

مذكرة ماستر

ميدان: الحقوق والعلوم السياسية

فرع: الحقوق

تخصص: قانون جنائي

رقم:

إعداد الطالب(ة):

(1) علاوي إيمان

(2) شتيوي سامية انصاف

يوم:

جريمة الإبتزاز الإلكتروني في التشريع الجزائري

لجنة المناقشة:

العضو 1	الرتبة	الجامعة	رئيسا
فضيل خان	دكتور	الجامعة	مشرفا
العضو 3	الرتبة	الجامعة	مناقشا

السنة الجامعية: 2025-2026

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

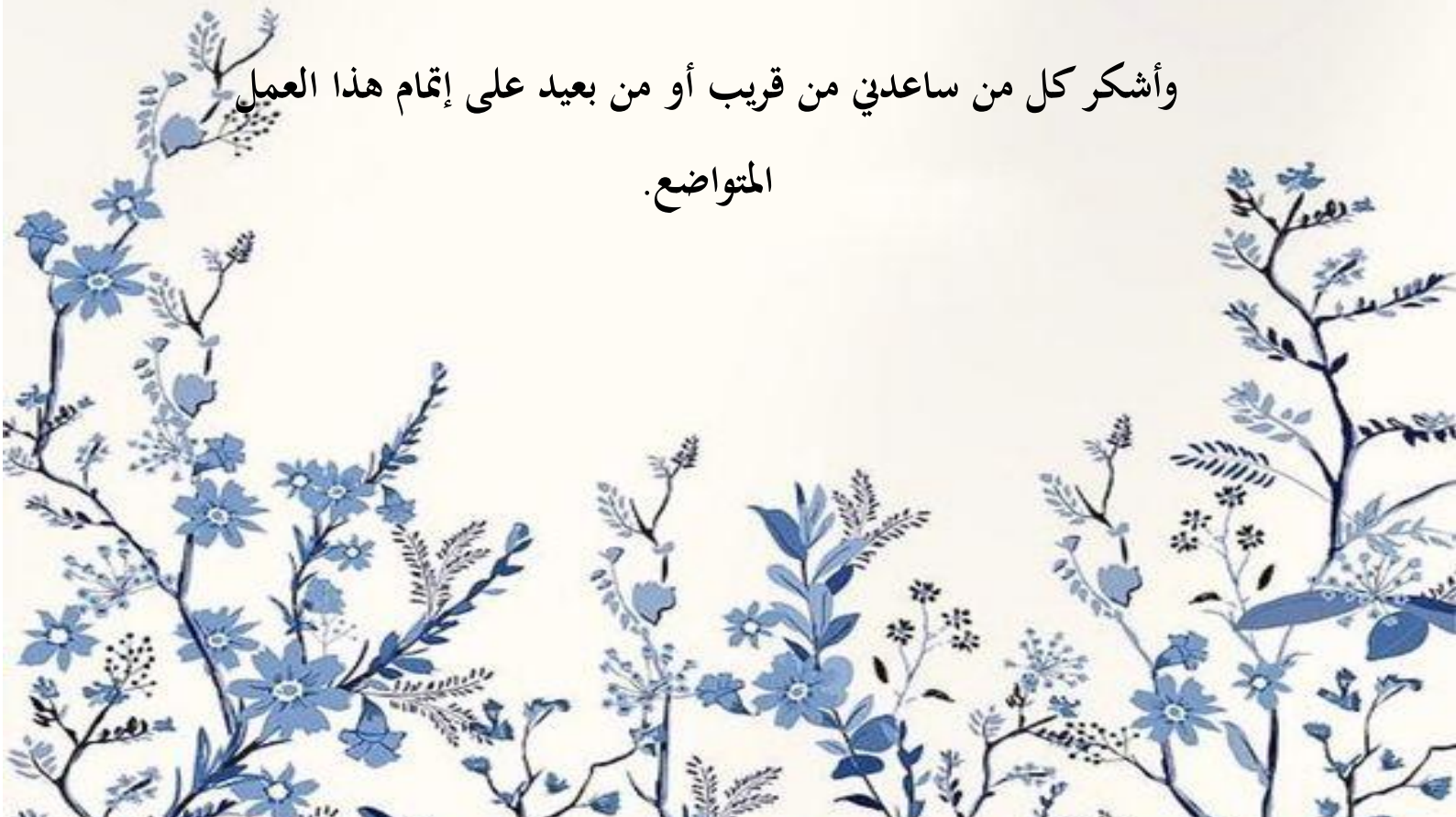
شكر وعرفان

أشكر الله سبحانه وتعالى أولا وأحمده كثيرا على أن سهل لي انجاز هذا العمل.

أتقدم بالشكر الكبير الى الأستاذ الفاضل الدكتور فضيل خان الذي أعانني كثيرا في انجاز هذه المذكرة ولم ييخل علي بالنصائح القيمة والتوجيهات وتشجيعي في إتمام هذا العمل على أكمل وجه فجزاك الله خيرا على كل ما قدمته لي.

كما لا أنسى أن أتقدم بالشكر الجزيل الى كافة الأساتذة بكلية الحقوق وأخص بالذكر الأساتذة الذين نهلنا من علمهم.

وأشكر كل من ساعدني من قريب أو من بعيد على إتمام هذا العمل المتواضع.



إهداء

إلى من غرسوا فينا حب العلم والطموح، وكانوا لنا سنداً طوال هذه المسيرة الأكاديمية...

إلى الينبوع الذي لا ينضب، ومن كللت جهودهم جباهنا بالنجاح والوصول.. آبائنا
الأوفياء (حفظهم الله ورعاهم).

إلى رموز التضحية والعطاء، من سهرت الليالي داعيةً لنا بالصلاح والتوفيق.. أمهاتنا
الغاليات (أدام الله عليهن الصحة والعافية).

إلى من بهم نشد وعاليهم نستند... إلى إخوتنا وأخواتنا وعائلاتنا الكريمة، الذين تقاسمنا
معهم ضغوط الدراسة، وكانوا لنا نعم العون والدافع للاستمرار.

إلى رفقاء الدرب والخطى... إلى كل صديقة وزميلة شاركتنا لحظات التعب والفرح، وإلى
كل من ترك أثراً جميلاً في حياتنا الجامعية.

إلى كل من أثار لنا طريقاً نحو العلم... إلى أساتذتنا الأجلاء الذين لم ييخلوا علينا
بتوجيهاتهم النيرة.

نهديكم ثمرة هذا الجهد العلمي المتواضع، سائلين الله عز وجل أن نكون فخراً لكم دائماً
وأبداً.

شتوي سامية انصاف

إهداء

بعد سنوات من الاجتهاد والسعي المتواصل سنوات حملت في طباقها التعب والصبر والتحديات
أقف اليوم على عتبة التخرج لأقدم ثمرة جهدي وما وصلت إليه بعد فضل الله وتوفيقه

فهذا الإنجاز لم يكن خطوة فردية

بل كان حصيلة دعم وحب ومساندة اشخاص كان لوجودهم أثر في مسيرتي أهدي هذا الإنجاز
إلى:

• والدي الذي علمني معنى الثبات والغرس الطيب والسير في الطريق الصحيح إلى من كان
الدعمه عزا لي ورضاه طريق نحو الفلاح له كل الامتنان والتقدير والفخر الذي يليق بمكانته في

حياتي

• إلى والدي نبع الحنان والقلب الداعي الذي لم يغلق بابه يوما إلى من كانت عيونها تلاحق خطواتي
خوفا على وحنانها قنديلي في كل مواجهة يا أمان ايامي ويا هدايا الله في عمري نجاحي هذا امتداد

لدعائك وقطف لثمار حبك وهدية متواضعة لقلبك الكبير لها أهدي نجاحي

• إلى جدي محامي الغالي الذي كان سبب حبي للقانون منذ طفولتي والذي زرع في داخلي معنى
العدالة والحكمة والإنصاف فكان له الأثر كبير في توجهي في هذا التخصص وكان دائما مصدر

دعم لي أهدي نجاحي له بكل حب واعتزاز

• إلى خالتي غالية، المحامية المتألقة، التي كانت مثالا لي للاجتهاد والطموح أهدي هذا العمل

المتواضع تقديراً لدعمك دائم وثقتك بي، حفصك الله ووفقك دائماً.

• إلى رفاق الرحلة أصدقائي الذين شاركوني الطريق وساهموا في صنع ذكريات لا تنسى وجودكم

كان مساحة رحبة لقلبي وسندا لتجاوز الصعوبات.

في هذا الطريق كان هناك سيفٌ يقطع عني الفشل كلما اقترب والقوة وأمان في الوقت نفسه وهو

ثقتي بالله ان العوض موجود. وها أنا اليوم أرفع مشروعني هذا عربون الشكر الله تعالى الذي وفقني

وأعاني ومنحني القدرة للوصول إلى هذه المرحلة التي لطالما حلمت بها

إيمان

مقدمة

شهدت العقود الأخيرة تقدماً هائلاً في مجال التكنولوجيا ووسائل الاتصال الحديثة، مما أدى إلى انتشار واسع لاستخدام شبكة الإنترنت والأنظمة المعلوماتية في مجالات الحياة اليومية المختلفة سواء على الصعيد الاقتصادي أو الاجتماعي أو الإداري. ورغم الفوائد الجمة التي نتجت عن هذه التقنيات، إلا أنها فتحت المجال لظهور شكل جديد من الجرائم يعرف باسم "الجرائم الإلكترونية" والتي باتت تُشكل تهديداً متزايداً في العصر الحديث.

وهذه الجرائم الإلكترونية تعتبر إحدى أخطر التحديات التي تواجه المجتمعات اليوم، وهذا بسبب ارتباطها الوثيق بالتطور التقني وسهولة تنفيذها مقارنة بالجرائم التقليدية، فضلاً عن صعوبة تتبع مرتكبيها في كثير من الأحيان. تعتمد هذه الجرائم عادة على استخدام أجهزة الحاسوب أو الشبكات الإلكترونية كأداة أو هدف للعمل الإجرامي، كما تتميز بقدرتها على تجاوز الحدود الجغرافية بسهولة.

لهذا السبب أصبحت مكافحتها ضرورة ملحة، ومن بين أخطر الجرائم الإلكترونية نجد "جريمة الابتزاز الإلكتروني" التي شهدت انتشاراً ملحوظاً مع التقدم التكنولوجي وازدياد استخدام وسائل التواصل الاجتماعي. وتتمثل هذه الجريمة في تهديد المجرم للضحية بنشر صور أو معلومات يترتب على انتشارها نتائج وآثار وخيمة على أفراد المجتمع، وهي من الظواهر المستجدة التي فرضت نفسها عليه.

1. أهمية البحث:

تبرز أهمية هذا البحث من خلال تسليط الضوء على واحدة من أخطر الجرائم الحديثة الناتجة عن التطور التكنولوجي والتوسع الكبير في استخدام وسائل الاتصال المعاصرة، فقد أصبحت هذه الجريمة تهدد أمن الأفراد والمؤسسات، مما يجعل تناولها ضمن الأبحاث القانونية ضرورة ملحة. وأسهم هذا البحث في تعزيز الدراسات القانونية المتعلقة بالجرائم الإلكترونية عبر تقديم شرح واضح لمفهوم الابتزاز الإلكتروني، خصائصه، آلياته القانونية، ووسائله المختلفة. وتتجلى أهمية البحث أيضاً في محاولة للكشف عن جوانب القصور التشريعي والإجرائي التي تعوق جهود مكافحة هذا النوع من الجرائم، مع تقييم فعالية النصوص القانونية المطبقة في مواجهتها.

بناءً على الحاجة الملحة لوضع هذا الموضوع موضع دراسة وتحليل، تعتبر هذه الجريمة من أخطر الجرائم المعلوماتية نظراً لأضرارها النفسية والاجتماعية العميقة، حيث تؤدي إلى تدمير الحياة الشخصية والمهنية للضحية، ويتفاقم أثرها في ظل سهولة تداول المعلومات وانتشارها عبر الإنترنت، إلى جانب الصعوبة البالغة في تدارك آثارها بمجرد نشرها.

كما أن التطور التكنولوجي سهل ارتكابها من خلال ابتكار طرق وأساليب جديدة ومتنوعة، وهذا بالنسبة للوسط الذي تقوم فيه هذه الجريمة وهو "المسرح الافتراضي"؛ لذا فإن التحقيق هنا يكون دقيقاً ويتطلب إجراءات قانونية قادرة على جمع الأدلة الرقمية وتحليلها، خاصة وأن الدليل الرقمي مستجد ويخضع لقواعد مختلفة في التعامل معه بسبب خطورة هذه الجريمة وتعدد أركانها.

2. أسباب اختيار الموضوع:

تتمثل أسباب اختيار هذا الموضوع في جانبين رئيسيين؛ أحدهما ذاتي والآخر موضوعي:

- **من الجانب الذاتي:** تتبع الرغبة في الدراسة من أهمية الظاهرة التي يتناولها، حيث إنها تمثل تحدياً كبيراً يهدد استقرار المجتمع ويثير قلقه.

- **أما من الجانب الموضوعي:** فإن اختيار الدراسة جاء نتيجة تزايد انتشار جريمة موضع البحث في المجتمع، مما يجعل من الضروري تسليط الضوء عليها وبحث أبعادها.

وتبرز أسباب هذه الدراسة بشكل خاص لإخلال هذه الجريمة بالقيم الاجتماعية والأعراف والتقاليد التي لها مكانة بارزة في المجتمعات العربية، والتي تولي اهتماماً كبيراً بكل ما يمس السمعة والشرف. والمثير للقلق أن هذه الجريمة تستهدف في أغلب حالاتها الفتيات، مما يضيف سبباً إضافياً من الضرورة ويسند في تناولها بحث علمي متعمق.

3. أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف أبرزها:

- التعرف على مفهوم جريمة الابتزاز الإلكتروني وبيان خصائصه.
- توضيح الأسباب والعوامل التي ساهمت في انتشار جريمة الابتزاز الإلكتروني.

- دراسة الوسائل والأساليب التي يعتمد عليها المبتزون الإلكترونيون في استدراج الضحايا وتهديدهم.
- إبراز الآثار النفسية والاجتماعية والأمنية التي تترتب على ضحايا الابتزاز الإلكتروني.
- بيان الأركان القانونية المكونة لجريمة الابتزاز الإلكتروني والعقوبات المقررة لها في التشريع الجزائري.

4. إشكالية الدراسة:

بناءً على الحاجة الملحة لوضع هذا الموضوع موضع دراسة وتحليل، ينبغي الإجابة على إشكالية الدراسة المتمثلة في:

هل تمكن التشريع الجزائري من ضمان حماية جنائية لازمة لضحايا الابتزاز الإلكتروني؟
ومن هنا تتفرع عدة مشكلات فرعية والتي تتمثل في:

1. ما هي أركان جريمة الابتزاز الإلكتروني وما مدى خطورتها؟
2. ما هي طرق جريمة الابتزاز الإلكتروني؟
3. ما هي وسائل جريمة الابتزاز الإلكتروني وفيما تتمثل آثارها؟
4. ما هي الإجراءات المتعلقة بالتحقيق في جريمة الابتزاز الإلكتروني؟
5. ما هي أدلة الإثبات الجنائي في جريمة الابتزاز الإلكتروني؟
6. ما مدى فعالية الآليات القانونية والتقنية في مكافحة جريمة الابتزاز الإلكتروني؟

5. المنهج المتبع:

وعلى هذا الأساس اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي بهدف الإحاطة بجريمة الابتزاز الإلكتروني من مختلف جوانبها، وذلك من خلال بيان مفهومها وآثارها والوسائل المستخدمة في ارتكابها.

ونظراً للتزايد الملحوظ في معدلات انتشار هذه الجريمة خلال السنوات الأخيرة، إضافة إلى ما تتميز به من خصوصية في أساليب وطرق تنفيذها، فقد انعكس ذلك على مضمون القوانين

والأنظمة التي سعت إلى مواكبة طبيعتها ومتغيراتها وآثارها المختلفة. ومن هذا المنطلق برزت الحاجة الملحة إلى تناول الموضوع بالدراسة والتحليل.

6. الدراسات السابقة:

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

➤ **دراسة عامة:** ركزت على الجرائم الإلكترونية بشكل شامل وأشارت إلى قصور التشريع

الجزائري في مواجهة الجرائم الرقمية الحديثة.

➤ **دراسات متخصصة:** أظهرت أن الابتزاز الإلكتروني لا يعالج بشكل صريح كافٍ في

القانون، مما يخلق إشكالات في التكيف والإثبات، خاصة في جرائم الابتزاز عبر مواقع

التواصل الاجتماعي.

➤ **دراسات مقارنة:** بينت تفوق بعض التشريعات الأجنبية (مثل الفرنسية) في معالجة الجريمة

رقمياً ودعت إلى تحديث قانون العقوبات الجزائري.

7. صعوبات الدراسة:

ولا يفوتنا القول إننا واجهنا صعوبات في دراسة موضوع جريمة الابتزاز الإلكتروني والتي تتمثل

في:

- قلة المراجع المتخصصة وحداثة الموضوع.
- التطور المستمر لأساليب الجريمة الإلكترونية، مما يصعب الإحاطة بها بشكل كامل.
- نقص الإحصائيات الدقيقة بسبب عدم تبليغ الضحايا عن هذه الجرائم، وهو ما يشكل عائقاً كبيراً أمام الدراسة والتحليل.

8. خطة الدراسة:

ولدراسة هذا الموضوع تم تقسيمه إلى فصلين رئيسيين:

الفصل الأول: وجاء تحت عنوان (الإطار الموضوعي لجريمة الابتزاز الإلكتروني)، وتناولنا فيه:

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني.

المبحث الثاني: تجريم الابتزاز الإلكتروني.

الفصل الثاني: وجاء بعنوان (الإطار الإجرائي لجريمة الابتزاز الإلكتروني)..

المبحث الأول: الاثبات في جريمة الابتزاز الإلكتروني

المبحث الثاني: ماهية الدليل الجنائي الرقمي

الفصل الأول:

الإطار الموضوعي لجريمة

الابتزاز الإلكتروني

تمهيد:

تعتبر جريمة الابتزاز الإلكتروني أكثر امتداداً وتطوراً على جريمة الابتزاز التقليدية التي تقع في عالم الواقعي حيث تعد جريمة الابتزاز الإلكتروني من جرائم الحديثة التي تندرج ضمن ما يعرف في علم جريمة بالجرائم الناعمة وهي جرائم لا تعتمد على عنف مادي مباشر بل ترتكب بأساليب غير محسوسة وبناء على ذلك تم تقسيم هذا الفصل إلى مبحثين خصص المبحث الأول لتعريف جريمة الابتزاز الإلكتروني وبيان مفهومها، بينما تناول المبحث الثاني مسألة تجريم هذه الجريمة والإطار القانوني المنظم لها.

المبحث الأول:

ماهية جريمة الابتزاز الإلكتروني

يتميز العصر الحالي بوتيرة متسارعة من التطور لا سيما في المجال الإلكتروني الذي أصبح جزءاً أساسياً من حياة الأفراد لما يقدمه من فوائد ومزايا متعددة. غير أنه له صور أخرى غير مقبول اجتماعياً وأصبحت مصدراً لكثير من الأضرار الاجتماعية وانعكست سلباً على العلاقات الإنسانية وأصبحت تؤثر على الحقوق والحريات الشخصية التي تتصل بالفرد وعلى رأسها حرمة حياة خاصة وهذا أمر استدعى دراسة مفهوم جريمة الابتزاز الإلكتروني ومعرفة أنواعها ومختلف وسائلها ونتطرق إلى الآثار المترتبة عنها وهذا ما سنتعرف عليه في هذا المبحث.

المطلب الأول: مفهوم جريمة الابتزاز الإلكتروني

يعد الابتزاز الإلكتروني نتيجة مباشرة لسوء استخدام التطور التكنولوجي، فقد أتاح هذا التطور للمجرم أن يتخفى خلف الشاشات ويمارس أفعالاً إجرامية تمس مصالح يحميها القانون حيث تتمحور هذه الجريمة هي تهديد مجني عليه أو ترهيبه بالنشر معلومات أو صور أو تسجيلات خاصة لا يرغب في كشفها بهدف تحقيق جاني على أهداف الإجرامية سواء كانت مادية أو معنوية، ويعتبر الابتزاز الإلكتروني من وسائل الإكراه على مجني عليه ومن خلال هذا المطلب سيتم تطرق إلى مفهوم الابتزاز الإلكتروني حيث في فرع أول ندرس تعريف الابتزاز الإلكتروني أما الفرع الثاني أنواع الابتزاز الإلكتروني.

الفرع الأول: تعريف الابتزاز الإلكتروني

الابتزاز الإلكتروني هو تهديد شخص بنشر معلومات أو صور خاصة به عبر الإنترنت لإجباره على القيام بشيء معين كدفع مال أو تنفيذ طلبات ويعد من أبرز الجرائم المعلوماتية مستحدثة.

أولاً: التعريف اللغوي

" يعرف الابتزاز لغة بأنه أخذ الشيء بجفاء وقهر وابتزّه مأخوذة من سلبه ورمى به ولم يرده، وهو فعل حاد في مثال "من عز بزة" ومعناه "من غلب سلب" ويقال ابتزت الشيء أي انتزعتَه وبزه يبزه بمعنى غلبه".¹

ثانياً: التعريف الاصطلاحي للابتزاز

"عرف على أنه أحد أشكال التلاعب القوية يقوم خلالها مبتز الذي تربطه علاقة أو صلة بالضحية بتهديده بطريقة مباشرة أو غير مباشرة بالعقاب إذا لم يحصل على مايرغب عندما يستخدم المقربون الخوف، والالتزام والشعور بالذنب للتلاعب بك وعرفه آخرون بأن "الابتزاز" هو القيام بالتهديد بكشف معلومات معنية عن شخص أو فعل شيء لتدمير الشخص مهدد ان لم يقوم الشخص بالاستجابة إلى بعض الطلبات".²

ثالثاً: التعريف الفقهي

يعرف الابتزاز بأنه " كل فعل أو سلوك من شأنه أن يبعث الخوف، في نفس المجني عليه بهدف الاضرار به أو بأي شخص آخر يهمله أمره يحمل المجني عليه إلى أن ينفذ ما يريده الجاني، ويقصد به الوعيد بنشر وزرع الخوف في النفس بالضغط على إرادة الإنسان وتخويله من أن ضرراً سيلحق أو سيلحق أشخاصاً وأشياء له بها صلة، وقيل أنه عملية تهديد يتعرض لها ضحية بأن يؤدي في بدنه أو ماله أو سمعته أو أحد ممن يهمله أمره بحق أو باطل من أجل الحصول على أمور مادية أو معنوية لصالح المبتز. ومحل الحماية في هذه الجريمة هي إرادة الشخص كونها تقيد حرية مجني عليه وتدفعه إلى ممارسة أفعال من شأنها الإضرار بنفسه أو

¹ حداد شماء، جبلي سعيدة، جريمة الابتزاز عبر الوسائل الإلكترونية في تشريع ج مركز جامعي عبد الحفيظ بواد صوف ميلة، معهد الحقوق، قسم الحقوق، القانون الجنائي، مذكرة مكملة لنيل شهادة ماستر، 224، 225، ص8.

² بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، جريمة الابتزاز الإلكتروني جامعة قاصدي مرباح - ورقلة - كلية حقوق وعلوم سياسية، قسم حقوق، قانون جنائي العلوم الجنائية، مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة ماستر أكاديمي، 2023، 2024.

ماله أو عرضه أو من يمت له بصلة ولهذا فهذا النوع من الجرائم فيه مساس بحرية المجني عليه وحرية اختياره".¹

رابعاً: التعريف الابتزاز بالنسبة للمشرع جزائري

"يعد الابتزاز الإلكتروني في القانون الجنائي الجزائري نوعاً من أنواع الجريمة السرقة فهو محوره التهديد بنشر معلومات خاصة التي يكون المبتز سرقها من الضحية، الخصوصية في نطاق الرقمنة، فالحق في الخصوصية من حقوق الدستورية الأساسية ملازمة واللصيقة للشخص الطبيعي بصفته الأساسية كأهل ولو أن القانون ج لا يحدد هذا المفهوم ومحدداته ما نبى عن تعقده وتشعب مراميه، بحيث يصبح الشخص معرضاً للانتهاك من ثم تسجيل محتوى متعلق به في العالم الرقمي مما يجعله غير قابل للمحو".²

نستنتج أن الابتزاز الإلكتروني يعد من الجرائم المتطورة التي ظهرت نتيجة تحديث التكنولوجي وزيادة في اعتماد على وسائل الاتصال الرقمية. وهذا باستخدام الأشخاص لوسائل التكنولوجيا الحديثة كالهواتف الذكية، مواقع تواصل الاجتماعي أو تطبيقات رقمية لتهديد شخص بنشر معلوماته وصوره وأسراره خاصة وهدف من هذا التهديد هو الحصول على مكاسب معينة كالمال أو أغراض غير مشروعة ويتم ذلك غالباً عن طريق إلحاق ضرر مادي أو معنوي بالضحية وتعتبر هذه الجريمة هي نوع من أنواع الجرائم الإلكترونية لاعتمادها على الفضاء الرقمي وتكنولوجي الحديث وهذا ما يجعلها في بعض الأحيان معقدة بسبب طبيعتها العابرة للحدود وصعوبة تعقب الجناة.

والقانون الجزائري لم يضع تعريف محدد ومستقل لجريمة الابتزاز الإلكتروني كجريمة منفردة لكن يستدل عليه من خلال عدة نصوص قانونية تتضمن الجرائم المتعلقة بالتهديد والابتزاز الواردة في قانون العقوبات الجزائري، كالجرائم المرتكبة وهذا باستخدام أنظمة المعالجة الآلية للبيانات،

¹ بن عامر ياسين، الابتزاز الإلكتروني للأطفال في التشريع الجزائري، دفاثر السياسة، جامعة قاصدي مرباح ورقلة، المجلد

16، العدد 02، 2024، ص 173.

² حداد شيماء، مرجع سابق، جبلي سعييدة ص 09.

والتي ينظمها القانون رقم 09 - 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وتتميز هذه الجريمة بطابع عالمي يتجاوز الحدود الجغرافية وسرعة انتشار مخاطر وأضرار ناتجة عنها نظر لاستخدام الإنترنت مع صعوبة تحديد هوية الجاني في بعض الحالات وهذا بسبب استخدام حسابات وهمية وأدوات إخفاء الهوية كذلك تهديد مباشرة للخصوصية والابتزاز الإلكتروني يعتبر تحدياً كبيراً للأنظمة القانونية والأمنية وهذا أمر يستدعي جهود لتعزيز الوعي وتطوير آليات الوقاية منه ومكافحة بشكل جدي.

الفرع الثاني: أنواع الابتزاز الإلكتروني.

ساهم التطور المتسارع في تقنيات الحاسوب الرقمي وتكنولوجيا المعلومات في نقل العديد من مظاهر النشاط الاجتماعي والثقافي والأساسي والاقتصادي من بيئة الواقعية إلى بيئة الافتراضية. إلا أن هذا التحول لم يخل من مخاطر، إذ أتاح إمكانية جمع البيانات وتخزينها والتوصل بشأنها، بل والوصول إليها بوسائل غير قانونية ومن دون علم أصحابها، مما يشكل تعدياً واضحاً على خصوصية الأفراد.

أولاً: بالنظر إلى شخص الضحية

تتنوع جرائم التهديد والابتزاز الإلكتروني وفقاً لطبيعة المجني عليه، سواء كان شخصية اعتبارية أم فرداً طبيعياً، ما يعكس تنوع الأهداف والأساليب المستخدمة في هذه النوعية من الجرائم.

1. الشخصيات الاعتبارية: تتضمن جرائم الابتزاز الإلكتروني التي تستهدف شخصيات معنوية مثل الحكومات، الشركات، والمؤسسات. في هذا النوع، يقوم الجاني بالحصول على معلومات حساسة أو سرية تتعلق بالكيان الضحية، ومن ثم يُقدّم على تهديده بنشر تلك المعلومات وفضحها أمام أطراف أخرى. غالباً ما تبدأ هذه الجرائم باختراق مواقع إلكترونية مهمة تتبع للمؤسسة المستهدفة، وتتصاعد لنتخذ شكل تهديد مباشر بالنشر أو الإعلان عن البيانات المسروقة، وفي بعض الحالات يتم السطو على الموقع الإلكتروني الخاص بالكيان المعرض للابتزاز. عادةً ما يعتمد الجناة على استغلال الجوانب المالية والسمعة المؤسسية للضحية لتحقيق مكاسب شخصية.

2. الأحداث: تختلف القوانين والتشريعات بين المجتمعات في تعريفها للأحداث بناءً على الاختلاف في تحديد سن التمييز وسن الرشد، والذي يرتبط بالعوامل الطبية والاجتماعية والثقافية ذات الطابع المحلي. وفيما يخص جرائم الابتزاز التي تستهدف الأحداث، يعتمد المجرم على تهديد الضحية بنشر صور خاصة أو تسجيلات مرئية أو محادثات ذات صلة بوقائع قد تسبب له الإحراج أو التقليل من شأنه أمام أسرته ووسطه الاجتماعي. تعد الفئة العمرية الصغيرة للأحداث وشغفهم الكبير بالتقنية ووسائل التواصل الاجتماعي عاملاً مُسهلاً لاستدراجهم إلى هذه الجرائم، وذلك نظراً لافتقارهم للتجربة الكافية وصغر سنهم. من هنا، يُمكن القول إن الأحداث يقعون ضمن الفئات الأكثر عرضة لهذه النوعية من الجرائم نظراً لضعف قدرتهم على مواجهة هذا النوع من التحديات التقنية والاجتماعية.¹

النساء 3: تمثل النساء الفئة الأكثر عرضة للابتزاز، خاصة إذا كان الجاني رجلاً. يتكرر التهديد في هذه الحالات بنشر صور حساسة أو فيديوهات خاصة للضحية. عادة ما يكون الهدف طلب مبالغ مالية أو إجبار الضحية على الامتثال لرغبات معينة. بالنسبة للنساء الأصغر سناً أو من هن في مواقع ضعف، فإن الخوف من الفضيحة الاجتماعية يدفعهن أحياناً للاستسلام لتلك التهديدات. وقد يتعلق الابتزاز أيضاً بفضح حياتهن المهنية إذا كانت الضحية سيدة أعمال أو النيل من سمعتها بنشر محادثات خاصة أو تسريبات قد تضر بمواقف شخصية أو سياسية.

الرجال 4: يتعرض الرجال للابتزاز عادة بسبب مكانتهم الاجتماعية أو السياسية أو بحكم أسرار عائلية قد يحملها الشخص، حيث يؤدي إفشاؤها إلى تشويه السمعة والإضرار بصورة الشخص أمام المجتمع، بل وحتى إلى التأثير على وضعه المالي. يمكن أن يكون الرجل أيضاً حالة استهداف، خاصة إذا كان في وضع مادي جيد أو يتعرض لفخاخ من محترفات

¹ عراب مريم، جريمة التهديد والابتزاز الإلكتروني " الدراسات القانونية المقارنة"، جامعة وهران 2، أحمد بن أحمد المجلد 07، العدد 01، 2024، ص1210.

على الإنترنت يستخدم صورته الخاصة أو مقاطع فيديو معينة لأغراض تهديدية تمس بسمعته ومركزه.¹

ثانياً: صور الابتزاز الإلكتروني بالنظر الى هدف المجرم من المجرم

تتنوع الأهداف التي يسعى المبتز إلى تحقيقها من خلال ارتكاب جريمة الابتزاز، ويتحدد ذلك بناءً على طبيعة كل جريمة وظروفها الخاصة. وفيما يلي تصنيف الأهداف الرئيسية التي قد يسعى إليها المبتز:

1. **الهدف المادي** : يُعتبر السعي وراء تحقيق منفعة مادية من أبرز وأشهر الأهداف التي تدفع المبتز لارتكاب جريمة الابتزاز. يتمثل هذا الهدف في مطالبة المجني عليه بمبالغ مالية أو العينية ذات قيمة مقابل الامتناع عن نشر معلومات أو أسرار قد تسبب إحراجاً أو ضرراً له أمام المجتمع. وتختلف القيمة المطلوبة وفقاً لطبيعة المجني عليه؛ إذ قد يكون شخصاً اعتبارياً كالشركات التجارية حيث ترتفع غالباً قيمة الطلبات المالية، أو فرداً سواء كان رجلاً أو امرأة، ما يجعل الحالة تعتمد على المستويات الاجتماعية والشخصية للضحية.

2. **الهدف الجنسي** : يعد هذا النوع من الأهداف متشابكاً بشكل كبير مع حالات الابتزاز التي تتضمن ضحايا من النساء أو الأطفال، ويزداد شيوعه إذا كانت الضحية تجمع بين كونها طفلاً وامرأة في الوقت ذاته. يتحقق الهدف الجنسي للمبتز عندما يطالب الضحية بالامتثال لرغباته الجنسية مقابل الامتناع عن كشف أسرارها. وفي بعض الحالات، قد يتضمن الأمر تهديد الضحية بممارسة أعمال ذات طبيعة جنسية مع طرف آخر غير المبتز نفسه. كما يمكن أن يكون طلب المبتز ذات طبيعة متكررة أو يمتد لعدد من المرات، وذلك بناءً على ظروف كل حالة. اللافت أن النساء يُشكلن النسبة الأكبر من ضحايا هذا النوع من الابتزاز.

3. **الهدف النفعي**: يتجسد هذا الهدف في رغبة المبتز بتحقيق منفعة محددة من المجني عليه عبر تهديده بكشف أسرارهِ علناً إذا لم يستجيب لمطالبه. تشمل هذه المطالب أحياناً القيام بأعمال غير مشروعة كالسرقة لصالح المبتز، الترويج للمواد المخدرة، أو التوسط لإنجاز مهمة معينة،

¹ ميمونة ناصر، مرجع سابق، ص 26.

سواءً كانت هذه المهمة قانونية أم مخالفة للقانون. يُجمع بين كل هذه الحالات عنصر الإكراه، حيث تُرتكب جريمة الابتزاز عند إرغام المجني عليه على تنفيذ فعل يتعارض مع إرادته. تظل هذه الأهداف المختلفة مرتبطة بالسياق الاجتماعي والأخلاقي الذي يفضي إلى وقوع الجريمة، مما يستدعي وجود آليات ردع فعالة وإجراءات وقائية لحماية الأفراد والمجتمعات من الوقوع ضحية لهذه الجرائم المؤثرة على الأمن الاجتماعي والنفسي

ثالثاً: صور الابتزاز الإلكتروني بالنظر الى وسائله

1. الابتزاز المادي: يُعرف بأنه قيام الجاني بتهديد الضحية باستخدام وسائل مادية ملموسة مثل الصور أو مقاطع الفيديو أو الوثائق. يتمثل الابتزاز المادي الإلكتروني في استخدام القنوات الإلكترونية المختلفة، بما فيها الرسائل والاتصالات التي تأخذ أشكالاً متعددة، كالنصوص أو الصور أو الأصوات أو البيانات. تُثقل هذه الوسائل عبر شبكات إلكترونية باستخدام أسلاك، ألياف بصرية، أو تقنيات كهرومغناطيسية.

2. الابتزاز المعنوي: فهو يعتمد على التهديد باستخدام وسائل غير ملموسة، مثل الكلمات أو العبارات الشديدة التي تُستخدم للترهيب أو التهديد بفضح معلومات معينة تخص الضحية. يُوجّه هذا التهديد بشكل يؤدي إلى ترسيخ اعتقاد قوي لدى الضحية بأن المبتز سيقوم فعلاً بتنفيذ تهديداته دون أدنى شك.¹

المطلب الثاني: وسائل الابتزاز الإلكتروني وأثاره

مع الانتشار الواسع للإنترنت ودخول التكنولوجيا في مختلف جوانب الحياة اليومية، أصبح العالم الرقمي فضاءً مفتوحاً للتواصل وتبادل المعلومات، لكنه في الوقت نفسه أتاح فرصاً لظهور جرائم جديدة، فمن بين هذه الجرائم جريمة الابتزاز الإلكتروني هذا النوع من جرائم يستغل ضعف الوعي أو الثقة الزائدة لدى المستخدمين، مما يجعله تهديداً حقيقياً لأمن الأفراد واستقرارهم النفسي والاجتماعي، ويستدعي الحذر واتخاذ إجراءات وقائية مستمرة ويقصد بالابتزاز برأي آخر هو كل

¹ عراب مريم، مرجع سابق، ص 1211-1212.

أسلوب يستعمل فيه التقدم التكنولوجي ووسائل الاتصال الحديثة للإيقاع بالضحية، حيث يتم استدراجها عبر مواقع التواصل الاجتماعي أو تطبيقات الهواتف الذكية، ثم خداعها للحصول على صور أو مقاطع خاصة دون علمها، ليتم بعد ذلك تهديدها بنشرها أو إجبارها على القيام بأفعال قد تضر بها ولا تقتصر خطورته على الجانب المادي فقط، بل تمتد آثاره لتشمل القلق النفسي، وفقدان الثقة والمشاكل الاجتماعية مما يجعل تصديه له ضرورة ملحة من خلال الوعي والحذر في استخدام الوسائل الرقمية.

وفي هذا المطلب سيتم التطرق إلى الوسائل الابتزاز الإلكتروني كفرع أول وآثاره مترتبة عن هذه الجريمة في الفرع الثاني.

الفرع الأول: وسائل الابتزاز الإلكتروني

كل جريمة لها وسائل وطرق مختلفة في ارتكابها ويتم تصيد ضحايا هذه الجريمة عن طريق مواقع التواصل الاجتماعي أو بعض تطبيقات هواتف ذكية ومن بين هذه مواقع تواصل لارتكاب هذه جريمة نجد أشهرها "فيسبوك (ميتا)، تيك توك، سناب شات، الانستغرام" وبناءً عليه سوف نتطرق لبعض هذه الوسائل.

أولاً: الحاسب الآلي، أو ما يُعرف بالكمبيوتر، هو جهاز إلكتروني مصمم لاستقبال البيانات والمعلومات التي نرغب في إدخالها وتخزينها، بالإضافة إلى حفظ المعلومات المرتبطة بالبرامج التطبيقية. يتمتع هذا الجهاز بقدرة فائقة على معالجة تلك البيانات بسرعة هائلة تفوق إمكانيات الإنسان، وذلك بعد تزويده بالمعلومات المسبقة والبرامج المخصصة لتأدية المهام المطلوبة.

ثانياً: برامج الحاسب الآلي، فقد عُرِّفت في نظام مكافحة الجرائم المعلوماتية السعودي على أنها مجموعة من الأوامر والبيانات التي تحتوي على توجيهات وتطبيقات. عند تشغيل هذه البرامج على الحاسب الآلي أو شبكاته، تقوم بتنفيذ الوظائف المطلوبة بدقة وكفاءة.¹

¹ بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، مرجع سابق، ص 24، 25.

ثالثاً: الإنترنت

تعدّ أحد أهم الاكتشافات والتطورات في تاريخ البشرية. فهي شبكة اتصالات عالمية تربط ملايين أجهزة الحاسوب حول العالم، وتشكل أكبر شبكة كمبيوتر على الإطلاق. تعتبر الإنترنت نتاج دمج تكنولوجيا الحاسوب مع تقنيات الاتصالات، مما أدى إلى إنشاء ما يُعرف بالشبكة العنكبوتية. تتيح هذه الشبكة ربط عدد هائل من الأجهزة من خلال وسائل اتصال متنوعة، سواء السلكية مثل الخطوط الهاتفية العامة والخاصة، أو اللاسلكية مثل الأقمار الصناعية والكابلات والألياف البصرية. بفضل هذه الوسائل المتقدمة، أصبحت الإنترنت شبكة دولية ضخمة تسمح بتبادل المعلومات، بحيث يمكن لأي شخص متصل بالشبكة إرسال واستقبال البيانات في أي وقت ومن أي مكان في العالم، شريطة توفر جهاز حاسوب ووسيلة اتصال فعالة.

1. البريد الإلكتروني: يُعد البريد الإلكتروني وسيلة فعّالة لتبادل الرسائل الإلكترونية بما في ذلك النصوص، الصور، والمقاطع الصوتية. وقد وفرت هذه الخدمة الكثير من الوقت، حيث تصل الرسائل إلى وجهتها في ثوانٍ معدودة بغض النظر عن بعد المسافة.

2. خدمة الدردشة: تتيح هذه الخدمة للأفراد من جميع أنحاء العالم التواصل فيما بينهم عبر الكتابة النصية، المكالمات الصوتية، أو مكالمات الفيديو. إنها وسيلة حديثة ومباشرة للتفاعل الاجتماعي عبر الفضاء الافتراضي.

3. الهواتف النقالة وملحقاتها وبرامجها: يستخدم البعض الهواتف النقالة بشكل غير مشروع كوسيلة لارتكاب الجرائم الإلكترونية، حيث يتم استغلال تقنيات الاتصال والبرامج المختلفة للتجسس أو التلصص على الآخرين. قد تشمل الملحقات المستخدمة في هذه الحالات الكاميرات، البلوتوث، وآلات التسجيل، بالإضافة إلى البرامج المتطورة التي يتم تثبيتها على الهواتف المحمولة. ونظرًا لقدرة الجناة على استخدام هذه الوسائل بطرق مبتكرة، يجد بعض الضحايا أنفسهم مضطرين للرضوخ لمطالب المجرمين.

تُبرز هذه النقاط الدور الكبير للإنترنت والتقنيات الحديثة في حياتنا اليومية بما لها من مزايا وما يمكن أن تتطوي عليه من مخاطر. لذا يتطلب الأمر الحرص والحذر عند استخدام هذه التقنيات لتحقيق أقصى استفادة منها مع تجنب الوقوع ضحيةً للاستخدامات السلبية.¹

نرى أن وسائل الابتزاز الإلكتروني من أبرز التحديات التي يواجهها الأفراد والمجتمعات في العصر الرقمي الحالي، حيث تستهدف هذه الوسائل استغلال ضعف الضحايا أو اختراق خصوصياتهم لتحقيق مكاسب مادية أو معنوية. وتعتمد تقنيات الابتزاز الإلكتروني على أساليب متعددة، مثل التهديد بنشر معلومات شخصية أو صور خاصة، واستخدام البيانات المسروقة من الحسابات الإلكترونية ولابتعاد على هذه جريمة متفاقمة يجب توخي الحذر وبمعنى أن يتم وقاية يتطلب الأمر نشر الوعي بين مستخدمين على أهمية حماية معلوماتهم الشخصية، واستخدام كلمات مرور قوية، وكذلك تفعيل خاصية المصادقة الثنائية على حسابات كما ينبغي تعزيز ثقافة الأمن الرقمي من خلال برامج تثقيفية والورش التدريبية التي تستهدف فئات المجتمع المختلفة.

الفرع الثاني: آثار الابتزاز الإلكتروني

يخلف الابتزاز الإلكتروني آثاراً خطيرة على الفرد والمجتمع، إذا يؤدي اجتماعياً إلى تشويه السمعة وتدهور العلاقات، ونفسياً إلى القلق والخوف وقد يصل إلى الاكتئاب، كما يشكل تهديداً أمنياً من خلال انتهاك الخصوصية واستغلال البيانات الشخصية مما يستدعي الحذر واتخاذ وسائل الحماية اللازمة.

أولاً: الآثار الاجتماعية

تشكل ظاهرة الابتزاز الإلكتروني تهديداً خطيراً للمجتمع والعائلة، حيث إن النساء يشكّلن النسبة الأكبر من الضحايا. وغالباً ما تؤدي هذه الظاهرة إلى تفكك الأسر، حيث تُجبر النساء المتضررات على الانفصال عن أزواجهن. ومن جهة أخرى، يتردد العديد من الفتيات اللواتي تعرضن للابتزاز في التقدم بشكوى قانونية خوفاً من الفضائح والتبعات السلبية، خاصة وأن

¹ عراب مريم، مرجع سابق، ص 1212-1213.

المجتمع المحيط بهنّ قد يصبح عائقاً رئيسياً أمام زواجهن في المستقبل. كما أن بعض الفتيات يرفضن فكرة الزواج بشكل تام خشية أن يكتشف شركاؤهن الجدد تفاصيل حياتهن السابقة . يمكن أن يمتد التأثير إلى تحطيم العلاقات الزوجية حتى بعد الزواج، فقد يؤدي الخوف من الابتزاز إلى الانفصال أو الطلاق. وفي بعض الحالات المأساوية، قد تُجبر الفتاة على الخضوع لرغبات المبتز، مما قد يؤدي إلى حمل غير مرغوب فيه. ومن هنا تنشأ مشكلات إضافية مثل محاولة الإجهاض أو التخلي عن الأطفال غير الشرعيين، وهو ما قد يؤدي إلى تطورات مأساوية كالقضاء على حياة الطفل أو تركه للعيش في الشوارع والانحراف، حيث يصبح مستقبله مليئاً بالمخاطر مثل السجن أو الموت .

تتسبب هذه الجريمة بزعة العلاقات الاجتماعية وكسر الثقة بين أفراد المجتمع، ما يؤدي إلى نشر القلق والخوف من الآخرين. وعادةً ما تعاني الضحايا من العزلة النفسية والاجتماعية جراء هذا النوع من الجرائم البشعة. علاوةً على ذلك، فإن الابتزاز الإلكتروني قد يؤثر سلباً على استقرار الأفراد النفسي ومستقبلهم المهني والشخصي، مما يزيد الحاجة لتوعية المجتمع ومكافحة هذه الظاهرة بوسائل قانونية وتربوية فعالة¹.

ثانياً: الآثار النفسية

تترتب على جريمة الابتزاز الإلكتروني آثار نفسية عميقة وسلبية للغاية على الضحية. ومن أبرز هذه الآثار: الإحساس الدائم بالتوتر والذنب، صعوبات النوم وفقدان التركيز، والخوف المستمر من الآخرين. وغالباً ما يعاني الضحية من انعدام الثقة في المحيطين به ويظل حساساً تجاه تصرفاتهم، خاصة إذا كانوا على دراية بوسائل التكنولوجيا الحديثة. بالإضافة إلى ذلك، قد تسيطر أفكار الانتقام أو التخلص من الظلم بشتى الوسائل على تفكير الضحية. وإذا تفاقم الوضع، قد يصل الأمر إلى حد التفكير بإيذاء النفس أو الانتحار بسبب الإحباط واليأس. وتُعد هذه المخاطر أكبر عندما يتعذر على الضحية طلب المساعدة بسبب الخجل أو الخوف من الفضيحة.

¹ بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، ص 27-28.

كما تسبب هذه الجرائم تدميرًا نفسيًا عميقًا عند بعض الفئات، خاصة الأطفال الذين يتعرضون للابتزاز الجنسي، وهو الشكل الأكثر شيوعًا بين حالات الابتزاز الإلكتروني. الآثار النفسية لهذا النوع من الجريمة تتسم بالحدة، حيث يعاني الضحايا من القلق الدائم وانخفاض الثقة بالنفس والخوف من التفاعل الاجتماعي. قد يصل الأمر إلى حالات اكتئاب حاد أو عزلة قسرية نتيجة الشعور بالعجز والمهانة. لذا يُنصح بتقديم الدعم النفسي والاجتماعي لهذه الفئة، والتواصل مع الجهات المختصة لضمان علاج الآثار النفسية واستعادة التوازن النفسي.

ثالثًا: الآثار الأمنية

جريمة الابتزاز الإلكتروني لها تأثيرات سلبية واضحة على الأمن الفردي والمجتمعي. فهي تعزز شعور الخوف لدى الأفراد تجاه سمعتهم وشرفهم، كما تقوّض أمن المجتمع بأكمله نتيجة ارتباطها بجرائم أخرى مثل الاغتصاب والدعارة والابتزاز المادي والاستيلاء على أموال الآخرين. هذه الجريمة تسهم في انتشار الفساد وتدهور القيم الأخلاقية داخل المجتمع، ما يجعل الأفراد يشعرون بفقدان الأمان على أنفسهم وأعراضهم وممتلكاتهم. وفي حالات متطرفة، قد يؤدي الابتزاز الإلكتروني إلى جرائم عنف أو حتى جريمة قتل بدافع الانتقام من الطرف المبتز الذي دمر حياة ضحيته بنشر محتوى سيء لسمعتها وشرفها.

في بعض المجتمعات العربية، يتفاقم الأثر الأمني نتيجة الأعراف الاجتماعية الصارمة التي قد تدفع أسرة الضحية للجوء إلى الانتقام بارتكاب جرائم قتل بحجة "غسل العار"، مما يُضيف أبعادًا خطيرة لهذه الجريمة ويجعلها تهديدًا ليس فقط للضحايا ولكن أيضًا لأفراد مجتمع.¹

إذاً تعتبر جريمة الابتزاز الإلكتروني من ظواهر الحديثة التي تحمل تأثيرات متعددة على المستويين الأخلاقي والاقتصادي. فمن جانب الأخلاقي يؤدي الابتزاز الإلكتروني إلى زعزعة ثقة الأفراد ببعضها البعض، حيث يتم استخدام المعلومات الشخصية أو الحساسة كوسيلة للضغط والإكراه، مما يؤدي إلى شعور الضحايا بالضعف والخوف، كما يسهم في انتشار السلوكيات غير

¹ وفاء محمد صقر، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مجلة بحوث القانونية والاقتصادية، كلية الحقوق-جامعة طنطا، مجلد 36، عدد 2، يوليو 2024، ص 474، 475، 476، 477.

الأخلاقية سواء لدى مرتكبي الجريمة أو لدى الضحايا الذين قد يجبرون على اتخاذ قرارات أخلاقية تتعارض مع مبادئهم وأخلاقهم الأساسية هذه بالنسبة للأثار ناتجة عن هذه الجريمة. أما من جانب الاقتصادي، فإن الابتزاز الإلكتروني يلحق أضراراً بالغة بالشركات والأفراد على حد سواء.

حيث يترتب على هذه جرائم خسائر مالية مباشرة، وهذا سببها مدفوعات التي قد يضطر الضحايا لتقديمها استجابة لمطالب المبتزين. إلى جانب ذلك، فإن الشركات تتعرض لأضرار غير مباشرة من خلال فقدان ثقة عملاء وتدهور سمعتها في السوق، الأمر الذي قد يترجم إلى انخفاض الإيرادات والإنتاجية. إضافة إلى هذا، تتكبد الدول تكاليف إضافية للتصدي لهذه الجرائم من خلال تعزيز أنظمة الأمن السيبراني وتطوير التشريعات التي تحد من انتشارها. في الأخير، إن التعامل مع آثار جريمة الابتزاز الإلكتروني يستدعي تبني استراتيجية تجمع بين توعية المجتمع، تعزيز القيم الأخلاقية مع تطوير البنية التحتية التقنية والقانونية، وهذا بهدف الحد من تأثيرها السلبي وتحقيق بيئة رقمية آمنة ومستدامة.

المبحث الثاني:

تجريم القانوني للابتزاز الإلكتروني

تستهدف الجريمة الإلكترونية الجانب الأخلاقي لدى الأفراد، خاصة في المجتمعات العربية التي تعتز بقيمها ومبادئها الفاضلة، إذ تؤثر هذه الجرائم سلباً على حياة الأفراد واستقرارهم. وقد سعت معظم التشريعات العربية إلى التصدي لهذه الظاهرة من خلال وضع قوانين رادعة تحدد أركان جريمة الابتزاز الإلكتروني وتجرمها بوضوح، إلى جانب اقتراح حلول للحد من آثارها السلبية والوقاية من الوقوع ضحية لها. وفي هذا المبحث، سنتناول تجريم الابتزاز الإلكتروني من خلال مطلبين: يتطرق الأول إلى أركان هذه الجريمة، بينما يخصص الثاني لبيان العقوبات المقررة لها.

المطلب الأول: أركان جريمة الابتزاز الإلكتروني

يعد الابتزاز أسلوباً من أساليب التهديد الذي يمارسه المبتز للضغط على الضحية وإجباره لرضوخ أمام مطالبه معتمداً هذا التهديد بغرض المساس بحرمة وشرف حياة الضحية أو الأشهار به ولقيام جريمة الابتزاز الإلكتروني وجب توافر أركانها حيث سنوضح أركانها في الفروع على النحو التالي:

الفرع الأول: ركن الشرعي

يعد نص التجريم والعقاب الأساس الذي يعتمد عليه في إضفاء الصفة الإجرامية على فعل معين وتقرير الجزاء المترتب عليه إذا يسري هذا النص من حيث الزمان والمكان وعلى الأشخاص الذين يرتكبون الفعل الإجرامي «لا جريمة ولا عقوبة إلا بنص» ومن هذا المنطلق برزت القاعدة القانونية الشهيرة وهي ركيزة دستورية وقانونية أساسية وضمانة أساسية لحماية الحقوق والحريات وفي هذا الإطار اهتمت عدة تشريعات عربية بتجريم الأفعال المادية التي

تكون جريمة الابتزاز الإلكتروني فاتجهت الى سن قوانين خاصة تعالج مختلف صور هذه الجريمة من خلال تقرير العقوبات المناسبة ووضع أساس قانوني ركن شرعي واضح له.¹

أولاً: الركن الشرعي في التشريع الجزائري

منح المشرع الجزائر أهمية بالغة لحرمة شخصية الافراد اعتبر الاعتداء عليها جريمة يعاقب عليها القانون حيث ان الجانب الشخصي والأخلاقي هو أخطر ما قد تستهدفه جريمة الابتزاز الإلكتروني في المجتمع الجزائري الذي يعتز بمبادئه وقيمه الفاضلة فمثل هذه الجريمة كفيلة بهدم حياة المجني عليه وفقدان كرامة عائلته وانتمائها للمجتمع، حيث نصت المادة 39 من الدستور انه: «لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه».

ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل اشكالها مضمونة ولم يكتف المشرع الجزائري بالاعتراف بالحق في الحياة الخاصة باعتبارها حقاً دستورياً مطلقاً بل اعتبره من الواجبات التي يجب على الافراد مراعاتها عند ممارستهم لحقوق الأخرى وألزمهم المحافظة عليها بسترتها حيث نصت المادة 63 من الدستور: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما ... ستر الحياة الخاصة".²

الفرع الثاني: الركن المادي

يعرف الركن المادي للجريمة (الواقعة الاجرامية) هو السلوك المادي الخارجي الذي يقصد تجريمه اي كل ما يدخل في كيان الجريمة وتكون له طبيعة مادية فتمسه الحواس وهو ضروري لقيامها اذ لا ديات الجريمة مما يترتب عليه انه لا يعتبر من يعرف القانون جرائم بدون ركن مادي ولذلك سماه البعض بما قبيل الركن المادي ما يدور في الازهان من افكار ورغبات وتطلعات طالما لم تنفذ سبيلها الى الحيز الخارجي. او هو السلوك الاجرامي لفعل بمظهر ملموس لانعدام

¹ . غلييلة الحسين، معاوي عبد الناصر، " الابتزاز الإلكتروني"، مذكر لنيل شهادة الماستر تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955، سكيكدة، جوان 2024، ص26،27.

² . بن سليمان محمد الطاهر، رسيوي رشيدة، وآخرون، " جريمة الابتزاز الإلكتروني"، مرجع سابق، ص30.

الركن المادي فيها حيث يقوم الركن المادي على ثلاث عناصر السلوك الاجرامي النتيجة الاجرامية والعلاقة السببية التي تربط بين الفعل والنتيجة.¹

السلوك الاجرامي: هو النشاط المادي للجريمة يعني الحركة التي يقوم بها الجاني للأحداث نتيجة إجرامية معينة وينقسم الى السلوك الإيجابي وهي الحركة العضوية الارادية التي يقوم بها الجاني اما السلبي فهو الامتناع الارادي عن حركة عضوية الزم القانون عن اتيانها حيث يتخذ بالقيام بفعل التهديد بنشر بيانات أو صور أو مقاطع فيديو للضحية، والقانون لا يميز ولا يهمله من أين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنه عثر عليها في جهاز الضحية المسروق أو المعثور عليه او المباع.²

النتيجة الاجرامية: تعد النتيجة الاجرامية الأثر المترتب على السلوك الاجرامي الذي يعاقب عليه القانون فهي الحقيقة المادية الى كيان ملموس في العالم الخارجي او انها الحقيقة القانونية. وتقع النتيجة في الجريمة الابتزاز الالكتروني لمجرد قيام المبتز بتهديد الضحية او المساس حرمة حياة الضحية الشخصية التي تعتبر امرا لا يجب الاطلاع عليه امام الملاء.³

العلاقة السببية: وهي ارتباط السلوك الاجرامي سواء كان سلبيا او ايجابيا والنتيجة المختل، غير ان هناك نوع من الجرائم التي تسمى بجرائم جرائم السلوك او جرائم الخطر وهي الجرائم التي تتم بمجرد ارتكاب السلوك المكون لها دون تحقق نتيجة إجرامية مادية ملموسة و منها يمكن لجريمة الابتزاز الالكتروني ان تتحقق دون تحقق نتيجة إجرامية وذلك بمجرد القيام بسلوك اجرامي، او مجرد الشروع فيها دون تحقق نتيجة معينة للمجني عليه، لذلك فان السلوك الاجرامي في جريمة الابتزاز يتمثل في طريقة الابتزاز عن طريق احد وسائل المعلوماتية والاتصالات المعروفة بمواقع التواصل الاجتماعي ويكون هذا الابتزاز بواسطة المواد التهديدية المتمثلة في الفيديوهات

¹ .د. عمار عباس الحسيني، "جريمة الابتزاز الالكتروني"، منشورات زين الحقوقية، لبنان، بيروت، ص234، 235.

² . بن سليمان محمد الطاهر، رسيوي رشيدة، وآخرون، " جريمة الابتزاز الالكتروني"، مرجع سابق، ص33.

³ . بن سليمان محمد الطاهر، رسيوي رشيدة، وآخرون، " مرجع سابق، ص33.

وصور خاصة او سرية و المعلومات سرية فاضحة للضحية وأيضاً السلوك الابتزازي ويكون بإسناد أمور زائفة او مفبركة.¹

الفرع الثالث: الركن المعنوي

لا يكفي لقيام جريمة الابتزاز الالكتروني توافر الركن الشرعي والركن المادي فقط لابد من توافر إرادة الجريمة المتمثل في الركن المعنوي او ما يسمى بالقصد الجرمي فيها والمتمثل في اتجاه إرادة الجاني نحو مباشرة السلوك الاجرامي. فهي تعد من الجرائم العمدية تأخذ صورة القصد الجنائي الذي يقوم بتوافر عنصرين العلم والإرادة.²

أولاً: القصد العام: يتمثل القصد العام في عنصرين:

العلم: وان يعلم الجاني حقيقة الفعل الذي ينتج جراء ارادته نحو ارتكابه وهذا ما يسمى ب عنصر العلم ففي جريمة الابتزاز الالكتروني هو ان يعلم المبتز نتيجة المتحصل عليها عند القيام بابتزاز الضحية جريمة يعاقب عليها القانون.

الإرادة: هو إرادة الجاني في تحقيق النتيجة غير مشروعة نحو المساس بحق او مصلحة الضحية التي يحميها القانون ومن ثم ينبغي ان تتجه إرادة المبتز الى تحقيق النتيجة المتمثلة في ابتزاز المجني عليه، وتنقسم الإرادة الى إرادة الفعل وإرادة النتيجة فلكي تقوم المسؤولية وجوب اثبات إرادة الفعل اتجهت الى القيام بهذا الفعل وذلك دون ان تقع الإرادة في عيب من عيوب الإرادة كان يكون مدركاً انه يحصل على شيء سري او خاص بالضحية فان كان مكرها فلا يوجد قصد جنائي ولا تقوم المسؤولية الجزائية للفعل على المكره

¹ . بن سليمان محمد الطاهر، رسيوي رشيدة، وآخرون، مرجع سابق، ص34.

² .د. عمار عباس الحسيني، "جريمة الابتزاز الالكتروني"، مرجع سابق، ص283.

ثانياً: القصد الخاص

بما ان الجريمة الابتزاز الالكتروني تعد من الجرائم التي تتطلب الماما واسعا ومعرفة متقدمة بتكنولوجيا المعلومات لتنفيذها فانه لا يمكن تصور وقوعها دون توافر القصد. فهي من الجرائم العمدية التي يكفي فيها القصد الجنائي العام ولا يشترط توافر القصد الخاص.¹

المطلب الثاني: عقوبة جريمة الابتزاز الالكتروني

بعد ان بينا اركان جريمة الابتزاز الالكتروني نفق هنا عن الاحكام العقابية الاصلية لهذه الجريمة حيث سنتناول العقوبات الاصلية والعقوبات التكميلية ثم الظروف المشددة حيث ان العقوبة من اهم الاثار التي تترتب على تجريم السلوك المعتدي في العقوبة لضمان تحقيق الردع الخاص للمجرم تحقيق الردع العام للمجتمع ككل. للعقوبة وجهين علاجي ووقائي فلكل جريمة عقوبة تتناسب معها متنوعة بين عقوبات اصلية وتكميلية.

الفرع الأول: العقوبات الاصلية والعقوبات التكميلية

أولاً: العقوبات الاصلية:

المادة 303 مكرر من قانون العقوبات الجزائري تنص على ما يلي:
"يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 إلى 300.000 دينار جزائري كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، وذلك بالتقاط أو تسجيل أو نقل، دون إذن صاحبها، أحاديث أو أقوال صادرة على انفراد أو في مكان خاص".²
كما تنص المادة 303 مكرر 1 على: "يعاقب بنفس العقوبات كل من تعمد حفظ أو توزيع أو بث التسجيلات أو الصور الملتقطة، دون إذن صاحبها".³

¹ . بن سليمان محمد الطاهر، رسيوي رشيدة، وآخرون، " جريمة الابتزاز الالكتروني"، مرجع سابق، ص36،37.

² . المادة 303 مكرر من قانون 06-23 من قانون الإجراءات الجزائية.

³ . المادة 303 مكرر 1 من قانون 06-23 من قانون الإجراءات الجزائية.

شرح المفصل لنص المادة

الجريمة: تعتمد المساس بحرمة الحياة الخاصة الأشخاص باي وسيلة كانت.

صور الجريمة:

- النقاط او تسجيل او نقل المكالمات أو الأحاديث خاصة او سرية بغير اذن او رضا صاحبها.
- التقاط او تسجيل او نقل صورة لشخص في مكان خاص بغير اذن صاحبها او رضاه.
- عقوبة الشروع:** يعاقب على الشروع في ارتكاب هذه الجنحة بالعقوبات ذاتها المقررة للجريمة تامة. ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة.

إضافات ذات صلة:

المادة 303 مكرر (1): " تعاقب المادة 303 مكرر 1 على الاحتفاظ بالتسجيلات او الصور المذكورة او وضعها في متناول الجمهور او الغير او استخدامها باي وسيلة كانت".

استثناءات:

لا تطبق هذه العقوبات إذا كان التقاط الصورة والتسجيل الصوتي بهدف التبليغ عن الجريمة للجهات الأمنية مثل تقنية الو شرطة وبشكل مقنن.

ثانيا: العقوبات التكميلية

العقوبة التكميلية هي الجزاء الذي يلحق بالمحكوم عليه استنادا الى صدور حكم بالعقوبة الاصلية غير انها لا تطبق الا إذا نص عليها القاضي في الحكم وهي بذلك تختلف عن العقوبة التبعية التي تترتب بقوة القانون بمجرد الحكم بالعقوبة الاصلية دون حاجة الى نص عليها صراحة في الحكم لارتباطها المباشر واللازم بهذه العقوبة من نظام مكافحة جرائم المعلوماتية السعودي على جواز الحكم.¹ حيث نصت المادة 13 ب: "مصادرة الأجهزة او البرامج او الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في النظام وكذلك الأموال المتحصلة

¹ .بن سليمان محمد الطاهر ، رسيوي رشيدة، وآخرون، " جريمة الابتزاز الإلكتروني"، مرجع سابق، ص38.

منها".¹ كما اجازت الحكم بإغلاق الموقع الإلكتروني أو مكان تقديم الخدمة إغلاقاً مؤقتاً أو نهائياً متى كان ذلك المكان مصدراً لارتكاب الجريمة وثبت ارتكابها بعلم مالكة.

وتعرف المصادرة بأنها الإلولة النهائية للمال إلى الدولة بغير مقابل وتختلف عن الغرامة من حيث الطبيعة القانونية إذا ان الغرامة عقوبة مالية نقدية تعد من العقوبات الأصلية في حين تعد المصادرة عقوبة عينية تكميلية تنصب على أشياء معينة ترتبط بالجريمة.

ويشترط للحكم بالمصادرة أن تكون الأشياء محلها مشروعة الحياة في الأصل، وأن تقوم بينها وبين الجريمة صلة مباشرة، كأن تكون قد استُخدمت في ارتكابها، أو كانت وسيلة لتنفيذها، أو كانت من الأموال المتحصلة عنها. وقد حدّدت المادة (13) هذه الصلة بذكرها الأجهزة والبرامج والوسائل المسببة في ارتكاب الجرائم المعلوماتية.

وبناءً على ذلك، لا يجوز نظاماً الحكم بمصادرة أشياء لا صلة لها بالجريمة، أو لم تتحصل منها، أو لم تكن معدّة أو مستخدمة في ارتكابها. كما يشترط أن تكون الأشياء المطلوب مصادرتها مضبوطة فعلياً وقت صدور الحكم، وإلا امتنع القضاء بالمصادرة لانقضاء محلها. والمصادرة في هذا النطاق ترد على أشياء مشروعة في ذاتها، إلا أن استعمالها في نشاط غير مشروع، كجريمة الابتزاز الإلكتروني، هو الذي يبرر إخضاعها لهذا الجزاء. كما يتمتع القاضي بسلطة تقديرية في الحكم بالمصادرة أو عدمه، على أن يكون ذلك مرتبطاً بالعقوبة الأصلية المقررة للجريمة، وهي السجن أو الغرامة أو كليهما. ولا يجوز الحكم بالمصادرة إذا كانت الأشياء المستخدمة في الجريمة مملوكة لغير الجاني، متى كان هذا الغير حسن النية، وذلك عملاً بما نصّت عليه المادة (13) بقولها: «مع عدم الإخلال بحقوق الغير حسن النية».

الفرع الثاني: الظروف المشددة للعقاب

هناك حالات تشدّ فيها العقوبة في جريمة الابتزاز الإلكتروني وذلك إذا تحقق شروط معينة. ويقصد بالظروف المشددة للعقوبة وهي الحالات والأفعال الموضوعية والشخصية التي يمكن ان

¹ . المادة 31 من نظام مكافحة الجرائم المعلوماتية.

تؤثر على تشديد العقوبة المقررة للجريمة المرتكبة هنا ان يحكم القاضي بالحكم الأعلى للعقوبة المقدرة او ان يحكم بكل العقوبتين الحبس والغرامة معا.

الظروف المشددة في قانون العقوبات العراقي:

- _ ارتكاب الجريمة بباعث دنيء.
- _ ارتكاب الجريمة بانتهاز فرصة ضعف إدراك المجني عليه او عجزه عن المقاومة او في ظروف لا تمكن الغير من الدفاع عنه.
- _ استعمال طرق وحشية لارتكاب الجريمة او التمثيل بالمجني عليه.
- _ استغلال الجاني في ارتكاب الجريمة صفته كموظف او اساءته استعمال سلطته او نفوذه المستمدين من وظيفته.
- اساءة استعمال المركز العام او الثقة المرتبطة به من اجل الحصول على مكسب شخصي او عرض او منح او قبول بعض الامتيازات مخالفة للمهام.
- _ ارتكاب او دعم مخالفة لأحكام قانون النزاهة او عرقلة كشفها.
- _ مخالفة اللوائح التنظيمية الصادرة عن المفوضية المعنية بالنزاهة الوطنية بخصوص الكشف عن المصالح المالية
- ويمكن تصور ارتكاب جريمة الابتزاز الالكتروني مقترنة بأحد الظروف المشددة العامة في أعلاه بما يستوجب تشديد عقوبتها.¹
- تتمثل الظروف المشددة لجريمة الابتزاز الالكتروني في قانون الجزائي في عدة نقاط الرئيسية حيث تزيد العقوبة عند توافرها.
- _ استخدام الوسائل الالكترونية : يعتبر استخدام الوسائط الرقمية (مواقع التواصل البريد الالكتروني) بحد ذاته ظرفا مشددا ووسيلة لارتكاب الجريمة.
- _ التهديد المصحوب بطلب (ابتزاز مالي) : إذا كان التهديد يهدف الى الحصول على أموال او منفعة غير مشروعة وهي اركان التهديد بالابتزاز.

¹ د. عمار عباس الحسيني، "جريمة الابتزاز الالكتروني"، مرجع سابق، ص 321، 322.

- _الحالة النفسية او صغر سن الضحية: إذا وقعت الجريمة على شخص في حالة ضعف او استغلال صغر سن الضحية او كونه من ذوي الاحتياجات الخاصة.
- _التشهير عبر الانترنت : نشر صور او مقاطع خادشة للحياء خاصة إذا كانت بين الخطيبين او الزوجين تعد ظروفًا مشددة.
- _العود الى الاجرام : ارتكاب الجريمة من شخص سبق ادانته بنفس الجريمة.¹

¹. المادة 287 و 371 من قانون العقوبات الجزائري.

خلاصة الفصل:

لقد تناولنا في الفصل الأول الإطار الموضوعي لجريمة الابتزاز الإلكتروني بوصفها أحد أبرز تجليات الجريمة المعلوماتية المعاصرة، حيث استُهل بتأصيل ماهيتها من المنظور اللغوي والاصطلاحي والفقهية، مع تصنيف أنماطها وفقاً لصفة المجني عليه والغرض الإجرامي المستهدف. كما انصبّت الدراسة على تحليل الوسائط التقنية الموظفة في هذا السلوك، بدءاً من المنظومات الحاسوبية وبرمجياتها وصولاً إلى شبكة الإنترنت والاتصالات النقالة، ليعقب ذلك تكييف الجريمة من الناحية القانونية عبر فحص بنيانها القائم على الأركان الشرعية والمادية والمعنوية. واختُتمت الفقرة باستعراض السياسة الجنائية في مواجهة هذه الظاهرة، من خلال تبيان العقوبات الأصلية والتكميلية المقررة لها، فضلاً عن تحديد المسؤولية الجزائية المترتبة على الشروع والاشتراك الجنائي فيها.

الفصل الثاني:

الإطار الاجرائي لجريمة الابتزاز

الالكتروني

تمهيد:

رغم الطبيعة الفريدة التي تتسم بها الجرائم الإلكترونية، وعلى رأسها جريمة الابتزاز الإلكتروني، تظل هذه السلوكيات ممنوعة قانونياً ويعاقب عليها التشريع المعمول به. وفيما يخص الإجراءات والآليات القانونية المتبعة لمكافحة هذا النوع من الجرائم، فإن عمليات البحث والتحقيق وجمع الأدلة تهدف أساساً إلى التوصل إلى الحقيقة القانونية. ويجري ذلك عبر أدلة تثبت بشكل مطلق تورط المتهم بالجريمة. وتبرز خصوصية هذا النوع من الجرائم من خلال طبيعة الدليل المستخدم، الذي يكون غالباً مرتبطاً باستخدام الحواسيب والهواتف الذكية وملحقاتها، إلى جانب البرامج والتقنيات الحديثة. يتمثل هذا الدليل عادة في بيانات رقمية مثل الشفرات والعناوين الإلكترونية. وبشكل عام، يلتزم الإثبات في المجال الجنائي بقواعد تهدف جميعها إلى تحقيق غاية أساسية وهي الكشف عن الحقيقة المتعلقة بالجريمة المرتكبة. بناءً على ما تم ذكره سابقاً، يمكن اعتبار عنوان هذا الفصل: "الإطار الإجرائي لجريمة الابتزاز الإلكتروني" نقطة انطلاق أساسية يتم من خلالها تقسيم محتوى الفصل إلى مبحثين رئيسيين:

المبحث الأول: يتناول في مطلبه إجراءات التحقيق في جريمة الابتزاز الإلكتروني والصعوبات التي قد تواجه المحققين أثناء هذا النوع من التحقيقات. أما **المبحث الثاني:** فيركز على موضوع الإثبات في جريمة الابتزاز الإلكتروني.

المبحث الاول:

إجراءات التحقيق في جريمة الابتزاز الإلكتروني

على الرغم من سن العديد من الدول لتشريعات حديثة تهدف إلى مكافحة الجريمة المعلوماتية، إلا أنه لا يزال هناك قصور في شمل كافة الجوانب الإجرائية المتعلقة بها. ومع التسارع المستمر في تطور تقنيات المعلومات والانتشار المتزايد لشبكة الإنترنت، أصبحت الحاجة ملحة لاعتماد أساليب تحقيق متطورة، مع الاستعانة بخبراء ذوي تخصص عالي، بالإضافة إلى تعزيز خبرة قضاة التحقيق في هذا المجال لضمان فعالية التصدي لهذه الجرائم.

بناءً على ذلك، قررنا تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: يناول إجراءات التحقيق العامة والخاصة في جريمة الابتزاز الإلكتروني.

المطلب الثاني: يشمل الصعوبات التي تواجه المحقق أو جهات التحقيق.

المطلب الأول: إجراءات التحقيق جريمة الابتزاز الإلكتروني

تتشابه آليات التحقيق في الجرائم الإلكترونية مع تلك المطبقة في الجرائم التقليدية، إذ تعتمد كلتا الجريمتين على مجموعة من الإجراءات الأساسية التي تشمل المعاينة، للتفتيش، الاستجواب، وجمع الأدلة وتحليلها مع الحرص على المحافظة عليها من أي تحريف حيث يعرف التحقيق على أنه عملية إجرائية يقوم بها المحقق بهدف الكشف عن ملابسات الجريمة وتحديد المسؤول عنها، وهذا لتقديمه إلى جهات القضائية لينال العقوبة المقررة له وفق ما تنص عليه القوانين. وعادة ما تأخذ هذه الإجراءات طابع تقني أو فني يتضمن على سبيل المثال تحليل الآثار الرقمية والبصمات الإلكترونية، بالإضافة إلى هذا استخدام أدوات برمجية متخصصة لتتبع وسائل الدخول إلى البيانات المخزنة داخل النظم الحاسوبية. وفي هذا المطلب سنتطرق إلى أهم إجراءات تحقيق عامة وخاصة لجريمة الابتزاز الإلكتروني.

الفرع الاول: الإجراءات العامة في جريمة الابتزاز الالكتروني

القواعد القانونية التقليدية أو العامة التي تنظم إجراءات التحقيق مثال التفتيش والمعاينة، قد لا تصلح وغير ملائمة للتعامل مع الجرائم الإلكترونية بسبب طبيعة هذا النوع من الجرائم والذي يعتمد على بيانات ومعلومات غير ملموسة. وفي هذا الفرع سوف ندرس أهم القواعد الإجرائية للتحقيق عامة لجرائم الإلكترونية.

أولاً: التفتيش

" التفتيش في بيئة إلكترونية يكون بالنسبة للشخص منهم أو مكان إقامته أو ضبط أشياء متعلقة بالجريمة في منزله، وهو من اختصاص النيابة العامة كأصل عام والضبطية كاستثناء، ويشمل التفتيش المكونات المادية للحاسب الآلي التي قد تكون في مسكن المتهم أو مكان عمله ومن خلال المواد (44-الى47) من قانون الإجراءات الجزئية بين مشرع إجراءات¹ التفتيش مثل الحصول على إذن مكتوب، وأن يكون تفتيش نهاراً من ساعة خامسة صباحاً إلى ثامنة مساءً، كما يشمل التفتيش في مجال الإلكترونيات عناصر غير مادية للحاسب الآلي".²

أ. "كيفية التفتيش الإلكتروني: يتكون نظام حاسوب من مكونات مادية وأخرى معنوية، كما أنه تربطه بغيره من الحواسيب شبكات اتصال بعيدة.

1. تفتيش المكونات المادية للحاسب الآلي: إن الولوج إلى مكونات المادية للحاسوب الآلي من أجل البحث عن أدلة مادية التي تكشف عن حقيقة الجريمة الإلكترونية ومرتكبيها تخضع لإجراءات التفتيش المألوفة، لأن حكم التفتيش في هذه البيانات يتوقف أساساً على طبيعة المكان الموجود فيه فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له علمه بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش

¹ فلاح عبد القادر، أيت عبد المالك نادية، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة - خميس مليانة، مجلد 04، عدد 02، سنة 2019، ص 167.

² فلاح عبد القادر، أيت عبد المالك نادية، مرجع سابق، ص 1697.

المساكن وملحقاتها، مع الأخذ بالاعتبار إذا كانت مكونات الكمبيوتر المراد تفتيشه منعزلة عن أجهزة الكمبيوتر أم أنها تتصل بأجهزة كمبيوتر أخرى في مكان آخر.

2. التفتيش في مكونات المعنوية (المنطقية) للحاسوب ومدى ملاءمتها: تُعرف على أنها مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة المعالجة البيانات بحيث تار جدل تشريعي وفقهي حول شأن مدى جواز تفتيش المكونات المعنوية أو المنطقية للحاسب تمهيداً لضبط الأدلة الإلكترونية.¹

3. التفتيش في شبكات الحاسوب (تفتيش عن بعد): تشير الشبكة المعلوماتية إلى ارتباط جهازين أو أكثر من أجهزة الحاسوب عبر وسائل اتصال، سواء كانت تعتمد على الكبلات أو تعمل لاسلكياً. إذا كانت هذه الأجهزة منظمة ضمن نفس الموقع الجغرافي، تُعرف بالشبكة المحلية. أما إذا كانت موزعة على أماكن مختلفة وتم ربطها باستخدام خطوط الهاتف أو تقنيات أخرى، فإننا نتحدث عن شبكة الإنترنت.

في هذه الحالة، قد تكون البيانات المخزنة في موقع فعلي ضمن نطاق قضائي مختلف، مما يثير إشكالية الاختصاص القضائي وفتح مجال لطرح تساؤلات حول تأثير تفتيش الأنظمة المرتبطة بالنظام الذي يتم تفتيشه بموجب إذن قانوني، خاصة إذا كانت هذه الأنظمة موجودة ضمن مناطق قضائية متعددة. يمكن تصور هذه الإشكالية في سياق حالتين مختلفتين يعبران عنها:

الحالة الأولى: اتصال حاسب المتهم بحاسب آلي آخر أو بمنظومة معلوماتية موجودة في موقع مختلف داخل إقليم الدولة نفسها.

تتحقق هذه الحالة عندما يقوم المتهم بنقل معلومات أو بيانات مرتبطة بجريمة إلكترونية عبر الإنترنت من جهازه إلى جهاز آخر أولى منظومة معلوماتية مملوكة للغير، حيث يتم تخزينها

¹ جبراني نورة، لعماري سهام، التحقيق في جريمة الإلكترونية، جامعة محمد بشير الإبراهيمي - برج بوعريج -، كلية حقوق وعلوم سياسية، إعلام آلي والإنترنت، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في حقوق، سنة 2023، 2024 ص 39-40.

هناك. وفي مثل هذا الوضع، قد تضطر سلطات التحقيق إلى تجاوز حدود الاختصاص المكاني، مما قد يمس بحرمة خصوصية الآخرين.¹

ولهذا السبب، اتجهت بعض التشريعات الإجرائية إلى معالجة هذه الإشكالية من خلال النص صراحة على جواز امتداد التفتيش ليشمل أجهزة الحاسوب أو أي منظومة معلوماتية مرتبطة بجهاز المتهم محل التفتيش، وذلك بهدف إثبات الجريمة دون التقيد بالحصول على إذن قضائي مسبق بشأن هذا الامتداد.

الحالة الثانية: ارتباط جهاز الحاسب الخاص بالمتهم بجهاز آخر أو بنظام معلوماتي في دولة أجنبية، وتظهر هذه الحالة ضمن جملة من التحديات التي تواجه السلطات القضائية أثناء جمع الأدلة الرقمية، وذلك في ظل لجوء الجناة إلى أساليب مبتكرة، مثل تخزين بياناتهم في أنظمة معلوماتية تقع خارج الحدود السيادية للدولة وبهذا يستفيد مرتكبو الجرائم من إمكانيات الاتصال عبر وسائل التكنولوجيا الحديثة بهدف إعاقة عمليات التحقيق وإبطاء مسار عدالة ومن هذا السياق تبرز إشكالية قانونية تتعلق بمدى مشروعية توسيع نطاق التفتيش ليشمل أنظمة معلوماتية موجودة خارج إقليم الوطني.

وقد أجاز القانون الفرنسي هذا الإجراء حيث نصت المادة 1/57 من قانون الإجراءات الجزائية على تمكين ضابط الشرطة القضائية من تفتيش الأنظمة المعلوماتية المرتبطة، حتى وإن كانت تلك الأنظمة تقع خارج حدود الدولة. ويشكل هذا النص إطاراً قانونياً يسمح بتجاوز القيد الجغرافي في حالات ضرورية، مما يعكس تطور التشريعات استجابة لتعقيدات الجرائم السيبرانية العابرة للحدود.

"وقد أجاز المشرع الجزائري تفتيش الأنظمة ولو كانت خارج إقليم الدولة، وذلك بموجب المادة 3/5 من القانون 90-04، حيث أجاز النص الحصول على معطيات المبحوث عنها ومخزنة في الأنظمة المتصلة والواقعة خارج الإقليم الوطني، والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى، وذلك بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة وفقاً

¹ جبراني نورة، مرجع سابق، ص 40، 41.

لمبدأ المعاملة بالمثل. وحسب المادة 2/16 من نفس القانون: من واجب سلطات التحقيق جزائرية أن تقدم جميع التسهيلات لمراقبة الاتصالات وتفتيش المنظومات المعلوماتية الموجودة على التراب الوطني متى طُلب منها ذلك مع مراعاة مبدأ المعاملة بالمثل والاتفاقيات الدولية.

الحالة الثالثة: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي، فالتنصت والأشكال الأخرى للمراقبة الإلكترونية، رغم أنها مثيرة للجدل، إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريباً، مثلما هو الأمر بالنسبة للمشرع الجزائري في مادة 04 الفقرة ج من القانون 04/09، أجاز النص استثناءات المراقبة الإلكترونية للوصول إلى الحقيقة واشترط أن تكون هي الحل الوحيد للوصول إلى الحقيقة، أما عن السلطة المختصة بالتفتيش فيختص قاضي التحقيق أملاً بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الملائمة بصددتها، فالنيابة العامة توجه الاتهام وقاضي التحقيق يباشر إجراءات التحقيق.¹

ثانياً: معاينة في جرائم الالكتروني:

"وهي رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ومعاينة مسرح الجرائم المعلوماتية. ويجب التفرقة بين حالتي معاينة الجرائم الواقعة على مكونات الحاسوب كشاشة العرض والأقراص... ومعاينة الجرائم الواقعة على مكونات غير مادية مثل كفحص مسار الإنترنت، معاينة أنظمة الاتصال بشبكة الإنترنت"².

تتبع سلطات التحقيق مجموعة من الإجراءات عند معاينة مسرح الجريمة الإلكترونية، وهذا لضمان سير عملية التحقيق بشكل دقيق ومنظم، ومن بين هذه الإجراءات:

تقييد دخول غير المخولين إلى مسرح الجريمة للحفاظ على سلامة الأدلة إلى جانب الالتزام بعدم التعامل مع الأجهزة الإلكترونية بأي شكل قد يؤثر على سلامتها أو يعرضها للتلف علاوة على ذلك يتم التعامل بحذر عند نقل أي وسائط معلوماتية، حيث يؤخذ في الحسبان التأكد من خلو

¹ بن سلمان محمد طاهر، رسوي رشيدة وآخرون، مرجع سابق، ص 47، 48.

² فلاح عبد القادر، أيت عبد المالك نادية، مرجع سابق، ص 1697.

المكان من عوامل قد تؤدي إلى إتلافها، كما تشمل توثيق الحالة الراهنة لمسرح الجريمة، بما في ذلك أخذ صور لشاشات الحاسب لضمان تسجيل الحالة الدقيقة للأجهزة قبل أي تدخل.¹ ومن هنا فإن المعاينة كإجراء تحقيق في جريمة الابتزاز الإلكتروني تعتبر خطوة هامة لتوثيق المعلومات وجمع الأدلة التي بها الضرورة لفهم ملابسات الجريمة، وهذا ما يقضي به التشريع الجزائري بحيث نستعمل المعاينة كأداة قانونية ضمن الإجراءات الجنائية وهذا من خلال سماح القانون لضباط الشرطة القضائية والقضاء بتحليل البيانات الرقمية، وتتبع مصادر الاتصال، وكذلك فحص الأجهزة المستخدمة في جريمة الابتزاز، ولا سيما القوانين المرتبطة بمكافحة الجرائم الإلكترونية تتيح للجهات المختصة اتخاذ تدابير مختلفة لضمان الأدلة الرقمية مع احترام الخصوصية ومن بين المواد ذات الصلة، نجد مواد قانون العقوبات الجزائري وقانون الوقاية من الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ومكافحتها، وتعتبر المعاينة خطوة محورية ضمن منظومة التحقيق فهي تعتبر أساس تحقيقات اللاحقة.

ثالثاً: ضبط الأدلة في جرائم الإلكترونية

"يقصد بضبط الأدلة إجراءات جمعها وهو خلاصة النهائية لآلية التفتيش الذي يؤدي يقصد به وضع اليد على جريمة المتعلقة به كالأقراص الصلبة، الأشرطة، برامج، طباعة، بطاقات الائتمان. وقد تبنى المشرع الجزائري في القانون 09 / 04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المؤرخ في 05 / 08 / 2009 إجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان (حجز المعطيات المعلوماتية) ولها المواد التالية (06، 07، 08)."²

والمقصود بعملية الضبط هو الاستحواذ على شيء يتعلق بجريمة تم ارتكابها، بحيث يسهم في كشف ملابساتها وتحديد الجاني، ومن الناحية القانونية، يمكن أن يصنف الضبط إما كأحد إجراءات الاستدلال أو كجزء من إجراءات التحقيق، وذلك وفقاً لطبيعته وحيثياته وفي حال كان

¹ جبراني نورة، لعماري سهام، مرجع سابق، ص 47.

² فلاح عبد القادر، أيت عبد المالك نادية، مرجع سابق، ص 1697، 1698.

الضبط نتيجة مباشرة لعملية تفتيش، فإن التحدي لا يكمن غالباً في جمع الأدلة المتعلقة بالمكونات المادية للحاسوب مثل البصمات، بل إن الإشكالية الأبرز تظهر عند التعامل مع الوسائل التقنية المستخدمة لتعطيل أو تدمير البيانات مثل الفيروسات، وأيضاً عند محاولة ضبط المكونات غير المادية للحاسوب. ويأتي ذلك في سياق تعدد التشريعات الإجرائية واختلاف الآراء القانونية حول إمكانية ضبط الأشياء غير المادية أو الكيانات الرقمية التي لا يمكن أن تكون بطبيعتها محلاً للاستحواذ المباشر.

سن المشرع الجزائري، بموجب القانون رقم 04-09 الصادر بتاريخ 05 أغسطس 2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها، مجموعة من الإجراءات الحديثة التي تهدف إلى ضبط وتحرير البيانات والمعطيات المعلوماتية، بالإضافة إلى الأدلة الرقمية الأخرى، مع مراعاة طبيعتها غير المادية وقد جاء ذلك تحت عنوان (حجز المعطيات المعلوماتية) وفقاً للقواعد الواردة في المواد 6 و7 و8 من هذا القانون.¹

وللكشف عن جرائم الابتزاز الإلكتروني، ضبط الدليل يُعد إحدى المراحل الجوهرية في إجراءات التحقيق العامة. وفي إطار التشريع الجزائري، يمثل هذا الإجراء حجر الزاوية في إثبات ارتكاب الجريمة وتحديد هوية جناة، مما يستدعي الالتزام بمبادئ قانونية دقيقة. وفي تشريع الجزائري، يُعرف ضبط الأدلة كأداة قانونية هدفها جمع الأدلة وتوثيقها بكيفية تحترم القوانين الإجرائية والمبادئ الدستورية، كضمانات حماية الخصوصية وصون حقوق الأفراد، ولتصبح هذه أدلة مأخوذة بها أمام القاضي، يجب أن تخضع إلى جملة من الشروط أهمها أن يتم جمعها وفق الطرق القانونية وفي إطار الصلاحيات الممنوحة للجهات المعنية.

وفي سياق الجرائم الإلكترونية بوجه عام والابتزاز الإلكتروني على وجه الخصوص، تبرز الاعتبارات التقنية والقانونية على حد سواء. القطاع التقني يفرض تحديات مرتبطة بتعقيد تتبع الأدلة في فضاء رقمي يتسم بالتحول السريع، بينما يتمثل الجانب القانوني في تأطير هذا التتبع ضمن حدود الاحترام الكامل لحقوق الإنسان وبالتالي، يتطلب جمع الأدلة الإلكترونية من جهة

¹ جبراني نورة، لعماري سهام، مرجع سابق، ص 45.

مختصة إعداداً دقيقاً وخبرة تقنية لضمان عدم انتهاك المبادئ الأساسية أو بطلان الأدلة بسبب مخالفة الإجراءات.

كذلك خصص التشريع الجزائري مواد قانونية لتنظيم هذه العمليات مع توسيع صلاحيات سلطات إنفاذ القانون بغية الكشف عن جرائم باستخدام أدوات حديثة وبرامج متطورة تساعد في تتبع النشاط الإلكتروني للمجرمين إلى جانب ذلك، تعد الرقابة القانونية والقضائية على عمليات ضبط الدليل عنصراً ضامناً للتوازن بين مكافحة الجريمة من جهة وحماية الحرية الفردية وحقوق المتهمين من جهة أخرى.

تتطلب اجراء ضبط الدليل في جرائم الابتزاز الإلكتروني إجراءات إذن مسبقاً من السلطة القضائية في غالب الأحيان لتجنب التعسف، مع التزام الجهات المعنية بتقديم تقارير دقيقة وشفافة عن الإجراءات المتخذة وبهذا الشكل، يحاول المشرع الجزائري صياغة مقاربة شاملة تسعى إلى مواجهة هذه الجرائم المستجدة بأساليب قانونية تضمن المصادقية والفعالية داخل الإطار القضائي.

رابعاً: الخبرة التقنية في مجال الجرائم الإلكترونية:

تتطلب التحقيقات في الجرائم الإلكترونية الاستعانة بخبرات متعددة ومتنوعة بسبب طبيعة الأساليب المستخدمة في تنفيذها، والتي تشمل (التلاعب بالبيانات، تغيير طريقة نقلها وبثها، أو العبث بالبرامج الأساسية والتطبيقية، فضلاً عن تزوير المستندات المدخلة إلى أنظمة الحاسوب أو تلك الناتجة عنها بعد المعالجة)، ومن الضروري أن يعمل خبير الجرائم الإلكترونية بشكل وثيق مع المحقق الجنائي لترتيب الأدلة المتاحة وتحديد أهميتها بناء على قيمتها الاستدلالية في مقابل، ويتحتم على المحقق الجنائي شرح الجوانب القانونية المتعلقة بعمل الخبراء، مع التركيز على أهمية الربط بين الأدلة الفنية والمعرفة العلمية وبين أركان الجريمة التي يتم النظر فيها بفعل الدعوى الجنائية المرفوعة ضد المتهم.¹

¹ مرابطين علاء الدين، محمادي مراد، خصوصية الجريمة الإلكترونية في التشريع الجزائري، جامعة محمد بشير الإبراهيمي - برج بوعريريج - كلية حقوق وعلوم سياسية، قانون الإعلام، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في حقوق، دفعة 2022/2023، ص 47، 48.

الخبرة التقنية تعتبر إحدى الأدوات الإجرائية المستخدمة في اجراءات التحقيق العام لجريمة الابتزاز الإلكتروني وفقاً للتشريع الجزائري. فمع تطور ملحوظ في مجالات التكنولوجيا والإنترنت، أصبحت الجرائم الإلكترونية تشكل تحدياً كبيراً أمام الأجهزة الأمنية والقانونية، لذلك كان من الضروري الاستعانة بالخبرة التقنية للتعامل مع هذه الأنواع من الجرائم بشكل دقيق وفعال.

تساهم الخبرة التقنية في تحليل الأدلة الرقمية، مثل الرسائل أو الملفات المتبادلة بين أطراف الجريمة وتتبع أثر المجرمين من خلال تقنيات متطورة كتحليل البيانات الرقمية، استرجاع المعلومات المحذوفة، وتعقب الأنشطة المشبوهة على الشبكات. كما أنها توفر وسائل لتحديد هوية مرتكبي الجرائم وتقديم أدلة قوية قابلة للاعتماد عليها أمام المحاكم.

وفي ظل التشريع الجزائري، يتم تنظيم استعمال الخبرة التقنية لضمان توافقها مع القوانين والإجراءات المعمول بها، وهذا لعدم انتهاك حقوق الأطراف المعنية ولا تستعمل بطرق غير قانونية. بناءً عليه يمكن اعتبار الخبرة التقنية جزءاً أساسياً من إجراءات التحقيق لمواجهة التحديات التي تطرحها جرائم الابتزاز الإلكتروني في العصر الحديث.

"ونظراً لطبيعة هذه الجرائم يتم فيها الاستعانة بخبير، وهو شخص يتمتع بمؤهلات عملية وقدرة في التحكم في مجال الإعلام الآلي. وهو ما نصت عليه المادة 05 الفقرة الأخيرة من قانون رقم 04-09 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيات الإعلام والاتصال وتخضع الخبرة لمجموعة من الضوابط لتكون لها نتائج أمام القضاء وهي:

- اختيار الخبير من جدول الخبراء مع أداء اليمين القانونية والتزامه بأداء مهامه بنفسه.
- اعتماد الخبير على وسائل علمية متطورة لإنجاز الخبرة"¹.

الفرع الثاني: إجراءات التحقيق الخاصة في جريمة الابتزاز الإلكتروني

نظراً للأهمية البالغة لقضايا الجرائم الإلكترونية وبأخص جريمة الابتزاز الإلكتروني، التي تعد من أخطر هذه الجرائم لما تتطوي عليه من تحديات في التعرف على هوية الجاني وصعوبة استخدام آليات التحقيق التقليدية بشكل فعال، فقد بادر المشرع الجزائري إلى اعتماد وسائل تحقيق

¹ فلاح عبد القادر، أيت عبد المالك نادية، مرجع سابق، ص 1698.

حديثاً بهدف مواجهة ووقوف في وجه هذه التحدياتتوجاء هذا من خلال إدخال تعديلات على قانون الإجراءات الجزائية، إضافة إلى ما نص عليه القانون رقم 04/09 حيث اعتمد على جملة من آليات التحقيق الخاصة في هذا النوع من الجرائم.

أولاً: مراقبة الاتصالات الالكترونية

تعتبر مراقبة الاتصالات الإلكترونية من أهم مصادر التحري مستعملة في تحقيق بالجرائم، سواء التقليدية منها أو جرائم المستحدثة المرتبطة بالإنترنت والمعروفة بالمراقبة الإلكترونية. وقد اعتمد المشرع الجزائري هذه الوسائل ضمن قانون الإجراءات الجزائية، من خلال تنظيم عمليات اعتراض المراسلات أو تسجيل المحادثات الصوتية والتقاط الصور.

ورغم إدراج هذه الأدوات ضمن التشريعات، إلا أن المشرع الجزائري لم يعتمد مصطلحاً موحداً للإشارة إليها، إذ نجد استخدام تعبير "المراقبة الإلكترونية" في بعض النصوص التشريعية مثل القانون رقم 04-09، بينما يظهر أحياناً مصطلح "أساليب التحري الخاصة". وبرغم التباين الاصطلاحي، تبقى هذه العبارات تشير إلى إجراءات متطابقة تختلف فقط من حيث الإطار القانوني الناظم لها. وفي هذا السياق، قام المشرع بتعديل قانون الإجراءات الجزائية عام 2006 بموجب القانون رقم 22-06، حيث حدد الحالات التي تعتمد فيها هذه الأساليب وقصر استخدامها على ست فئات من الجرائم الخطيرة بما في ذلك الجرائم المعلوماتية، وتتضمن هذه الأساليب ما يلي:

أ. اعتراض المراسلات:

المراسلات تشير إلى جميع الخطابات والرسائل والطرود والبرقيات بشكل عام، لكن وفقاً للمادة 65 مكرر 5 من قانون إج ج، تم تقييد مفهوم المراسلات لتشمل فقط تلك التي تتم عبر وسائل الاتصال السلكية واللاسلكية، وبذلك استبعدت المراسلات العادية من هذا التعريف.¹

¹ بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، مرجع سابق، ص 49، 50.

ب. تسجيل الأصوات:

يشير تسجيل الأصوات إلى عملية مراقبة الأحاديث وتسجيلها، وكذلك الاتصالات التي تتم عبر الوسائل السلكية أو اللاسلكية. وتفيد هذه العملية بإجراء مراقبة تشمل كافة أدوات الاتصال سواء كانت تعتمد على الأسلاك أو تعمل بشكل لاسلكي. وينفذ ذلك من خلال وضع تقني معين دون الحصول على موافقة مسبقة من الأطراف المعنية بهدف التقاط وتثبيت وبث وتسجيل المحادثات. يجري هذا الأمر بشكل خاص أو سري من قبل فرد أو مجموعة من الأفراد.

ج. التقاط الصور:

هي تلك العملية التقنية التي تكون بواسطة التقاط صور لفرد أو عدة أفراد يتم تواجدهم في مكان معين. وتتسم هذه الإجراءات بالسرية التامة لأن بها مساساً بحرمة الحياة الخاصة للأشخاص والمصونة دستورياً.

ثانياً: حفظ المعطيات المتعلقة بحركة السير:

تُعد المعطيات المرتبطة بحركة السير جزءاً أساسياً من عملية التواصل عبر منظومة معلوماتية، حيث تشمل هذه المنظومة على إنتاج بيانات تشمل مصدر الاتصال، الوجهة المستقبلية، المسار الذي يتم اتخاذه، بالإضافة إلى توقيت الاتصال، وحجمه، ونوع الخدمة المستخدمة.

وفي هذا السياق، أقر المشرع الجزائري، على غرار التشريعات الحديثة الأخرى بضرورة التزام مقدمي الخدمات بالاحتفاظ بهذه البيانات، وذلك بهدف تمكين الجهات المختصة من تتبع أي أثر يمكن أن يخلفه النشاط الإجرامي مهما كان نوعه.¹

ثالثاً: التسرب الالكتروني أو الاختراق:

نظم المشرع الجزائري هذا الإجراء من خلال المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية، حيث تم التطرق إلى مفهومه وشروطه.

¹ بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، مرجع سابق، ص 50، 51.

يتمثل التسرب في نطاق الجرائم الإلكترونية في القيام ضباط أو أعوان الشرطة القضائية بالدخول إلى العالم الافتراضي عن طريق اختراق مواقع معينة أو المشاركة في محادثات في غرف الدردشة، متقمصين دور شخصيات تبدو وكأنها ضحايا أو وسطاء وهميين بهدف الإيقاع بالجناة، وهو ما يعرف بالتسرب الإلكتروني أو الاختراق.¹

المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الابتزاز الإلكتروني

تُعد جريمة الابتزاز الإلكتروني من الظواهر المتنامية التي أفرزها التطور التكنولوجي المتسارع والثورة الرقمية في عصرنا الحالي. وباعتبار أن هذه الجريمة ترتبط ارتباطاً وثيقاً باستخدام الوسائل الإلكترونية وشبكة الإنترنت، فإنها تفرض تحديات مختلفة على جهات التحقيق، خاصة في ظل تعقدها التقني والتشريعية.

في السياق الجزائري، تواجه الجهات المختصة بجمع الأدلة وتحليلها وإثبات الجرائم صعوبات كثيرة تتعلق بالطبيعة المستحدثة لهذه الجريمة، وبالبيئة القانونية التي قد تعاني من ثغرات تشريعية تحول دون التصدي الفعال لها. يضاف إلى ذلك العوائق المتعلقة بالتعاون الدولي، بالنظر إلى الطابع العابر للحدود الذي يميز الجرائم الإلكترونية عموماً، مما يزيد من تعقيد مهمة التحقيق والوصول إلى مرتكبيها. في هذا الإطار، يصبح من الضروري دراسة التحديات التي تعترض طريق الجهات المختصة في الكشف عن جرائم الابتزاز الإلكتروني في الجزائر.

الفرع الأول: الصعوبات التي تواجه جهات التحقيق واكتشاف الجريمة

تتمثل هذه الجرائم في اعتمادها بشكل كبير على الوسائط الإلكترونية والشبكات الرقمية التي تتطلب مستوى عالٍ من التحليل الفني والمعلوماتي بالإضافة إلى ذلك، يضاف إلى التحديات الأمنية والتقنية بعداً ثاني يتمثل في الافتقار إلى تشريعات شاملة ومتخصصة بصورة كافية لمكافحة الجرائم الإلكترونية، وتأخر وضع أطر قانونية تتناسب مع حجم التطور الإلكتروني والجرائم المرتبطة به. وعليه فإن تعزيز قدرات فرق التحقيق والفضاء على مستوى التواصل التشريعي والتقني يعد أمراً بالغ الأهمية لمواجهة هذه التحديات.

¹ فلاح عبد القادر، أية عبد المالك نادية، مرجع سابق، ص 1698.

أولاً: حق الانسان في خصوصية

العديد من التشريعات في مختلف الدول قامت بتجريم التعدي على الحياة الخاصة للأفراد عبر شبكة الإنترنت. وقد تم التأكيد على هذا الحق في ميثاق الأمم المتحدة الصادر عام 1948، بما في ذلك المادة 15 منه، كما أن جميع الإعلانات العالمية لحقوق الإنسان شددت على أهمية حماية الخصوصية والحياة الشخصية. وحرصت الدساتير والأنظمة القانونية في الدول العربية على مواكبة ما دعت إليه هذه الإعلانات لضمان صون هذه الحقوق.

ثانياً: نقص خبرة العالمين بجهات التحقيق

لا تزال جهات التحقيق تواجه تحديات كبيرة تتمثل في نقص الخبراء الفنيين وقلة التدريب المتخصص في التعامل مع الأدلة الرقمية، بما يشمل البحث عنها واستخلاصها بشكل صحيح. بالإضافة إلى ذلك، يتطلب التحقيق مع المجرمين ذوي المهارات التقنية العالية خبرة خاصة، إذ يعتمد هؤلاء المجرمون على تكتيكات معقدة للهروب من المحققين عبر إغراقهم بالتفاصيل التقنية الدقيقة التي قد لا يكونون على دراية جيدة بها. بحيث في هذا النوع من الجرائم الإلكترونية مثل تهديد والابتزاز عبر الإنترنت، من الضروري أن يمتلك المحقق الجنائي مهارات تقنية متقدمة تدمج بين القدرة على استخدام الأدوات التكنولوجية الحديثة وقراءة أبعاد الجريمة الإلكترونية وتقييم خطورة جاني.

يضاف إلى ذلك أهمية معرفة المحقق بمكونات الأجهزة المادية وملحقاتها مثل الطابعات، المساحات الضوئية والكاميرات، من أجل تحليل مدى ارتباطها بالجهاز الأساسي والتحقق من علاقتها بالجريمة. كما يعد تقييم وسائط تخزين الأدلة الرقمية أمراً بالغ الأهمية لتحديد صلتها بالإنترنت ومعرفة ما إذا كانت جزءاً من أدوات الجريمة أم لا، ما يساهم في تعزيز مصداقية التحقيقات وكشف خيوط الجرائم المعقدة.¹

¹ عراب مريم، مرجع سابق، ص 1216.

ثالثاً: فقدان الآثار المادية للجريمة:

تعتبر صعوبة إثبات جرائم الابتزاز الإلكتروني واحدة من أبرز التحديات، وذلك بسبب سهولة إخفاء الأدلة الرقمية أو تلفها وإمكانية تدميرها بسرعة.

بالإضافة إلى ذلك هناك العديد من الجرائم المعلوماتية التي قد تحدث دون أن يدرك الضحايا وقوعها، لاسيما تلك المرتبطة بالاختراقات التي تهدف إلى سرقة البيانات الشخصية هذا الأمر يمنح الجناة الفرصة للتحرك بحرية داخل المواقع المستهدفة قبل تنفيذ جرائمهم. كما أن تعقيد عملية إثبات هذه الجرائم يعد عاملاً رئيسياً يشجع على ارتكابها، إذ يمنح المجرمين شعوراً بأنهم قادرون على الإفلات من العقاب.¹

الفرع الثاني: الصعوبات التي تواجه جهات التحقيق منغلقة بالجانب القضائي

تواجه جهات التحقيق العديد من الصعوبات المتعلقة بالجانب القضائي، والتي تنبع غالباً من تعقيدات النظام القانوني وتشابك الإجراءات القضائية. تتجلى هذه الصعوبات في تضارب النصوص القانونية، وطول مدة زمنية لازمة لاستكمال التحقيقات، إضافة إلى التحديات المرتبطة بجمع الأدلة وإثباتها بما يتوافق مع المعايير القضائية وتطوير آليات قانونية وأدوات تقنية ملائمة للتعامل مع هذا النوع من جرائم إلكترونية متنامية بما يضمن حماية الضحايا وتقديم الجناة إلى العدالة وفقاً للإطار القانوني الوطني والدولي.

أولاً: تنازع الاختصاص

تنازع الاختصاص يعد تحدياً يؤثر بشكل كبير على فعالية عمل جهات الضبط والتحقيق، خاصة في معالجة الجرائم المتعلقة بالابتزاز الإلكتروني. هذا النوع من الجرائم يتميز بكونه عابراً للحدود الإقليمية، حيث قد يكون الجاني مقيماً أو يعمل في دولة مختلفة تماماً عن الدولة التي ينتمي إليها الضحية. ويؤدي هذا الوضع إلى إشكالية حول تطبيق العقوبات، إذا اختلف النظام

¹ اسلام عزت محمد ندا، المواجهة الجنائية والأمنية لجرائم الابتزاز الإلكتروني (دراسة مقارنة)، مجلة البحوث الفقهية والقانونية، رقم الإيداع 6359، العدد 50، سنة 2024، ص 579.

القانوني بين الدول من حيث العقوبة المناسبة وآلية تنفيذها، مما يثير أسئلة معقدة بشأن تحديد القانون الواجب التطبيق وضمان تحقيق العدالة في مثل هذه القضايا.¹

ثانياً: قصور التعاون القضائي الدولي في مكافحة جريمة الابتزاز الالكتروني:

يشكل التعاون الدولي دعامة أساسية للتصدي لمختلف الجرائم الإلكترونية، والتي تتسم بنموها السريع وانتشارها عبر الفضاء الرقمي. وتعد جريمة واحدة من أبرز هذه الجرائم التي تشكل تهديداً متزايداً للأفراد والدول على حد سواء. ولا يقتصر خطرها على الجانب المادي فقط، بل يمتد ليجمع أبعاداً اجتماعية ونفسية وغيرها. ومع التعقيد المتزايد في أساليب الابتزاز الإلكتروني، أصبح تعزيز التعاون الدولي أمراً لا غنى عنه لتحقيق استجابة أكثر فعالية، ومع ذلك يصطدم هذا التعاون بعدد من التصديات التي تعيق الجهود المبذولة لمكافحة هذه الجرائم الإلكترونية، فقد أصبحت الجرائم المعلوماتية تصدياً دقيقاً ومعقداً يتطلب تضافر الجهود الدولية بشكل أكبر لمواجهة بجدية وفعالية.

في ظل عالم مترابط بشبكات اتصال متقدمة ودقيقة تنتقل البيانات والمعلومات بين مناطق متباعدة باستخدام تقنيات لا تضمن دائماً حماية شاملة. هذه البيانات تكون عرضة للتلاعب عبر الحدود، سواء خلال نقلها أو تخزينها، مما قد يؤدي إلى أضرار جسيمة للأفراد أو الدول أو حتى الشركات. وبناءً على ذلك، يصبح من الضروري تعزيز التعاون الدولي على نطاق واسع للتصدي لجرائم الإنترنت والحد من آثارها المدمرة على مختلف الأصعدة.

ثالثاً: عدم وجود نموذج موحد للنشاط الإجرامي

الأنظمة القانونية المعتمدة في العديد من الدول لمكافحة جرائم المعلوماتية تفتقر إلى توافق عام حول نماذج إساءة استخدام النظام المعلوماتية وشبكة الإنترنت التي يجب تصنيفها كالجرائم.²

¹ بوشعير الحسن، حداد شعيب، جريمة الابتزاز - دراسة مقارنة - جامعة محمد البشير الإبراهيمي - برج بوعرييج - كلية الحقوق وعلوم سياسية، قانون الإعلام الآلي والإنترنت، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في قانون العام، 2023/2022، ص 94.

² حداد شيماء، جبلي سعيده، مرجع سابق، ص 55، 56.

فما قد يعد مباحاً في بعض الأنظمة قد يعتبر محرماً في نظم أخرى، يعود ذلك إلى مجموعة من العوامل أبرزها الاختلاف في الديانات والعادات والتقاليد والثقافات بين المجتمعات المختلفة.

رابعاً: اختلاف النظم القانونية الإجرائية

يعود ذلك إلى تنوع واختلاف الأنظمة القانونية الإجرائية، حيث قد تكون أساليب التحري والتحقيق والمحاكمة التي تثبت فعاليتها وفائدتها في دولة معينة عديمة الجدوى وغير فعالة في دولة أخرى¹.

خامساً: عدم وجود قنوات اتصال

غياب التواصل الفعال بين الدول لتبادل الأدلة والمعلومات يشكل عائقاً كبيراً أمام تحقيق التعاون الدولي في مجال مكافحة الجريمة. يعد انعدام التنسيق والتعاون بين الدول فيما يتعلق بالإجراءات وجمع الاستدلالات وإجراء التحقيقات أحد التحديات الرئيسية، لاسيما أن جمع دليل متعلق بجريمة ما قد يتطلب الوصول إلى معلومات تقع خارج نطاق الدولة المعنية، وهو ما يجعل هذه العملية في غاية الصعوبة.

سادساً: التجريم المزدوج

يُشترط في مبدأ التسليم المزدوج أن يكون السلوك الإجرامي المنسوب للشخص المطلوب تسليمه مجرمًا بموجب قوانين الدولة الطالبة والدولة المطلوب إليها التسليم. فإذا لم يكن هذا السلوك مجرمًا في تشريع الدولة الطالبة، فلا يمكن تصور وجود دعوى عمومية أو ملاحقة جزائية أو تنفيذ عقوبة جنائية، وبالمثل، لا يمكن للدولة المطلوب إليها التسليم فرض عقوبة على سلوك لا يعتبر جرمًا وفقاً لقوانينها. ويعود ذلك أيضاً إلى غياب اتفاقيات ثنائية للتعاون بين الدولتين في هذا الشأن، مما يعزز من أهمية وجود إطار قانوني يضمن التنسيق والتفاهم في مثل هذه الحالات.²

¹ حداد شيماء، جبلي سعيدة، مرجع سابق، ص 56.

² بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، مرجع سابق، ص 56، 57.

سابعاً: صعوبات الإنابة القضائية الدولية

ينص النص على أنه يجب تكليف السلطات القضائية المطلوبة باتخاذ الإجراءات اللازمة لإجراء التحقيق لصالح السلطة القضائية المختصة في دولة الطالبة، مع الالتزام التام باحترام الحقوق والحريات الانسان المعترف بها دولياً. وفي المقابل تلتزم الدولة الطالبة بتقديم المعاملة متبادلة باحترام النتائج القانونية التي توصل إليها الدولة المقدم منها المساعدة القضائية. ومع ذلك تواجه أعمال الإنابة القضائية غالباً ببطء وتعقيد كبير، مما يتعارض مع الحاجة إلى الاستجابة السريعة في مواجهة هذا النوع من الجرائم.¹

المبحث الثاني:

الاثبات في جريمة الابتزاز الالكتروني

تعد مسألة تأصيل الماهية القانونية للأدلة الجنائية من المرتكزات الجوهرية والمسائل الحاسمة في فقه القانون الجنائي، إذ تمثل حجر الزاوية في بناء القناعة القضائية وضمانة لاستقامة البحث القانوني الرصين. وانطلاقاً من ضرورة الإحاطة بهذا المفهوم إحاطةً شاملةً ومنضبطة، يقتضي المنهج التحليلي استجلاء الدلالات الاصطلاحية لكل مفردة على استقلال، سعياً للوصول إلى تعريف جامع لـ 'الدليل الجنائي' بمفهومه التقليدي؛ ومن ثم الانتقال إلى بلورة مفهوم دقيق لـ 'الدليل الجنائي الرقمي' في ضوء المستجدات التقنية المعاصرة. وعليه، فإن خطة المعالجة تفرض التدرج في تناول بدءاً من التعريف العام لـ 'الدليل'، مروراً بخصائص 'الدليل الجنائي'، وصولاً إلى تحديد الضوابط والمعايير التي تُعرّف 'الدليل الجنائي الرقمي' بوصفه ركيزة مستحدثة في منظومة الإثبات الجنائي.

¹ بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، مرجع سابق، ص 58.

المطلب الأول: ماهية الدليل الجنائي الرقمي

الدليل الجنائي هو من أكثر المصطلحات تداولاً في الفقه الجنائي لاسيما مسألة الإثبات، فبدونه لا يمكن إلحاق الفعل بالفاعل، ومن المعلوم أن الدليل الجنائي الرقمي باعتباره فرعاً من فروع الدليل الجنائي وأحد صوره فال يستقيم الحديث عليه الا بعد التطرق الى الدليل الجنائي باعتباره الاصل.

وعليه فإن المقصود بالدليل الجنائي سيتم الإشارة اليه في (الفرع الأول) ومن ثم نتطرق الى شروطه في (الفرع الثاني).

الفرع الأول: مفهوم الدليل الجنائي الرقمي

أولاً: تعريفه

هناك عدة تعريفات لدليل الرقمي تباينت بين التوسع والتضييق نذكر منها مايلي:

"الدليل المأخوذ من اجهزة الكمبيوتر ويكون في شكل مجالات او نبضات مغناطيسية او كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور والأصوات والاشكال والرسوم وذلك من اجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الاخذ به امام أجهزة انفاذ وتطبيق القانون"

وقد عرفت المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 الدليل الرقمي بأنه : " المعلومات ذات قيمة المحتملة والمخزنة او المنقولة في صورة رقمية".

وقد عرفت المنظمة العالمية لدليل الكمبيوتر الأدلة ذات صلة على النحو التالي:

الدليل الرقمي الأصلي: هو الأشياء المادية او المعلوماتية المتصلة بهذه الأشياء المادية عند الضبط.

الدليل الرقمي المزدوج: فهو كل الأشياء المتعلقة بالبيانات عند ضبط شيء الملموس الأصلي.¹

كما يُعرّف المشرع المصري الدليل الرقمي في المادة 1 من القانون 175 لسنة 2018 شأن مكافحة جرائم تقنية المعلومات بأنه: " كل معلومات رقمية تتمتع بقوة أو قيمة ثبوتية، سواء كانت مخزنة أو منقولة أو مستخرجة من أجهزة الحاسوب اللّآلي أو الشبكات المعلوماتية وما في حكمها، بحيث يمكن تجميعها وتحليلها باستخدام تقنيات متخصصة مثل البرامج أو التطبيقات الرقمية " باعتباره كل مُعطى معلوماتي يتخذ هيئة رقمية ويتمتع بحجية قانونية في الإثبات، وسواء كان هذا الدليل في حالة سكون كمادة مخزنة، أو في حالة تدفق كمعلومات منقولة، أو حتى كبيانات مستخرجة من النظم المعلوماتية أو ما يلحق بها من وسائط تقنية؛ فإن ماهيته القانونية تتبلور في كونه مادة قابلة للمعالجة الفنية عبر عمليات التجميع والتحليل المنهجي باستخدام برمجيات وتطبيقات متخصصة، بما يضمن استخلاص الحقيقة القضائية من الحيز الافتراضي ونقلها إلى حيز اليقين القانوني.²

وعلى خلاف المقاربات التعريفية المباشرة، نهج المشرع الجزائري مسلكاً موضوعياً في تقنين الدليل الإلكتروني عبر المادة 323 مكرر 1 من القانون المدني، التي أقرت بمبدأ المعادلة الوظيفية بين المحررات التقليدية والإلكترونية، مشروطةً بالتحقق من هوية المصدر وضمان سلامة المحتوى من التعديل؛ وهو ذات التوجه الذي تبناه المشرع الفرنسي في القانون المدني بوضعه معايير الحجية القائمة على الموثوقية التقنية. وبالانتقال من النطاق المدني إلى الحقل الجنائي والإجرائي، وتحديداً ضمن أحكام قانون العقوبات والقانون 04-09 وقانون حماية البيانات الشخصية، تكرست الذاتية القانونية للدليل الرقمي في الجزائر باعتباره وعاءً معلوماتياً يشمل كافة البيانات المخزنة أو المعالجة تقنياً—كالرسائل والملفات والتسجيلات الرقمية—مما يجعله ركيزة

¹. أمير فرج يوسف، "الاثبات الجنائي للجريمة الإلكترونية"، الطبعة الأولى، مكتبة الوفاء القانونية، سنة 2016، الإسكندرية، مصر، ص 287، 288.

². درابلة العمري سليم، "حجية الدليل الرقمي في الإثبات الجنائي"، شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، 2025، ص 38، 42.

جوهرية في منظومة التحقيقات القضائية الحديثة الرامية لمواجهة الجرائم المعلوماتية والتقليدية على حد سواء.¹

ثانياً: أنواع الدليل الرقمي الجنائي

ينقسم الدليل الجنائي الرقمي الى نوعين: الأول يتمثل في الأدلة الجنائية الرقمية التي اعدت لتكوين وسيلة اثبات واما النوع الثاني يتمثل في الأدلة الجنائية الرقمية التي لم تعد لتكون وسيلة اثبات.

- النوع الأول: هو الأدلة الرقمية المعدة كوسيلة إثبات، وهي البيانات والمعلومات التي يتم إنشاؤها أو حفظها بواسطة الحاسب الآلي بشكل تلقائي أو منظم بهدف إمكانية الرجوع إليها والاستفادة منها في الإثبات. ويشمل هذا النوع مخرجات الحاسب الآلي التي لا يتدخل الإنسان مباشرة في إنشائها، مثل فواتير البطاقات الذكية وسجلات الهواتف النقالة، إضافة إلى البيانات التي يكون جزء منها مُنشأً إلكترونياً وجزء آخر تم إدخاله أو تخزينه بواسطة المستخدم، مثل رسائل غرف المحادثة على الإنترنت والبريد الإلكتروني. وتتميز هذه الأدلة بأنها منظمة وقابلة للحفظ والاسترجاع، مما يجعلها ذات أهمية كبيرة في التحقيقات الجنائية والإثبات القضائي.

- أما النوع الثاني: فهو الأدلة الرقمية غير المعدة أصلاً كوسيلة إثبات، وهي الأدلة التي تنشأ بصورة غير مباشرة نتيجة استخدام الأفراد للحاسب الآلي أو الإنترنت أو الشبكات المعلوماتية، دون أن يقصد المستخدم إنشاء دليل يمكن الاستناد إليه قانونياً. ويتمثل هذا النوع في الآثار الرقمية التي يتركها المستخدم أثناء نشاطه الإلكتروني، مثل الرسائل المرسلة والمستقبلة، وسجلات التصفح، وعمليات الدخول والخروج، والأنشطة المختلفة التي تتم عبر الأجهزة أو الشبكات. وتكمن أهمية هذه الأدلة في قدرتها على كشف تصرفات المستخدم وتتبع نشاطه الرقمي، لذلك تُعد من الوسائل المهمة التي يعتمد عليها المحققون في اكتشاف الجرائم الإلكترونية وإثباته.

¹ .درايلة العمري سليم، المرجع السابق، ص43.

كما ان وزارة العدل في الولايات المتحدة الامريكية قسمت الدليل الرقمي الى ثلاث اقسام:

1- السجلات المخزنة في الحاسب الآلي: وهي البيانات والوثائق التي يتم حفظها وتخزينها داخل أجهزة الحاسب الآلي، مثل رسائل البريد الإلكتروني، وملفات معالجة النصوص، ورسائل المحادثات عبر الإنترنت، حيث يمكن الرجوع إليها واستخدامها كوسيلة إثبات رقمية.

2- السجلات المنشأة بواسطة الحاسب الآلي: وهي البيانات التي يقوم الحاسب الآلي بإنشائها تلقائياً دون تدخل مباشر من الأفراد، وتعد من مخرجات الأنظمة الإلكترونية، مثل سجلات الهواتف النقالة والتقارير والبيانات الناتجة عن العمليات الإلكترونية المختلفة.

3- السجلات المدخلة والمعالجة إلكترونياً: وهي البيانات التي يُدخلها المستخدم إلى الحاسب الآلي ليتم إنشاؤها أو معالجتها بواسطة البرامج الحاسوبية، مثل المستندات المكتوبة عبر برامج الأوفيس أو جداول الإكسل التي تخضع للعمليات الحسابية والمعالجة الرقمي لكن يبدو ان من اهم الأقسام الرئيسية للأدلة الرقمية تقتصر على مايلي:

القسم الأول: ادلة رقمية متعلقة بأجهزة الحاسب الالي وشبكاتها

القسم الثاني: ادلة رقمية متعلقة بالإنترنت

القسم الثالث: ادلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية

القسم الرابع: ادلة رقمية متعلقة بالشبكة العالمية للمعلومات.¹

ثانياً: خصائص الدليل الرقمي

الدليل الرقمي الجنائي له عدة خصائص تميزه عن غيره من الأدلة الجنائية التقليدية، وهذا ما سيتم توضيحه من خلال العناصر الآتية:

¹ . ماكوك أرسلان عبد الله كاكويس، "الدليل الرقمي وحجته في الإثبات الجنائي"، الطبعة الأولى، دار وليد للنشر والتوزيع والبرمجيات، القاهرة، مصر، 2022، ص40،41،42.

1. الدليل الجنائي الرقمي هو دليل علمي وتقني ذو طبيعة مزدوجة:

يُعد الدليل الجنائي الرقمي دليلاً علمياً ذا طبيعة تقنية مزدوجة؛ فهو كيان غير ملموس يتكون من بيانات إلكترونية مخزنة، مما يميزه عن الأدلة المادية التقليدية ويجعل استخراجها وتحليلها رهناً باستخدام وسائل برمجية متطورة وخبرات تقنية متخصصة. وتتجلى مصداقية هذا الدليل في خضوعه لمعايير علمية دقيقة، مثل "البصمة الرقمية" (Hash Values) التي تضمن سلامة البيانات من التعديل وتطابق النسخ المستخرجة مع أصولها، مما دفع التشريعات الدولية لتحديث قوانينها لضبط التعامل معه. ويبرز دور الخبير التقني كعنصر جوهري في معاونة سلطات التحقيق والقضاء على فهم الماهية الفنية للدليل وتتبع تاريخ إنشائه أو التلاعب به، لضمان تحويل تلك "الذبذبات الرقمية" إلى حقائق قانونية ملموسة تخدم العدالة وتكشف عن الحقيقة الجنائية بيقين علمي.¹

2. الدليل الرقمي دليل متطور ومتنوع:

يتميز الدليل الرقمي بخاصية التنوع والشمول، إذ لا ينحصر في قالب واحد بل يمتد ليشمل كافة أشكال البيانات (نصوص، صور، أصوات، ومرئيات) المستمدة من مصادر متعددة كأجهزة الحاسب، شبكات الإنترنت، وبروتوكولات تبادل المعلومات، وصولاً إلى الهواتف الذكية. هذا التعدد يمنح الدليل قدرة فائقة على كشف الجرائم المعلوماتية المتطورة (كالنصب والاحتيال)، سواء استُخدمت هذه الأدلة منفردة أو مجتمعة لإدانة الجاني أو تبرئة المتهم. ورغم هذا الثراء المعلوماتي، يواجه ضبط الدليل الرقمي تحديات تقنية معقدة تفرضها أنظمة حماية المواقع العالمية وتقنيات التشفير وكلمات المرور التي يستخدمها الجناة لإخفاء آثارهم، مما يربط تطور هذا الدليل وتنوعه طردياً بالتسارع التقني المستمر وحاجة الأفراد المتزايدة للوسائل التكنولوجية.²

¹. درابلة العمري سليم، مرجع سابق، ص 44 الى 49.

². مأكوك أرسلان عبد الله كاكه ويس، مرجع سابق، ص 47 الى 49.

3. صعوبة التخلص من الدليل الرقمي:

يتمتع الدليل الرقمي بخاصية الاستمرارية والعصيان على الإتلاف، حيث يصعب التخلص منه نهائياً حتى في حالات الحذف أو الإلغاء؛ إذ تتيح البرمجيات المتخصصة استعادة البيانات المسحوبة بدقة وكشف أي محاولات للتلاعب أو التعديل قام بها الجاني، وهو ما يمنحه تفوقاً تقنياً على الأدلة التقليدية كشهادة الشهود التي تعثرها عوارض النسيان. كما أن قدرة هذا الدليل على التنسخ المطابق للأصل تضمن بقاءه وحمايته من الضياع، مما يجعل من أثر الجريمة الرقمية سجلاً ثابتاً يسهل استرجاعه وتقديمه كدليل إثبات قاطع أمام القضاء، ويقلص فرص فرار الجناة من قبضة العدالة مهما بلغت مهاراتهم في محاولة محو آثارهم الإلكترونية.¹

4. الدليل الجنائي الرقمي دليل عابر للحدود

يُعد الدليل الجنائي الرقمي دليلاً عابراً للحدود بامتياز، إذ يتجاوز النطاق الإقليمي والولايات القضائية التقليدية بفضل طبيعته الديناميكية وتقنيات الحوسبة السحابية التي تتيح تخزين البيانات وتداولها عالمياً. ومع التطور المذهل في أحجام الأجهزة وقدراتها المعالجة — من الحواسيب الضخمة إلى الأجهزة المدمجة في الهواتف والشرائح الدقيقة — أصبح الدليل الرقمي يتسم بالعالمية، مما يفرض تحديات قانونية معقدة تتعلق بسيادة الدول وإجراءات التفتيش والضبط العابر للحدود. وهذا الواقع يستوجب تنسيقاً دولياً دقيقاً وتدابير قانونية استثنائية لتعقب الأدلة وضبطها دون المساس بالاستقلالية القضائية للدول، مع ضمان استغلال خصائص هذا الدليل من تنوع واستمرارية وصعوبة في الإتلاف لتحقيق العدالة الناجزة في مواجهة الجريمة المعلوماتية.²

¹. مأكوك أرسلان عبد الله كاكه ويس، مرجع سابق، ص 49.

². درابلة العمري سليم، مرجع سابق، ص 54، 55.

الفرع الثاني: شروط الدليل الجنائي الرقمي

يشترط في الدليل الرقمي، حتى يُعتدّ به كأساس لإثبات الحقيقة في الدعاوى الجنائية، توافر مجموعة من الشروط القانونية والتقنية. وتتمثل هذه الشروط أساسًا في ضرورة أن يكون الدليل الرقمي خاليًا من الشك وقاطعًا في دلالته، وأن يتم الحصول عليه بطرق مشروعة وفقًا للإجراءات التي يحددها القانون، إضافة إلى وجوب قابليته للمناقشة وتمكين الخصوم من الاطلاع عليه ومناقشته أمام الجهات القضائية المختصة. وفيما يلي عرض لهذه الشروط بشيء من التفصيل

أ_مشروعية الدليل الرقمي:

يُشترط لقبول الدليل الرقمي والاعتماد عليه في تكوين قناعة القاضي أن يكون متحصّلًا عليه بطرق مشروعة ووفقًا للإجراءات التي يقرّها القانون. فالقاضي الجنائي لا يجوز له الاستناد في حكمه إلا إلى أدلة مشروعة، أما الأدلة الناتجة عن إجراءات مخالفة للقانون فلا يُعتدّ بها ويتعين استبعادها، حتى ولو كانت مدعّمة بأدلة أخرى صحيحة ومشروعة.

وتقوم المشروعية على مبدأ احترام أحكام القانون والالتزام بمقتضياته في جميع مراحل البحث والتحري، باعتبارها ضمانة أساسية لحماية الحقوق والحريات الفردية من أي تعسف أو تجاوز من قبل السلطات العامة، وذلك في الحدود التي يجيزها القانون حفاظًا على النظام العام وتحقيقًا للتوازن بين مصلحة المجتمع وحقوق الأفراد.

ب _دليل رقمي غير قابل للشك:

يُشترط في الدليل الرقمي أن يتسم باليقين والوضوح، إذ لا يجوز المساس بقرينة البراءة أو افتراض خلافتها إلا إذا بلغ اقتناع القاضي درجة اليقين القضائي. ويتحقق هذا الاقتناع من خلال ما يُعرض عليه من أدلة ومخرجات إلكترونية وما تستقر عليه قناعته بشأن دلالتها وقوتها الإثباتية. ومن ثمّ، يعتمد القاضي على ما توفره هذه الأدلة الرقمية من مؤشرات وقرائن تقنية لتحديد مدى صحة نسبة الجريمة للمعلوماتية إلى شخص معين من عدمها.

جـ. دليل رقمي غير قابل للنقاش:

لا يجوز للقاضي أن يؤسس حكمه إلا على الأدلة التي تُعرض عليه أثناء المرافعات والتي تمت مناقشتها بصورة علنية وشفوية وحضورية من قبل أطراف الدعوى، احتراماً لمبدأ المواجهة وحقوق الدفاع.

وعليه، فإن الأدلة المستمدة من جرائم الحاسب الآلي والإنترنت تخضع بدورها للمناقشة أمام المحكمة عند الاستناد إليها كوسيلة للإثبات، بحيث يجب عرضها ومناقشتها مباشرة أمام القاضي الجزائي خلال الجلسة، لا الاكتفاء بما ورد بشأنها في ملف التحقيق الابتدائي.¹

المطلب الثاني: الصعوبات الإثبات في جريمة الابتزاز الإلكتروني:

نظراً لكون هذه الجريمة تُرتكب في الخفاء من قبل أشخاص يتمتعون غالباً بمهارات تقنية عالية ودرجة من الذكاء في إخفاء آثارهم، ورغم الجهود المبذولة لمكافحة الجريمة الإلكترونية وبوجه خاص جريمة الابتزاز الإلكتروني، إلا أن السلطات المختصة تواجه عدة صعوبات في مجال الإثبات بالدليل الرقمي. وتعود هذه الصعوبات إلى جملة من العوامل، من أهمها ما يرتبط بطبيعة الدليل الرقمي ذاته من حيث قابليته للتغيير أو الإتلاف وصعوبة تتبعه، إضافة إلى معوقات أخرى تتعلق بضعف أو تعقيد آليات التعاون الدولي في مجال مكافحة هذا النوع من الجرائم العابرة للحدود.

¹ . بن سليمان، مرجع سابق، ص 63، 64.

الفرع الأول: الصعوبات المرتبطة بالدليل ذاته:

1. سهولة تدمير ومحو الدليل الرقمي الجنائي:

حرص الجاني في جرائم الابتزاز الإلكتروني على إخفاء ومحو جميع الآثار الرقمية بعد توجيه التهديد إلى المجني عليه، مما يجعل الوصول إلى الأدلة أمراً بالغ الصعوبة، وقد يكون مستحيلاً في بعض الحالات.

2. الطبيعة غير المرئية للدليل الجنائي الرقمي:

تميّز الدليل الجنائي الرقمي بطبيعة خاصة تجعله مختلفاً عن الأدلة الجنائية التقليدية، إذ يوجد ضمن بيئة افتراضية وتقنية مغايرة تماماً لمسرح الجريمة التقليدي. ويتمثل هذا الدليل في صورة نبضات أو إشارات ومجالات إلكترونية ومغناطيسية تُكوّن بيانات ومعلومات رقمية داخل الأنظمة المعلوماتية. ونظراً لكونه غير ملموس وغير مرئي بالمعنى المادي التقليدي، فإن ذلك يثير العديد من الصعوبات المرتبطة بعمليات جمعه وتحليله واستخراجه، الأمر الذي يقتضي توافر خبرة فنية وتقنية متخصصة لدى المحققين والقائمين على إجراءات التحري والتحقيق الجنائي الرقمي

3. إعاقة الوصول إلى الدليل الرقمي الجنائي:

يعتمد مرتكبو الجرائم المعلوماتية إلى استخدام أحدث الوسائل التقنية والأساليب الإلكترونية بهدف عرقلة الوصول إلى أدلة الإدانة والحيلولة دون جمعها أو ضبطها. ومن أبرز هذه الوسائل اللجوء إلى تقنيات التشفير التي تحول دون الاطلاع على البيانات والمعلومات الرقمية، إضافة إلى فرض تدابير أمنية معقدة تعيق عمليات التفتيش والفحص الفني، كاستخدام كلمات المرور وأنظمة الحماية الإلكترونية. كما يلجأ الجاني في كثير من الأحيان إلى إخفاء هويته أثناء استخدام شبكة الإنترنت، وذلك من خلال الاستعانة ببرامج وتطبيقات متخصصة تعمل على طمس هويته

الرقمية وإخفاء آثاره الإلكترونية، الأمر الذي يزيد من صعوبة تعقب الجاني والوصول إلى الدليل الجنائي الرقمي.¹

4. صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي:

تتميز جريمة الابتزاز الإلكتروني عن الجرائم التقليدية بكونها تُرتكب في بيئة إلكترونية افتراضية تقوم على البيانات والرموز الرقمية، وتفتقر في الغالب إلى المظاهر المادية التقليدية للجريمة، كاستعمال العنف الظاهر أو ترك آثار محسوسة. وهو ما يترتب عنه صعوبة الحصول على أدلة مادية تقليدية، مثل بصمات الأصابع أو آثار الدم، الأمر الذي يجعل عملية كشف الجاني وتتبع هويته أكثر تعقيداً ويطرح تحديات كبيرة أمام جهات التحري والتحقيق.

5. صعوبات المتعلقة بالخبرة:

عدّ نقص الخبرة التقنية لدى بعض القائمين على التحقيق، من رجال الضبط القضائي وأعضاء النيابة العامة، من أبرز الصعوبات التي تعترض عملية الإثبات في جرائم الابتزاز الإلكتروني. ويتجلى ذلك في ضعف الإلمام بمهارات استخدام أجهزة الحاسب الآلي وملحقاته، وكذا محدودية الخبرة في أساليب استجواب المجرم الإلكتروني والتعامل مع الأدلة الرقمية. ويؤثر هذا النقص سلباً على سير التحقيق، لا سيما فيما يتعلق بضبط الأدلة الرقمية وتأمينها والمحافظة عليها من التلف أو الضياع، كإتلاف الأقراص الصلبة أو الوسائط الممغنطة الحاملة للبيانات والمعلومات.²

ومن ثمّ، فإن مواجهة هذا النوع من الجرائم تقتضي ضرورة تأهيل وتكوين العنصر البشري المختص، من محققين ورجال ضبط قضائي، بما يضمن مواكبة التطورات التقنية المتسارعة، مع الحرص على التكوين المستمر في المجال الرقمي وكل المستجدات المرتبطة بجرائم المعلوماتية.

¹ . أوساسي فؤاد، "دور الدليل الرقمي في الإثبات الجنائي"، مذكرة ماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور-الجلفة، الجزائر، 2020، ص33،34.
² . بن سليمان، مرجع سابق، ص67.

الفرع الثاني: صعوبة التعاون الدولي:

يُعدّ اختلاف التشريعات الوطنية بشأن تجريم أفعال الابتزاز الإلكتروني من أبرز العوائق التي تعترض مكافحة هذا النوع من الجرائم، إذ تتباين القواعد القانونية من دولة إلى أخرى من حيث التجريم والعقاب والإجراءات المتبعة، الأمر الذي يزيد من صعوبة ملاحقة الجناة وتتبعهم. وعلى الرغم من الدعوات المتزايدة إلى تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، إلا أنّ هذا التعاون ما يزال يواجه عدة معوقات تحدّ من فعاليته، ومن أبرز هذه المعوقات:

1. عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية:

يرجع جانب من الصعوبات المرتبطة بمكافحة جرائم الابتزاز الإلكتروني إلى غياب اتفاق دولي موحد بشأن صور إساءة استخدام نظم المعلومات وتحديد الأفعال المكوّنة للجريمة، فضلاً عن تباين التشريعات الوطنية في تجريم هذه الأفعال من دولة إلى أخرى. ويترتب على هذا الاختلاف تعقيد إجراءات ملاحقة الجناة واعتراضها بعدة عراقيل قانونية وإجرائية، إذ قد يُعدّ الفعل مباحاً في دولة معينة وغير معاقب عليه، في حين يُصنّف في دولة أخرى ضمن الأفعال المجرّمة. كما يمتد هذا التباين إلى إجراءات التحقيق والتحري والمحاكمة، حيث تختلف الوسائل والأساليب المعتمدة من نظام قانوني إلى آخر؛ فقد تُعتبر بعض الإجراءات، كالمراقبة الإلكترونية، وسائل مشروعة وفعّالة للإثبات في دولة ما، بينما لا يُسمح باللجوء إليها في دولة أخرى أو تُعدّ عديمة الأثر القانوني، حتى وإن تم الحصول على الدليل بصورة مشروعة داخل نطاق قضائي معين

2. مشكلة الاختصاص في جريمة الابتزاز الإلكتروني:

تتمحور إشكالية مكافحة الجريمة الإلكترونية حول عجز معايير الاختصاص القضائي التقليدية عن استيعاب الطبيعة الافتراضية للسيولة المعلوماتية؛ إذ يؤدي تداخل الشبكات وعبرها للحدود إلى تشتت عناصر الجريمة بين عدة دول، مما يوجد صراعاً في القوانين الإجرائية الواجبة التطبيق لاستخراج الدليل الرقمي. وحيث إن القواعد الكلاسيكية للاختصاص المكاني القائمة على

القاعدة الثلاثية (مكان وقوع الفعل، موطن الجاني، أو مكان القبض عليه) قد صيغت لجرائم مادية محددة الحيز، فإنها تفتقر للمرونة اللازمة لمواجهة جرائم 'لا مادية' لا تعترف بالسيادة الجغرافية، مما يجعل من التعاون الدولي وتوحيد التشريعات حتمية قانونية لضمان عدم الإفلات من العقاب. وفي هذا السياق، تبنى المشرع الجزائري مقاربة حديثة بموجب القانون 04-09 وتعديلات قانون الإجراءات الجزائية (لاسيما المادة 329)، حيث تم تجاوز العقوبات المكانية عبر إقرار نظام الاختصاص الموسع، والذي تجسد فعليا من خلال الأقطاب القضائية المنشأة بموجب المرسوم التنفيذي رقم 06-348 والمعدل بالمرسوم 16-267؛ وهو ما منح لبعض وكلاء الجمهورية وقضاة التحقيق ولاية قضائية ممتدة تتلأم مع مقتضيات التحري في الجرائم المعلوماتية المعقدة.

3. الصعوبات الخاصة بالمساعدات القضائية الدولية وتدريب الكوادر:

تتجلى المعوقات المرتبطة بمنظومة التعاون الدولي وتأهيل العنصر البشري في مواجهة الإجرام المعلوماتي من خلال المحورين الآتيين:

أ- الصعوبات الخاصة بالمساعدات القضائية الدولية:

تعد الإنابة القضائية الدولية من الركائز الأساسية للتعاون الجنائي الدولي، إلا أن تفعيلها يصطدم بآلية الاعتماد على القنوات الدبلوماسية التقليدية التي تتسم بالبطء الشديد والتعقيدات الإجرائية. وهذا النسق البيروقراطي يتنافى كليا مع الطبيعة الديناميكية لجرائم الإنترنت التي تتميز بسرعة التنفيذ واختفاء الأثر الرقمي، مما يحد من فعالية الملاحقة الجنائية العابرة للحدود.

ب- الصعوبات الخاصة بالتعاون الدولي في مجال التدريب:

تتمحور هذه التحديات حول التفاوت في المستويات والقدرات الفردية للمتدربين، وهو ما يؤثر سلباً على تجانس عملية اكتساب المهارات التقنية اللازمة. فالفوارق في الخلفيات العلمية والتقنية تحول دون تحقيق استيعاب متكافئ للمتطلبات المعقدة للتكنولوجيا الرقمية، مما يشكل عائقاً أمام

إعداد كوادر قضائية وأمنية مؤهلة بشكل موحد لمواجهة التطور المتسارع في أساليب ارتكاب الجرائم الإلكترونية.¹

¹ . بن سليمان، مرجع سابق، ص 68 69.70.71 .

خلاصة الفصل:

لقد تطرقنا في هذا الفصل الإطار الإجرائي لجريمة الابتزاز الإلكتروني، حيث تم تسليط الضوء على آليات التحقيق بشقيها العام والخاص، مع تحليل أبعاد الإشكاليات الإجرائية التي تكتنف هذا النوع من الجرائم؛ بدءاً من معوقات الكشف عن الجريمة، وصولاً إلى التحديات القضائية المرتبطة بتحديد القانون واجب التطبيق والجهة القضائية المختصة. كما عرجت الدراسة على نظام الإثبات الجنائي وخصوصيته في البيئة الرقمية، بالتركيز على الدليل الرقمي بوصفه الركيزة الجوهرية للإثبات، من خلال تبيان ماهيته، وشروط صحته وقبوله قانوناً، مع رصد الصعوبات الفنية والموضوعية الكامنة في الدليل ذاته. وفي ختام الفصل، تم تناول معوقات التعاون الدولي، لاسيما إشكالية غياب نموذج دولي موحد للتجريم، وما يترتب عليه من تنازع في الاختصاص القضائي، فضلاً عن العقبات التي تواجه المساعدات القضائية المتبادلة وبرامج تدريب الكوادر البشرية المتخصصة.

خاتمة

تُعد جريمة الابتزاز الإلكتروني من أبرز الجرائم المستحدثة التي أفرزتها الثورة التقنية، وهي ما يصطلح عليه في الفقه الجنائي بـ "الجرائم الناعمة"؛ كونها تفتقر لعنصر العنف المادي الملموس. فهي في جوهرها الامتداد الرقمي لجريمة الابتزاز التقليدية، إلا أنها تختلف عنها في المسرح والوسيلة؛ فبينما تترك الجريمة التقليدية أثراً مادياً في عالم الواقع، تتدثر الجريمة الإلكترونية بعباءة العالم الافتراضي القائم على الرموز والتشفير، مما يضع جهات التحقيق أمام تحديات جسيمة في التعامل مع "الدليل الرقمي" وضبطه.

لقد أضحى هذا النوع من الإجرام هاجساً يؤرق مستخدمي التكنولوجيا الحديثة، مما دفع الدول - وأمام تسارع وتيرة التحول الرقمي - إلى تحديث منظوماتها القانونية لتواكب هذا التطور. وقد تجلّى ذلك في ضرورة إرساء نصوص تشريعية رادعة وخصوصية تعالج ثغرات الجرائم التقليدية.

وفي ختام دراستنا لموضوع "جريمة الابتزاز الإلكتروني"، نكون قد أحطنا بالإطار الموضوعي لهذه الجريمة من حيث ماهيتها وأركانها وفق ما نص عليه القانون 07-18، كما بحثنا في الجانب الإجرائي المتعلق بآليات التحقيق الجنائي وطرق الإثبات الرقمي، لنخلص في النهاية إلى جملة من النتائج والتوصيات التي نوجزها فيما يلي:

➤ لم يتفق الفقهاء على تقديم جامع لجريمة الابتزاز.

➤ جريمة الابتزاز الإلكتروني صورة من صور الجرائم الحديثة حيث تتم باستخدام وسائل وتقنيات جديدة.

➤ خلافاً للابتزاز التقليدي، يعتمد الابتزاز الإلكتروني على وسائل تقنية كالهواتف المزودة بكاميرات لانتهاك الحرمات، وذلك عبر تصوير وتسجيل ونشر تفاصيل الحياة الخاصة.

➤ تتحقق جريمة الابتزاز الإلكتروني بأن نشاط الجاني يهدف إلى تهديد الضحية، بغض النظر عن الوسيلة المستخدمة ما دام القصد هو إجبار المجني عليه على اتخاذ موقف معين أو التوقف عن فعل ما.

- جريمة الابتزاز عابرة للحدود، فقد يكون الجاني في دولة والضحية في دولة أخرى.
- سهولة ارتكابها من قبل الجاني كونها لا تتطلب جهد عضلي أو الانتقال إلى مكان الحادثة.
- جريمة الابتزاز قد تتسبب في جرائم أشد بعدها كالزنا أو القتل، وجريمة الخطف إلخ...
- الدليل الرقمي أهم أدلة الإثبات في جريمة الابتزاز الإلكتروني، إلا أن التعامل معه يحتاج إلى خبرات معينة وأجهزة متخصصة وفريق عمل متكامل الخبرة.
- ساهم غياب التوحيد التشريعي الدولي في تجريم الابتزاز الإلكتروني في خلق ملاذات آمنة لـ الجناة من العقاب، خاصة في الدول التي لم تتبنّ تشريعات نوعية لمكافحة هذا السلوك.
- على النقص من المشرع الجزائري والمصري اللذين استحدثا نصوص خاصة لمواجهة هذه الظاهرة.

المقترحات:

- ✓ ان التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية خاصة فيما يتعلق بجريمة الابتزاز الإلكتروني.
- ✓ إصدار قانون خاص يجرم الابتزاز الإلكتروني في الدول التي لا يوجد في تشريعها نص ليكون الردع بشقيه العام والخاص ذا فاعلية أكبر.
- ✓ البد من تعاون كل مؤسسات التعليم والتعليم العالي، ودور العبادة إقامة دراسات وندوات حول مخاطر هذه الجريمة الدخيلة على المجتمعات العربية والإسلامية.
- ✓ أن يعين أخصائيين نفسانيين واجتماعيين تكون مهمتهم التواصل مع كل من تعرض للابتزاز مهما كان جنس وسن الضحية.
- ✓ عقد دورات مكثفة لتدريب وتأهيل العاملين بجهات التحقيق والجهات القضائية، بكل أساليب التحقيق الحديثة، والتعامل مع الدليل الرقمي حتى لا تفلت الجرائم من بين يدي رجال التحقيق بسبب قلة الخبرة في التعامل مع الدليل الرقمي.

✓ زيادة التعاون الدولي، وذلك بوضع آلية موحدة تجرم الابتزاز الالكتروني كي لا يفلت المجرم من العقاب نتيجة تساهل بعض الاظمة وتشدد أخرى.

قائمة المصادر

والعراجع

I. قائمة المصادر

أولاً: القوانين

1. قانون العقوبات الجزائري، المادة 303 مكرر والمادة 303 مكرر 1 (المعدل والمتمم بالقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات/قانون الإجراءات الجزائية حسب السياق المذكور).
2. نظام مكافحة الجرائم المعلوماتية، المادة 31.

II. قائمة المراجع

أولاً: الكتب المتخصصة

1. أمير فرج يوسف، "الإثبات الجنائي للجريمة الإلكترونية"، الطبعة الأولى، مكتبة الوفاء القانونية، الإسكندرية، مصر، سنة 2016.
2. د. عمار عباس الحسيني، "جريمة الابتزاز الإلكتروني"، منشورات زين الحقوقية، بيروت، لبنان، (د.س.).
3. ماركوك أرسلان عبد الله كاكويس، "الدليل الرقمي وحجتيه في الإثبات الجنائي"، الطبعة الأولى، دار وليد للنشر والتوزيع والبرمجيات، القاهرة، مصر، 2022.

ثانياً: الأطروحات والمذكرات الجامعية

1. بن سلمان محمد طاهر، رسيوي رشيدة وآخرون، "جريمة الابتزاز الإلكتروني"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح - ورقلة، السنة الجامعية 2023/2024.
2. بوشعير الحسن، حداد شعيب، "جريمة الابتزاز - دراسة مقارنة"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في القانون العام، تخصص قانون الإعلام الآلي والإنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعرييج، السنة الجامعية 2022/2023.

3. جبراني نورة، لعماري سهام، "التحقيق في الجريمة الإلكترونية"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، تخصص إعلام آلي وإنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعرييج، سنة 2023/2024.
4. حداد شماء، جبلي سعيدة، "جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري"، مذكرة مكمل لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، معهد الحقوق، المركز الجامعي عبد الحفيظ بالصوف - ميله، (د.س.).
5. درابلة العمري سليم، "حجية الدليل الرقمي في الإثبات الجنائي"، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجزائر 1، سنة 2025.
6. غليلة الحسين، معاوي عبد الناصر، "الابتزاز الإلكتروني"، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 - سكيكدة، جوان 2024.
7. مرابطين علاء الدين، محمادي مراد، "خصوصية الجريمة الإلكترونية في التشريع الجزائري"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، تخصص قانون الإعلام، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي - برج بوعرييج، دفعة 2022/2023.
8. ميمونة ناصر، "الآليات القانونية لحماية الأشخاص من جريمة الابتزاز الإلكتروني"، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة غرداية، (د.س.).

ثالثا: المجالات العلمية والمنشورات الدورية

1. إسلام عزت محمد ندا، "المواجهة الجنائية والأمنية لجرائم الابتزاز الإلكتروني (دراسة مقارنة)"، مجلة البحوث الفقهية والقانونية، العدد 50، سنة 2024.
2. بن عامر ياسين، "الابتزاز الإلكتروني للأطفال في التشريع الجزائري"، مجلة دفاتر السياسة، جامعة قاصدي مرباح - ورقلة، المجلد 16، العدد 02، سنة 2024.
3. عراب مريم، "جريمة التهديد والابتزاز الإلكتروني"، مجلة الدراسات القانونية المقارنة، جامعة وهران 2 أحمد بن أحمد، المجلد 07، العدد 01.

قائمة المصادر والمراجع

4. فلاح عبد القادر، أيت عبد المالك نادية، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة - خميس مليانة، المجلد 04، العدد 02، سنة 2019.
5. وفاء محمد صقر، "جريمة الابتزاز الإلكتروني (دراسة مقارنة)"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة طنطا، المجلد 36، العدد 2، يوليو 2024.

فهرس

المحتويات

الصفحة	العنوان
	الواجهة
	الشكر والعرفان
	الاهداء
أ	مقدمة
	الفصل الأول: الإطار الموضوعي لجريمة الابتزاز الالكتروني
02	تمهيد
03	المبحث الأول: ماهية جريمة الابتزاز الالكتروني
03	المطلب الأول: مفهوم جريمة الابتزاز الالكتروني
9	المطلب الثاني: وسائل الابتزاز الالكتروني وأثاره
16	المبحث الثاني: تجريم القانوني للابتزاز الالكتروني
16	المطلب الأول: اركان جريمة الابتزاز الالكتروني
20	المطلب الثاني: عقوبة جريمة الابتزاز الالكتروني
25	خلاصة الفصل
	الفصل الثاني: الإطار الاجرائي لجريمة الابتزاز الالكتروني
27	تمهيد
28	المبحث الأول: إجراءات التحقيق في جريمة الابتزاز الإلكتروني
28	المطلب الأول: إجراءات التحقيق في جريمة الابتزاز الالكتروني
39	المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الابتزاز الإلكتروني
44	المبحث الثاني: الاثبات في جريمة الابتزاز الالكتروني
45	المطلب الأول: ماهية الدليل الجنائي الرقمي
52	المطلب الثاني: الصعوبات الأثبات في جريمة الابتزاز الإلكتروني
58	خلاصة الفصل
60	خاتمة
64	قائمة مصادر ومراجع
	فهرس المحتويات
	الملاحق
	ملخص

الملاحق

الجمهورية الجزائرية الديمقراطية الشعبية
باسم الشعب الجزائري
حكم

مجلس قضاء بسكرة
 محكمة : طولقة
 قسم الجنج

بالجلسة العلنية المنعقدة بمقر محكمة طولقة
 بتاريخ: العاشر من شهر ماي سنة المين و واحد و عشرون
 النظار في قضايا الجنج
 برئاسة السيد (ة):
 ومساعدة السيد (ة):
 وبحضور السيد (ة):
 رئيسا
 أمين ضبط
 وكيل الجمهورية

رقم الجدول:
 رقم الفهرس:
 تاريخ الحكم:

المثول الفوري

صدر الحكم الجزائي الآتي بيانه بين الأطراف التالية
 السيد وكيل الجمهورية - مدعيا باسم الحق العام.
 من جهة

النيابة ضد /

طبيعة الجرم /

جنحة انتحال اسم الغير في
 ظروف قد تؤدي لفقد حكم في
 صحيفة السوابق القضائية
 وجنحة المساس بحرمة
 الحياة الخاصة للأشخاص

1 () من مواليد: 1-ب: طولقة
 لين: لم
 الساكن:

بمساعدة الأستاذ (ة): ديدوح سماح

من جهة تلبية

ضد /

1 () من مواليد: 1-ب: 1
 لين: لزهرة و
 الساكن: بلدية ليشانة
 بمساعدة الأستاذ (ة)

من جهة اخرى

****بيان وقائع الدعوى****

حيث أن المتهم
 متابع من طرف نيابة محكمة طولقة لارتكابه جنحتي انتحال اسم
 الغير والمساس بحرمة الحياة الخاصة للأشخاص الفعلان المنوه والمعاقب عليهما بنص المادتين
 249 و 303 مكرر من قانون العقوبات وذلك بتاريخ 2021/04/11 ومنذ زمن لم يمض عليه
 أمد التقادم بعد بالمكان المسمى طولقة بدائرة اختصاص محكمة طولقة مجلس قضاء بسكرة.
 حيث أن المتهم أحيل على محكمة الجنج وفقا لإجراءات المثول الفوري المشار إليها بالمادتين
 333 و 339 مكرر من قانون الإجراءات الجزائية للإجابة عن التهمة المنسوبة إليه.
 حيث يستخلص من ملف القضية أنه بتاريخ 2021/04/12 تقدم المسمر
 بشكوى لأمن دائرة طولقة ضد المسمى
 صور فوتوغرافية للعائلة والخاصة بشقيقته المسماة
 في أجل قيام هذا الأخير بهتيد سميحه بشكر
 وذكر الشاكي أنه شقيق



الرجعة طبق الأصل

صفحة 1 من 3

المسند. التي على علاقة بالمشتكى منه عبر حسابه الفايسبوكي¹ .
أن المعنى استغل حسابه الفايسبوكي وصورته الشخصية في التواصل مع سماعين وبسماع
المشتكى منه صرح أنه قام بإرسال صور للعائلة وذلك باسم حساب الفايسبوك أمين مينو كما أنه
أعاد فتح حساب الفايسبوكي الخاص بالشاكية بعد عملية مسح من طرفها بمعوية زوجها السابق
وأنه يوجد بهاتفه 128 صورة خاصة بالمسماة وفاء ومنها صور في وضعيات

مخلّة بالحياة .
حيث أن المحكمة نبهت المتهم أن له الحق في مهلة لتحضير دفاعه وفقا للمادة 339 مكرر 05
وارتأت المحكمة تأجيل القضية بطلب من دفاع الضحية وأمرت المحكمة بعد سماع لطلبات ممثل
النيابة والمتهم بوضعه الحبس المؤقت.

حيث أن
حضر الجلسة واعترف باستخدام حساب فاييسبوكي باسم أمين مينو
وذكر أنه قام بإرسال رسالة نصية للمسمى صابر طلب منه خلاله تنازل شقيقته عن الشكوى
وأضاف أنه استعمل صورة الضحية حتى يتمكن التواصل مع أقارب الضحية وخاصة ابنة
شقيقته.

حيث أن الضحية ح .
لم يحضر الجلسة للإدلاء بأقواله .
حيث أن دفاع الض
التمست تعويض قدره خمسمائة ألف دينار جزائري لكل
طرف مدني.

حيث أن ممثل الحق العام التمس في إفادته إدانة المتهم بسنتين حبس نافذ ومائة ألف دينار غرامة
نافذة.

حيث أن دفاع المتهم الأستاذة .
التمسوا البراءة لموكلهم لعدم قيام
الجريمة.

حيث أن الكلمة الأخيرة أعطيت للمتهم طبقا للنص المادة 353 من قانون الإجراءات الجزائية
والتمس البراءة.

****وعليه فإن المحكمة****

بعد الإطلاع على المادة 328 وما بعدها من قانون الإجراءات الجزائية.
بعد الاطلاع على المادتين 249 و303 مكرر من قانون العقوبات.
بعد النظر قانونا.

في الدعوى العمومية

حيث يستفاد من أوراق الملف وما دار بالجلسة أن المتهم قام بقيامه بإرسال صور تتضمن
مواضع خادشة للحياة تتعلق بشقيقة المجني عليه ووضعها تحت تصرف الغير وذلك من خلال
الحساب الفاييسبوكي الخاص بالضحية أمين مينو وذلك ثابت من خلال تصريحات المتهم أمام
الضبطية القضائية ولدى سماعه عند المثل الفوري من كون المعنى قام بإرسال الصور لشقيقها
فضلا على قيام المتهم باستغلال حساب الضحية وصورته الشخصية حتى يتمكن له بتيان أفعاله
المجرمة الماسة بالأشخاص وهو ما قد يؤدي إلى متابعة الضحية أو الإضرار به.
حيث أن الوقائع تنطبق على النموذج القانوني لجنتي انتحال اسم الغير والمساس بحرمة الحياة
الخاصة للأشخاص الفعلان المنوه والمعاقب عليهما بنص المادتين 249 و303 مكرر من قانون
العقوبات وعليه يتعين إدانة المتهم ومعاقبته طبقا للقانون.

حيث أن المحكمة ارتأت إسعاف المتهم بموجبات الرأفة المقررة بنص المادة 592 من قانون
الإجراءات الجزائية وتطبيق عقوبة موقوفة التنفيذ بالنسبة للعقوبة السالبة للحرية لكونه لم يسبق
الحكم عليه نهائيا بجريمة من جرائم القانون العام وقد تم إحاطته علما بأنه في حالة صدور حكم
جديد بالإدانة فإن العقوبة الأولى ستند دون أن يكون من الممكن أن تلتبس بالعقوبة الثانية.

في الدعوى المدنية

حيث أن من المقرر قانونا أن الحق في الدعوى المدنية يتعلق بالمطالبة بالتعويض عن الضرر
الناجم عن جنحة بكل من أصابهم شخصا ضرر مباشر تسبب عن الجريمة.
حيث أن دفاع الضحية قد التمس تمكنه من تعويض جراء الضرر اللاحق به وعليه الاستجابة

لطلبه بعد خفضه للحد المعقول.
حيث أن المصاريف القضائية على عاتق المحكوم عليه وفقا للمادة 367 من قانون الإجراءات الجزائية.
حيث أن الإكراه البدني يحدد بأقصاه.

****ولهذه الأسباب****

حكمت المحكمة حال فصلها في قضايا الجнг علنيا ابتدائيا حضوريا وجاهيا :
في الدعوى العمومية: إدانة المدّ
قيد حكم في صحيفة السوابق القضائية و المساس بحرمة الحياة الخاصة للأشخاص الفعلان المنوه
و المعاقب عليه بنص المادتين 249 و 303 مكرر من قانون العقوبات و معاقبته بسنة (01)
حبس موقوفة التنفيذ و عشرون ألف دينار جزائري (20.000 دج) غرامة نافذة.
في الدعوى المدنية: إلزام المدان من تمكين الطرف المدعى
ن من تعويض قدره
خمسون ألف دينار جزائري (50.000 دج) ، والمصاريف على الفضائيه على عاتق المحكوم
عليه والمقدرة بـ 800 دينار جزائري ، مع تحديد مدة الإكراه البدني بحددها الأقصى.
بذا صدر هذا الحكم و أفصح به جهارا بالجلسة العلنية المنعقدة بالتاريخ و المكان المذكورين
أعلاه، و إثباتا لصحته أمضي أصله من طرفنا نحن الرئيس و أمين الضبط.

أمين الضبط

الرئيس (ة)



ملخص المذكرة :

تناقش هذه المذكرة جريمة الابتزاز الإلكتروني من زاويتين؛ حيث يتناول الفصل الأول (الإطار الموضوعي) ماهية وتجريم هذه الجريمة باعتبارها سلوكاً مستحدثاً يعتمد على الوسائل التقنية الحديثة لانتهاك حرمة الحياة الخاصة وتهديد الضحايا لإجبارهم على فعل أو امتناع، مبرزةً خصائصها كجريمة عابرة للحدود وسهلة الارتكاب، ومحدرةً من مخاطر الفراغ التشريعي الدولي الذي يخلق ملاذات آمنة للجناة. بينما يستعرض الفصل الثاني (الإطار الإجرائي) الجانب التطبيقي للمواجهة، حيث يركز المبحث الأول منه على إجراءات التحقيق والصعوبات التقنية والقانونية والاجتماعية التي تواجه المحققين بسبب التشفير وتنازع الاختصاص القضائي، في حين يسلط المبحث الثاني الضوء على الإثبات الجنائي ومحوية الدليل الرقمي الذي، رغم أهميته القصوى، يفرض تحديات جمة في حفظه والتعامل معه، مما يتطلب استعانةً بأجهزة متخصصة وفرق عمل متكاملة الخبرة لضمان سلامته وقبوله قضائياً.

الكلمات المفتاحية:

الابتزاز الإلكتروني، الجريمة السيبرانية، الدليل الرقمي، التحقيق الجنائي الرقمي، اختراق الحياة الخاصة، الجرائم العابرة للحدود، التنازع القضائي.

Study Summary:

This thesis examines the crime of electronic extortion from two main perspectives. Chapter One (The Substantive Framework) defines and criminalizes this modern phenomenon, exploring how it leverages digital technologies to violate personal privacy and coerce victims into specific actions or omissions. It highlights the crime's distinct characteristics—such as its transboundary nature and ease of execution—while warning against international legislative gaps that create safe havens for perpetrators. Meanwhile, Chapter Two (The Procedural Framework) addresses practical enforcement. Its First Section details criminal investigation procedures along with the technical, legal, and social hurdles investigators face due to data encryption and jurisdictional conflicts. The Second Section emphasizes criminal evidence, focusing on the pivotal role of digital forensics. Despite its critical importance, digital evidence poses severe challenges regarding preservation and authenticity, requiring specialized tools and highly skilled expert teams to ensure its admissibility in court.

Keywords:

Electronic Extortion, Cybercrime, Digital Evidence, Digital Forensics Investigation, Privacy Violation, Transboundary Crimes, Jurisdictional Conflict

