

مذكرة

لنيل شهادة الماستر

تحت عنوان

آليات مكافحة الإبتزاز الإلكتروني في التشريع

الشعبة

حقوق

التخصص

علم الجريمة

تحت إشراف الأستاذ (ة) :

– د. محفوظ أكرام

من إعداد الطالب (ة) :

– مكشتي مسعودة

اللجنة المناقشة:

المؤسسة	الصفة	الرتبة	لقب واسم الأستاذ
جامعة وهران 1 أحمد بن بلة	رئيسا	أستاذ مساعد	د. بلوط سماح
جامعة وهران 1 أحمد بن بلة	مشرفا مقررًا	أستاذ محاضر "ب"	د. محفوظ كرام
جامعة وهران 1 أحمد بن بلة	عضوا مناقشا	أستاذ مساعد	د. حميدي أميمة خديجة

السنة الجامعية : 2026/2025م

قال الله تعالى:

"وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا
فَقَدْ اخْتَمَلُوا بُهْتَانًا وَإِثْمًا مُّبِينًا" [الأحزاب: 58]

شكر وعرفان

الحمد لله وشكرًا له على فضله، وعلى توفيقه لنا في إنجاز هذا العمل المتواضع. قبل كل أحد، الشكر للواحد الأحد الفرد الصمد، الذي أمدنا بالقوة والعون والسداد لإنجاز هذا العمل، وندعوه عز وجل أن يجعله خالصًا لوجهه الكريم.

ثم أتوجه بجزيل الشكر والتقدير إلى الأستاذة المشرفة الدكتورة محفوظ إكرام ، لما قدّمته لنا من توجيه كريم، وملاحظات بناءة، ودعم متواصل طيلة فترة هذا البحث. فقد كان لملاحظاته وتوجيهاته النيرة الأثر الكبير في إخراج هذا العمل في حلتّه النهائية. ولا يفوتنا أن نشكر كل الأساتذة الأفاضل الذين وضعوا بصمتهم في مسارنا الجامعي لإيصالنا الى ما نحن إليه.

إهداء

وَأَخِرُ دَعْوَاهُمْ أَنْ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ.

الحمد لله الذي ما انتهى درب، ولا ختم جهد، ولا تم سعي إلا بفضلِهِ. ما سلكنَا البدايات إلا بتيسيره وما بلغنا النهايات إلا بتوفيقه و ما حققنا الغايات إلا بفضلِهِ فالحمد لله الذي وفقني

لتتمين هذه الخطوة في مسيرتي الدراسية

إلى من قرن الله الإحسان إليهما بطاعته

إلى الوالدين الكريمين

أسأل الله دوام الصحة والعافية لهما

إلى أخواتي وأخوتي الأعزاء شاكراً ومقدرة لهم تشجيعهم و مساندتهم

إلى كل الصديقات والزملاء

إلى هؤلاء جميعاً أهدي ثمرة هذا العمل..

قائمة المختصرات

الصفحة	ص
الطبعة	ط
العدد	ع
قانون العقوبات	ق ع

مقدمة

مقدمة:

شهد العالم خلال العقود الأخيرة انفجاراً معرفياً وتكنولوجياً غير مسبوق، انعكس بشكل واضح على الانتشار الواسع للإنترنت ومنصات التواصل الاجتماعي التي أصبحت تستقطب جميع الشرائح العمرية دون استثناء. وقد أتاح هذا التطور مساحات رحبة للتفاعل الإنساني، حتى غدا العالم بمثابة فضاء واحد مفتوح يتشارك فيه الأفراد الحوار والتبادل الثقافي بشكل آني، متجاوزين بذلك القيود التقليدية للزمان والمكان. غير أن هذا الانفتاح الرقمي يفرض في المقابل ضرورة الانتباه إلى التحديات المرتبطة به، لا سيما ما يتعلق بالأمن الرقمي وحماية الخصوصية. وكما هو شأن أي تقدم تكنولوجي، فإن هذه الطفرة لم تكن بمنأى عن المخاطر. إذ أسهمت البيئة التقنية المتقدمة في بروز أنماط مستحدثة من الجريمة، يأتي في مقدمتها الجرائم الإلكترونية بوجه عام، وجريمة الابتزاز الإلكتروني على وجه الخصوص، التي أصبحت تمثل تهديداً متنامياً لأمن الأفراد على المستوى العالمي. وتعد جريمة الابتزاز الإلكتروني من الجرائم المستحدثة نسبياً، حيث تقوم بها فئات معينة واستغلال تقنيات متطورة واستخدامها لتنفيذ مخططاتهم الدنيئة ضد فئات أخرى، يجعلون منها فرصة للاستغلال من خلال التهديد أو نشر صور ومقاطع فيديو ينده لها الجبين، أو باختراق الحسابات الشخصية أو استخدام برامج التجسس ومراقبة الضحايا والتواصل معهم بطرق خفية وسرية.

ففي ظل الانفجار المعرفي والتكنولوجي الذي شهده العالم من خلال العقود الأخيرة شهد تطورات كبيرة وسريعة في استخدام الأنترنت ووسائل التواصل الاجتماعي الذي توافدت عليها جميع الفئات العمرية، هذا التطور فتح أبواب واسعة وآفاقاً للتفاعل والتواصل بين الأفراد من جميع أنحاء العالم حتى أصبح العالم كأنه ساحة واحدة يتقاسم فيها الأفراد الحديث والتبادل الثقافي بشكل مستمر دون أن تكون هناك حدوداً وقيود يفرضها الزمان والمكان في ظل الانفتاح

الواسع على العالم الرقمي أصبح من الضروري التفطن للتحديات التي قد يترتب عليها وبالخصوص فيما يتعلق بأمان الرقمي والخصوصية.

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

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

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

ومن هنا جاءت هذه الدراسة كمساهمة علمية تهدف إلى تحليل الظاهرة قانونياً وتوعية

المجتمع

فهم جريمة الابتزاز الإلكتروني والوقوف على أسباب تصاعدها.

التعرف على خطورة هذه الجريمة وتأثيراتها على الأفراد والمجتمعات.

تحليل طرق ارتكابها والأساليب المستخدمة من طرف الجناة.

التعرف على كيفية اكتشاف الجريمة والتحقيق فيها من قبل الجهات المختصة.

تقييم مدى كفاية وفعالية النصوص القانونية الموضوعية والإجرائية الحالية في التصدي لجريمة الابتزاز الإلكتروني.

تنبثق أهمية هذه الدراسة من تناولها لظاهرة حديثة تُعد من أبرز التحديات التي أفرزها العصر الرقمي، والمتمثلة في جريمة الابتزاز الإلكتروني. فقد اتسع نطاق هذه الجريمة بشكل ملحوظ، وارتبطت ارتباطاً وثيقاً بتطورات الشبكة المعلوماتية وانتشار منصات التواصل الاجتماعي. وتتميز هذه الجريمة بخصائص تميزها عن الجرائم التقليدية، سواء من حيث الوسائل المستخدمة أو طبيعة الأفعال المرتكبة، إذ تعتمد على أدوات تقنية متقدمة وتستغل الفضاء السيبراني عابر الحدود. وقد أظهرت التقارير ارتفاعاً عالمياً في حوادث الابتزاز الإلكتروني، مما يستدعي تطوير آليات للتعامل معها تتناسب مع طبيعتها الخاصة، سواء على المستوى القانوني أو التقني.

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

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

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

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

وبناءً على الحاجة الملحة لوضع هذا الموضوع موضع دراسة وتحليل، ينبني ذلك على الإجابة على إشكالية الدراسة المتمثلة في: إلى أي حد استجابت النصوص القانونية في الجزائر للتحديات الناشئة عن جريمة الابتزاز المعلوماتي؟

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

– ما المقصود بجريمة الابتزاز الإلكتروني؟ وما هي أركانها ومدى خطورتها؟

– ما هي الإجراءات المتعلقة بالتحقيق في جريمة الابتزاز الإلكتروني؟

– ما أهم القوانين والمرسسات لمكافحة والحد من جريمة الابتزاز الإلكتروني؟

ولإحاطة شاملة بالإشكالية المطروحة والإجابة عن تساؤلاتها الفرعية، تم الاعتماد على خطة بحثية متوازنة قُسمت إلى فصلين رئيسيين؛ خُصص الفصل الأول لدراسة "الإطار المفاهيمي لجريمة الابتزاز الإلكتروني"، وفيه تم تناول الظاهرة عبر مبحثين؛ استعرض المبحث الأول ماهية الابتزاز الإلكتروني من خلال تحديد مفهومه بدقة ورصد خطورته الإجرامية وصوره، بينما ركّز المبحث الثاني على صور هذا الابتزاز ووسائل ارتكابه، مع تبيان أركانه القانونية في التشريع الجزائري، لينتهي هذا الفصل بخلاصة جامعة لأبرز ما ورد فيه.

أما الفصل الثاني، فقد أُفرد لمعالجة "إجراءات وآليات مكافحة جريمة الابتزاز الإلكتروني في التشريع الجزائري"، وجاء بدوره مقسماً إلى مبحثين؛ خُصص المبحث الأول للبحث في التكليف القانوني لهذه الجريمة ومدى استيعاب النصوص لها، بالتطبيق على قانون العقوبات والقانون رقم 04-09 المتعلق بجرائم تكنولوجيات الإعلام والاتصال. وفي المبحث الثاني، تم تسليط

الضوء على الجانب الإجرائي والمؤسساتي من خلال تتبع آليات البحث والتحري في هذه الجرائم، ورصد دور الهيئات والمؤسسات الوطنية المنوط بها الوقاية من الابتزاز الإلكتروني ومكافحته، ليُختتم الفصل بخلاصة توجيهية تمهد للنتائج والتوصيات العامة للدراسة.».

على الرغم من الأهمية البالغة والمخرجات المتوخاة من هذه الدراسة، إلا أن إنجازها واجه جملة من الصعوبات الموضوعية والمنهجية التي فرضتها طبيعة الظاهرة المدروسة، ويمكن حصر أبرزها في التطور التقني المتسارع مقابل جمود النص القانوني تمثلت إحدى أبرز العقبات في شح الكتب المتخصصة بالجريمة الإلكترونية في الجزائر على الرغم من وجود العديد من المقالات والمذكرات.

بالنظر إلى الطبيعة المزدوجة للموضوع (تقنية وقانونية)، تطلب البحث الاطلاع على مراجع معلوماتية وتقنية متخصصة إلى جانب المراجع القانونية، لضمان الإحاطة الكاملة بأركان الجريمة ووسائل ارتكابها وآليات مكافحتها.

الفصل الأول:

الاطار المفاهيمي لجريمة الإبتزاز

تعتبر جريمة الابتزاز الإلكتروني من الجرائم المستحدثة ، ويطلق عليها في علم الجريمة الجرائم الناعمة، التي تخلو من العنف وهي احدى صور الجريمة الإلكترونية.

فالابتزاز الإلكتروني هو الوجه الآخر لجريمة الإبتزاز التقليدية التي ترتكب في عالم مادي، وفي مسرح جريمة تقليدي حيث يترك الجاني آثار كالبصمات أو الدماء، لكن الابتزاز الإلكتروني فيتم في عالم افتراضي مليء بالرموز والشفرات تحدد نقاط الاتصال والتكنولوجيا الرقمية، حيث تعتمد هذه الجريمة أساسا على وسائل التكنولوجيا الحديثة.

وقد ارتأينا الى تقسم الفصل الى مبحثين تناولنا في المبحث الأول ماهية جريمة الابتزاز الإلكتروني وفي المبحث الثاني صور و اركان للابتزاز الإلكتروني.

المبحث الأول: ما هية الابتزاز الإلكتروني

تعد جريمة الابتزاز الإلكتروني تحدياً تشريعياً معاصراً يتطلب تدخلاً قانونياً حازماً لمواكبة قصور القواعد التقليدية عن استيعاب الطبيعة الافتراضية للفعل الجرمي؛ إذ يفرض هذا النمط المستحدث من الجرائم ضرورة إعادة تكييف النصوص الجزائية وتحديثها لضمان شمولية الحماية القانونية للحق في حرمة الحياة الخاصة وصون أمن المعلومات. ويستدعي ذلك دراسة المرتكزات التشريعية التي تجرم أفعال التهديد الممزوجة بالطلب عبر الوسائط الرقمية، مع تحليل الأركان المادية والمعنوية للجريمة، والوقوف على مدى فاعلية العقوبات المقررة إجرائياً لردع الجناة في ظل تعدد مسألة الإثبات الجنائي الرقمي، وهو ما سيتم تفصيله من خلال استقصاء النصوص القانونية والحلول الإجرائية التي تبناها المشرع لمواجهة هذه الظاهرة.

المطلب الأول: مفهوم الابتزاز الإلكتروني

سننطلق في هذا المطلب لتعريف جريمة الابتزاز الإلكتروني انطلاقاً من التعريف اللغوي، مروراً بالتعريف الاصطلاحي والفقهية وتمييزه عن غيره من المفاهيم المشابهة على النحو التالي:

الفرع الأول: تعريف الابتزاز الإلكتروني

لابتزاز الإلكتروني جريمة معلوماتية وأخلاقية في آنٍ واحد قوامها استغلال الفضاء الرقمي وهي جريمة تمس في جوهرها الحرية الشخصية والكرامة الإنسانية والحياة الخاصة، وتُجرّمها

أولاً: التعريف اللغوي

ورد مصطلح الابتزاز في معاجم اللغة وتناوله أصحاب المعاجم ومن أهم ما ورد في:

اللغوين مصدر: ابتز

معناه من غلب سلب ويژه بزه بزا عليه وعصيه، وبز الشيء انتزعه، ومنه ابتز جارية: إذا جردها من ثيابها والبز أخذ الشيء بحفاء وقهر¹

يعرف الابتزاز لغة بأنه أخذ الشيء بحفاء وقهر.

ابتزّه سلبه، ورمى به، ولم يرده.

¹ محمد بن مكرم بن منظور، المان العرب دار الصادرة بريت 2010، مع 5 من 112

وهو من الفعل بز يبره بزاً، وجاء في المثل من عز بز " ومعناه " من غلب سلب " ويقال ابتزت الشيء أي انتزعت، ويزه يبره بمعنى غلبه.¹

بالنظر إلى الابتزاز من الناحية اللغوية، يتبين أن الكلمة تحمل جذورا دلالية غنية ومتشعبة تساعد على فهم عمق هذا المفهوم ومظاهره المختلفة فكلمة ابتزاز مأخوذة من الجذر الثلاثي ب ز ز)، وهو جذر يدل في أصله على السلب والانفصال والانتزاع ويقال في اللغة: بر فلان فلانا متاعه أي أخذه منه عنوة أو عليه، ومنه جاء الفعل ابتز" بصيغة المزيد للدلالة على المبالغة في الفعل أو الاستمرار فيه وعليه فإن الابتزاز لا يقتصر على المال فحسب. بل يشمل كل ما يمكن انتزاعه قسراً سواء كان مادياً كالأموال أو معنوياً كالمعلومات أو الأفعال. أو السكوت على أمر معين.²

ثانياً: التعريف الاصطلاحي.

1- التعريف الاصطلاحي للابتزاز

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

هو نمط سلوكي آخر للفساد الإداري يجرى مع بعض الموظفين من العاملين في الأجهزة المسؤولة عن حماية ونشر الأمن والطمأنينة أو مراقبة النشاطات الاقتصادية أو غيرها من الأجهزة التحقيقية والتأديبية والعقابية كالسجون والمحاكم أو من قبل اللجان الإنضباطية ونقاط التفتيش والسيطرة والمرور والتفتيش الصحي والرقابة على الأسفار ودوائر البلدية وموظفي الجمارك العاملين بالمطارات أو نقاط الحدود فغالباً ما يلجأ بعض هؤلاء إلى ابتزاز المراجعين والمتهمين ممن تشوب قضاياهم أو تنقلاتهم شائبة عن طريق

¹ مروة صالح الدين محمد، الدليل الالكتروني ومدى حجتيه في الاثبات الجنائي، الطبعة الاولى، المكتب العربي للمعارف، دار البحوث القانونية، القاهرة، مصر، سنة 2021، ص 33

² مروة صالح الدين محمد، مرجع سابق، ص 33

³ مصطفى محمد الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، ط1، مركز الكتاب الأكاديمي عمان 2020

تخويفهم أو تهديدهم الإرغامهم على دفع المبالغ أو تقديم الأشياء العينة أو يعرضونهم للإيذاء الجسدي أو التعذيب النفسي أو التوقيف أو المراقبة أو فضحهم عبر وسائل الإعلام والصاق التهم بهم والإساءة لسمعتهم.

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

ويمكن تعريف الابتزاز الإلكتروني فقهيّاً بأنه: كل تهديد يصدر من شخص تجاه غيره، باستخدام وسائل إلكترونية، من أجل حمله على القيام بفعل أو الامتناع عنه، بغير حق، مع استغلال معلومات أو صور أو بيانات خاصة تم الحصول عليها بوسيلة مشروعة أو غير مشروعة،²

وعرفه آخرون " الابتزاز هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص المهدد إن لم يقدّم الشخص بالاستجابة إلى بعض الطلبات"³

2-تعريف الابتزاز الالكتروني

جريمة التهديد والابتزاز الإلكتروني هي إحدى صور الجرائم الإلكترونية (Cyber-crimes) وهي تتكون من مقطعين هما الجريمة (Crime)، والمقطع الآخر (Cyber) وهي السيبرانية، ويستخدم مصطلح الإلكتروني لوصف فكرة أن الجريمة تتم من خلال التقنية الحديثة، أما الجريمة فهي تلك الأفعال المخالفة للقانون، وقد اصطلح على تعريف الجرائم الإلكترونية بأنها : " المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي

¹ محسن عباس حميد، جريمة الابتزاز الإلكتروني مجلة القانون للدراسات والبحوث القانونية الاصدار 22، مجلد 23، جامعة دي قار، العراق، 2021، ص601.

² حسني عبد الكريمي يونس، خليل يوسف جندي، الابتزاز الالكتروني والجرائم الالكترونية المفهوم و الاسباب، الطبعة الاولى، دار الكفاءة المعرفة، عمان، الاردن، سنة 2021، ص40.

³ حورية المتوكل، جريمة الابتزاز الإلكتروني، المجلة الإلكترونية للأبحاث القانونية ع (11) 2023، ص 5

مباشر أو غير مباشر باستخدام شبكات الاتصال مثل الانترنت (غرف الدردشة، البريد الإلكتروني، والهاتف النقال، والحاسب الآلي".¹

وعرف بعضهم جريمة الابتزاز الإلكتروني على أنها الحصول على وثائق وصور ومعلومات عن الضحية من خلال الوسائل الإلكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عنه عن طريق استخدام الوسائل الإلكترونية لتحقيق أهداف يسعى لتحقيقها المبتز".

أما جريمة الابتزاز الإلكتروني فقد عرفها بعضهم على أنها محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعي أو اعتباري بالإكراه وبالتهديد بفضح سر وقع عليه الابتزاز أو هي استغلال القوة مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتاً أو دائماً.

وقد عرف جانب من الفقه الابتزاز التقليدي بأنه " الضغط الذي يباشره شخص على إرادة شخص آخر الحمله على ارتكاب جريمة معينة.

وقال جانب آخر من الفقه بأن الابتزاز هو : " القيام بتهديد شخص بفضح أمره ما لم يستجب المهتد إلى تنفيذ طلبات الجاني، وغالباً ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف، أو تتعلق بحرمة الحياة الخاصة للشخص المهتد الذي يتم ابتزازه

كما تم تعريف الابتزاز بأنه ما يمارسه المجرم المبتز من تهديد وسلوك للمجني عليه بعد حصوله على معلومات تخص المجني عليه كالتسجيلات الصوتية، أو الصور الشخصية بهدف تحقيق رغباته التي يسعى إليها سواء أكانت مادية أو معنوية².

3-التعريف التشريعي للابتزاز الإلكتروني

عادة المشرع لا يضع تعريفات و إنما أحكاماً تحدد السلوك المجرم فالتعريف متروك للفقه، لكن قد يتبنى المشرع تعريفاً من التعريفات لفض اللبس وتبيان المراد بالسلوك الإجرامي فقد نظم المشرع الفرنسي الابتزاز في المواد 312-1 إلى 312-3 ووضع تعريفاً للجريمة في المادة 312 1 بالقول:

¹ عراب مريم جريمة التهديد والابتزاز الإلكتروني مجلة الدراسات القانونية المقارنة المجلد 07 العدد 01 (2021)، ص 1207

² بن سليمان محمد الطاهر رسيوي رشيدة دراجي عزالدين ، جريمة الابتزاز الإلكتروني مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر جامعة قاصدي مرباح – ورقلة، 2024/2023، ص 18

هو كل فعل يتم عن طريق العنف أو التهديد بالعنف أو الإكراه من أجل الحصول على توقيع أو تعهد أو تنازل لإفشاء سر أو تسليم أموال أو ممتلكات

لم يتطرق المشرع الجزائي لجريمة الابتزاز وإنما تناوله من خلال النصوص العامة لجريمة التهديد وميز المشرع الجزائي بين نوعين من التهديد

-التهديد المجرد ويقتصر فيه الجاني بإلقاء الرعب والخوف في نفس الضحية ويعاقب عليه بالمادة

285 ق ع

-التهديد المصحوب بطلب أو تكليف بأمر أو الامتناع عن فعل، وهو أشد خطورة من التهديد المجرد وهو ما يدخل في مفهوم الابتزاز فهو يدر نفعاً مادياً للمبتز، يعاقب عليه بالمواد 284-286-371 ق ع¹

وما ذكرته المواد 284 و286 و371 ق ع ج ، ولو أنه كان من الأفضل ذكرها في نصوص قانونية واضحة تأخذ بعين الاعتبار المستجدات التكنولوجية التي أصبحت جزء منها، وأيضاً نظراً لانتشارها وخطورتها على اعتبار أن هذا النوع من المواد المسيئة أصبحت تنتج ثم تروج عبر الوسائط الرقمية، أو تنتج بشكل مباشر أمام جمهور يشاهدها، حيث يتم استغلال قوة الهوية المجهولة للجناة للإساءة للأشخاص، مثل تظاهر المتصيد بأنه صديق حتى يكتسب ثقة الشخص ومن ثم يطلب منه رقم هاتفه بغرض التواصل معه في العالم الحقيقي، لاستغلاله فعلها أو الاكتفاء بالتسجيل أو التصوير أو الدردشة ذات الطابع الإباحي ومن ثم ابتزازه فإذا رفض قام بالتشهير به ومن جهة أخرى فإن جعل المعلومات الشخصية متاحة للعموم، يشكل خطورة على الحياة الخاصة نظراً للاستعمال المستشري لها خصوصاً على الجيل الجديد الذين أصبح يبالغ في نشر أدق خصوصياته على صفحاته الخاصة².

وإجمالاً يمكن تعريف الابتزاز الإلكتروني بأنه كل فعل غير مشروع يستهدف منفعة غير مشروعة بأي صورة من الصور والوسائل التي يعتمد عليها الجاني، وهذا يفيد أن الجاني يطلب من الشخص المبتز دفع مبالغ مالية مقابل عدم نشر صور أو محادثات صوتية أو مرئية أو رسائل كتابية

¹ ينظر: القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات المؤرخ في 06/06/1966 ، جريدة الرسمية عدد 71 المؤرخ في 10/11/2004.

² فاطمة العرفي ، حجة الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون، المجلد 8، عدد خاص، 02 ، 2022، ص 496

على الشبكة العنكبوتية كما قد يطلب الجاني من الضحية إذا كانت فتاة ممارسة الفاحشة معه أو مع غيره كي لا يرسل كل ما يخصها إلى أقاربها أو التشهير بها على وسائل التواصل الاجتماعي، كم يمكن أن يطلب من الضحية القيام ببعض الأعمال الغير قانونية رغماً عن إرادته.¹

كما عرف فقهاء القانون الجنائي التهديد بأنه : " كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخرشة للشرف، وقد يحمله التهديد تحت تأثير ذلك الخوف إلى استجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب"، وهناك من عرفه بأنه: " تخويف المجني عليه وإلقاء حالة الرعب في نفسه وإزعاجه من ضرر معين يراد إيقاعه به". وهو " ترويع المجني عليه وإلقاء الرعب في قلبه يتوعده بإنزال شر عليه". واستنادا لكل هذه التعاريف نستخلص بأن التهديد من الجرائم التي من شأنها أن تحدث أثرا خطيرا في نفس المجني عليه، تتمثل في إلحاق حالة الرعب والقلق لما سيلحق به أو بشخص له علاقة به أو بماله أو إفشاء أمور ماسة بحياته الشخصية أو بشرفه.²

الفرع الثاني: تمييز الابتزاز الإلكتروني عن الجرائم المشابهة له

شكل الفصل بين مفهوم الابتزاز الإلكتروني والمفاهيم المشابهة له عبئاً استلزم دقة عالية في التحديد والتعريف لعدم الوقوع في خلط المفاهيم.

أولاً - التهديد التقليدي و التهديد الإلكتروني

يتميز الابتزاز الإلكتروني عن جريمة الابتزاز التقليدية على الرغم من أن كلا منهما عبارة عن تهديد بإيقاع أذى ويقترن بطلب منفعة مالية أو معنوية أو جنسية، ويظهر ذلك من خلال:

- 1 - من حيث الضرر الابتزاز الإلكتروني واسع ضرره وممتد تأثيره حيث تصل الفضيحة لآلاف الأشخاص بخلاف الابتزاز التقليدي الذي يتميز بأنه محدود الأثر والنطاق؛
- 2 - يسهل في الابتزاز الإلكتروني محو الفعل وآثاره بخلاف الابتزاز التقليدي الأمر الذي يجعل من الصعب اكتشاف الجريمة وإثباتها ومعرفة فاعلها؛
- 3- الابتزاز الإلكتروني من الجرائم الناعمة التي يجني منها الفاعل مبالغ مالية كبيرة لاسيما إذا كان الضحايا شركات كبيرة أو أشخاصا أثرياء بخلاف الابتزاز التقليدي.¹

¹ حورية المتوكل، جريمة الابتزاز الإلكتروني، المجلة الإلكترونية للأبحاث القانونية ع (11) 2023، ص 5

² عراب مريم ، مرجع سابق، ص 1207.

ثانيا - جريمة الابتزاز وجرائم المساس بالحياة الخاصة

تشترك جريمة المساس بالحياة الخاصة مع جريمة الابتزاز في أن الجاني يحوز معلومات عن الضحية تمس الحياة الخاصة متمثلة في صور أو تسجيلات صوتية أو فيديو تتعلق بخصوصية الضحية تكون محلا للابتزاز وكذلك تمس بخصوصية الضحية، وتختلف جريمة الابتزاز عن الجرائم الماسة بالحياة الخاصة في أن الجاني قد يحوز أي معلومات تخص الضحية في شكل وقائع أو أحداث أو مستندات من شأنها في حالة إفشاءها المساس بسمعة الضحية، فمحل الابتزاز أوسع في جريمة الابتزاز مقارنة بالمساس بالحياة الخاصة والذي هو المعلومات أو وقائع أو محررات وغيرها قد تكون متعلقة بالحياة الخاصة وقد تكون ذات طابع مهني أو سياسي أو غيرها من المجالات²

المطلب الثاني: الخطورة الاجرامية للابتزاز الالكتروني

ظهرت جريمة الابتزاز الإلكتروني نتاج تقنية المعلومات التي أكسبتها لونا وطابعا خاصا يختلف عن الجرائم التقليدية ومن بين خصائصها³:

.سهولة وسرعة التنفيذ، وسهولة الوقوع في فخها بسبب غياب الرقابة الأمنية؛

.صعوبة اكتشافها إلا باستخدام وسائل أمنية ذات تقنية عالية؛

.عابرة للحدود مما يترتب عليها تنازع الاختصاص؛

.صعوبة قياس الضرر المترتب عليها كونه يمس الكيان المعنوي؛

. تعد جرائم دون عنف جرائم ناعمة؛

. ذكاء وحرفية الجاني وتزوده بالعلم والثقافة التكنولوجية ؛

. سهولة إتلاف الأدلة من طرف الجناة؛

. قلة الإبلاغ عن الجريمة إما لعدم اكتشاف الضحية لها، أو خوفا من التشهير.

¹ بن عمر ياسين الابتزاز الالكتروني للأطفال في التشريع الجزائري دفاتر السياسة والقانون المجلد : 16 / العدد : 02 (2024) ص174

² بن عمر ياسين المرجع نفسه، ص174

³ ميمونة ثامر، الآليات القانونية لحماية الأشخاص من جريمة الابتزاز الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق ، جامعة غرداية، 2023/2024، ص 24

فبعد انتشار بنوك المعلومات أو ما يسمى بهستيريا التواصل الاجتماعي عبر شبكة الأنترنت من خلال مواقع الدردشة، إذا كثيرا من الناس كبارا أو صغارا يضعون معلومات شخصية، وصور ومقاطع فيديو خاصة بهم والتي تكون عرضة للمتطفلين أو الهاكرز أو محرمي الأنترنت الذين احترفوا سلوكيات الاعتداء على خصوصية الأفراد عبر الوسائل الإلكترونية، خاصة الضعفاء منهم كالنساء والمراهقين، وتكمن خطورة التهديد هنا في جعل هؤلاء الضحايا يقبلون على الانتحار أو القتل من قبل عائلاتهم.¹

في الوقت الذي يعرف الإحجام عن الإبلاغ ورفع قضايا على المجرمين، لأنه غالبا ما تكون مثل هذه التهديدات والابتزازات محرجة للضحايا، وفي كثير من الأحيان ما تكون مدمرة لحياة الضحية الاجتماعية، وهو ما أدى إلى عدم وجود إحصائيات إلى هذا النوع من الجرائم.

والمشكلة أن الأشخاص يفرطون في خصوصيتهم عبر الأنترنت مما يشكل خطرا على حياتهم من كل أشكال وصور الإعتداء عليها، في الوقت الذي لم يفرده المشرع الجنائي نصوص خاصة لحماية خصوصية الأفراد عبر الأنترنت.

وبالتالي فإن حياة الأشخاص وشعورهم بالأمان في أموالهم وعرضهم، من أهم الأمور أو الأغراض السياسية التي يجب على المجتمعات مراعاتها، بتوفير حماية قانونية فعالة تهدف إلى إيقاع من يعتدي عليها تحت طائلة القانون.²

¹ بن عمر ياسين، المرجع نفسه، ص 174

² عراب مريم، مرجع سابق، ص 1207.

المبحث الثاني: صور و اركان للابتزاز الإلكتروني

بمجرد اكتمال المقومات المفاهيمية للابتزاز الإلكتروني، كان لزماً على المشرع الجزائري أن يحدد الأطر القانونية التي تحكم هذه الجريمة من خلال ضبط صورها المتعددة وتعيين الأركان التي تقوم عليها. فمع التطور التكنولوجي، لم يعد الابتزاز يقتصر على الطرق التقليدية، بل اتخذ أشكالاً رقمية تتسم بالسرعة والقدرة على التخفي، مما استدعى تفكيك هذه الظاهرة في هذا المبحث. سنحاول من خلال المطلب الأول استعراض مختلف الصور والوسائل التي يتخذها الابتزاز الإلكتروني في ظل التشريع الجزائري، لننتقل في المطلب الثاني إلى تشريح الأركان القانونية (المادية والمعنوية) الضرورية لقيام هذه الجريمة وتوقيع العقاب عليها.

المطلب الأول: صور الابتزاز الإلكتروني ووسائله

مع توسّع استخدام الإنترنت وشبكات التواصل الاجتماعي، وتوّع وسائل الاتصال الحديثة برزت جريمة الابتزاز الإلكتروني كظاهرة متعددة الأشكال لا تقتصر على نمط واحد أو دافع واحد، بل تتجلى في مجموعة من الصور التي تختلف من حيث الهدف، والوسيلة، والضحية وراء كل صورة من هذه الصور تقف مجموعة من الوسائل التقنية والسلوكية التي يستغلّها المبتزون. ومن ثم فإن تحليل صور الابتزاز الإلكتروني ووسائله يُعدّ خطوة أساسية لفهم آليات ارتكاب الجريمة

الفرع الأول: صور الابتزاز الإلكتروني

تبدأ العلاقة بين طرفي الابتزاز عن طريق الثقة الوهمية المتبادلة والأساليب الملتوية والمخادعة والوعد الكاذبة ثم تتطور حتى يكون باستطاعة المبتز الحصول على بعض أسرار ضحيته ويحتفظ بها ومن ثم تبدأ عملية المساومة والابتزاز .

تتعدد أسباب ودوافع الابتزاز بحسب شخصية الهدف ومدى قابليته للدخول في هذه الدائرة ولكن في أغلب الأحوال هو الخل السلوكي لدى احد الطرفين، المبتز أو الضحية.

يمثل الاستخدام السلبي للشبكة العنكبوتية عاملاً مهماً في انتشار جرائم الابتزاز التي يستغلها المبتزون وتعد جرائم ابتزاز النساء من أكثر أنواع الابتزاز انتشاراً وشهرة إذ تعتبر جريمة الابتزاز الإلكتروني للنساء النموذج المثالي لهذا النوع من الإجرام لا سيما عندما يكون المبتز رجلاً والضحية امرأة وهذا لا يمنع من القول إن جريمة الابتزاز الإلكتروني من الجرائم المتشعبة الصور حيث تنتوع

هذه الصور تارة بالنظر إلى الهدف المرتقب من الجريمة وتارة أخرى بحسب المنفعة التي تعود على المبتز، ومن أبرز تلك الصور:¹

أولا من حيث المنفعة

ويأخذ العديد من الصور ومن بينها :

1- الابتزاز الإلكتروني المالي:

يعد من أكثر أشكال الابتزاز الإلكتروني شيوعا، ويقوم على تهديد الضحية بنشر صور أو معلومات خاصة ما لم تدفع مبلغا ماليا وغالبا ما يستخدم الجناة تطبيقات المحادثة أو البريد الإلكتروني أو مواقع التواصل الاجتماعي للوصول إلى الضحايا، وكيف هذا النوع في التشريع الجزائري ضمن جريمة التهديد للحصول على منفعة مادية المنصوص عليها في المادة 371 من قانون العقوبات، ويعززه القانون 04-09 من خلال تجريم استخدام الوسائط التكنولوجية لهذا الغرض، خاصة في المادة 13 التي تنص على معاقبة كل من يستخدم تكنولوجيا الإعلام والاتصال لارتكاب أفعال التهديد أو الابتزاز.²

2- الابتزاز العاطفي:

- . ويقصد به موقف أو كلام يأخذه ممارس ليسبب لدى الطرف الآخر احساسا بالخجل أو بالخطأ ، أو ليحمله مسؤولية لا يتحملها ، يستخدم الابتزاز العاطفي لتحقيق سيطرة عاطفية ونفسية على الآخرين ولجعل الآخر يشعر أنه مدين أو مذنب في حق الشخص الذي يبتزه ، وهو أسلوب دنيء في التعامل مع الآخرين»³.

ويتألف الابتزاز العاطفي من خلال « ست مراحل وهي الطلب والمقاومة والضعف والتهديد والتكرار ، بحيث أن هذا النوع يتم من خلال الضغط العاطفي واستغلال المشاعر واعتماد على حالة الخجل الشديد

¹ سليمان محمد الطاهر - رسيوي رشيدة - دراجي عز الدين، مرجع سابق، ص 18

² لقانون رقم 04-09 المؤرخ في 5 أغسطس 2009، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 غشت 2009..

³ حنيشي حمزة ياسين تى شوشاي إبراهيم مهدي ، آليات حماية الطفل من الابتزاز الإلكتروني مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق جامعة غرداية كلية الحقوق والعلوم السياسية قسم الحقوق، 2024/2023، ص

الذي يولدها الضغط من هذا النوع ، باستعمال ما يسيء لمشاعر الضحية ، في سبيل الوصول للغاية التي يقصدها المبتز.¹

3 الابتزاز المادي:

ويُعرف بأنه « محاولة الحصول على المكاسب المادية عن طريق الاكراه استغلالا لحالة ضعف 24 . كما أنه « من أهم وأكثر الأهداف التي يهدف المبتز إلى تحقيقها من ارتكابه جريمة الابتزاز هي تحقيق منفعة مادية، وذلك بطلب مبالغ مالية أو عينية ذات قيمة من المجني عليه ، وذلك مقابل ألا يقوم المبتز بنشر الأسرار التي يخشى المجني عليه نشرها على الملأ.²

4- الابتزاز باستخدام محتوى مزيف ، الفبركة الرقمية

مع تطور أدوات تعديل الصور والفيديوهات مثل تقنية Deepfake ، برز نوع جديد من الابتزاز يتمثل في إنشاء محتوى مزيف يبدو حقيقيا، يتم استخدامه لإخضاع الضحية أو تهديدها، وهو نوع معقد من الجرائم لأنه يجمع بين التزوير الرقمي والتشهير، ويعاقب عليه قانون 09-04 باعتباره استخداما غير مشروع لتكنولوجيات الإعلام من أجل الإضرار بالغير.³

وبجدر الإشارة الى أنه يوجد أنواع أخرى من الابتزاز الالكتروني يصعب حصرها مثل الابتزاز الالكتروني المهني والابتزاز الالكتروني السياسي لكن قد ركزنا على أنواع السابقة لكونها من أكثر الأنواع انتشارا.

ثانيا: صور الابتزاز الالكتروني من حث الهدف

ومن أبرز صورته:⁴

1-هدف نفعي:

¹ ، بحوث ندوة الابتزاز المفهوم الأسباب العلاج ، مركز باحثات الدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية بجامعة الملك سعود الملك ، الرياض المملكة العربية السعودية ، ص 17.

² حنيشي حمزة ياسين توشوشاي إبراهيم مهدي ، مرجع سابق، ص 19

³ غزالي نور الهدى، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني وفق التشريع الجزائري . مذكرة التخرج لنيل شهادة الماستر في الحقوق. جامعة عبد الحميد بن باديس – مستغانم، 2024/2025، ص22

⁴ سليمان محمد الطاهر – رسيوي رشيدة – دراجي عز الدين، مرجع سابق، ص 22

يتحقق ذلك بقيام المبتز بتهديد الضحية بإذاعة أسرارها و نشرها للملأ و ذلك اذا لم يلبي طلباته أو لم يحقق مصلحة للمبتز، فقد تكون المنفعة المرجوة من الابتزاز الإلكتروني عمل غير مشروع كتتفيذ سرقة الصالح المبتز أو ترويج مخدرات، أو يكون عمل مشروع كالتوسط لدى شخص لإتمام عمل، طالما كان العمل ضد إرادة المجني عليه فقد تحققت جريمة الابتزاز الإلكتروني¹.

2-هدف انتقامي

ويكون نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته.

يؤدي الجانب النفسي دورا في عملية الابتزاز الإلكتروني ، وذلك باعتبار أن المجني عليه يعيش صراعا داخليا نتيجة أن الجاني سيقوم بتنفيذ تهديداته ضده في أي وقت شاء ما يدفعه الى تلبية طلبات الجاني تجنباً للفضيحة، حيث يستمتع الجاني بأذية المجني عليه واستماعة لتوسلاته وما يزيد الأمر سوءاً أن يقوم الجاني بتصوير المجني عليه، ويطلب منه ذكر أي بيانات تتعلق به كما يكون الدافع لدى الجاني هو الإنتقام من المجني عليه عن طريق الحاق الأذى به وإساءة سمعته بنشر صورته عن طريق شبكة الانترنت.

3-هدف غير أخلاقي (جنسي):

يتمثل هذا النوع من الابتزاز في قيام الجاني بتهديد الضحية بنشر صور أو مقاطع فيديو جنسية أو حميمية، غالباً ما تكون قد حصل عليها خلال علاقات إلكترونية أو عن طريق تصويرها خلسة دون علمها. ويُعد هذا السلوك انتهاكاً خطيراً للخصوصية واعتداءً صريحاً على الفرد والمجتمع ككل.

وقد تصدى المشرع الجزائري لهذه الظاهرة من خلال تكريس عقوبات في نصوص قانونية متعددة،، منها المادة 303 مكرر من قانون العقوبات، التي تجرم الاعتداء على الحياة الخاصة بتسجيل أو تصوير أو نشر صور دون رضا الشخص المعني، والمادة 333 مكرر 1 المتعلقة بالتحرش الجنسي، فضلا عن أحكام قانون 04-09 التي تجرم هذا النوع من الممارسات الرقمية².

¹ نفس الصفحة نفس الموضع

² ينظر: قانون 04-09، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، سالف الذكر.

ينقسم الإبتزاز الجنسي الى قسمين :¹

-الابتزاز الجنسي الواقعي فيقع هذا النوع من الإبتزاز بقيام المبتز بالحصول على معلومات من الضحية بعد ارتباطه بعلاقة كان يقوم بالنقاط صور تمس الضحية، أو يملك مقاطع فيلمية، أو مقاطع صوتية و بها يصل الأمر إلى حصول المبتز على رقم هاتف ولي أمر الضحية و من ثم تهديده بفضح أمره إذا لم يستجب لرغباته الجنسية و الغير أخلاقية.

-أما الإبتزاز الجنسي الإلكتروني فيتحقق عن طريق وسائل الاتصال الإلكترونية والأنترنت ، والمبتز في هذا النوع يعتبر مجرماً خفياً يسعى للحصول على معلومات تخص الضحية.

الفرع الثاني: وسائل الابتزاز الالكتروني

ان التطور الذي يشهده العالم اليوم والانتشار الهائل لوسائل التواصل الاجتماعي وغيرها من التقنيات والتطبيقات الحديثة المتمكنة التي جعلت من العالم شبيه بقرية واحدة بإمكان الجميع الالتقاء والتواصل واتمام العديد من الأعمال والصفقات والأنشطة وكله عن طريق الأنترنت الذي هو اليوم ضرورة وحاجة ملحة وهامة لا بد منها ولا يمكن الاستغناء عنها بأي شكل من الأشكال فتقريباً كل الأعمال اليوم تتم من خلاله ، الا أن في المقابل هناك العديد من التجاوزات والانتهاكات التي تحدث جراء هذا التطور ومن خلال الأنترنت ووسائله العديدة والكثيرة وهذا ما أدى الى ظهور نوع جديد من الجرائم وهي الجرائم الالكترونية التي هي اليوم تشكل خطر كبير على الأفراد وحتى الدول ، وجريمة الابتزاز الالكتروني من الجرائم الالكترونية المنتشرة بكثرة وبالأخص في الأونة الأخيرة فهي من أخطر الجرائم السيبرانية التي تهدد أمن واستقرار الدول والشعوب على حد سواء لأن وسائل التواصل الاجتماعي سهلت كثيراً وساهمت في قيام هذه الجريمة وفي انتشارها المروع المخيف.²

لم يحدد المشرع الجزائري الوسيلة التي يتم بها نشر أو إذاعة الصور الخادشة بل يتم هذا السلوك بأية وسيلة كانت، فيمكن أن تكون عن طريق التبادل اليدوي أو لصقها في أماكن عامة أو وسط العائلة وغيرها، غير أنه في حالة ما اذا استعمل الجاني وسائل التكنولوجيا الحديثة فإن العقوبة تكون أشد.

¹ سليمان محمد الطاهر — رسيوي رشيدة — دراجي عز الدين، مرجع سابق،، ص 22

² نورة طاع الله ، جريمة الإبتزاز الإلكتروني في القانون الجزائري، كيان اللا رواية للنشر الإلكتروني، متاح على الرابط <https://larewaia.blogspot.com/?m=1> تاريخ الاطلاع/ 2026/05/02، سا 01:20

يتم تصيد ضحايا الإبتزاز الإلكتروني بشكل عام عن طريق الحاسب الآلي، ولواحقه، وبرامجه، و عن طريق شبكة الانترنت مواقع التواصل الاجتماعي، أو بعض تطبيقات الهواتف الذكية¹.

ومن أشهر مواقع التواصل الاجتماعي استخداما لتصيد الضحايا هي²:

فيسبوك (ميتا) و تيك توك و سناب شات و الإنستغرام .

أولاً: الحاسب الآلي

الحاسب الآلي (الكمبيوتر) هو جهاز إلكتروني قادر على استقبال معطيات المعلومات التي نرغب في إدخالها وتخزينها وكذا تخزين المعلومات الخاصة بالبرامج التطبيقية للقيام بمعالجة هذه الأخيرة بسرعة فائقة يستحيل على الإنسان القيام بها وذلك بعد أن يدخل عليه لإنشاء معلومات مسبقة وبرامج متخصصة.

وفي التشريع الأمريكي ورد تعريف الكمبيوتر أو الحاسب الآلي على أنه: « جهاز إلكتروني بصري كيميائي كهربائي أو جهاز إعداد معلومات ذات سرعة عالية يؤدي إلى وظائف حسابية أو تخزينية ويشمل على أي تسهيل تخزين المعلومات أو تسهيل اتصالات مباشرة مقترنة أو تعمل بالاقتران مع هذا الجهاز³ ».

ثانياً : برامج الحاسب الآلي.

نصت التعليمات النموذجية لحماية البرمجية الصادرة عن المكتب الدولي للمنظمة العالمية للملكية الفكرية عام 1978 صراحة على شمولية وصف البرنامج مجال حماية البرامج، وعرفته بأنه التقديم الكامل والمفصل لمختلف العمليات شفوياً أو تخطيطياً أو غيرهما بشكل كاف بقصد تحديد مجموعة التعليمات

¹ دلال وردة ، جريمة التهديد أو نشر أو اذاعة صور خادشة التي تقع بين الخاطبين أو الزوجين المستحدثة بالقانون رقم 24/06 المعدل والمتمم لقانون ، العقوبات الجزائري، المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار - الجزائر المجلد: 09، العدد 02 السنة 2025، ص 145.

² بن زيطة عبد الهادي حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط01

³ سلامة عماد محمد الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج الجزء الأول، دار وائل للنشر الإسكندرية 2005 ص 26

المكونة لبرنامج الحاسوب فالبرنامج والحاسوب هما إحدى الوسائل للوصول إلى النتيجة أو الاختراع الجديد، ويقوم البرنامج بتكملة الطريقة الصناعية، إذ لولاه لما تم التوصل إلى النتيجة المطلوبة.¹

المشرع الجزائري لم يعرف برامج الحاسب الآلي صراحة لكن أورد ذكره في سياق الأمر 03-05 فنظر إليها كمصنفات أدبية أو فنية محمية بما نصه «المصنفات الأدبية المكتوبة مثل محاولات الأدبية مثل والبحوث العلمية والتقنية والروايات والقصص القصائد الشعرية وبرامج حاسوب ومصنفات الشفوية مثل المحاضرات الخطب المواعظ وباقي مصنفات التي تمثلها»²

ثالثا: الأنترنت :

تعتبر الأنترنت شبكة دولية إلكترونية متعددة الأبعاد والخدمات، وهي أضخم شبكة معلومات الحواسيب منتشرة في العالم، كما تعد أداة تواصلية بين شبكات المعلوماتية دونما اعتبار للحدود الفاصلة بين الدول، فهي تحتوي على آلاف من شبكات الحواسيب المحلية والدولية المرتبطة ببعضها البعض، إما بطريق خطوط الهاتف، أو الأقمار الصناعية، وتمتد عبر العالم لتؤلف شبكة هائلة، بحيث يمكن للمستخدمولوج إليها في أي مكان وزمان، شرط توافر حاسب آلي مزود بموديم أو هاتف نقال، متصل بشبكة الأنترنت، مع تحميل وسائل الإتصال لتلقي وإرسال البيانات.

1. الهاتف النقال وبرامجه: يستخدم المبتز الهاتف للقيام بجريمته مستعملا برامج التجسس المحمولة، أو التصوير بالكاميرا، أو سرقة المعلومات بالبلوتوث، أو التسجيل الصوتي.

2. خدمة الدردشة: يسمح هذا البرنامج بتجمع الأشخاص من مختلف أنحاء العالم، وقد يكون من ضمن الأشخاص من يمتن الإبتزاز الإلكتروني، فيتصيد فريسته عبر هذه الدردشات، مثل غرف ومواقع الدردشات الصوتية والكتابية.

3 البريد الإلكتروني : قد يكون البريد الإلكتروني بيئة لارتكاب جريمة الإبتزاز، عن طريق إرسال روابط مفخخة على سبيل المثال، أو سرقة الرمز السري.

¹ بختي بوبكر النظام القانوني لبرامج الحاسب الآلي في التشريع الجزائري مجلة الأستاذ الباحث للدراسات القانونية والسياسية - المجلد 05 - العدد 02 - السنة 2020، ص108

² الأمر رقم 03-05 مؤرخ في جمادى الأولى 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد 44 المؤرخة في 23 يوليو 2003

ومن طرق الابتزاز الإلكتروني الجديدة استغلال الدين في التواصل مع الشخص، حيث يقوم المبتز بانتحال صفة شيخ راقى يقوم بفك سحر المجني عليه، ويطلب منه إرسال صور له ومقاطع ليجعلها مادية ابتزاز لاحقاً¹.

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني في التشريع الجزائري

الابتزاز الإلكتروني يعني الحصول على معلومات سرية إلكترونية للشخص لا يرغب في إذاعتها في الفضاء العام سواء بواسطة الاختراق والسرقة أو عن طريق استغلال الثقة والأمان ثم التهديد والمساومة بجعل المنشور مقترحا للعامة مقابل الحصول على مكاسب مادية أو معنوية أو جنسية أو ارتكاب جريمة، وما يمثله ذلك من ضغط على إرادة الضحية وتخويله بالفضيحة والتشهير بأي وسيلة رقمية، فهذه الجريمة تمر بعدة مراحل:²

الحصول على معلومات وبيانات سرية متعلقة بالحياة الخاصة للضحية سواء عن طريق الثقة أو عن طريق توريطها في جريمة أو قضية أخلاقية ممكن تحدث بليلة في الرأي العام أو عن طريق اختراق جهازها وسرقة محتوياتها أو الغش والتجسس الإلكتروني من صور وفيديوهات وتسجيلات ودرشات أو عن طريق صناعة محتوى رقمي ملفق للضحية أو استرجاعه من هاتف أو لوح الكتروني مبيع... إلخ.

مرحلة الابتزاز عن طريق الضغط والتهديد بنشر تلك المعلومات التي لا ترغب الضحية في إذاعتها، وهي مرحلة تتعلق بارغام الضحية على شراء سكوت الجاني من تنفيذ تهديداته، فهي مرحلة السيطرة على الضحية حتى تصبح معدومة الاختيار فلا يكون أمامها غير الرضوخ لطلبات المبتز وإلا تعرضت للأذى النفسي والجسدي

أن يكون التهديد بأي وسيلة تقنية، كتابة صوتا عن طريق التسجيل أو بواسطة بقصد الحصول مكسب مادي أو معنوي أو جنسي أو أي شئ آخر دون وجه حق، ولا يهم كون الشئ المتزع ملكا للضحية أو لغيرها أو كون الانتزاع لصالح الغير.

في حال تعنت الضحية ورفضها تلبية مطالب المبتز مهما كان نوعها مادية أو أو معنوية أو جنسية، تأتي مرحلة التشهير عن طريق نشر الأسرار الخاصة علانية بواسطة منصة رقمية مثل الفاسبوك أو انستاجرام أو سنابشات أو غيرها

¹ ميمونة ثامر، مرجع سابق، ص 27

² فاطمة العرفي، مرجع سابق، ص 498

وتزداد خطورة هذا الفعل متى تم التلاعب في الصورة عن طريق (الفوتوشوب وفي الفيديوها عن طريق (المونتاج) أو تعديل الصوت عن طريق برامج وتطبيقات رقمية متطورة، مما يعطي انطباع فيه مغالطة عن الضحية ويصورها كأنها فاسقة خارج عن الأخلاق¹

الفرع الأول: الركن المادي لجريمة الإبتزاز الإلكتروني

يقصد بالركن المادي للجريمة السلوك الخارجي المادي الذي يجرمه القانون ، ويتكون من السلوك الإجرامي والنتيجة والعلاقة السببية:²

بالرجوع إلى جريمة الابتزاز الإلكتروني فإن هذا الركن يمثل الإطار العملي للجريمة، ويتجلى في السلوك الإجرامي المتمثل في التهديد أو الضغط باستخدام الوسائل التكنولوجية بقصد حمل المجني عليه على القيام بفعل أو الامتناع عنه لتحقيق مصلحة غير مشروعة للجاني، ويتكون الركن المادي في جريمة الابتزاز الإلكتروني من عدة عناصر مترابطة، وهي : السلوك الإجرامي ذاته الوسيلة المستعملة، محل الجريمة، والعلاقة السببية بين الفعل والنتيجة.

1- السلوك الإجرامي:

يكون الركن المادي في جريمة الابتزاز الإلكتروني بدخول الجاني بطريقة متعمدة إلى موقع إلكتروني، أو نظام معلوماتي لا يملك الجاني حق الدخول فيه، ويهدد المجني عليه للقيام بفعل أو الإمتناع عنه، سواء أكان هذا الفعل أو الإمتناع مشروعاً أو غير مشروع ويتمثل الركن المادي في التهديد المقترن بطلب، وشرطه أن يكون إيذاء أو يترك أثراً في نفس المجني عليه، يدفعه إلى تنفيذ طلب المبتز دون إرادته. كان يكون الطلب مادياً أو جنسياً وإذا رفض المجني عليه ينفذ الجاني تهديده.³

قد يكون السلوك الإجرامي تهديداً أو تشهيراً أو إلحاق الضرر بالمجني عليه

أ-التهديد: هو فعل إجرامي من الجاني إلى المجني عليه ينال من حريته وطمأنينته، وقد يمتد إلى حواشي المجني عليه الذين يهتمهم أمرهم كزوجته وأبنائه . والتهديد الإلكتروني لا يختلف عن التهديد التقليدي سواء شفاهة أو كتابة أو رموزاً أو شعارات. إما بنشر بيانات أو صور أو مقاطع فيديو حصل عليها بطريق الاختراق، أو سرقة جهاز الضحية، وسواء أكان التهديد عن طريق البريد الإلكتروني، أو

¹ فاطمة العرفي، مرجع سابق، ص 498- 499

² برحال امال، جريمة الابتزاز عبر الوسائل الإلكترونية، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة العربي التبسي، تبسة 2019 2020، ص 42.

³ ميمونة ثامر ، مرجع سابق ، ص 30

غرف الدردشة، أو التسجيل الصوتي أو المنتديات، ما من شأنه أن يكون المجني عليه تحت رحمة الجاني، ولا يهم هذا الأخير أن ينوي تنفيذ الأمر المهدد به أم لا، المهم ألا يكون التهديد هزلًا. فيكفي لتحقيق التهديد أن يكون من شأنه ترويع المجني عليه، بحيث يحمله على تنفيذ طلبات المبتز. بل ويعتبر أيضًا تهديدًا إخبار شخص آخر وقام هذا الأخير بنقل التهديد للمجني عليه¹.

ب-التشهير: بالآخرين لكل فرد الحق في إخفاء حياته الخاصة التي يحميها القانون باعتبارها ملكًا له، ولا يجوز الإطلاع عليها دون رضاه. إلا أنه نتيجة التقدم التكنولوجي في الأجهزة المستحدثة، أصبح من السهل اجتياز أي حاجز من تسجيل أو تصوير أو نقل الأحاديث ونسخها، لهدف وتشويه سمعة الأشخاص، أو طبيعة عملهم، أو التعرض لأسرهم بهدف الإبتزاز أو الإنتقام أو لمجرد الضرر. وقد حصل أن قام تلميذ في الثانوية بتصوير أستاذته التي منحته علامة صفر في مادة مهمة وأطلق الشائعات في صفحة فيسبوك مزيفة باسمها.

ج-مدى توافر ركن الضرر في جريمة الإبتزاز الإلكتروني :

الضرر هو ما يصيب الإنسان في حق من حقوقه أو في مصلحة مشروعة له، وهو إما ضرر مادي يلحق الإنسان في ماله أو جسده: ²

-التهديد الذي يكون محله الجسد ويكون بالعنف ضد الجسد مثل القتل أو الضرب.

-التهديد الذي يكون محله المال كأن يهدد المجني عليه بترك وظيفته وإلا سيقوم الجاني بحرق منزله.

أو ضرر معنوي، كان ينصب الإيذاء على الشرف والسمعة أو المكانة الاجتماعية أو المركز الوظيفي، كمن يسند له أنه يتردد على محلات الدعارة أو فار من مستشفى الأمراض العقلية.

وبالتالي الضرر المتطلب هو الضرر المحتمل حتى ولو يلحق ضررًا باعتبار أن الفعل بحد ذاته جريمة مثل التصنت والإلتقاط ، والدخول غير المشروع إلى موقع إلكتروني ، أو عن طريق استدراج الضحية في مراسلات وأحاديث للحصول على معلومات أو صور لاستخدامها فيما بعد للإبتزاز، وإجبار المجني عليه لتنفيذ رغباته، ولخشية الفضيحة ينفذها هذا الأخير .

2-العلاقة السببية:

¹ ميمونة ثامر ، مرجع سابق ، ص 30

² نفسه، ص 31

وهي الرابط بين سلوك الجاني والفعل الذي قام به والأثر المترتب والواقع جراء قيامه بفعله وهي من أهم شروط قيام المسؤولية الجنائية، فيجب أن يكون الفعل الصادر عن الجاني ذو علاقة سبب أدى بدوره إلى أثر انتقل إلى الجاني وبالنظر إلى العلاقة السببية نجد أن من السهولة تحديد علاقة السبب في الجريمة فمثلا إذا قام أحدهم بضرب آخر فقتله فإن علاقة السبب تكمن في السبب المؤدي على الوفاة وهي الضرب الذي أدى لحدوث كدمات أخلت في نظام عمل أجهزة الجسم أو اخترقت الجلد ومزقته حتى نزفت دماء الضحية ومات.¹

3- النتيجة:

تتمثل في التهديد بنشر محتوى رقمي موضوعه إفشاء أو نسبة أمور شائنة من شأنها تلطيخ سمعة المهدد أو تمس باعتباره بحيث يشكل ضغطا على إرادة الضحية ويدفعه للرضوخ لمطالب المبتز دون رضاه منعا للحدوث التشهير والفضيحة في الفضاء الرقمي وبالتالي خسارته لسمعته. فالجريمة غير متعلقة بتحقيق النتيجة وإنما بثبوت طلب أو مساومة الجاني للضحية وتهديد بفقد سمعته وفضحه أمام العلن.²

أي أن الركن المادي في هذه الجريمة ثلاثة صور ويكفي توفر أحدها لقيام الجريمة، بحيث لا يشترط اجتماعها معا حيث تتوفر النشاط الإجرامي بحيث تشترك هذه الأفعال في انطوائها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر، وعلىه فإن الاعتداء على المعطيات في نظام المعالجة ، أي البيانات التي أدخلت لمعالجتها و تحولت إلى معطيات عبارة عن رموز أو إرشادات تمثل تلك المعلومة، أي بيانات تمت معالجتها أي الجريمة تقع على المعطيات إلى البيانات التي تمت معالجتها، دون المعلومة ذاتها، بحيث أن المعلومة التي لم تعالج بصد لا تدخل ضمن نطاق الجريمة، كذلك يخرج من نطاق الجريمة المعلومات التي انفصلت عن النظام وسجلت على شريط أو قرص مدمج لأنها أصبحت خارج النظام، بحيث أن المشرع هنا يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بأن اتخذت خطوة أو أكثر في مراحل معالجتها، أو المعلومة التي انفصلت عن النظام ثم أعيد إدخالها.

¹ حداد شيماء جبلي سعيده جريمة الابتزاز عبر الوسائل الالكترونية في التشريع الجزائري مذكرة مكمله لنيل شهادة

الماستر المركز الجامعي عبد الحفيظ بوصوف ميله، 2024/2023، ص 20

² بن عمر ياسين، مرجع سابق، ص 177

وسوف نبين فيما يلي المقصود بالأفعال المكونة لهذه الجريمة،¹

1- الوسيلة المستعملة

تعد الوسيلة من العناصر التي تمنح الجريمة وصفها الإلكتروني، إذ تختلف عن الابتزاز التقليدي بكونها تتم باستعمال وسائل الاتصال الحديثة كالحواسيب والهواتف الذكية، التطبيقات الرقمية، والبريد الإلكتروني، وغيرها من الوسائل الرقمية، ويشترط أن تتم هذه الأفعال في الفضاء الرقمي حتى تدرج ضمن فئة الجرائم السيبرانية ما يتطلب توافر الكفاءة التقنية في التحقيق وجمع الأدلة الرقمية، وهذا ما أكدته التعديلات التشريعية الأخيرة التي وسعت من نطاق التجريم ليشمل الجرائم المرتكبة عبر الوسائط التكنولوجية.

2- محل الجريمة

يقصد به الشيء الذي يقع عليه السلوك الإجرامي أي المصلحة المحمية قانونا، وهي في هذه الحالة حرمة الحياة الخاصة، وسرية المعلومات، وكرامة الشخص المستهدف، فقد يكون محل الجريمة صورة أو مقطعاً مرئياً أو تسجيلاً صوتياً أو رسالة نصية تتضمن مضمونا خاصا أو حميميا، وبالتالي فإن الاعتداء لا يقع فقط على البيانات أو المحتوى بحد ذاته، بل على الخصوصية والحرمة التي يرضى أن تحاط بها هذه العناصر.²

الفرع الثاني: الركن المعنوي لجريمة الإبتزاز الإلكتروني

يمثل الركن المعنوي القصد الجنائي البعد الذهني أو النفسي للجريمة، ويعبر عن الإرادة الحرة الواعية التي تصدر عن الجاني لارتكاب فعل غير مشروع يحرمه القانون ، ويختلف هذا الركن عن الركن المادي الذي يتجسد في فعل خارجي ملموس، إذ يركز على النية الداخلية أو الدافع الذهني الذي حرك الجاني نحو ارتكاب السلوك الإجرامي ، وفي جريمة الابتزاز الإلكتروني بعد القصد الجنائي أحد أهم

¹ بوحفص راوية، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، جامعة محمد خيضر - بسكرة - 2017/2018، ص32

² سامية بوشريط الابتزاز الإلكتروني كجريمة مستحدثة في القانون الجزائري دراسة تحليلية للمادة 303 مكرر 1 مجلة العلوم القانونية والسياسية، جامعة قسنطينة، العدد 10، 2022، ص 64

أركان التجريم، لأنه يميز الفعل الجرمي عن الأفعال المباحة التي قد تشابهها في الشكل مثل نشر معلومة على شبكة رقمية، لكنه يختلف عنها في الغاية والمقصد¹.

من خلال إسقراء نص المادة 394 مكرر 1 من قانون العقوبات المعدل و المتمم، يتبين أن جريمة التلاعب بمعطيات الحاسب الآلي هي جريمة عمدية يتخذ فيها ركن المعنوي صورة القصد الجنائي العام بعنصرية العلم والإرادة، فيكفي أن يعلم الجاني بأن نشاطه غير مشروع وتتجه إرادته إلى فعل الإدخال أو المحو أو التعديل بهدف تغيير المعطيات .

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجاني العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بصاحب النظام، بل تتوفر الجريمة ويتحقق ركنها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي، لا أنه ليس عنصرا في الجريمة، أي أن الجريمة لا تتطلب قصد جنائي خاص².

الركن المعنوي في جريمة الابتزاز الإلكتروني يعتبر أساس المسؤولية الجنائية، ولا يمكن إدانة الجاني ما لم يثبت أن فعله قد صدر عن إرادة حرة وعن نية تهدف إلى الإضرار بالغير أو ابتزازه، وتكمن خطورته في أنه غالبا ما يمارس عن بعد وفي بيئة رقمية تخفي شخصية الجاني، مما يفرض على القضاء والخبراء التقنيين بذل جهود مضاعفة للكشف عن نية الإجرام الرقمي وتقديم الدليل القاطع على توفر القصد الجنائي³. النفسي للجاني، باعتبار الجانب المادي هو السلوك المكون للجريمة، ويعبر عنه بالقصد الجنائي (العلم والإرادة) 10.

- العلم: أن يعلم الجاني وقت اقتراف فعله أن المنفعة التي حصل عليها هي ثمرة التهديد الذي صدر عنه، وأنه ليس له الحق فيما يلزم الضحية بتنفيذه. فلا بد أن يعلم الجاني بنتيجة السلوك المرتكب، والحصول على صور فاضحة، مقابل الحصول على منفعة جريمة يعاقب عليها القانون.

وقد أكد القضاء الفرنسي ذلك حينما قررت محكمة النقض الفرنسية " أن القصد الجنائي يتوافر حين يدرك الشخص أنه يحصل بالقوة أو بالعنف أو الإكراه ما كان لا يمكن الحصول عليه من خلال

¹ ربيعة خريس الجرائم الإلكترونية في التشريع الجزائري ، دراسة تحليلية مقارنة، دار هومة الجزائر، 2020، ص 137

² انور الدين زروقي الجريمة الإلكترونية في التشريع الجزائري الطبيعة والأركان والجزاءات دار العلوم للنشر والتوزيع 212الجزائر، 2022، ص212

³ ميمونة ثامر ، مرجع سابق ، ص 34

إنفاق طوعي الإلكتروني التي تعتبر من الجرائم التي تحتاج إلى احتراف تكنولوجيا المعلومات بمهارة من أجل تنفيذها، فلا يمكن تصور حصولها من دون قصد، ولا حاجة لشرط توفر القصد الجنائي الخاص لأنها جرائم عمدية. كما يجب أن يكون التهديد جدي بدرجة كافية للتأثير في نفسية الضحية¹.

- الإرادة: يجب أن تتجه إرادة الجاني في جريمة الإبتزاز الإلكتروني إلى تهديد المجني عليه الإرغامه على تنفيذ طلباته، كما أكدت ذلك محكمة النقض الفرنسية. إن توافر القصد الجنائي يشترط أن تتجه نية الشخص إلى استخدام تهديدات غير مشروعة الإلزام الآخرين بالدخول في التزامات أو تحويل أموال دون إرادتهم أو لا مبرر لها.²

فلكي تقوم المسؤولية الجنائية يجب أن تكون إرادة الفاعل قد اتجهت إلى القيام بالفعل المجرم دون أن يكون هناك عيب في هذه الإرادة، كأن يكون الجاني مكرها على القيام بالفعل المجرم .. كما يجب أن تتجه إرادة المبتز إلى تحقيق النتيجة من سلوكه المجرم، كالحصول على منفعة مالية أو جنسية، ولا عبرة للبائع أن يكون نبيلاً أو غير ذلك في قيام المسؤولية الجنائية، كأن يكون البائع الحصول على أموال لأمه المريضة، فبتوافر القصد الجنائي العام تقوم جريمة الإبتزاز الإلكتروني التي تعتبر من الجرائم التي تحتاج إلى احتراف تكنولوجيا المعلومات بمهارة من أجل تنفيذها، فلا يمكن تصور حصولها من دون قصد، ولا حاجة لشرط توفر القصد الجنائي الخاص لأنها جرائم عمدية. كما يجب أن يكون التهديد جدي بدرجة كافية للتأثير في نفسية الضحية .

الفرع الثالث: الركن الشرعي لجريمة الإبتزاز الإلكتروني

يعتبر الركن الشرعي في الجريمة هو نص التجريم والعقاب، ومبدأ الشرعية يقتضي في جميع التشريعات أن لا جريمة ولا عقوبة إلا بنص. فالنصوص القانونية هي جدار حماية لأمن الإنسان وخصوصيته. وأي شخص يحاول كسر هذه الحواجز أو اختراقها بعد مدانا ويستحق العقاب المقرر لفعله. ومع تزايد الجرائم الإلكترونية، باشرت معظم الدول لمواجهتها إما بسن تشريع قانون مستقل، أو الإكتفاء بتطبيق النصوص التقليدية أو إدخال تعديلات عليها وذلك بحسب قدراتها وظروفها ومصالحها.³

¹ عاشور أميل جبار المسؤولية الجنائية عن جريمة الابتزاز في مواقع التواصل الاجتماعي، (دراسة مقارنة)، مجلة أبحاث ميسان 124 م (السادس عشر)، ع (31) 2020، ص

² نفس المرجع، ص 34

³ مريم عراب المرجع السابق، ص 1209

فالركن الشرعي هو تجريم الفعل ووضع العقوبة المقررة له، ومعظم الدول سنت تشريعا جنائيا للجريمة الإلكترونية والتهديد الإلكتروني.

ورغم أن المشرع الجزائري لم يتطرق لجريمة الإبتزاز الإلكتروني في قانون خاص فقد اكتفى بجريمة التهديد الكلاسيكية، إلا أنه أولى حماية خاصة لحرمة الحياة الخاصة في الدستور وفي قوانين أخرى التي من شأن هذه الجريمة أن تهدمها.

ففي المادة 39 من دستور 1996 نصت على ما يلي : لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ، والمادة 24 من المرسوم الرئاسي المتعلق بالمنظومة الإحصائية» لا يحق للمصلحة المؤتمنة أن تكشف أو تنشر المعلومات الفردية الواردة في الإستمارات التي تنص على التسجيل الإحصائي ولها علاقة بالحياة الشخصية والعائلية وعلى العموم الوقائع والتصرفات الخصوصية ، ورتبت العقاب عند استعمال المعلومات الشخصية المتحصل عليها

لم يلتفت المشرع الجزائري إلى الوسيلة المستخدمة في ارتكاب الجريمة بل جعلها عامة وبالتالي تدخل الجرائم المرتكبة بالتقنية ضمن هذه المادة.

كما نص المشرع الجزائري في المادة 47 في القانون المدني على المساس بحق من الحقوق الملازمة للشخصية، وعليه فكل اعتداء على هذا الحق بأي صورة كانت ينشئ للمضرور حق المطالبة بالتعويض المناسب، وذلك بالرجوع إلى نصوص القانون المدني من 126 المواد 131 إلى 134 ومن 181 إلى 182 مكرر

تبنى المشرع الجزائري الشمولية في تجريمه للأفعال التي يكون مسرحها إلكتروني من خلال القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وأحالنا إلى القواعد التقليدية المطبقة على جريمة التهديد الكلاسيكية المادة 02 من قانون 09/04 والابتزاز الإلكتروني صورة مستجدة من الإبتزاز العادي المنصوص عليه في قانون العقوبات المادة 37 والمادة 11 والمادة 128¹ .

وخلاصة القول ان المشرع الجزائري تبنى في تجريمه للأفعال التي تكون مسرحها إلكتروني، وذلك من خلال القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما يستشف من نص المادة 02 منه التي جرمت الأفعال الإجرامية

¹ ميمونة ثامر ، مرجع سابق ، ص 30.

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

فجريمة التهديد التقليدية التي غالبا ما تسمى بالنتشهير لم تتغير من حيث الأركان في ظل التحولات الرقمية والمعلوماتية، إذا يأبه المشرع بالوسيلة التي ترتكب بها الجريمة مدام أنها تتصرف إلى ذات تتصرف إلى ذات النتيجة الإجرامية إي المساس بالحياة الخاصة، وما الابتزاز الإلكتروني إلا صورة مستجدة للتهديد والابتزاز التقليدي المنصوص عليه في المادة 371 من قانون العقوبات الجزائري، وإذا كانت العديد من التشريعات تعتبر الابتزاز الإلكتروني والتهديد مصطلحين لهما نفس المدلول، بيد أنه من وجهتنا نكون أمام جريمة الابتزاز إذا حصل تهديد مصحوبا بحمل الضحية للقيام بعمل أو الامتناع عنه أما جريمة التهديد فتتصرف إلى الوعيد دون مطالبة المبتز للمجني عليه وإرغامه على القيام بعمل¹

¹ أكرم ديب دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني، مجلة الحقوق والعلوم السياسية، (16)، ع (01) 404 2023، ص 10.

خلاصة الفصل:

تناول الفصل الأول من الدراسة الإطار الموضوعي الجريمة الابتزاز الإلكتروني كصورة من صور الجريمة الإلكترونية، فتم من خلال هذا الفصل التطرق إلى الماهية الابتزاز الإلكتروني لغويا واصطلاحا وفقهيا كما تم التطرق إلى أنواع الابتزاز الإلكتروني بالنظر الشخص الضحية والهدف المرجو من المجنى عليه ثم تعرضنا إلى وسائل الابتزاز الإلكتروني للحاسب الآلي ، برامجه الانترنت والهاتف النقال ، ثم تجريم ظاهرة الابتزاز الإلكتروني من خلال التعرض إلى أركان الجريمة الشرعي المادي والمعنوي)..

الفصل الثاني

إجراءات وآليات مكافحة جريمة الإبتزاز
الإلكتروني في التشريع الجزائري

إذا كانت الجرائم المعلوماتية بصفة عامة، وجريمة الابتزاز الإلكتروني بصفة خاصة، تتميز بطابعها الافتراضي العابر للحدود وقدرة مرتكبيها على التخفي الرقمي، فإن ذلك يضع الأجهزة القضائية والضبطية القضائية أمام تحديات إجرائية غير تقليدية. فإجراءات التحقيق في هذا النوع من الجرائم تتطلب توازناً دقيقاً بين ضرورة الفعالية التقنية في اقتفاء الأثر الرقمي، وبين وجوب احترام الحريات الفردية وحرمة الحياة الخاصة التي كفلها الدستور والقانون.

ومن هنا تبرز ضرورة تسليط الضوء على التشريعات المعلقة بها والجراءات المتبعة في مكافحة هذه الجريمة واطارها المؤسسي .

ومن اجل الالمام بهذا الجانب من الدراسة سنقوم بتقسيمه الى مبحثين التكيف القانوني للابتزاز الالكتروني في القانون الجزائري حيث سنتناول في المبحث الاول ثم نتطرق الى اجراءات مكافحة جريمة الابتزاز الالكتروني واطارها المؤسسي في المبحث الثاني

المبحث الاول: التكيف القانوني للابتزاز الالكتروني في القانون الجزائري

يولي المشرع الجزائري أهمية بالغة لجزر جريمة الابتزاز الإلكتروني بالنظر لما تمثله من مساس خطير بحرية الأفراد وكرامتهم وخصوصيتهم، وقد سعى إلى تجريم مختلف صورها من خلال تكيفها ضمن أطر قانونية متعددة سواء في قانون العقوبات أو القانون رقم 18-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تم التنصيص في هذا السياق على عقوبات أصلية وأخرى تكميلية تختلف بحسب خطورة الفعل. ويتم تناول ذلك من خلال دراسة الابتزاز الإلكتروني في قانون العقوبات في المطلب الاول ثم الابتزاز الإلكتروني في قانون جرائم الاعلام والاتصال 09/04 كمطلب ثان

المطلب الاول: الابتزاز الالكتروني في قانون العقوبات

تعتبر العقوبة الأثر القانوني الأبرز المترتب على تجريم السلوك إذ عمد المشرع إلى ربط كل فعل أو امتناع يشكل مخالفة لنصوصه الموضوعية بجزاء جنائي محدد وتهدف هذه العقوبة إلى ترسيخ ازدواجية الردع: الردع الخاص الذي يستهدف تأهيل المجرم والردع العام الذي يسعى لتحسين المجتمع ومنع الجريمة مستقبلاً.

بالعودة الى الابتزاز الإلكتروني فالمشرع الجزائري لم يضع موضوع مستقل لجريمة الابتزاز الإلكتروني وعليه هذه الجريمة تأخذ حكم الابتزاز عموماً¹

هذه الجريمة في أغلب الدول تكون قاسية وتصل إلى الحبس لسنوات وغرامات مالية كبيرة، فالإعلان العالمي لحقوق الإنسان يقر في مادته صراحة، المادة 12 يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات، كما اهتم الدستور الجزائري المؤرخ في 6 مارس 2016، هو الآخر بهذا الموضوع في مادته 40" حيث تضمن الدولة، عدم

¹ فاطمة العرفي ، مرجع سابق، ص504

انتهاك حرمة الإنسان، ويحضر أي عنف بدني أو معنوي أو أي مساس بالكرامة. المعاملة القاسية أو اللاإنسانية أو المهينة يجمعها القانون.¹

الفرع الأول: العقوبات المقررة

أن المشرع الجزائري أولى حماية خاصة لحرية الأفراد وحياتهم الخاصة لما يترتب عليها من أضرار تلحق بهؤلاء الأشخاص، وقد تطرق لهذا في المواد 303 مكرر و 303 مكرر 1 من قانون العقوبات الجزائري 23/06 ، والعقوبة تتراوح بين الحبس من 6 أشهر إلى 3 سنوات حبسا نافذا، وغرامة مالية من 50 ألف دينار إلى 300 ألف دينار، وهذه العقوبات تخص كل من تعدد المساس بخصوصية حياة الأشخاص، بأي تقنية كانت، سواء عن طريق التقاط أو تسجيل أو نقل مكالمات سرية أو خاصة بغير إذن صاحبها أو رضاه، إلى جانب ذلك يعاقب القانون على الشروع في ارتكاب الجثة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة تامة الأركان، كما يضع تنازل الضحية عن القضية، أو صفحه عن المتهم حدا للمتابعة الجزائية، والمدنية، طبقا لقانون العقوبات الجزائري.

أولا: العقوبات الأصلية

التهديد هو الإعلان عن شر يراد إلحاقه بشخص معين، من شأنه أن يسبب له اضطرابا معنويا، وقد يكون محررا موقعا، أو غير موقع عليه، أو بالصور أو الرموز، أو بالكلام حيث تنص المادة 284 من قانون العقوبات الجزائري كل من هدد بارتكاب جرائم القتل أو السجن أو أي اعتداء آخر على الأشخاص مما يعاقب عليه بالإعدام أو السجن المؤبد وكان ذلك بمحرر موقع عليه أو غير موقع عليه أو بصورة أو رموز أو أي شعارات يعاقب بالحبس من سنتين إلى 10 سنوات وبغرامة من 500 إلى 5000 د.ج إذا كان التهديد مصحوبا بأمر بإيداع مبلغ من النقود في مكان معين أو بتنفيذ أي شرط آخر".

¹ مقال بعنوان : الابتزاز والتشهير الإلكتروني وعقوبته في القانون الجزائري: جريدة العالم اليوم ، العدد 2590، الصادر بتاريخ 2026/05/08، نسخة الكترونية متاح على الرابط <https://www.elalem-elidara.dz/?p=54676> تاريخ الاطلاع: 2026/05/09، سا 14:32

كما تنص المادة 285 من ق ع الجزائري: " إذا لم يكن التهديد مصحوبا بأي أمر أو شرط قد يعاقب الجاني بالحبس من سنة إلى ثلاث سنوات وبغرامة من 500 إلى 2500 د.ج. وتنص المادة 286 من قانون العقوبات الجزائري: " إذا كان التهديد مصحوبا بأمر أو شرط شفهي، فيعاقب الجاني بالحبس من ستة أشهر إلى سنتين والغرامة من 500 إلى 1500 د.ج. أما المادة 287 من قانون العقوبات الجزائري فتتص: كل من هدد بالاعتداء أو العنف المنصوص عليه في المادة 284 وذلك بإحدى الطرق المنصوص عليها في المواد من 284 إلى 287 يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 500 إلى 1000 د.ج إذا كان التهديد مصحوبا بأمر أو شرط، وفي المادة 371 من قانون العقوبات الجزائري، وقد جاءت جريمة الابتزاز ضمن جنحة التشهير والمساومة ولم ينص القانون الجزائري على وضعية معينة للابتزاز أو طريقة ما وإنما تحقق الابتزاز في أي وسيلة ، كاف لإيقاع العقوبة.¹

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

ثانيا: العقوبات التكميلية

العقوبات التكميلية هي تلك العقوبات التي تصيب الجاني بناءً على الحكم بالعقوبة الأصلية وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءً على الحكم بالعقوبة الأصلية دون الحاجة لإصدار حكم تبعية فهو مرتبط ارتباطاً مباشراً ووثيق بالعقوبة الأصلية.

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

¹ حمدان مداح سيف الاسلام شوية، جريمة الابتزاز في المدينة الجديدة -دراسة ميدانية بمدينة الكاليتوسة عناية-، مجلة العلوم الاجتماعية والإنسانية، جامعة باتنة 1 املجد 22 ،العدد ،ديسمبر، 2021م، ص 131

² غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، ص215

- وقد تكون المصادرة عامة، أي أيلولة كل أموال المحكوم عليه وإضافتها إلى ملكية الدولة. وقد تكون المصادرة خاصة أي أيلولة مال من أموال المحكوم عليه وإضافتها إلى ملكية الدولة. ولقد جاءت المادة 394 مكرر 6 من قانون العقوبات الجزائري صريحة، على ما يلي:
- المصادرة للأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية؛
 - إغلاق المواقع التي تكون محلاً للجريمة؛
 - إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت يعلم مالكيها.¹

الفرع الثاني: الظروف المشددة والمعفية من العقاب لجريمة الابتزاز الإلكتروني

في التشريع الجزائري، تُعدّ الوسيلة الإلكترونية في حد ذاتها ظرفاً مشدداً لجريمة الابتزاز التقليدية، وتظهر الظروف المشددة التالية:

أولاً: الظروف المشددة للعقاب لجريمة الابتزاز الإلكتروني

هناك حالات تشدد فيها العقوبة في جريمة الابتزاز الإلكتروني وذلك حال تحقق شروط معينة ويقصد بالتشديد هنا أن يحكم القاضي بالحكم الأعلى للعقوبة المقدرة أو أن يحكم بكل العقوبتين الحبس والغرامة معاً.

والعلة في تشديد العقوبة فإذا ارتكبت الجريمة من خلال تنظيم إجرامي حيث استشعر المنظم خطورة الفعل على المجتمع ، وذلك من خلال ممارستها في إطار إجرامي منظم يؤدي إلى استفحال هذه الجريمة كما تشدد في حال ارتكبتها موظف عمومي ، فالمفروض أنه شخص مختار بعناية وفيه توضع ثقة الدولة فيجب أن يكون فوق كل شبهة كذلك إذا ارتبط الابتزاز الإلكتروني بالتهديد أو بالقتل وأن تقع الجريمة ضد فئة يحق حمايتهم جنائياً بقدر أكبر من الفئات الأخرى كما يعتبر موجبا لتشديد صدور أحكام محلية، أو أجنبية سابقة في حق المبتز في جرائم مماثلة ، ويبدو أن سبب التشديد هذا يرجع لنفس فكرة التشديد حال العودة والخطورة الإجرامية.

¹ حداد شيماء جبلي سعيدة، مرجع سابق، ص22

أما المادة 42 من ق ع تنص على انه تقضي المحكمة بإبعاد الأجنبي الذي حكم عليه بالإدانة لارتكاب أي جريمة من الجرائم المنصوصة عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها. فيتم إبعاد الأجنبي بعد تنفيذه العقوبة الأصلية.¹

ثانيا: الظروف المعفية من العقاب لجريمة الابتزاز الإلكتروني

إن الإعفاء من العقوبة ليس له عاقلة بالسياسة الجنائية أو عاقلة بالقواعد العامة للمسؤولية الجزائية المرتكب الجريمة.

1- عقوبة الشروع في جريمة الابتزاز الإلكتروني:

يقصد بالشروع البدء في التنفيذ في الجريمة التي يعقد الجاني العزم على ارتكابها ولكنه لا يصل إلى النتيجة التي يريد تحقيقها فهي جريمة ناقصة لعدم اكتمال النتيجة الإجرامية المرجوة.

وحسب القانون الجزائري يعاقب على الشروع في ارتكاب الجناة المنصوص عليها في المادة 303 مكرر بالعقوبات المقررة للجريمة التامة.²

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

2- عقوبة الاشتراك في جريمة الابتزاز عبر الوسائل الإلكترونية:

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

¹ آمال برحال ، المرجع السابق ، ص 31

² ق ع 15/04 سالف الذكر

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

وهذا ما نصت عليه المادة 42 من قانون العقوبات الجزائري " يعتبر شريكا في الجريمة من لم يشترك اشتراكاً مباشراً، ولكنه ساعد بكل الطرف أو علون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها من علمه بذلك..¹

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

كما تناول المشرع في المادة 394 مكرر 5 عقوبة الاشتراك في جريمة الابتزاز الإلكتروني وجاء في سندها كل من شارك في مجموعة أو اتفاق تالف بغرض الإعداد الجريمة أو هذا التحضير بعرض الإعداد الجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسداً بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.³

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

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

¹ ق ع 15/04 سالف الذكر

² قانون العقوبات الجزائري 15/04 سالف الذكر

³ ق ع الجزائري 15 /04 سالف الذكر

المطلب الثاني: قانون جرائم الاعلام والاتصال 09/04

قامت السلطات التشريعية في الجزائر مؤخرا، ولو بصورة جزئية بمعالجة نقص القوانين المتعلقة بالجرائم الإلكترونية القانون 09_04

وذلك تم من خلال إضافة مواد قانونية تعاقب الاعتداءات المتعلقة بالنظام المعلوماتي والمتمثلة في الجريمة الإلكترونية وذلك بموجب القانون 15/04 الذي تم إصداره في 10 نوفمبر 2004 والذي يتضمن تعديلات على قانون العقوبات.

ونجد أن المشرع الجزائري نص على تجريم الجريمة الإلكترونية في مختلف نصوص القانونية نذكر منها¹:

1-جريمة التوصل أو الدخول غير المصرح به نصت عليه المادة 394 مكرر من قانون العقوبات بقولها "يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . المادة 394 مكرر من قانون العقوبات²

وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله أو يحاول ذلك " المادة 394 مكرر

2- جريمة التزوير المعلوماتي : نص عليها المشرع في نص المادة 394 مكرر من قانون العقوبات

3-جريمة الاستيلاء على المعطيات: نصت عليها المادة 394 مكرر 2 بقولها "كل من يقوم عمدا وبطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو

¹ القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 غشت سنة 2009، ص 5.

² القانون 15/04 ق ع سالف لذكر

معالجة أو مراسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم المواد 394، 304 مكرر 1 و 2 م ع 15/04 الذي تم إصداره في 10 نوفمبر 2004¹ هذا القانون يعكس السياسة الجديدة للجزائر في مكافحة الجريمة المتعلقة بتكنولوجيا الإعلام والاتصال ويتضمن تدابير إجرائية أهمها:

- تعزيز صلاحيات أجهزة التحقيق؛
- إشراك المتعاملين التقنيين شركات الاتصالات و مقدمو خدمة الأنترنت؛
- تعزيز المساعدة القانونية والتعاون الدولي².

بالرجوع إلى القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 2 فقرة ب منه نجدها تنص على ما يلي: " يقصد في مفهوم هذا القانون بما يأتي³:

- منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"

نصت هذه المادة على الجرائم المرتكبة عبر منظومة معلوماتية أو نظام الاتصالات الإلكترونية وبما أن المادة تشمل كل الجرائم التي تقع باستخدام تكنولوجيا الإعلام والاتصال فإنها تحتوي على جريمة التهديد بواسطة منظومة معلوماتية)، فالنصوص التقليدية المتعلقة بجريمة التهديد التقليدية صالحة لتطبيقها على جريمة التهديد المرتكبة على مواقع التواصل الاجتماعي.

التهديد يؤثر على شخص المجني عليه فيلقي الخوف والرعب والاضطراب في نفسه مما يجعله غير قادر على القيام بأعماله المعتادة و هو واقع تحت الخوف والتهديد، كما هو ما يمس حقه في

¹ عناصر خيرة -رواج إلهام شهرة ، الجريمة الإلكترونية في ظل القانون 04/09 " بين الواقع والمأمول"، مجلة البحوث القانونية والاقتصادية المركز الجامعي الشريف بوشوشة - أفلو الجزائر، ص747

² " سويسري فتحة التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها" مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022، ص13

³ القانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر

أن يعيش حياته الطبيعية وهو متحرر من الضغوط النفسية والرهبة من أن يتعرض إلى أذى في نفسه أو ماله، أما التهديد الإلكتروني فهو يحصل باستعمال وسائل و وسائط الكترونية فهو عملية تهديد وترهيب الضحية بنشر صورته أو تسريب معلومات سرية تخصه مقابل دفعه إلى دفع مبلغا ماليا أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل، وعادة ما يتم تهديد الضحايا عن طريق وسائل التواصل الاجتماعي جريمة التهديد التقليدية لم تتغير من حيث الأركان في زمن المعلوماتية، فالمشرع لا يأبه بالوسيلة التي ترتكب بها الجريمة غالبا وإن كانت جريمة التهديد لها أساليب جديدة في مجال المعلوماتية، فغالبا ما يكون التهديد الواقع على الأشخاص مصحوبا بأمر أو الامتناع عنه يجعل المجني عليه يستجيب له وما كان ليستجيب في الأصل إن كانت إرادته حرة، وانتشار مواقع التواصل الاجتماعي وما تقدمه من سهولة التواصل مع الغير تعددت الجرائم على هذه المواقع كالدخول إلى حساب المجني عليه بطريقة غير مشروعة وأخذ أسراره و تهديده بها¹ و تجدر الإشارة إلى أن المشرع الجزائري قد صادق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 08 سبتمبر 2014 وقد جرمت هذه الاتفاقية المساس بالبرامج والأنظمة في المواد 7 و 8 و 9 منها.

بعد تفاقم الاعتداءات على معطيات الكمبيوتر نتيجة ضعف الحماية الفنية، تدخل المشرع الجزائري بموجب القانون رقم 09_04 الخاص بالقواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، إذ أجزت المادة 03 منه مراقبة الاتصالات الإلكترونية²، لكن هذه المراقبة ليست مطلقة؛ حيث قيدتها المادة 04 من نفس القانون حين حددت الحالات التي يلجأ فيها للمراقبة الإلكترونية مع الحصول على إذن مكتوب من السلطة القضائية، وحددت القانون السالف الذكر بعض القواعد الاجرائية كالتفتيش والحجز في المواد 05_06، كما قام هذا القانون بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال

¹ عكوش سبهام الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري مجلة السياسة العالمية، المجلد (6) العدد (1)، السنة (2022) ص 1300

² قانون 04/09 الخاص بالقواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها سالف الذكر

ومكافحته، وكذا تفعيل المراقبة عن بعد من خلال المساعدة القضائية الدولية بمساعدة الهيئة السالف الذكر ، في المواد 16_17_18 منه¹.

المبحث الثاني: إجراءات مكافحة جريمة الابتزاز الإلكتروني واطارها

المؤسسي

الجريمة الإلكترونية بوجه عام، والابتزاز الإلكتروني بوجه خاص، تمثل تحدياً استثنائياً أمام منظومة العدالة الجنائية الجزائرية، لا لجسامة أثرها على الأفراد والمجتمع فحسب، بل لطبيعتها التقنية الخاصة التي تجعلها جريمة عابرة للحدود، متجددة الأساليب، متلاشية الأدلة. فالمجرم الإلكتروني لا يترك بالضرورة أثراً مادياً مرئياً كما في الجرائم التقليدية، بل يختبئ خلف شاشات وشبكات وهويات مزيفة، مستغلاً ثغرات التقنية وضعف الوعي القانوني لدى ضحاياه. ود تم تقسيم المبحث الى مطلبين المطلب الاول: البحث والتحري في جرایم الابتزاز الإلكتروني أما المطلب الثاني بعنوان الاذار المؤسسي للوقاية من جريمة الابتزاز الإلكتروني.

المطلب الاول: البحث والتحري في جرایم الابتزاز الإلكتروني

جريمة الابتزاز الإلكتروني من أكثر من الجرائم التي تخضع للتحديات التي تواجهها اليوم العدالة في العصر الرقمي، ويرجع ذلك على تعقيداتها التي تتميز بالخفاء وعبورها للحدود الوطنية، ونرى أن خطورة هذه الجريمة تكمن في الأساليب والوسائل التي تطبق بواسطتها كل أشكال التهديدات والابتزازات، والنيل من الضحايا وتقييد حرياتهم الشخصية واخذ حقوقهم ونشر الرعب في أنفسهم، كل هذا ترى أن جهات التحقيق تسعى جاهدة لضبط وكشف غموض هذه الجريمة وملاساتها والتصدي لمرتكبيها وذلك بما يسمى التحقيق الذي نتناوله كفرع أول ثم إجراءات التحقيق المستحدثة كفرع ثان

الفرع الاول: التحقيق

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

أولاً: تحريك الدعوى العمومية.

¹ حنيشي حمزة ياسين توشوشاي إبراهيم مهدي ، مرجع سابق، ص 19.

رغم اختلاف الجرائم الإلكترونية بشكل عام عن الجرائم التقليدية، وهو ما يلقي بعبء على سلطات التحقيق، من ضرورة تطوير إجراءات التحقيق لكي تتناسب مع التحقيق في الجرائم الإلكترونية بصفة عامة، وفي الابتزاز الإلكتروني بصفة خاصة، فأیضا یظل نظام الإجراءات الجزائية في قواعد التحقيق هو السائد، مع ضرورة اعتبار الفوارق الموضوعية في التحقيق، حيث أن هناك صعوبات تثار أثناء التحقيق تنبع من طبيعة جريمة التهديد بالابتزاز الإلكتروني.¹

1- التبليغ. يعرف المبلغ هو ذلك الشخص الذي يقوم بالإخبار والتبليغ عن الواقعة، وقد يكون المبلغ ذاته المجني عليه الذي استهدفته الجريمة، وهو الذي تضرر من وقوعها وقد يكون الشخص المبلغ على صلة بأطرافها قد يكون صديقا أو قريبا أو جارا بل قد يكون محاميا، لأن أخذ أطرافها على انه في الحالة الأخيرة يتم اثبات الصلة بإثبات التوكيل ورقمه وجهه توثيقه، إذا تقدم المبلغ ببلاغ نيابة عن المجني عليه.²

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

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

- حفظ الرسائل والمحادثات المرسلة من طرف المبتز الذي تشتمل على صور وتهديدات.
- لقطات الشاشة مأخوذة من المحادثات أو الرسائل التهديدية.
- حفظ أسماء الحسابات أو أرقام الهواتف والروابط التي استعملها المبتز.

2 التحقيق والتحري:

تعد إجراءات التحقيق الخاصة أداة فعالة لمكافحة جريمة الابتزاز الإلكتروني، لكنها تبقى ذات طابع استثنائي يتطلب التزاما صارما بالشروط القانونية، حتى لا تتحول من وسيلة لحماية المجتمع إلى تهديد للحقوق والحريات الدستورية ومن هنا تظهر أهمية التكوين المستمر للقضاة وضباط

¹ عراب مريم، مرجع سابق/ ص 1215

² خالد ممدوح إبراهيم، من التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، مصر،

الشرطة القضائية في مجال التقنيات الحديثة والتحقيق الرقمي، بما يضمن حسن تطبيق النصوص القانونية وتحقيق العدالة الرقمية المنشودة.

أ- الأجهزة المكلفة بالبحث والتحري في جريمة الابتزاز الإلكتروني:

يناط بالبحث في جريمة الابتزاز الإلكتروني عدة جهات رسمية، تتكامل أدوارها وتتسق فيما بينها وفقا لما ينص عليه قانون الإجراءات الجزائية والقوانين ذات الصلة بمكافحة الجريمة الإلكترونية، وتأتي في مقدمة هذه الأجهزة:

ب- الشرطة القضائية المختصة في الجرائم: السيبرانية وهي مصالح تابعة للأمن الوطني والدرك الوطني، تضم وحدات تقنية متخصصة في ميدان مكافحة الجرائم المعلوماتية، وقد تم إنشاء فرق خاصة بمكافحة الجريمة السيبرانية على مستوى المديرات الولائية للأمن الوطني وتزويدها بوسائل رقمية حديثة، وخبرات بشرية مؤهلة في مجال تحليل الأدلة الرقمية، تتولى مهام التحري في الجرائم المرتكبة عبر وسائل الاتصال التكنولوجي، بما فيها الابتزاز الإلكتروني.

ج - فرقة مكافحة الجرائم المعلوماتية التابعة للدرك الوطني: والتي تتميز بكفاءات عالية في مجال تتبع الرقمي والتحقيق التقني، خاصة في المناطق غير الحضرية أو المعزولة، حيث تكون صلاحيات الدرك الوطني أوسع، وتتكفل هذه الفرق بتحليل البيانات الرقمية، والتنسيق مع مزودي خدمات الإنترنت لجمع المعطيات التقنية¹.

ثانيا: صعوبات الإثبات في جريمة الابتزاز الإلكتروني.

بعد الإثبات حجر الزاوية في العملية الجزائية إذ لا يمكن إقامة الدعوى الجنائية ومعاينة الجاني دون توفر أدلة قانونية تقطع بوقوع الجريمة ونسبتها إلى فاعلها، غير أن جريمة الابتزاز

¹ اعصام المكي، الإثبات الجنائي بالوسائل العلمية المدنية في التشريع الجزائري، النيل مذكرة الماستر،

قسم العلوم السياسية جامعة عبد الحب ابن باديس مستعالم، سنة 2016/2017 م 49

الإلكتروني باعتبارها من الجرائم المستحدثة والمعقدة تقنيا، تطرح إشكاليات عميقة في مجال الإثبات تختلف عن تلك المطروحة في الجرائم التقليدية و ذلك أن هذه الجريمة ترتكب في فضاء افتراضي يفتقر إلى الحدود المكانية الواضحة، وتتم غالبا من خلال وسائل إلكترونية يصعب تعقبها أو تتعرض للتلاشي السريع بفعل طبيعة البيانات الرقمية القابلة للتعديل أو الإخفاء، كما أنهم يستخدمون تقنيات متطورة كالتشفير وتزوير الهويات الرقمية والبرمجيات الخبيثة، ما يصعب على جهات التحقيق الوصول إلى أدلة مادية ملموسة يمكن البناء عليها في إسناد الاتهام.

1 - الصعوبات التقنية للإثبات :

تشكل الطبيعة التقنية للابتزاز الإلكتروني تحديا كبيرا أمام الأجهزة القضائية والأمنية، إذ يعتمدون على وسائل رقمية معقدة لتنفيذ الجريمة مثل استخدام تطبيقات المراسلة المشفرة وإخفاء الهوية عبر الشبكات الخاصة الافتراضية أو حتى ارتكاب الجريمة عبر خوادم موجودة في دول أجنبية كما أن طبيعة الأدلة الرقمية نفسها تطرح إشكالية فهي أدلة غير مادية قابلة للحذف أو التعديل أو التشفير، ما يجعل عملية جمعها وتوثيقها وتحليلها تتطلب خبرة تقنية عالية وأدوات متقدمة في مجال الجرائم المعلوماتية، وأي تقصير في التعامل معها تقنيا قد يؤدي إلى ضياعها أو فقدان قيمتها القضائية.

تتجلى الصعوبات التقنية في جريمة الابتزاز الإلكتروني في تعقيد طبيعة الجريمة ذاتها وارتباطها الوثيق بتكنولوجيا المعلومات والاتصال، حيث أصبحت هذه الجريمة تستند إلى أدوات تكنولوجية متطورة تصعب من عملية تتبع مصدرها أو التحقق من مصداقيتها و من بين هذه الصعوبات أن المجرمين غالبا ما يستعملون برامج لإخفاء الهوية، أو يمررون اتصالاتهم عبر سيرفرات موزعة في بلدان مختلفة، وهو ما يؤدي إلى تشتيت التحقيقات وتداخل الاختصاصات القضائية، ويعيق سرعة الوصول إلى الأدلة.

كما أن بعض حالات الابتزاز تستخدم فيها برمجيات انتحالي (Spoofing Software) فتظهر المبتز وكأنه جهة رسمية أو معروفة، وهو ما يربك الضحية ويؤثر على وضوح الوقائع أثناء التحقيق وفي كثير من الأحيان، تخزن الأدلة مثل الرسائل أو الصور أو تسجيلات الصوت على خدمات سحابية مشفرة (Cloud) Storage) تتطلب إذنا قضائيا للتفتيش الرقمي. وربما تحتاج إلى التعاون مع شركات أجنبية لا تلتزم بالضرورة بالقوانين الوطنية أو لا تملك تمثيلا قانونيا داخل الجزائر

2- المعاينة:

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

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

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

أ -مسرح تقليدي:

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

ب -مسرح افتراضي:

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

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

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

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

-ملاحظة واثبات حالة التوصيلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل حيث عرض الأمر على القضاء.

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

-التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة

ما قد يوجد من بصمات ويلاحظ أن الآثار المعلوماتية والرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة، والبريد الإلكتروني الفيديو الرقمي الصوت الرقمي، غرفة الدردشة المحادثات الملفات المخزنة في الكمبيوتر الصور المرئية.

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

3- . الشهادة

يجوز طبقا للمادة 88 من قانون الإجراءات الجزائية الجزائري لقاضي التحقيق سماع كل شخص يرى فائدة من سماع شهادته سواء كان شاهد نفي أو إثبات، ويعتبر أداء الشهادة إجراء من إجراءات التحقيق، ويقصد به الإدلاء بمعلومات تتعلق بالجريمة أمام سلطة التحقيق بالشروط التي حددها القانون، فهو إقرار من الشاهد بأمر رآه أو سمعه أو أدركه بأية حاسة من حواسه.

ولا نقل الشهادة أهمية في الجريمة الإلكترونية عن باقي الإجراءات في الحصول على الدليل الإلكتروني، فالقاعدة العامة تقتضي أن يلتزم الشاهد بالإفصاح بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها، والإدلاء بكل ما يكشف الحقيقة.

للمحقق في الجرائم المعلوماتية أن يسمع الشهود وهم الأشخاص الذين كانوا في مسرح الجريمة أو لديهم معلومات تقنية تنفيذ الكشف عن الجريمة، وغالبا ما يكون الشاهد المعلوماتي من أصحاب الخبرة والمتخصصون في مجال تكنولوجيا الإعلام والاتصال، والذين لهم المعرفة الكافية بنظام المعالجة الآلية للبيانات.

كما يوجد نوع آخر من الشهادة وهو الشهادة عبر الأنترنت وتفترض هذه النوعية من الشهادة حصولها في مرحلة التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضرا ماديا أو جسديا أمام المحكمة، وإنما يتم سماع شهادته عبر الأنترنت بشكل سمعي ومرئي، والشاهد هنا يبرز في هيئته الكاملة، فيبدو كما لو كان حاضرا حيث تظهر للمحكمة ردود أفعاله الطبيعية عندما توجه له الأسئلة، الأمر الذي يتيح للمحكمة تقدير قيمة هذه الشهادة 20.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات.

4- القرائن

القرينة مأخوذة من كلمة مقارنة وتعرف بأنها استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات، أي يقصد بها دلالة واقعة قام الدليل عليها على واقعة أخرى لم يقم عليها دليل بطريق الاستنتاج المنطقي، فالقرينة على هذا النحو تعتبر دليل إثبات غير مباشر وهي بذلك تتميز عن باقي الأدلة كالشهادة والاعتراف التي تعتبر أدلة مباشرة على الواقعة المراد إثباتها.

القاعدة أن القرائن والدلائل لا ترقى إلى مرتبة الأدلة ولا يجوز الاستناد إليها منفردة في الحكم إلا إلى جانب دليل أو أدلة متنوعة، فدورها هو تدعيم الأدلة التي طرحت

وتجدر الإشارة إلى أن الدليل الرقمي يعد من فئة القرائن القضائية التي يعود تقدير قيمتها إلى قاضي الموضوع فمعرفة عنوان الأنترنت الرقمي مثلا "IPadresse" يشير إلى الحاسوب الذي

ارتكبت بواسطته الجريمة فقط، ولا يؤدي إلى معرفة الفاعل بدقة، وذلك بخلاف الدليل العلمي الذي يحدد بصمة الأصبع مثلا وغيرها من الأدلة التي تشير إلى الفاعل الحقيقي بدقة متناهية¹.

ثالثا: التفتيش في البيئة الإلكترونية

يعتبر التفتيش الإلكتروني اجراء من الاجراءات التي تهدف إلى البحث عن ملابسات الجريمة، كما يعد من أهم وأخطر إجراءات تحقيق في جرائم المعلوماتية وذلك من خلال مساس بالحريات الخاصة للأفراد المكفولة دستوريا، ولقد من المشرع الجزائري جملة من التعديلات لمواجهة الجرائم المعلوماتية من خلال التفتيش والضبط.

التفتيش إجراء من اجراء تحقيق التي تستهدف البحث عن الحقيقة في مستودع السر لذلك يعتبر من اهم اجراءات التحقيق يكفي كشف الحقيقة، لأنه غالبا ما يفسر عن ادلة مادية تؤيد نسبة الجريمة إلى المتهم والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى ادلة مادية تسهم في بيان وظهور الحقيقة، ونتيجة لذلك بعد تفتيش نظام الحاسوب والانترنت من اخطر المراحل حال اتخاذ الاجراءات الجنائية ضد مرتكب الجريمة الإلكترونية، لكون محل التفتيش هنا وهو الحاسوب والشبكات محل جدل فقهي متزايد يوما بعد يوم.²

ثار خلاف فقهي بشأن جواز تفتيش المكونات المعنوية للحاسوب لأنه لا يحتوي على ماديات فمنهم من ذهب إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب، باعتباره وسيلة للإثبات المادي، بهدف ضبط أدلة مادية للكشف 225 عن الحقيقة، وهذا يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي .

أما فيما يخص مدى خضوع شبكات الحاسوب للتفتيش عن بعد، فبالرجوع لقانون الإجراءات الجزائية الجزائري فقد ورد نص على حالة وجود الحاسوب الثاني المتصل بالأول المراد تفتيشه موجود على التراب الجزائري، أجاز ذلك شرط أن يكون قد صدر أمر من وكيل الجمهورية أو

¹ عراب مريم مرجع سابق، ص 1221

² حداد شيماء جبلي سعيدة، مرجع سابق، ص33

قاضي التحقيق بتفتيش مفتوح يمتد على مستوى التراب الوطني بكامله طبقا للمادة 47 من قانون الإجراءات الجزائية في فقرتها الأخيرة.

لكن الإشكال يطرح هو عندما يكون الحاسوب المراد تفتيشه في دولة أخرى، لأن التفتيش هنا يتعارض مع تمسك كل دولة في سيادتها وحدودها الإقليمية، وهذا ما يواجه سلطات التحقيق من مشاكل الجمع الأدلة الإلكترونية.

ونتيجة لذلك أدخلت بعض الدول تعديلات في قانون الإجراءات الجزائية لتجيز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، ومن ذلك المشرع الجزائري الذي أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، حيث أجازت الفقرة 3 من المادة 5 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها لسنة 2009 الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.

الفرع الثاني: إجراءات التحقيق المستحدثة:

قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية الجديد 06-22 والقانون 09-04 ، وذلك لأن الإجراءات التقليدية لم تعد تسع الجرائم الإلكترونية التي تطورت وتناسى خطرها، ومن هذه الإجراءات التسرب الإلكتروني، إعتراض المراسلات وتسجيل الأصوات والنقاط الصور المراقبة الإلكترونية).

1- التسرب: نظمه المشرع الجزائري في ثمان مواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 حيث تناول مفهوم التسرب وشروط إجراءه وآثاره 250.

المادة 65 مكرر قيدت الجرائم المذكورة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

المادة 65 مكرر 11: إذا اقتضت ضروريات التحري أو التحقيق في إحدى الجرائم المنصوص عليها في المادة 65 مكرر 5 يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب".

تنص المادة 65 مكرر 12 التسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية لمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم".

تكون عملية التسرب في الجرائم الإلكترونية في ولوج ضابط الشرطة القضائية إلى العالم الافتراضي، ومشاركته في محادثات غرف الدردشة، أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات، أو انخراطه في نوادي الهاكر مستخدما إسمًا مستعارًا لاستدراجهم والكشف عن أعمالهم¹.

2- الاستجواب

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

ويقصد به أيضًا هو استجواب المتهم ومجاوبته بالأدلة المختلفة القائمة قبله ومناقشته فيها مناقشة تفصيلية كي يفقدها أو كان منكرا للتهمة أو يعترف إذا شاء الاعتراف بارتكاب الواقعة، فالاستجواب يحقق في المرحلة الأولى من التحقيق الابتدائي الغاية منه وهو جمع الأدلة لذا لا يجوز إجراء الاستجواب في مرحلة المحاكمة إلا إذا قبله المتهم هو محاميه والاستجواب لا يكون إلا بتوجيه التهمة ومناقشة المتهم تفصيليا عنها ومواجهته بالأدلة القائمة ضده لاستجواب بمجرد سؤال المتهم عما هو منسوب إليه وإحاطته².

3- الدليل الرقمي:

يعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات مغناطيسية أو نبضات كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا

¹ ميمونة ثامر، مرجع سابق، ص 65

² أيمن عبد الله فكري، الاستجواب الجنائي الإلكتروني، مجلة البحوث الفقهية والقانونية مجلة علمية محكمة، كلية الشريعة والقانون بدمنهور، ع الثالث والأربعون (2023)، ص 977

خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، ويتطلب البحث في ماهية الدليل الرقمي التعرض لتعريفه، ثم التعرف على حجبيته.

هناك عدة تعريفات للدليل الرقمي تباينت بين التوسع والتضييق، نذكر منها :
هو " أية بيانات مخزنة أو منقولة بواسطة الحاسوب، تدعم أية نظرية حول كيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة ".¹

وهو " المعلومات والبيانات ذات القيمة الاستقصائية والمخزنة أو المنقولة عبر جهاز إلكتروني "

ويعود السبب في تسميته بالدليل الرقمي، هو أن البيانات داخل العالم الافتراضي، بجميع صورها سواء أكانت صوراً أو تسجيلات أو نصوصاً، تأخذ شكل أرقام، ومن ثم يتم تحويل هذه الأرقام عند عرضها إلى صورة أو تسجيل أو نص.²

رغم تطور إجراءات الاستدلال والتحري والتحقيق في الجرائم الإلكترونية ومن ضمنها الابتزاز الإلكتروني، إلا أن هناك الكثير من المعوقات التي تمنع الحصول على أدلة رقمية قوية نظراً السهولة محو الأدلة التي تمكن من الاستدلال على هوية الجاني والتلاعب فيها، فهي جريمة هلامية تستوجب خبرة وتقنيات متطورة جداً، وتتمثل الصعوبات في:

محددات الخصوصية التي هي حقوق لصيقة بالشخصية محمية دستورياً، وأي انتهاك من أجل مقتضيات التحقيق يستوجب الإذن المسبب قانونياً.

ديناميكية هكذا نوع من الجرائم وتطوراتها السريعة بالموازاة مع جمود التشريعات وضعف خبرة موظفي تطبيق القوانين يصعب عمليات الحصول على الأدلة الرقمية.

تتازع القوانين والاختصاص مع عدم أو ضعف التنسيق بين الدول يعصّب عملية الحصول على الأدلة الرقمية من حيث الضبط والتفتيش، خصوصاً متى كانت عناصر جريمة الابتزاز الإلكتروني موزعة بين عدة دول.

سهولة محو الأدلة مما يحول دون تعقب الجناة، وذلك لتضليل الجهات الأمنية حيث يتم التلاعب في الأدلة ومسحها والعبث فيها للافلات من العقاب، خصوصاً في ظل احتراف الجناة لعمليات التشفير والترميز.

¹ عراب مريم مرجع سابق، ص 1222

² عراب مريم مرجع سابق، ص 1222

نقص الخبرة مما يؤثر على عملية التحقيق برمتها من حيث ضبط الأدلة حمايتها واحرازها حتى لا يتم إتلافها وضياعها، مثل إتلاف القرص الصلب أو الأقراص الممغنطة أو أوعية المعلومات التي تخزن فيها البيانات.¹

4- اعتراض المراسلات وتسجيل الأصوات والنقاط الصور (المراقبة الإلكترونية)

أورد المشرع الجزائري هذه الأساليب بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، والذي أفرد الفصل الرابع منه تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والنقاط الصور"، في المواد من 65 مكرر 5 إلى غاية 65 مكرر 10.

لم يعرف المشرع الجزائري المراقبة الإلكترونية لا في مواد قانون الإجراءات الجزائية ولا في القانون رقم 04/09 المتعلق بقواعد مكافحة جرائم تكنولوجيا الإعلام والاتصال والوقاية منها، وبالرجوع لتعريف الفقهاء فقد اختلفوا في ذلك، فذهب اتجاه للقول بأنها : " إجراء تحقيق مباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي الجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض".

واكتفى المشرع الجزائري بوضع تعريف للاتصالات الإلكترونية في الفصل الأول من القانون 04/09 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها وبالتحديد المادة 2 منه والتي نصت على: "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، وبالتالي فالمشرع الجزائري قد أعطى مفهوما واسعا للاتصالات الإلكترونية لتشمل كل اتصال يقوم به الشخص أيا كانت الوسيلة الإلكترونية المستعملة في ذلك.²

¹ فاطمة العرفي ، مرجع سابق، ص 503

² عراب مريم مرجع سابق، ص 1222

المطلب الثاني: الاطار المؤسسي للوقاية ومكافحة جريمة الابتزاز الالكتروني

يشمل الإطار المؤسسي للوقاية ومكافحة جريمة الابتزاز الإلكتروني مجموعة متكاملة من الهياكل القانونية، الأمنية، والتقنية التي تعمل على الحد من هذه الظاهرة، وحماية الأفراد والمؤسسات من تهديدات الفضاء الرقمي.

الفرع الاول: دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال ومكافحتها

من بين الآليات التي أوجدها المشرع الجزائري في مجال الوقاية والمكافحة من الجريمة المعلوماتية إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب القانون رقم 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص المادة 13 منه التي تنص على: "تتأه هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"¹

كما نصت المادة 14 من نفس القانون على مجموعة من المهام المسندة لهذه الهيئة:²

مهام الهيئة :

1 - الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم التجسس على الاتصالات

¹ القانون رقم 09/04 سالف الذكر

² القانون رقم 09/04 القانون نفسه

والرسائل الإلكترونية، التلاعب بحسابات العملاء أو ببطاقات إئتمانهم، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية... إلخ

من أجل القيام بمهامها فلها تركيز تحليل إستقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال والاتصال بكل من مصالح الأمن والدرك الوطنيين إدارات ومصالح الدولة المديریات العامة، وكذلك كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها.

2-تقديم المساعدة المصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية المديریات العامة المختلفة فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.

2 -مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بحسب نص المادة 14 من القانون 09/04 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 13 و 14 من القانون 09/04 تتعلق بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هذه الهيئة تتمثل في:

تنشيط وتنسيق عمليات الوقاية من الجرائم المعلوماتية ومكافحتها أي تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشاركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات بما في ذلك جمع المعلومات وإنجاز الخبرات القضائية.¹

¹ المرسوم رئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 40، الصادرة بتاريخ . (06 ص، 2020 يوليو 18

تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجده.

التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة المادة 4 فقرة 2 من القانون 09/04 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به¹

الفرع الثاني: دور هيئات الضبط الإلكتروني والشرطة القضائية المتخصصة.

تعد هيئات الضبط الإلكتروني من الفاعلين الأساسيين في المنظومة الوطنية لمكافحة الجرائم السيبرانية، خاصة جريمة الابتزاز الإلكتروني التي باتت من أبرز صور التعدي على الحياة الخاصة عبر الفضاء الرقمي، وتتمثل هذه الهيئات في الجزائر بوجه خاص في سلطة ضبط البريد والاتصالات الإلكترونية، وهي الهيئة التي أنشئت بموجب القانون رقم 04-18 المؤرخ في 10 ماي 2018 كلفت بمراقبة الأنشطة الرقمية وضمان احترام المتعاملين للضوابط القانونية والتقنية المتعلقة باستعمال الشبكات الإلكترونية، وتكمن أهمية هذه الهيئات في كونها تشكل صلة وصل بين التشريع والممارسة، حيث تسهر على تنفيذ القوانين المتعلقة بحماية البيانات، وتأمين البنى التحتية الرقمية، ومراقبة خدمات الإنترنت ومزوديه، بما يحد من استغلال الثغرات في الأنظمة الإلكترونية لتنفيذ عمليات الابتزاز أو التهديد أو الاختراق.

وتسند إلى هذه الهيئات جملة من المهام ذات طابع وقائي وتنظيمي، أبرزها ضبط سوق الاتصالات الإلكترونية، ومنح التراخيص للمتعاملين مع الالتزام بالشروط الأمنية، والزامهم بوضع وسائل حماية للبيانات الشخصية للمستخدمين، مثل التشفير، وسجلات التتبع، والتخزين الآمن، كما تقوم هذه الهيئات بالتنسيق مع السلطات القضائية والأمنية لتقديم المعلومات الفنية عند الضرورة، وتتدخل كذلك في متابعة الشكاوى المتعلقة بالممارسات غير المشروعة التي تتم عبر الشبكات، وهو ما يعد أداة فعالة في كشف ومعالجة محاولات الابتزاز قبل تفاقمها.

1 القانون رقم 09/04 سالف الذكر

علاوة على ذلك تلعب هيئات الضبط دورا مهما في الرقابة الاستباقية على المحتوى الرقمي إذ يمكنها مطالبة مزودي الخدمات بحجب أو إزالة المواقع والحسابات المشبوهة، أو التي ثبت تورطها في الابتزاز أو بث محتوى عثار أو تهديدي، كما تسهم هذه الهيئات في نشر الثقافة القانونية والتقنية لدى المستخدمين من خلال إعداد أدلة استخدام آمنة، وتنظيم دورات توعية بالتنسيق مع الجمعيات والمجتمع المدني مما يعزز من الوعي الرقمي ويدعم الوقاية المجتمعية.

الفرع الثالث: دور سلطة ضبط البريد والاتصالات الإلكترونية في الجزائر في الوقاية من جريمة الابتزاز الإلكتروني:

تعد سلطة ضبط البريد والاتصالات الإلكترونية في الجزائر من الهيئات التقنية ذات الطابع التنظيمي والرقابي التي تلعب دورا مركزيا في الوقاية من الجريمة السيبرانية عامة، وجريمة الابتزاز الإلكتروني بوجه خاص، وذلك في إطار تنفيذ أحكام القانون رقم 04-18 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنيط بهذه السلطة مهام تنظيم قطاع الاتصالات الإلكترونية وضمان سيره بانتظام، من خلال فرض الرقابة التقنية على الشبكات ومراقبة احترام المتعاملين للالتزامات الأمنية المفروضة عليهم، لاسيما ما يتعلق بسرية المراسلات الإلكترونية، وحماية بيانات المستخدمين، وتأمين قنوات الاتصال من الاختراق أو التلاعب، وبذلك فإن هذه الهيئة تساهم بشكل فعال في الحد من استغلال البنية التحتية الرقمية في ارتكاب جرائم الابتزاز، التي تعتمد غالبا على نشر محتوى خاص أو تهديد الضحية به عبر وسائط الاتصال¹.

وقد حولت القوانين الوطنية لهذه السلطة صلاحيات واسعة في مجال مراقبة مزودي خدمات الاتصالات والإنترنت، والزامهم باعتماد آليات تقنية متقدمة تكفل كشف محاولات التجسس أو التهديد أو الابتزاز، وتخزين البيانات الرقمية بطريقة تضمن تتبع المستخدمين في حال وقوع جريمة

¹ غزالي نور الهدى ، مرجع سابق، ص 72

كما تقوم السلطة بتحديد المعايير التقنية الواجب احترامها من قبل الشركات العاملة في القطاع، بما في ذلك الشروط المتعلقة بالأمن السيبراني، وتستطيع اتخاذ إجراءات تأديبية أو حتى تعليق أو سحب التراخيص في حالة الإخلال بالواجبات القانونية. وهذا البعد الرقابي يشكل خط الدفاع الأول ضد الجريمة الإلكترونية، من خلال الحيلولة دون إساءة استخدام الشبكات الوطنية.¹

الفرع الرابع التعاون الدولي في مواجهة الابتزاز الإلكتروني: تعتبر مشكلة الابتزاز

الإلكتروني قضية عالمية لا تتوقف عند حدود الدول، مما يستدعي التعاون الدولي لمكافحتها. لذا من المهم تبادل المعلومات بين الدول المختلفة وتعزيز التنسيق بين الأجهزة الأمنية لملاحقة المجرمين الإلكترونيين. ساهمت الاتفاقيات الدولية مثل "اتفاقية بودابست" بشأن الجرائم الإلكترونية في وضع إطار قانوني للتعاون بين الدول في مكافحة الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني

إن تعزيز التعاون بين الدول يتطلب تبادل الخبرات والأدوات التقنية المتقدمة للملاحقة المجرمين على الصعيدين الإقليمي والدولي، مما يمكن الدول من ملاحقة الجرائم عبر الحدود الإلكترونية وتقديم الجناة إلى العدالة بشكل فعال.

يعد الابتزاز الإلكتروني نموذجا للجريمة الإلكترونية التي تفرض تحديات أخلاقية معقدة على الأفراد والمجتمع. إذ تؤدي هذه الجريمة إلى انتهاك القيم الأخلاقية مثل الأمانة، الخصوصية، والاحترام، ما يساهم في زعزعة المنظومة الأخلاقية القائمة. فمع تزايد استخدام التكنولوجيا الرقمية، أصبحت فرص استغلال الأفراد عبر الإنترنت أكثر انتشاراً، مما يفرض تهديداً مباشراً على أخلاقيات التفاعل الرقمي، ويجعل من الضروري تعزيز الوعي الأخلاقي والأمني للحد من هذه الظواهر.²

¹ نفس المرجع، نفس الموضع.

² سامية حمريش صليحة رحالي الجريمة الإلكترونية وانعكاساتها على المنظومة الأخلاقية الابتزاز الإلكتروني - أنموذجا - مجلة الباحث للدراسات الأكاديمية، المجلد 12، العدد: 02 السنة: 2025، ص 378

خلاصة الفصل:

يعتمد المشرع الجزائري في مكافحة جريمة الابتزاز الإلكتروني على إطار قانوني مزدوج يجمع بين القواعد العامة في قانون العقوبات والقوانين الخاصة (الضبط الأدلة الرقمية، معزراً إياها بآليات مؤسسية كالشرطة السبرانية؛ الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال ومكافحتها بالإضافة إلى التعاون الدولي من خلال المواثيق الدولية الخاصة بهذا النوع من الجرائم، لضمان الوقاية والقمع الفعال لهذا التهديد العابر للحدود

خاتمة

خاتمة:

تصنف جريمة الابتزاز الإلكتروني كأحدى أبرز مظاهر الجرائم السيبرانية المستحدثة التي تخرج عن النمط التقليدي للجريمة، وفي سياق علم الجريمة تُدرج ضمن الجرائم الناعمة لكونها تعتمد على الإكراه النفسي والمعنوي بدلاً من العنف المادي ونظراً لأن هذه الجريمة تتشكل في بيئة افتراضية قائمة على الأنظمة الرقمية والبيانات المشفرة فإنها تفرض تحديات معقدة أمام جهات التحقيق الجنائي، لا سيما فيما يتعلق برصد الدليل الرقمي واستخلاصه والتعامل مع عقبات إثباته قانونياً.

وأمام هذه الثورة حاولت الدول تطوير تشريعاتها لتواكب هذا النوع من الجرائم المستحدثة، ثم تنبّهت الضرورة لإفراد نصوص تشريعية خاصة بهذه الجريمة الإلكترونية.

وبعد استكمال دراسة موضوع البحث المتمثل في جريمة الابتزاز الإلكتروني التي تناولنا من خلالها الإطار الموضوعي للجريمة الذي تحدث عن ماهية الابتزاز الإلكتروني وتجريمه كما تطرقنا إلى الجانب الإجرائي للجريمة موضوع البحث من خلال التطرق إلى التحقيق في الجريمة والإثبات فيها، نصل في الأخير إلى أهم النتائج و المقترحات.

النتائج:

– تصنف جريمة الابتزاز الإلكتروني بأنها من "الجرائم الناعمة" أو "جرائم الياقات البيضاء" لأنها تعتمد على الإكراه النفسي والمعنوي بدلاً من استخدام القوة البدنية أو الأسلحة التقليدية حيث يستغل الجاني البيانات أو الصور أو المعلومات السرية للضحية كأداة ضغط. ومع ذلك لم يتفق الفقهاء على تعريف جامع الجريمة الابتزاز الإلكتروني

- يعتبر مسرح ارتكاب الجريمة وهو الواقع الافتراضي لان أساس ارتكابها هو استخدام التكنولوجيا الحديثة المتمثلة في شبكة الانترنت ومواقع التواصل الاجتماعي. ويمكن أن تتم الجريمة والطرفان (الجاني والضحية) في قارتين مختلفتين، مما يلغي مفهوم مسرح الجريمة التقليدي.
- ما يميز هذه الجريمة سهولة ارتكابها من قبل الجاني كونها لا تتطلب جهد عضلي أو الانتقال إلى مكان الحادث؛
- تواجه أجهزة التحقيق الجنائي والقضائي تحديات كبرى حددتها الأبحاث الصادرة عن معاهد الأدلة الجنائية الدولية، ومن أبرزها سرعة التلاشي والتعديل: للدليل الرقمي - 5 صعوبة الإثبات الجنائي أي إثبات أن الدليل لم يتعرض للتعديل أو العبث منذ لحظة ضبطه وحتى تقديمه للمحكمة. تنازع الاختصاص القضائي الدولي :
- جريمة الابتزاز الإلكتروني لها خصوصية في التحقيق و تستلزم فريق عمل من المختصين أو المؤهلين الاستيعاب التطورات الحديثة في التحقيق مع مجرم ذكي له صفات تختلف عن صفات المجرم التقليدي؛
- غياب تنظيم قانوني خاص بالأدلة الرقمية في التشريع الجزائري رغم ما تشهده البيئة الافتراضية من سلوكيات إجرامية استفحلت بشكل غير مسبوق، ووجود فراغ تشريعي يعتري الدليل الرقمي وكيفية التعامل مع هذا النوع من الأدلة؛
- قصور نصوص التجريم في المنظومة القانونية الجزائرية في مجابهة واحتواء جريمة الابتزاز الإلكتروني في ظل غياب نص تشريعي واضح من منطلق مبدأ الشرعية الجزائية لتجريم مثل هاته النشاطات الإجرامية، وإحالة تحريمها إلى جريمة التهديد في صورتها التقليدية؛

- إحجام المجني عليه عن التبليغ واستخدام الجناة برامج إخفاء الهوية في جريمة الابتزاز الإلكتروني يعد من أهم التحديات التي تواجه الدليل الرقمي، وهو ما يساعد على ضياع هذا الأخير وإهداره.

المقترحات:

- ان التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية خاصة فيما يتعلق بجريمة الابتزاز الإلكتروني؛

- لابد من تعاون كل مؤسسات التعليم والتعلم العالي، و دور العبادة الإقامة دراسات وندوات حول مخاطر هذه الجريمة الدخيلة على المجتمعات العربية والإسلامية ؛

- اعتبار التهديد بإفشاء أمور خادشة للشرف وتوجيه عبارات فضائحية تمس سمعة الضحية جريمة ابتزاز، ويكفي للعقاب بموجبها أن يكون الجاني قد أعد رسالة التهديد لتصل إلى علم المراد تهديده سواء أرسلها إليه مباشرة أم أبلغ بها؛

- وجوب النص صراحة على تجريم الابتزاز الإلكتروني والذي يتضمن التهديد والمساومة بمنتوج رقمي للحصول على مزايا مادية أو معنوية أو جنسية. مع تشديد العقوبات أو اعتبار النت ظرف مشدد للعقوبة، لأن تطبيق القانون التقليدي غير كاف ودائما تكون عقوبته أخف.

أخذ تدابير الحيلة والحذر من خلال تقوية الحسابات الافتراضية عن طريق تفعيل إجراءات الخصوصية اختيار كلمات سرية قوية وتغييرها دوريا.

وخلاصة القول يُمثل الابتزاز الإلكتروني نمطاً جرمياً مستحدثاً يقع ضمن منظومة الجرائم المعلوماتية العابرة للحدود، ويُعرف فقهيًا بـ 'الجريمة الناعمة' لخلوه من مظاهر القوة البدنية. تنبثق هذه الجريمة من الفضاء الافتراضي المعقد برموزه وشيفراته، مما يضع أجهزة إنفاذ

القانون والتحقيق الجنائي أمام تحديات استثنائية؛ ترتبط أساسًا بطبيعة الدليل الرقمي وحجيته، والصعوبات التقنية والإجرائية التي تكتنف عملية ضبطه وصونه من التلشي.

قائمة المصادر والمراجع

أولاً: المصادر:

1. محمد بن مكرم بن منظور، المان العرب دار الصادرة بريت 2010، مج 5

ثانياً المراجع باللغة العربية

أ- الكتب

2. انور الدين زروقي الجريمة الإلكترونية في التشريع الجزائري الطبيعة والأركان والجزاءات دار العلوم للنشر والتوزيع 212 الجزائر، 2022،
3. بن زيطة عبد الهادي حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط1
4. حسني عبد الكريمي يونس، خليل يوسف جندي، الابتزاز الإلكتروني والجرائم الإلكترونية المفهوم واسباب، الطبعة الاولى، دار الكفاءة المعرفة، عمان، الاردن، سنة 2021،.
5. خالد ممدوح إبراهيم، من التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، مصر، 2009،
6. ربيعة خريس الجرائم الإلكترونية في التشريع الجزائري ، دراسة تحليلية مقارنة، دار هومة الجزائر، 2020،
7. سلامة عماد محمد الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج الجزء الأول، دار وائل للنشر الإسكندرية 2005
8. غنية باطللي، الجريمة الإلكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، دون مكان نشر دون تاريخ نشر
9. مروة صالح الدين محمد، الدليل الإلكتروني ومدى حجتيه في الإثبات الجنائي، الطبعة الاولى، المكتب العربي للمعارف، دار البحوث القانونية ، القاهرة، مصر، سنة 2021،
10. مصطفى محمد الرواشدة، جريمة الابتزاز الإلكتروني في القانون الأردني، ط1، مركز الكتاب الأكاديمي عمان 2020

ب- المذكرات ورسائل التخرج

11. اعصام المكي، الإثبات الجنائي بالوسائل العلمية المدينة في التشريع الجزائري، النيل مذكرة الماستر، قسم العلوم السياسية جامعة عبد الحب ابن باديس مستعالم، سنة 2016/2017

12. برحال امال، جريمة الابتزاز عبر الوسائل الإلكترونية، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة العربي التبسي، تبسة 2019 2020.
13. بن سليمان محمد الطاهر رسيوي رشيدة دراجي عز الدين ، جريمة الابتزاز الالكتروني مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر جامعة قاصدي مرباح - ورقلة، 2024/2023،
14. بوحفص راوية، الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملّة من متطلبات نيل شهادة الماستر في الحقوق، جامعة محمد خيضر - بسكرة -2018/2017
15. حداد شيماء جبلي سعيدة جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري مذكرة مكملّة لنيل شهادة الماستر المركز الجامعي عبد الحفيظ بوصوف ميلة، 2024/2023،
16. حنيشي حمزة ياسين توشوشاي إبراهيم مهدي ، آليات حماية الطفل من الابتزاز الالكتروني مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق جامعة غرداية كلية الحقوق والعلوم السياسية قسم الحقوق، 2024/2023،
17. غزالي نور الهدى، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني وفق التشريع الجزائري . مذكرة التخرج لنيل شهادة الماستر في الحقوق. جامعة عبد الحميد بن باديس - مستغانم، 2025/2024،
18. ميمونة ثامر، الآليات القانونية لحماية الأشخاص من جريمة الابتزاز الإلكتروني، مذكرة لنيل شهادة الماستر الأكاديمي في الحقوق ، جامعة غرداية، 2025/2024،

د - المجلات والدوريات

19. محسن عباس حميد، جريمة الابتزاز الإلكتروني مجلة القانون للدراسات والبحوث القانونية الاصدار 22، مجلد 23، .، جامعة دي قار، العراق، 2021،
20. حورية المتوكل، جريمة الابتزاز الإلكتروني، المجلة الإلكترونية للأبحاث القانونية ع (11) 2023،
21. عراب مريم جريمة التهديد والابتزاز الإلكتروني مجلة الدراسات القانونية المقارنة المجلد 07 العدد 01 (2021)،
22. بن عمر ياسين الابتزاز الالكتروني للأطفال في التشريع الجزائري دفاتر السياسة والقانون المجلد : 16 / العدد : 02 (2024)
23. فاطمة العرفي ، حجة الدليل الرقمي قي إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون، المجلد8، عدد خاص، 02 ، 2022،

24. دلال وردة ، جريمة التهديد أو نشر أو اذاعة صور خادشة التي تقع بين الخاطبين أو الزوجين المستحدثة بالقانون رقم 24/06 المعدل والمتمم لقانون ، العقوبات الجزائي، المجلة الأفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، ادرار - الجزائر المجلد: 09، العدد 02 السنة 2025،
25. بختي بوبكر النظام القانوني لبرامج الحاسب الآلي في التشريع الجزائري مجلة الأستاذ الباحث للدراسات القانونية والسياسية - المجلد 05 - العدد 02 - السنة 2020،
26. سامية بوشريط الابتزاز الإلكتروني كجريمة مستحدثة في القانون الجزائري دراسة تحليلية للمادة 303 مكرر 1 مجلة العلوم القانونية والسياسية، جامعة قسنطينة، العدد 10، 2022
27. عناصر خيرة -رواج إلهام شهرة ، الجريمة الالكترونية في ظل القانون 04/09 " بين الواقع والمأمول"، مجلة البحوث القانونية والاقتصادية المركز الجامعي الشريف بوشوشة - أفلو الجزائر،
28. عناصر خيرة -رواج إلهام شهرة ، الجريمة الالكترونية في ظل القانون 04/09 " بين الواقع والمأمول"، مجلة البحوث القانونية والاقتصادية المركز الجامعي الشريف بوشوشة - أفلو الجزائر،
29. عاشور أميل جبار المسؤولية الجنائية عن جريمة الابتزاز في مواقع التواصل الاجتماعي، (دراسة مقارنة)، مجلة أبحاث ميسان 124 م (السادس عشر)، ع (31) 2020،
30. أكرم ديب دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني، مجلة الحقوق والعلوم السياسية، (16)، ع (01) 404 2023،
31. حمدان مداح سيف الاسلام شوية، جريمة الابتزاز في المدينة الجديدة -دراسة ميدانية بمدينة الكاليتوسة عنابة-، مجلة العلوم الاجتماعية والإنسانية، جامعة باتنة 1 المجلد 22، العدد ،ديسمبر، 2021م،
32. عكوش سبهام الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري مجلة السياسة العالمية، المجلد (6) العدد (1)، السنة (2022)
33. ايمن عبد الله فكري، الاستجواب الجنائي الإلكتروني، مجلة البحوث الفقهية والقانونية مجلة علمية محكمة، كلية الشريعة والقانون بدمنهور، ع الثالث والأربعون) 2023،
34. سامية حمريش صليحة رحالي الجريمة الإلكترونية وانعكاساتها على المنظومة الأخلاقية الابتزاز الإلكتروني - أنموذجا - مجلة الباحث للدراسات الأكاديمية، المجلد 12، العدد: 02 السنة: 2025،

د- الندوات والأعمال الدراسية

35. بحوث ندوة الابتزاز المفهوم الأسباب العلاج ، مركز باحثات الدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية بجامعة الملك سعود الملك ، الرياض المملكة العربية السعودية ،

36. سويسبي فتيحة التكييف القانوني لجرائم المعلوماتية والإشكالات العملية المترتبة عنها" مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية بتاريخ 18 جانفي 2022،

ج-القوانين والمراسيم

37. القانون رقم 04-09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 غشت سنة 2009، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 غشت سنة 2009،

38. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات المؤرخ في 06/06/1966، جريدة الرسمية عدد 71 المؤرخ في 10/11/2004.

39. لقانون رقم 04-09 المؤرخ في 5 أغسطس 2009، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة بتاريخ 16 غشت 2009.

40. المرسوم رئاسي رقم 20-183 المؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، عدد 40، الصادرة بتاريخ . (06 ص، 2020 يوليو 18

41. الأمر رقم 03-05 مؤرخ في جمادى الأولى 1424 الموافق 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر عدد 44 المؤرخة في 23 يوليو 2003

ه مواقع الانترنت

42. نورة طاع الله ، جريمة الإبتزاز الإلكتروني في القانون الجزائري، كيان اللا رواية للنشر الالكتروني، متاح على الرابط <https://larewaia.blogspot.com/?m=1> تاريخ الاطلاع/ 2026/05/02، سا 01:20

43. مقال بعنوان : الابتزاز والتشهير الإلكتروني وعقوبته في القانون الجزائري: جريدة العالم اليوم ، العدد 2590، الصادر بتاريخ 2026/05/08، نسخة الكترونية متاح على الرابط <https://www.elalem-elidara.dz/?p=54676> تاريخ الاطلاع: 2026/05/09، سا 14:32

فهرس المحتويات

الصفحة	العنوان
	شكر وعرفان
	إهداء
	قائمة المختصرات
أ-هـ	مقدمة
الفصل الأول: ماهية السب في الشريعة الإسلامية والقانون الوضعي	
7	تمهيد
8	المبحث الأول: ماهية الابتزاز الالكتروني
8	المطلب الأول: مفهوم الابتزاز الالكتروني
8	الفرع الأول: تعريف الابتزاز الالكتروني
8	أولاً: التعريف اللغوي
9	ثانياً: التعريف الاصطلاحي.
12	الفرع الثاني: تمييز الابتزاز الالكتروني عن الجرائم المشابهة له
13	أولاً - التهديد التقليدي و التهديد الالكتروني
14	ثانياً - جريمة الابتزاز وجرائم المساس بالحياة الخاصة
14	المطلب الثاني: الخطورة الاجرامية للابتزاز الالكتروني
16	المبحث الثاني: صور واركاز للابتزاز الالكتروني
16	المطلب الأول: صور الابتزاز الالكتروني ووسائله

16	الفرع الأول: صور الابتزاز الالكتروني
17	أولا من حيث المنفعة
18	ثانيا: صور الابتزاز الالكتروني من حث الهدف
20	الفرع الثاني: وسائل الابتزاز الالكتروني
21	أولا: الحاسب الآلي
21	ثانيا : برامج الحاسب الآلي.
21	ثالثا: الأنترنت:
22	المطلب الثاني: اركان جريمه الابتزاز الالكتروني في التشريع الجزائري
23	الفرع الأول: الركن المادي لجريمة الإبتزاز الإلكتروني
27	الفرع الثاني: الركن المعنوي لجريمة الإبتزاز الإلكتروني
29	الفرع الثالث: الركن الشرعي لجريمة الإبتزاز الإلكتروني
30	خلاصة الفصل
الفصل الثاني: إجراءات وآليات مكافحة لجريمة الإبتزاز الإلكتروني في التشريع الجزائري	
34	المبحث الاول: التكيف القانوني للابتزاز الالكتروني في القانون الجزائري
34	المطلب الاول: الابتزاز الالكتروني في قانون العقوبات
35	الفرع الأول: العقوبات المقررة
35	أولا: العقوبات الاصلية

36	ثانيا: العقوبات التكميلية
37	الفرع الثاني: الظروف المشددة والمعفية من العقاب لجريمة الإبتزاز الإلكتروني
37	أولا: الظروف المشددة للعقاب لجريمة الإبتزاز الإلكتروني
38	ثانيا: الظروف المعفية من العقاب لجريمة الإبتزاز الإلكتروني
40	المطلب الثاني: قانون جرائم الاعلام والاتصال 09/04
43	المبحث الثاني: اجراءات مكافحة جريمة الابتزاز الالكتروني واطارها المؤسسي
43	المطلب الاول: البحث والتحري في جرائم الابتزاز الالكتروني
43	الفرع الاول: التحقيق
43	أولا: تحريك الدعوى العمومية.
45	ثانيا: صعوبات الاثبات في جريمة الابتزاز الالكتروني.
50	ثالثا: التفتيش في البيئة الإلكترونية
51	الفرع الثاني: إجراءات التحقيق المستحدثة
55	المطلب الثاني: الاطار المؤسسي للوقاية ومكافحة جريمة الابتزاز الالكتروني
55	الفرع الاول: دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال ومكافحتها
57	الفرع الثاني: دور هيئات الضبط الإلكتروني والشرطة القضائية

فهرس المحتويات

	المتخصصة.
58	الفرع الثالث: دور سلطة ضبط البريد والاتصالات الإلكترونية في الجزائر في الوقاية من جريمة الابتزاز الإلكتروني
58	خلاصة الفصل
62	خاتمة
66	قائمة المراجع
	فهرس محتويات

ملخص

ملخص:

تتناول هذه الدراسة موضوع "جريمة الابتزاز الإلكتروني في التشريع الجزائري" باعتبارها واحدة من أخطر الجرائم المستحدثة التي أفرزتها الثورة التكنولوجية المعاصرة. تهدف الدراسة إلى تفكيك الإطار المفاهيمي والقانوني لهذه الجريمة، مع بيان آليات مكافحتها على الصعيدين الإجرائي والمؤسسي في الجزائر.

وقد تم تقسيم البحث إلى فصلين رئيسيين؛ خُصص الفصل الأول للبحث في ماهية الابتزاز الإلكتروني وتمييزه عن الجرائم اللصيقة، بالإضافة إلى تبيان خطورته الإجرامية وصوره ووسائله التقنية. كما ركز هذا الفصل على تشريح الأركان القانونية للجريمة (الركن المادي، المعنوي، والشرعي) وفقاً للتشريع الجزائري.

بينما استعرض الفصل الثاني إجراءات وآليات مكافحة الابتزاز الإلكتروني، بدءاً بالتكييف القانوني في قانون العقوبات والقانون رقم 09/04 المتعلق بجرائم الإعلام والاتصال، مروراً بالعقوبات الأصلية والتكميلية والظروف المشددة والمعفية. واختتمت الدراسة بالبحث في الوسائل الإجرائية المستحدثة للتحري والتفتيش في البيئة الإلكترونية، مع تسليط الضوء على الدور المؤسسي للهيئات المتخصصة كالهيئة الوطنية للوقاية من جرائم الإعلام والاتصال، وسلطة ضبط البريد والاتصالات الإلكترونية، والشرطة القضائية المتخصصة.

الكلمات المفتاحية: ابتزاز الكتروني، جرائم الاتصال، تشريع جزائري ، قانون العقوبات، وسائل الكترونية

. Abstract :

This study addresses the topic of "The Crime of Electronic Extortion (Cyber-extortion) in Algerian Legislation," considering it one of the most dangerous contemporary crimes emerging from the modern technological revolution. The study aims to deconstruct the conceptual and legal framework of this crime, while highlighting the mechanisms for combating it on both procedural and institutional levels in Algeria.

The research is divided into two main chapters. The first chapter is dedicated to examining the nature of electronic extortion and distinguishing it from closely related crimes, in addition to demonstrating its criminal gravity, forms, and technical means. This chapter also focuses on analyzing the legal elements of the crime (the material element, the mental element, and the statutory element) in accordance with Algerian legislation.

Meanwhile, the second chapter reviews the procedures and mechanisms for combating electronic extortion, starting with its legal characterization in the Penal Code and Law No. 04-09 related to information and communication crimes, through the primary and complementary penalties, as well as aggravating and exempting circumstances. The study concludes by exploring the newly developed procedural means for investigation and search within the electronic environment, while highlighting the institutional role of specialized bodies, such as the National Authority for the Prevention and Combating of Information and Communication Crimes, the Post and Electronic Communications Regulatory Authority, and the specialized judicial police.

Keywords : Electronic Extortion -Communication Crimes - Algerian Legislation - Penal Code - Electronic Means.

Résumé :

Cette étude porte sur le délit d'extorsion électronique (cyber-extorsion) dans la législation algérienne, le considérant comme l'un des crimes contemporains les plus dangereux issus de la révolution technologique moderne. Elle vise à déconstruire le cadre conceptuel et juridique de ce délit, tout en mettant en lumière les mécanismes de lutte contre celui-ci aux niveaux procédural et institutionnel en Algérie.

La recherche est divisée en deux chapitres principaux. Le premier chapitre est consacré à l'examen de la nature de l'extorsion électronique et à sa distinction par rapport aux infractions apparentées, ainsi qu'à la démonstration de sa gravité, de ses formes et de ses moyens techniques. Ce chapitre analyse également les éléments constitutifs de l'infraction (l'élément matériel, l'élément moral et l'élément légal) conformément à la législation algérienne.

Le second chapitre examine les procédures et les mécanismes de lutte contre l'extorsion électronique, en commençant par sa qualification juridique dans le Code pénal et la loi n° 04-09 relative aux infractions liées à l'information et à la communication, en passant par les peines principales et complémentaires, ainsi que les circonstances aggravantes et atténuantes. L'étude conclut en explorant les nouveaux moyens procéduraux d'enquête et de recherche en milieu électronique, tout en soulignant le rôle institutionnel d'organismes spécialisés, tels que l'Autorité nationale de prévention et de lutte contre la criminalité de l'information et de la communication, l'Autorité de régulation des postes et des communications électroniques et la police judiciaire spécialisée.

Mots-clés : Extorsion électronique – Infractions de la communication – Législation algérienne – Code pénal – Moyens électroniques.