفعل جنحة (من شهرين الى 5 سنوات مثلا): يكون الاختصاص لمحكمة الجنح، أي قسم الجنح بالمحكمة الابتدائية فيما عدا الاستثناءات المنصوص عليها في المادة 382 من قانون الاجراءات الجزائية.

2 _جناية إذا تجاوزت العقوبة أكثر من5 سنوات أو وجدت ظروف مشددة مثل (التهديد بنشر الصور الفاضحة، استغلال القصر...) هنا يكون الاختصاص لمحكمة الجنايات التابعة للمجلس القضائي حسب المادة 249 قانون الاجراءات الجزائية.

---

1 – أنظر المادة 37 من قانون الإجراءات الجزائية الجزائري

2 – سعيدة بعرة، **الجريمة الإلكترونية في التشريع الجزائري، دراسة** مقارنة، (مذكرة ماستر كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة) _ 2016، ص93.

ولأن الطبيعة التقنية المعقدة أمام الجرائم المعلوماتية تفرض على رجال القضاء لتكوين مهني من متابعة هذه الجرائم، فقد خصصها المشرع مع بعض انواع الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة العابرة للحدود الوطنية وجرائم تبييض الأموال والجرائم المتعلقة بالإرهاب والجرائم المتعلقة بالتشريع الخاص، بالصرف بإجراءات خاصة إذ جعل الاختصاص ينعقد في دائرة اختصاص أخرى، وهذا ما نصت عليه المواد 37 _40 والمادة 329 من قانون الإجراءات الجزائية.[1]

✓ **إجراءات المحاكمة:**

تبدأ المحكمة جلستها بإعلان افتتاحها بعبارة: "باسم الشعب الجزائري، الجلسة علنية"، بعدها تنادي على جميع الأطراف المعنية بالقضية، مثل المتهم، الضحية، الشهود، والمسؤول المدني، وذلك للتأكد من حضورهم.

إذا كان أحدهم غائبًا، تتحقق المحكمة من هويته ومن تبليغه بالتهمة الموجهة إليه والمادة القانونية التي تنطبق عليه.

أما إذا ثبت غيابه دون عذر مقبول، فقد تقرر المحكمة تأجيل القضية إلى أقرب جلسة ممكنة.

وفي هذه الحالة طبقاً لأحكام المادة 339 "مكرر6" المتحدثة بموجب الأمر02/ 15المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية التي تنص على إذا قررت المحكمة تأجيل القضية.

يمكنها بعد الإستماع إلأى طلبات النيابة العامة والمتهم ودفاعه اتخاد التدابير التالية:

1. ترك المتهم حراً.
2. إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 من قانون الإجراءات الجزائية الجزائري.
3. وضع المتهم الحبس المؤقت والإشارة إلى أن هذه التدابير لا تقبل الاستئناف.[2]

المطلب الثاني: المعيقات التي تواجه جهات التحقيق في جريمة لابتزاز الإلكتروني:

في زمن أصبحت فيه التكنولوجيا جزءاً لا يتجزأ من حياتنا اليومية، ظهرت أشكال جديدة من الجرائم لم نكن نعرفها من قبل، ومن بينها جريمة الابتزاز الإلكتروني، التي أصبحت تؤرق الكثير من الأفراد وتهدد

1 – سعيدة بعرة، المرجع السابق، ص93.

2 – أنظر المادة 339مكرر6 من قانون الإجراءات الجزائية الجزائري

خصوصيتهم وأمانهم. ومع انتشار هذه الظاهرة، برز دور جهات التحقيق في محاولة كشف الجناة وإيقافهم عند حدهم.

لكن الواقع يثبت أن طريق التحقيق في مثل هذه الجرائم ليس مفروشاً بالورود، بل تعترضه الكثير من العقبات. فهناك صعوبات قانونية، حيث لا تزال بعض التشريعات عاجزة عن مجاراة تطور الجريمة الرقمية. وهناك أيضاً مشاكل تقنية، فالجناة غالباً ما يستخدمون وسائل متطورة لإخفاء هويتهم، مثل الشبكات المظلمة والبرمجيات المشفّرة، ما يجعل من عملية التتبع أمراً معقداً جداً.

ولا يقتصر الأمر على ذلك، بل إن التعاون الدولي في هذا المجال غالباً ما يكون ضعيفاً أو بطيئاً، خاصة عندما يكون الفاعل موجوداً خارج حدود الدولة، ما يجعل من مهمة التحقيق تحدياً حقيقياً يفرض على الجهات المختصة التفكير في حلول جديدة ومبتكرة لمواكبة هذا النوع من الجرائم.

الفرع لأول: عائق اكتشاف الجريمة المرتكبة عبر شبكة الأنترنت:

<u>أولا</u>: عوائق تتعلق بالجريمة المعلوماتية

قد تتعرض اكتشاف الجريمة الإلكترونية لعدة صعوبات من بينها:

1-خفاء الجريمة وغياب الدليل المرئي المكان بالقرأة فهمه.

2-افتقاد أكثر أثار التقليدية.

3-إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية الغنية كاستخدام كلمات الشر حول مواقع تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع عليها أو استنساخها.

4-سهولة محو الدليل او تدميره في زمن قصر جدا، ومن الأمثلة على ذلك قيام أحد المهربين الأسلحة في النمسا بإدخال تعديلات على لأوامر العادية للنظام عن طريق استخدام جهاز الحاسب لآلي الذي يستخدموه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطبيعة إلى هذا الحاسب من خلال لوحة مفاتيحه مما تمكنه من نحو وتدمير كافة الديانات الكاملة.

كما يمكن للجاني محو الأدلة التي يمكن أن تكون ضده ويمكنه تدميرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذ ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف

بالمحو السريع عدم استطاعة هذه السلطات من إقامة الدليل ضده، وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعه إلى الخطأ في نظام الحساب لألي أو في الشبكة أو في لأجهزة.[1]

ثانيا: فقدان لأثار المادية الجريمة:

تضل الجريمة المرتكبة عبر الأنترنت مجهولة مالم يبلغ عنها للجهات المهنية لاستدلالات أو التحقيق الجنائي، فهي تعتبر جرائم غير تقليدية لا تختلف عن الجرائم المادية حيث تضع الوسيلة التي ترتكب بها الجريمة ضمن قالي غير تقليدي تصرا إلى ارتكابها يتم عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب لآلي، وشبكة الاتصالات بصورة آلية كما تنساب الكهرباء عبر الأسلاك، ويكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو حتى قواعد بيانات أو أنظمة بأكملها، فتأتي من هنا مشكلة ضبط هذه المعطيات التي تبقي في الحالة المستعمل، إلا أنها في بعض لأحيان لا تتواجد عادة لدي مصالح الشرطة القضائية المكلفة بالبحث أو حتى حالة حجز المعطيات الرقمية، فإن البيانات التي تحصل عليها لا تتضمن آثار أو بصمات يمكن استبدال من خلالها على صاحبها.[2]

كما تجد صعوبة التوصل إلى للجاني فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام اسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت، فيصعب تحديد الجاني وتحديد موقع اتصاله.

-تنازع القوانين الجنائية من حيث المكان، إذا أن هناك مبادئ تحكم تطبيق القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الجرائم في الخارج.

-عدم ظهور الدليل المادي الجريمة الإلكترونية أو أثار مادي ملموس.

-عجز الوسائل التقليدية عن ضبط أثار الجريمة الإلكترونية.[3]

الفرع الثاني: العوائق المتعلقة بجهات التحقيق.

إن بعض هده العوائق ترجع إلي شخصية المحقق مثل: التهيب في استخدام جهاز الكمبيوتر والتهيب في استخدام الأنترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

1 - عائشة بن قارة مصطفى، المرجع السابق، ص65.

2 - صغير يوسف، المرجع السابق، ط1، ص117

3 - نايري عائشة، المرجع السابق، ص 55-56.

أما البعض الأخر يتعلق بالنواحي الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، كما تجد أن نقص المهارات في استخدام الكمبيوتر والأنترنت، وعدم توفر المعرفة بأساليب ارتكاب الجرائم المعلوماتية، وقلة الخبرة في مجال التحقيق في جرائم الكمبيوتر والأنترنت تنقص المعرفة بالغة الإنجليزية، لاسيما ان للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة أصبحت تشكل الطابع المميز لمحادثتهم واختلاف أساليب التفاهم معهم، وليس هذا فحسب بل اختصر المعلومات في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بالغة المختصرات وهي لغة جديدة ومتطورة.

وكل هذا دفع بمعتادي الإجرام المعلوماتي أن يطلقوا على أنفسهم صفة النخبة وفي ذات الوقت يطلقون على رجال إنقاذ القانون صفة الضعفاء أو القاصرين.[1]

من بين أبرز الصعوبات التي تواجه التحقيق في جريمة التهديد والابتزاز الإلكتروني، يمكن التمييز بين نوعين من الصعوبات:

أولاً: الصعوبات الموضوعية، وتتمثل فيما يلي:

1_الطبيعة المعقدة والفنية للجريمة الإلكترونية، والتي تجعل من الصعب استخراج البيانات من الأجهزة المستعملة كالهواتف أو الحواسيب.

2_غموض النصوص القانونية وعدم وضوحها في بعض الأحيان، مما يصعّب على الجهات القضائية تفسيرها وتطبيقها.

3_ استعمال لغة تقنية دقيقة في مجريات التحقيق والمحاكمة، ما يتطلب تكويناً متخصصاً للمحققين والقضاة

4_تعقيد الإجراءات المتعلقة بجمع الأدلة، خاصة تلك التي تستدعي تعاون جهات خارجية وسلطات بحث وتحري متقدمة.

ثانيًا: الصعوبات الإدارية، والتي تتجلى في

1_صعوبة تحديد الجهة المسؤولة عن متابعة الجريمة عند بدايتها.

2_نقص التنسيق بين مختلف الجهات المعنية بالكشف عن هذه الجرائم.

3_البطء في تحريك المتابعة القانونية ضد مرتكبي الجرائم الإلكترونية.

1 – خالد ممدوح إبراهيم، المرجع نفسه، ص ص69_70.

المبحث الثاني: الأدلة الجنائية في إثبات وقوع جريمة الابتزاز عبر الوسائل الإلكترونية.

تعتبر الجرائم المعلوماتية صنفاً جديدا من الجرائم، وذلك لارتكابها بتقنية حديثة وهي تكنلوجية المعلومات والاتصالات، وظهر بذلك نوع جديد من المجرمين لينتقل بالجريمة من صورتها التقليدية إلى إلكترونية حديثة مما استوجب تحول الدليل الجنائي من صورته التقليدية إلى الرقمية وإذا كان الدليل الجنائي التقليدي يشترط لقبوله امام القضاء أن يكون صريحاً ومباشراً وذالا بذاته على الواقعة المراد إتباعها، فإن الدليل الجنائي الرقمي هو الآخر يجي ان يتوافر على خصائص كي يتم قبوله أمام القضاء.[1]

وعليه فإن في إطار هذه الإشكالية يمكن طرح التساؤل الآتي:

ما المقصود بالدليل الجنائي الرقمي؟

ما هي الشروط المهمة لتحقق من صحة الدليل الرقمي والمصادر المتحصل عليها؟

المطلب الأول: ماهية الدليل الجنائي الرقمي.

يعد الدليل الرقمي من أدلة الإثبات الجنائي المستحدثة، التي أفرزتها التطورات الجارية والمتسارعة بتقنية الاتصالات والمعلومات، والتي تقتنيها وتحدثها بما يتفق مع متطلبات العصر.

وهذا النوع من الأدلة هي أدلة تمكن أجهزة العدالة من مواجهة الجرائم المعلوماتية المستحدثة بدأت الأسلوب المعلوماتي، كما تساعد في الكشف عن الجرائم التقليدية بحسابات دقيقة لا يتطرق اليها الشك.[2]

إن عبارة الدليل الرقمي تتكون من شقين: الدليل، الرقمي.

ومصطلح الدليل: ما تقوم به الحجة لثبوت وصحة القضية.

ومصطلح الرقمي: يطلق عليه النظام الرقمي أو عملية الرقمنة.

الفرع الاول: مفهوم الدليل الرقمي.

هو كل وسيلة مرخص بها أو مسموح بها قانونا، لإثبات وجود أو عدم وجود الواقعة المرتكبة او صحة او كذب وقوعها، أي أنه الدليل مطلوب للإثبات الجنائي الرقمي لكي لا يكون ثمة فصلا في الدعوى الجنائية (الدعوى العمومية) بالبراءة أو الادانة، والدليل هو قوام حكم القاضي وله أن يقدر أهميته وملائمته، ويجب

---

1 – بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائري (دراسة مقارنة)، **المجلة القانونية للبحث القانوني**، م (5)، ع (1)، ص277.

2 – حسام توكل موسى، **حجية الأدلة الرقمية في الإثبات الجنائي**، دراسة في ضوء القانون 175_2018، في شأن مكافحة جرائم تقينية المعلومات، ط1_2023، ص17.

على القاضي ان يطلب من المدعي إثبات دعواه ولا يقبل منه ادعاءه مجرداً من دليل اثباته، وان يناقش هذا الدليل ولا يقضي له بمقتضاه الا بعد استثاقه من صدق الدليل وصلاحيته بإثبات الحق المدعى به او نفيه، ولا يقتصر الأمر على ذلك بل يجب ان يقبل مقدم الدليل مناقشة خصمه للدليل الذي قدمه وأن مستعدا للرد عليه.[1]

والادلة الرقمية هي جميع الأدلة المستمدة من البيانات المخزنة أو المنتجة بواسطة أجهزة الحاسب الآلي أو الأنظمة المعلوماتية أو المنقولة بواسطتها، التي يمكن اعتمادها بوصفها وسيلة إثبات امام المحكمة.

والأدلة الرقمية هي المعلومات أو البيانات المخزنة أو المنقولة بتنسيق ثنائي، التي يمكن الاعتماد عليها بوصفها أدلة لدى المحاكم ويمكن أن توجد هذه الأدلة على أجهزة متنوعة مثل: الحواسيب، الهواتف المحمولة، الألواح الذكية، او الكاميرات، أجهزة الأنترنت.[2]

كما يعرف بأنه معلومات يقبلها المنطق والعقل ويعتمدها العلم، ويتم الحصول عليها بإجراءات قانونية علمية يترجم البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة أو جانٍ أو مجني عليه.

الفرع الثاني: شروط تحقق من صحة الدليل الرقمي والمصادر المتحصل عليها:

<u>أولا</u>: شروط تحقق من صحة الدليل الرقمي:

- **مشروعية الدليل الرقمي:**

1. الدليل الرقمي يجب أن يكون مشروعا:

أي أن إجراءات جمع الأدلة الرقمية المتحصل عليها من الحاسب الآلي إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة ولا تصلح بأن تكون أدلة تبني عليها الإدانة في المواد الجزائية، فإجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور

1 – محمود مدين، **فن التحقيق والإثبات في الجرائم الإلكترونية**، ط1 _ المصرية للنشر والتوزيع_2020، ص106.

2 – عبد الرزاق مرجان، الدليل **الإسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية**، جامعة نايف العربية للعلوم الأمنية، دار جامعة نايف للنشر 2024، ص15.

وإلا فإن الدليل المستمد بطريقة مخالفة للأحكام الواردة في الدستور يكون باطلا بطلانا مطلقا وذلك لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به، كما أن المحكمة أن تقضي به من تلقاء نفسها.[1]

2. يجب أن يكون الدليل غير قابل للشك:

أي لابد أن يكون يقيني، ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي إلى يقين، حيث يصل إليه القاضي بعد عرض الأدلة الرقمية، فمن خلال ما يعرض عليه من مخرجات إلكترونية، فما ينطبع من ذهنه من تصورات واحتمالات بالنسبة لها سيحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.[2]

3. إمكانية مناقشة الدليل الإلكتروني:

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة فالقاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت الحرية المناقشة أطراف الدعوى إذ لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصل المناقشة فيها حضوريا أمامه، وهذا يعني أن الأدلة المتحصل عليها من جرائم الحاسوب والأنترنت سواء كانت مطبوعة أم بيانات معروفة على شاشة الحاسوب أم كانت بيانات مدرجة في حاملات البيانات أم اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصغرات فلمية وكل هذه ستكون محلا المناقشة عند الأخّذ بها كأدلة إثبات أمام المحكمة.[3]

ثانيا: المناظر المتحصل عليها:

إن الحصول على هذه الأدلة يستوجب الإحاطة بجميع مصادر المتعددة وذلك من أجل تحصيل الدليل الرقمي والحفاظ على حجيته أمام الفضاء وأن التعرف على مصادره يعتبر الخطوة الأولى في طريق التحقيق الجنائي الرقمي.

---

1 – بن الطيبي مبارك، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، **مجلة القانون والعلوم السياسية**، جامع أحمد دراية –أدرار–م (5)، ع(2) _2019، ص 27

2 – آمال برحال، **جريمة الابتزاز عبر الوسائل الإلكترونية**، (مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي_ تبسة) 2019_2020، ص91.

3 – بن الطيبي مبارك، المرجع السابق، ص27_28.

- **إجراء الإرشاد الجنائي:**

الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها للولوج للعالم الافتراضي باهي عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستعملين صفات وهمية من أجل الكشف عن هذه الجرائم تكشف المجرمين فهذا الإجراء لا يتطلب جهد مادي كبير حيث يقوم ضباط الشرطة القضائية أو يكلف غيره من دوي الاختصاص وهذا بعد الحصول على إذن رسمي القيام بمهام البحث والتحري للجرائم على ضبط مرتكبيها ولقد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت اسم التسرب من خلال النصوص والمواد "65 مكرر 5 إلى غاية المواد 65مكرر18 من ق، إ، ج " وذلك بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق تحت رقابة وكيل الجمهورية لمدة "4 أشهر قليلة لتجديد".[1]

- **إجراء الوضع تحت المراقبة إليكترونية:**

فهي العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجميع البيانات والمعلومات للمشتبه فيه من أجل تحقيق غرض أمني أو غرض أخر وهي مرتبط ارتباطا وثيقا بالزمن وقد أجاز المشرع الجزائري المراقبة الإلكترونية في جرائم المعلوماتية عن طريق اعتراض المراسلات التي تتم بواسطة الوسائل الاتصال السلكية ولاسلكية، كما أجاز كل ترتيبات التقنية لها دون علم المعنيين ودون موافقتهم بغية الحصول على تسجيلات الكلام الصادرة عنهم بصفة سرية أو خاصة ويكون ذلك بإذن من وكيل الجمهورية.

- **تعاون مقدمي خدمات الأنترنت والسلطات القضائية:**

إن المشرع قد فرض على مستخدمي الأنترنت مجموعة من الالتزامات من أجل السلطات القضائية وذلك في أعمال التحقيق وذلك من خلال قانون رقم 09/04 في فصله الرابع تحت عنوان "إلتزامات مقدمي الخدمات " ومن أهم الالتزامات الواردة نجد:

الالتزام بمساعدة السلطات والالتزام بحفظ المعطيات المتعلقة بحركة السير.[2]

1 – آمال برحال، المرجع السابق، ص93.

2 – آمال برحال، المرجع السابق، ص93_94.

المطلب الثاني: صعوبات الإثبات الجنائي في جريمة لابتزاز الإلكتروني:

تعتبر جريمة لابتزاز الإلكتروني من الجرائم المعقدة والخطيرة وذلك لما لها من أثار نفسية واجتماعية واقتصادية على الضحايا، وتكمن خطورتها في أنها تتم عن بعد وغالبا ما تكون من وراء الشاشات وأسماء مستعارة مما يصعب عملية تعقب الجاني وإثبات مسؤوليته.

ويعتبر الإثبات الجنائي في هذه الجرائم أحد أكبر التحديات التي تواجه جهات التحقيق والقضاء وذلك نظرا لخصوصية الدليل الرقمي وسهولة طمسه أو تعديله كما نجد بأن الطبيعة النفسية والاجتماعية للجريمة تدفع العديد من الضحايا إلى عدم التبليغ وذلك خوفا من الفضيحة أو الإحراج ماما يزيد صعوبة الإثبات الجنائي.

ومن هنا يمكننا تسليط الضوء على أبرز الصعوبات القانونية والعلمية التي تعيق عملية الإثبات الجنائي في جريمة لابتزاز الإلكتروني ولهذا نقوم بطرح الإشكالية التالية:

-ماهي أهم الصعوبات المرتبطة بالدليل نفسه؟

-وماهي الصعوبات التي تواجه التعاون الدولي ؟.

وهذا ما سنقوم بتوضيحه في الفرعين الآتيين بحيث سوف نتناول في:

الفرع الأول: الصعوبات المرتبطة بالدليل نفسه.

أما في الفرع الثاني: والذي سيكون مختص بالصعوبات أو العراقيل التي تواجه التعاون الدولي.

الفرع الأول: الصعوبات المرتبطة بالدليل نفسه:

الدليل الجنائي في الجرائم المعلوماتية له طبيعة خاصة، فهو ذو طابع فني في غاية الدقة، فضلا عن ذلك فيتميز بصعوبة استخلاصه أن يتطلب مهارة في التحكم بالتقنية العالية للحاسب الآلي. ويمكننا أن نذكر أهم الصعوبات المتعلقة بطبيعة الدليل والتي تعترض المحقق اثناء تحريه عن الجريمة المعلوماتية وذلك على النحو التالي:

1. أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة:

تتنوع الأدلة المعلوماتية من حيث طبيعتها مثل سجلات الحاسب الالي ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، ولذا فهذه الأدلة تثير أمام القضاء مشكلات عديدة؛ ولاسيما فيما يتصل بمدى قبولها وحجيتها والمعايير اللازمة لذلك.

2. الضخامة البالغة لكم البيانات المتعين فحصها:

تحتوي الانظمة المعلوماتية على كم هائل من البيانات والمعلومات، بحيث أن طباعة هذه المعلومات على الورق يتطلب مئات الالاف من الصفحات، اما حجز البيانات الالكترونية فلا يقلل من صعوبة البحث عن الدليل الرقمي، فضخامة حجم هذه البيانات يجعل من مهمة الاطلاع عليها بصفة كلية امرا مستحيلا مما يجعل من الاستعانة بالخبرة الفنية لتحديد ما يجب ضبطه امر لا مناص منه، اذ لا بد من الاستعانة بما تتيحه التكنولوجيا الحديثة في نظم المعالجة الآلية للمعطيات في مجال فحص والتدقيق في هذه المعطيات التي تحتوي على دليل الجريمة او كما يعرف بالدليل الرقمي.[1]

3. سهولة محو الدليل أو تعديله:

من الصعوبات التي يمكن أن تعترض عملية الحصول على الدليل الرقمي وبالتالي إثبات الجريمة المعلوماتية ونسبتها إلى المتهم سهولة تعديل الدليل الرقمي أو محوه وتدميره في فترة زمنية وجيزة، كونه دليل غير مرئي فهو عبارة عن نبضات مغناطيسية وبالتالي فمحوها يكون سهلا ولا يترك أي أثر بعكس ما هو الحال عليه بالنسبة للدليل المادي، كما أن الجاني يستطيع تدميره من بعد ومن أي منطقة من العالم، فضلا عن سهولة تنصله عن هذا العمل، كما أن الجاني يستطيع الدفع بأن الدليل قد تم تعديله فمجرد ضربات على لوحة المفاتيح تستطيع تغيير بيانات بإدانة شخص أو تبرئته لذلك فإن غالبية هذا النوع من الجرائم إما أن يقيد باسم مجهول لاستعمال أصحابها أسماء مستعارة، أو دخولهم إلى شبكة الإنترنت من خلال مقاهي الإنترنت مما يتعذر الوصول إلى الجناة الحقيقيين لتلك الجرائم وعليه نجد أن القاضي يصعب عليه إدانة شخص دون أن يتأكد يقينيا بأن هذا الشخص هو المذنب في ارتكاب الجريمة ويرى جانب من الفقه حول ضرورة تدخل المشرع بإضافة حالة ارتكاب الجرائم المعلوماتية كظرف استثنائي يسمح لرجال السلطة العامة القيام بضبط الأدلة عند وقوع الجريمة

دون الحصول على إذن سابق من النيابة العامة لتفادي مثل هذه الدفوعات.[2]

4. الطبيعة الخاصة للدليل في الجرائم المعلوماتية

فهو ليس بدليل مرئي يمكن فهمه بمجرد القراءة، ويتمثل الجرائم التي تقع عليها أو بواسطتها – في بيانات غير مرئية لا تفصح عن شخصية معينة عادة. حسب ما تتيحه النظم المعلوماتية من أدلة على

1 – معتوق عبد اللطيف، المرجع السابق، ص117.

2 – بن فردية محمد، المرجع السابق، ص215_216.

وتظهر هذه المشكلة بصفة خاصة بالنسبة لجرائم الانترنت مثل، الجرائم التي ترتكز على البريد الإلكتروني في ارتكابها، حيث يكون من الصعب على جهات التحري تحديد مصدر المرسل، ويسهل ارتكاب جرائم الاعتداء على النظم المعلوماتية بسبب هذه الطبيعة غير المرئية لدليل. الجريمة، والأمثلة كثيرة بهذا الخصوص، ومنها قيام أحد المبرمجين بمركز حاسبات إحدى الشركات الألمانية بإعداد برنامج في حاسب الشركة يتيح له ادخال بيانات مرتبات أشخاص وهميين إلى ذاكرة الحاسب وتحويل هذه المرتبات الى حساب خاص له، وحتى لا تتم طباعة هذه البيانات على الأوراق، فقد أجرى الجاني تعديلا على البرنامج يمنع امكانية طباعة هذه البيانات الوهمية في كشف الرواتب عند مراجعتها، كما نجح في اقتطاع الأموال التي تحصل عليها من حساب اجمالي الضرائب بحيث لا تظهر هذه الأموال في حسابات الشركة ولا يمكن ادراك وجود عجز في ميزانيتها، وبعد اكتشاف أمره صدقة بعد استيلائه على مبلغ 193.000 مارك حكم عليه بالحبس سنتين بتهمة الاحتيال واساءة الائتمان

5. صعوبة الوصول إلى الدليل:

حيث تقوم الشركات الكبرى والمواقع العالمية المعروفة على الانترنت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلالة عليها أو نسخها، ويمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه وذلك من خلال استخدامه كلم مرور بعد تخريب الموقع مثلا، أو استخدامه تقنيات التشفير.[1]

ولصعوبة استخلاص الدليل في مثل هذه الجرائم يري المختصين في جرائم الحساب الآلي أن هدا الجهاز وما يقعد عليه من جرائم معلوماتية يعد تحديد هائلا لرجال الأمن وذلك أن رجل الأمن غير متخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية عالية.[2]

الفرع الثاني: صعوبة التعاون الدولي:

يعتبر التعاون الدولي ركيزة أساسية في مواجهة مختلف الجرائم إلكترونية وذلك بسبب التطور السريع لها وتوسعها في الفضاء الرقمي وعلى رأسها جريمة الابتزاز الإلكتروني التي تمثل تهديدا متزايدا للأفراد والدول على حد سواء إلا أنها لا تقتصر على الجانب المادي فقط بل تمتد لتشمل مختلف الأبعاد منها

1 – معتوق عبد اللطيف، المرجع السابق، ص116.

2 – عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت**، ط1، دار الفكر الجامعي مصر، ص89.

النفسية والاجتماعية وغيرها ومع تعقد أساليب الابتزاز وغيرها بات التعاون الدولي أمر ضروريا من أجل مواجهة مختلف هده الجرائم بفعالية أكثر، إلا أن هذا التعاون يصطدم بالعديد من الصعوبات التي أصبحت تعتبر بمثابة عائق من أجل التصدي لهده الجريمة الإلكترونية بحيث أصبحت تشكل تحديا دقيقا من أجل محاربة هذه الظاهرة.

في عالم مزدحم بشبكات اتصالية دقيقة ومتطورة تنقل وتشغل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، ما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية ومن بينها جرائم الإنترنت أمرا محتما.[1]

ومن بين أكثر الصعوبات التي تواجهها نجد:

1. **عدم وجود نموذج موحد النشاط الإجرامي:**

فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية لا يوجد فيها اتفاق عام مشترك حول نماذج إساءة استخدام النظام المعلوماتي وشبكة الأنترنت الواجب تجريمها، فما يكون مباحا في بعض الأنظمة يكون محرما في أنظمة أخرى، ويرجع ذلك إلى عدة عوامل كاختلاف العادات والتقاليد والديانات والثقافات من مجتمع لأخر.

2. **اختلاف النظم القانونية الإجرائية:**

ويكون ذلك بسبب تنوع واختلاف النظم القانونية الإجرائية حيث نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى.

3. **عدم وجود معاهدات ثنائية أو جماعية بين الدول:**

وحتى في حالة وجودها فإنها تكون قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم والبرامج الحاسب الآلي وشبكة الأنترنت.

4. **مشكلة الاختصاص في جرائم الأنترنت:**

وتثار هذه المشكلة بالنسبة للاختصاص على المستوى الدولي وذلك للاختلاف التشريعات والنظم القانونية من دولة لأخرى حيث ينجم عنها تنازع الاختصاص بين هذه الدول بالنسبة للجرائم المتعلقة

1 – عبد العزيز لطفي جاد الله، **أمن المجتمع الإلكتروني بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية**، ط1، مكتبة الوفاء القانونية الاسكندرية، 2017، ص187.

بالأنترنت التي تتميز بكونها عابرة للحدود، فيحدث أن ترتكب داخل إقليم دولة معينة إلا أنها تمتد إلى خارج إقليم دولة أخرى ماما يعني خضوعها لأكثر من قانون جنائي.[1]

كما نجد أيضا:

5. القصور التشريعي الدول والتعارض بين مصالحها:

حيث نجد أن الاختلاف في الأنظمة القانونية الدول يعد عقبة كبيرة تعترض سبيل التعاون الدولي بين تلك الدول في مجال مكافحة جرائم التوقيع إليكترونية وذلك لما يترتب عنه من مشكلات تطبيق القانون في الواقع العلمي، بالإضافة إلى قصور غالبية النظم التشريعية للدول وذلك من خلال وضع مفهوم محدد للجرائم، كما نجد قصورها في النظام القانوني خاصة لمختلف تلك الجرائم مما يجعل التعاون الدولي أمرا صعبا وهذا ما ينعكس بالسلب على مختلف القرارات في مختلف المجالات الفكرية والقوانين في مختلف الدول.

6. المشكلات الخاصة بالإنابة القضائية الدولية:

وكذلك من إشكاليات التعاون الدولي في مجال مكافحة جرائم التوقيع أو الابتزاز الإلكتروني خاصة المتعلقة بالإنابة القضائية الدولية أو ما يعرف بإشكالية "فكرة السيادة "والتي تعني بدورها أن "**الدولة** هي السلطة العليا ولا تعلوها أي سلطة في الداخل والخارج" بما يعني ذلك من استئثار جهة الحكم في الدولة بكافة اختصاصات السلطة ومظاهرها دون أن تخضع في ذلك لأي جهة أعلى ودون أن تشارك معها في تلك السلطة أو أي جهة مماثلة مما ينتج عنها من اصطدام بفكرة السيادة.[2]

ونجد أيضا صعوبات التعاون الدولي المتصلة بمجالات التدريب تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات.

ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأقران المتدربين لاسيما

---

1 – الطيبي البركة، إشكالية الإثبات في الجرائم إلكترونية، مخبر القانون والتنمية المحلية، جامعة أدرار، **مجلة أفاق علمية**، م (11)، ع (1) _ 2019، ص 279.

2 – ترجمان نسيمة، التعاون الدولي في مكافحة جرائم التوقيع إلكترونية، **مجلة صوت القانون**، جامعة ابن خلدون تيارت م (7) ع(1)، 2021، ص 6 –70.

في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه وجد بعض الأشخاص ممن لا يعي في هذا المجال شيء على النظير يوجد أُناس على درجة كبيرة من المعرفة والثقافة في هذا المجال.

بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نصف التعاون الدولي في هذا المجال.

أيضا من الصعوبات التي قد تؤثر على العملية التدريبية وعلى التعاون الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية وعدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلا تاما ومتقنا، من حيث ما يدور بها من وقائع وملابسات وإجراءات، وما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية.[1]

1 – عبد العزيز لطفي جاد الله، المرجع السابق، ص191.

خلاصة الفصل:

يتناول هذا الفصل جل الإجراءات القانونية والفنية التي تعتمدها السلطات المختصة في مكافحة جريمة الابتزاز الالكتروني، وكل اجراءات التحقيق بدأً من تلقي الشكوى مروراً بجمع الأدلة الرقمية وتحليلها وتقديمها كوسائل إثبات أمام الجهات القضائية، وتبرز الأهمية في التعامل مع هذا النوع من الجرائم في طابعها الفني المعقد للأدلة الرقمية والتي تستوجب خبرات فنية دقيقة لضمان مشروعيتها وجوهرها القانوني، كما يناقش هذا الفصل كل أنواع الأدلة المستخدمة مثل: الرسائل الالكترونية وكل تطبيقات التواصل الاجتماعي والبيانات المستخرجة من الأجهزة أو الخوادم، كما يؤكد على ضرورة تعزيز الكفاءات التقنية لذى الجهات المختصة وتطوير آليات التعاون بين مختلف الأطراف المعنية بما في ذلك مزودي الخدمات الرقمية من أجل فعالية التحقيقات والإثبات في هذا المجال، وفي ختام هذا الفصل يتم التأكيد على تطوير قدرات الجهات الأمنية والقضائية للتصدي لهذا النوع من الجرائم بما يتضمن التحولات التكنولوجية المتسارعة.

خاتمة

خاتمة:

مع اتساع الاعتماد على التكنولوجيا في جميع مجالات الحياة، لم تعد الجرائم التقليدية هي الوحيدة التي تهدد أمن الأفراد واستقرار المجتمعات، بل ظهرت جرائم جديدة تستغل هذا التطور التكنولوجي لتحقيق أهداف إجرامية خطيرة، من بينها جريمة الابتزاز الإلكتروني، التي تُعد من أبرز الجرائم المعاصرة وأكثرها تعقيدًا من حيث الوسائل والأساليب فقد أصبحت التكنولوجيا حاضرة في جميع مجالات الحياة من الهواتف الذكية، وشبكات التواصل الاجتماعي والبريد الالكتروني ألى التخزين الحسابي وكاميرات المراقبة والتطبيقات الذكية، ورغم ان هذه الادوات صُممت لخدمة الانسان وتسهيل حياته الا ان الاشخاص أساؤوا استخدامها فحولوها الى وسائل لارتكاب الجرائم الخفية التي يصعب اكتشافها كما نرى اثرها على الأفراد، خاصة مع سهولة ارتكابها من وراء الشاشات، وصعوبة تعقب الجناة نظرًا لاعتمادهم على وسائل تقنية متقدمة تساعدهم على إخفاء هويتهم أو حتى التمويه بمواقع جغرافية مزيفة. كما تبين أن المشرع الجزائري وإن أبدى وعيًا جزئيًا بخطورة هذه الجريمة، إلا أن النصوص القانونية المخصصة لها لا تزال تعاني من بعض الغموض والقصور، ما يؤثر سلبًا على فعالية مواجهتها.

وبناءً على ما سبق، توصلنا إلى جملة من النتائج، يمكن التطرق اليها في النقاط التالية منها:

- أن جريمة الابتزاز الإلكتروني لا تزال تُعالج في أغلب الحالات ضمن الإطار العام للابتزاز أو التهديد في قانون العقوبات، دون وجود نصوص صريحة ومفصلة تأخذ بعين الاعتبار خصوصية الوسائل الإلكترونية.
- أن إثبات هذا النوع من الجرائم يُعد تحديًا كبيرًا، نظرًا لاعتماد الجناة على حسابات وهمية، وبرامج تشفير، وشبكات افتراضية خاصة(VPN) ، ما يجعل الوصول إليهم أمرًا معقدًا دون تجهيزات تقنية متطورة.
- أن الجهات المكلفة بالتحقيق والمتابعة في مثل هذه الجرائم ما زالت في حاجة ماسة إلى دعم تقني وتكوين متخصص يمكنها من التعامل مع الأدلة الرقمية بكفاءة عالية
- أن الضحايا، خصوصًا من فئة النساء والقصر، غالبًا ما يترددون في التبليغ عن هذه الجرائم بسبب الخوف من الفضيحة أو فقدان السمعة، وهو ما يشجع المجرمين على التمادي في أفعالهم.
- أن التنسيق بين مختلف الهيئات الأمنية والقضائية، وحتى الدولية، ما زال دون المستوى المطلوب، رغم الطابع العابر للحدود الذي يميز هذا النوع من الجرائم.

وبناءً على ما سبق، توصلنا إلى جملة من التوصيات، نراها ضرورية لتعزيز فعالية التصدي لجريمة الابتزاز الإلكتروني، منها:

- ضرورة تبني نصوص قانونية خاصة تتعلق بالابتزاز الإلكتروني، توضح تعريفه وأركانه وصوره المختلفة، بما ينسجم مع التطورات الحاصلة في العالم الرقمي.
- تطوير قدرات الجهات الأمنية والقضائية من خلال إدماج التكوين المستمر في مجال الجرائم الإلكترونية، مع التركيز على آليات التحقيق الرقمي، وجمع الأدلة الإلكترونية وحفظها.
- استحداث وحدات مختصة في التحقيق في الجرائم الإلكترونية على مستوى كل ولاية، تكون مزودة بكوادر بشرية مؤهلة وتجهيزات تقنية متقدمة.
- تعزيز التوعية المجتمعية حول خطورة الابتزاز الإلكتروني، وضرورة الحذر في التعامل مع الوسائل الإلكترونية، لاسيما عند مشاركة المعلومات والصور الشخصية، وتشجيع ثقافة التبليغ عبر قنوات مضمونة تحترم خصوصية الضحية.
- تدعيم التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، من خلال الاتفاقيات الثنائية والمتعددة الأطراف، لتبادل المعلومات والخبرات وملاحقة الجناة عبر الحدود.
- إدراج مادة دراسية حول التوعية الرقمية ضمن البرامج التعليمية، خاصة في الطورين المتوسط والثانوي، تُعرّف التلاميذ بمخاطر الإنترنت وأساليب الوقاية من الابتزاز والجرائم الإلكترونية عمومًا.
- إنشاء منصة وطنية إلكترونية للتبليغ عن الجرائم الإلكترونية، تكون سهلة الاستخدام وآمنة، وتُتيح للضحايا الإبلاغ بسرية تامة، مع توفير الدعم القانوني والنفسي
- تفعيل دور الإعلام الوطني (التلفزيون، الإذاعة، الصحافة، المنصات الرقمية) في نشر ثقافة الحذر الرقمي، عبر حملات توعية موجهة لمختلف شرائح المجتمع.
- إشراك المجتمع المدني والجمعيات المختصة في التكنولوجيا وحقوق الإنسان، للمساهمة في التوعية والمرافقة النفسية والاجتماعية للضحايا.
- العمل على تحديث التشريعات باستمرار، لمواكبة تطور الوسائل الرقمية وتنوع أساليب الجريمة، بما في ذلك النصوص الخاصة بأدلة الإثبات الرقمي وإجراءات التحري.
- تشجيع البحث العلمي في مجال الأمن السيبراني والجرائم الإلكترونية، عبر تمويل مشاريع بحث جامعية وإنشاء مخابر متخصصة تدرس الظاهرة وتقترح حلولًا وطنية فعالة.
- فرض رقابة أكثر صرامة على مقاهي الإنترنت والأماكن العمومية التي تقدم خدمات اتصال غير مراقبة، وتسجيل البيانات الأساسية لمستخدميها عند الضرورة.

- وضع دليل إجرائي موحد للتحقيق في الجرائم الإلكترونية موجه للضبطية القضائية، يوضح الخطوات المثلى لجمع الأدلة الرقمية والحفاظ عليها.
- تعزيز أطر التعاون بين شركات الاتصالات والهيئات الأمنية لتسهيل عملية تتبع الحسابات المشبوهة وتوفير البيانات اللازمة للتحقيق، مع احترام حقوق الخصوصية.
- إطلاق حملات دورية لمحو الأمية الرقمية خاصة في المناطق الريفية والنائية، حيث يكون الوعي ضعيفًا، مما يجعل السكان عرضة للابتزاز أو الاستغلال الإلكتروني.

وفي الأخير، لا يسعنا إلا أن نؤكد على أن مكافحة جريمة الابتزاز الإلكتروني ليست مسؤولية المشرع فقط، بل هي مسؤولية مشتركة تشمل الدولة بكل مؤسساتها، والمجتمع بكل فئاته. فبيئة إلكترونية آمنة لا تتحقق إلا بتضافر الجهود القانونية، الأمنية، التكنولوجية، والتوعوية، بما يضمن حماية الأفراد، والحفاظ على كرامتهم وخصوصيتهم في الفضاء الرقمي.

ملخص الدراسة:

تتناول هذه الدراسة موضوع جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري، باعتبارها من الجرائم المستحدثة الناتجة عن التوسع في استخدام تكنولوجيا المعلومات. وتهدف إلى تسليط الضوء على الإطار القانوني المنظم لها، من خلال تحليل النصوص القانونية ذات الصلة في قانون العقوبات وقانون الوقاية من الجرائم الإلكترونية كما تركز الدراسة على أركان الجريمة، المادي منها والمعنوي، مع إبراز الوسائل التقنية المستخدمة، كوسائل التواصل الاجتماعي والبريد الإلكتروني. كما تستعرض الصعوبات التي تواجه السلطات المختصة في الكشف عن مرتكبي هذه الجرائم، مثل صعوبة التتبع الرقمي ونقص الخبرة الفنية. وخلصت الدراسة إلى أن المشرع الجزائري ما زال بحاجة إلى مزيد من التحديث القانوني لمواكبة تطورات الجريمة الإلكترونية. ومن بين التوصيات: تعزيز التكوين المتخصص للضبطية القضائية، وتطوير الوسائل التقنية للتحقيق، ونشر الوعي القانوني بين المواطنين لحمايتهم من الوقوع ضحية للابتزاز، الإلكتروني.

الكلمات المفتاحية: الابتزاز، الوسائل الإلكترونية، التشريع الجزائري.

Abstract:

This study addresses the issue of electronic extortion under Algerian legislation, considering it one of the emerging crimes resulting from the growing use of information technology. It aims to highlight the legal framework by analyzing relevant provisions in the Penal Code and the Law on the Prevention of Cybercrimes.

It focuses on the crime's material and moral elements, and the technical means used, such as social media and email. It also discusses the challenges faced by competent authorities in identifying perpetrators, including digital tracking difficulties and lack of technical expertise.

The study concludes that Algerian legislation still requires legal updates to match the developments in cybercrime. It recommends enhancing training for judicial police, developing technical investigation tools, and increasing legal awareness among citizens to protect them from electronic extortion.

Key word: Blackmail ،Electronic means ،Algerian legislation

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر:

❖ **القرآن الكريم:**

- سورة يوسف الآية :32.

❖ **السنة النبوية:**

- أخرجه الترمذي في سننه _ محمد بن عيسى بن سورة الترميذي (المتوفي 279ه)_ت أحمد شاكر، ط2 1395ه_1975م باب ما جاء في تعظيم المؤمن (4_378) برقم 2032.

❖ **القوانين:**

- قانون رقم "04/82" المؤرخ في 13 فبراير 1982 من(ج ر7)، المتضمن قانون العقوبات المعدل والمتمم للأمر رقم 156/66، المؤرخ في 18 صفر 1386 الموافق ل8 يونيو 1966
الجريدة الرسمية العدد 30 لسنة 1966.

- قانون "03/82" المؤرخ في 13 فبراير1982(ج ر:1982/49)، المتضمن قانون الإجراءات الجزائية المعدل والمتمم للأمر10/95، المؤرخ في25 فبراير1995، الجريدة الرسمية، العدد17 لسنة1995 .

ثانيا: المراجع:

❖ **الكتب:**

- جناجرة بلال، **الانترنت والابتزاز الالكتروني**، دون ط.
- ممدوح إبراهيم خالد، **فن التحقيق الجنائي في الجرائم الإلكترونية**، ط1، دار الفكر الجامعي مصر، 2009 .
- عادل سلبي زهراء، **جريمة الابتزاز الإلكتروني (دراسة مقارنة)**، الطبعة الأولى، شركة دار الاكاديميون للنشر والتوزيع الأردن _ 2020.
- سليمان عبد الرزاق الغديان، جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد27، مجلة البحوث الأمنية، العدد 69، جانفي 2018.
- عبد العزيز لطفي جاد الله، **أمن المجتمع الإلكتروني بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية**، ط1، مكتبة الوفاء القانونية الاسكندرية، 2017.
- عائشة بن قارة مصطفى، **حجية الدليل الجنائي في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامعة الجديدة _الإسكندرية_ 2010.

- عبد الرزاق مرجان، **الدليل الإسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية،** جامعة نايف العربية للعلوم الأمنية، دار جامعة نايف للنشر 2024.

- عبد الفتاح بيومي حجازي، **جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي،** دار الكتب القانونية القاهرة2007.

- عبد الفتاح بيومي حجازي، **مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت،** الطبعة الأولى، دار الفكر الجامعي مصر2006.

- عبد الفتاح بيومي حجازي، **جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي،** دار الكتب القانونية القاهرة2007.

- عبد الفتاح بيومي حجازي، مبادىء الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي مصر2006.

- محمد شنه، **إجراءات البحث والتحري عن الجرائم في التشريع الجزائري،** ط1، ألفا لنشر والتوزيع 2024.

- محمود مدين، **فن التحقيق والإثبات في الجرائم الإلكترونية،** ط1، المصرية للنتشر والتوزيع2020.

- محمود نجيب حسني، **شرح قانون العقوبات،** القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية _ القاهرة 1972.

- مصطفى محمد الراوشدة، جريمة الإبتزاز الإلكتروني في القانون الإردني، الطبعة الأولى، مركز الكتاب الأكاديمي عمان2020.

- ميرفت محمد حبايبه، **مكافحة الجريمة الالكترونية،** دراسة مقارنة في التشريع الجزائري والفلسطيني، داراليازوري العلمية للنشر والتوزيع _2022.

- نجيب محمد ديابلو، **الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي،** ط، 1 المركز المغاربي، شرق الأدنى للدراسات الإستراتيجية، جانفي 2024.

- هشام فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية،** مكتبة الآلات الحديثة، آسيوط مصر، ط1، 1994.

- ضياء مصطفى عثمان، **السرقة الألكترونية،** دراسة فقهية، دار النفاس للنشر والتوزيع ط1، 2011.

❖ **المقالات العلمية:**

- أكرم ديب، **دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني**، مجلة الحقوق والعلوم السياسية، جامعة خنشلة المجلد 16، العدد 01، 2023.

- ايمن عبد الله فكري، الإستجواب الجنائي الإلكتروني، **مجلة البحوث الفقهية والقانونية مجلة علمية محكمة**، كلية الشريعة والقانون بدمنهور، بحث مستهل من العدد الثالث والاربعون اكتوبر 2023.

- بن الطيبي مبارك، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، **مجلة القانون والعلوم السياسية**، جامع أحمد دراية –أدرار–المجلد 5، العدد2، 2019.

- بن فريدة محمد، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائري (دراسة مقارنة) **المجلة القانونية للبحث القانوني**، المجلد 5، العدد1، 2024.

- ترجمان نسيمة، التعاون الدولي في مكافحة جرائم التوقيع إلكترونية،، **مجلة صوت القانون** جامعة إبن خلدون تيارت المجلد 7 العدد 1، ماي 2020.

- حورية المتوكل، جريمة الإبتزاز الإلكتروني، **المجلة الإلكترونية للأبحات القانونية**، العدد 11_2023.

- رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، بحث مقدم في إطار أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة_نوفمبر_ 2015.

- ريهام عاطف معروف، الإبتزاز الإلكتروني، **مجلة روح القوانين**، كلية الحقوق، جامعة طنطا عدد خاص _ المؤتمر العلمي الدولي الثامن_ التكنولوجيا والقانون.

- الطيبي البركة، إشكالية الإثبات في الجرائم إلكترونية، **مخبر القانون والتنمية المحلية**، جامعة أدرار، مجلة أفاق علمية المجلد 11، العدد 1. 2019.

- عاشور أميل جبار، المسؤولية الجنائية عن جريمة الإبتزاز في مواقع التواصل الإجتماعي (دراسة مقارنة)، **مجلة أبحاث ميسان**، المجلد السادس عشر، العدد الواحد والثلاثون حزيران، 2020.

- عز الدين عثماني، اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية **مجلة دائرة البحوث والدراسات القانونية والسياسية**، مخبر المؤسسات الدستورية والنظم السياسية، العدد الرابع جانفي 2018.

- فاطمة العرفي، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري، **مجلة صوت القانون**، المجلد الثامن، عدد خاص 02، 2022.

- فيصل عبد الله الرويس، الوعي الاجتماعي بظاهرة الابتزاز الالكتروني لدى الاسرة في المجتمع السعودي (دراسة ميدانية للعامل والآثار)، **مجلة كلية الآداب والعلوم الإنسانية** جامعة شقراء المملكة العربية السعودية، العدد33، الجزء الثاني، 2020.

- م، م محسن عباس حميد، جريمة الإبتزاز_الإلكتروني، **مجلة القانون للدراسات والبحوث القانونية**، العدد الثاني والعشرون، جامعة دي قار، 2021.

- محمد سعيد عبد العاطي، جريمة الإبتزاز الإلكتروني (دراسة مقارنة)، **مجلة قطاع الشريعة والقانون**، كلية العدالة الجنائية جامعة نايف العربية العلوم الأمنية، العدد16، أغسطس2024.

- مخلوف علمي، ضوابط التفتيش في الجرائم الإلكترونية، **مجلة المعيار**، **جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة** العدد، 2024.

- مريم عراب، جريمة التهديد والإبتزاز الإلكتروني، **مجلة الدراسات القانونية المقارنة** مجلد07 العدد01، كلية الحقوق والعلوم السياسية، جامعة وهران 02_ احمد بن احمد، 2021.

- وفاء محمد سقر، جريمة الإبتزاز الإلكتروني (دراسة مقارنة)، **مجلة البحوث القانونية والاقتصادية**، كلية الحقوق جامعة بني سويف، المجلد 36، العدد2، جويلية 2024.

- ياسين بن عمر، الابتزاز الإلكتروني للأطفال في التشريع الجزائري، **دفاتر السياسة والقانون** المجلد 16 العدد 2، 2024.

- يحي الشديدي، **الشهادة في الجريمة الإلكترونية**، مجلة جامعة البعث العدد، 50، 2016.

❖ **<u>المذكرات والأطروحات الجامعية</u>**:

- معتوق عبد اللطيف، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع** المقارن، (مذكرة لنيل شهادة الماجيستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر _باتنة) 2012_2011.

- محمد علي احمد ابو علي، **جريمة الإبتزاز الإلكتروني في التشريع الفلسطيني**، (مذكرة لاستكمال متطلبات درجة الماجيستر في تخصص العلوم الجنائية، كلية الدراسات العليا، الجامعة العربية الأمريكية_ 2022/9).

- عبد القادر كيحول، **التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية**، (مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة)2019 .

- صغير يوسف، **الجريمة المرتكبة عبر الأنترنت،** (شهادة الماجيستير كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه " القانون الأساسي والعلوم السياسية " جامعة مولود معمري تيزي وزو)2013.

- سعيدة بعرة، **الجريمة الإلكترونية في التشريع الجزائري (** دراسة مقارنة)، (مذكرة ماستر كلية الحقوق والعلوم السياسية جامعة محمد خيضر_بسكرة) 2015_2016.

- بن فردية محمد، **الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، (** أطروحة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة الجزائر1) 2015.

- آمال برحال، **جريمة الإبتزاز عبر الوسائل الإلكترونية،** (مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة) 2019_2020.

❖ **المطبوعات:**

- مغزيلي نوال، **تقنيات الإعلام والاتصال،** محاضرة أُلقيت على طلبة السنة ثانية ماستر تخصص قانون جنائي، معهد الحقوق المركز الجامعي عبد الحفيظ بوالصوف 2024_2025.

❖ **الوثائق الإلكترونية:**

- صالح بن عبد الله حميد، بحوث ندوة الابتزاز، المفهوم، الاسباب، العلاج، الرياض، ص66 منشور على موقع archive.org. تم الاطلاع عليه بتاريخ 2 ماي 2025 على الساعة 11:23.

الفهرس: