جامعة عين تموشنت _بلحاج بوشعيب_

كلية الحقوق

قسم الحقوق

جريمة الابتزاز في ظل التحول الرقمي

مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص _قانون خاص_

من اعداد الطالبتين:

- بوعقلش سندس براءة
- بوجمعي خديجة

تحت اشراف:

- الأستاذة عنتر اسماء

لجنة المناقشة:

أ.د شيخ نسيمة... أستاذة... جامعة عين تموشنت... رئيسا

د. عنتر أسماء... أستاذة محاضرة ب... جامعة عين تموشنت... مشرفا

د. خرشي عثمان... أستاذ محاضر أ... جامعة عين تموشنت... مناقشا

السنة الجامعية: 2025_2026


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبفضله وتوفيقه تذلل الصعاب، والصلاة والسلام على نبي الهدى ورسول الرحمة.

يخالجنا شعور بالفخر والاعتزاز ونحن نخط بكلمات الشكر والتقدير أسمى عبارات الامتنان إلى كل من أضاء لنا طريق العلم والبحث، ونخص بالذكر

أستاذتنا المشرفة الفاضلة الدكتورة "عنتر أسماء"، التي لم تبخل علينا بنصائحها التوجيهية القيمة، وصبرها، وسعة صدرها طيلة فترة إعداد هذه المذكرة.

كما نتوجه بجزيل الشكر وعظيم الامتنـان إلى السادة الأفاضل أعضاء لجنة المناقشة الموقرة، لقَبولهم تقييم هذا العمل المتواضع وإثرائه بملاحظاتهم السديدة والقيمة.

ولا يفوتنا أن نتقدم بالشكر الجزيل إلى كل أساتذتنا الكرام في الكلية الذين نهلنا من بحر علمهم، وإلى كل من مد لنا يد العون والمساعدة من قريب أو بعيد لإنجاز هذا البحث المتواضع

الاهداء

بوعقلش سندس براءة

الى من تشرق الأرض بنور وجههما، إلى نبع العطاء ومصدر فخري وإلهامي في هذه الحياة ..**والداي الكريمين**، حفظهما الله وأطال في عمرهما جزاءً لما قدماه لي من دعوات ودعم لا ينقطع.

إلى السند والدفء الذي يحيط بي، إلى **ابنت خالتي الغالية وزوجها الكريم**، الذين فتحوا لي قلبهما وبيتهما، وكانوا لي نعم العون والملاذ، ووفروا لي كل سبل الراحة والطمأنينة لأركز في دراستي وأصل إلى هذا اليوم.

إلى من بهم تزداد الحياة وتكتمل الفرحة، إخوتي وأخواتي الأعزاء :**رؤى، ضياء، وبهاء**، رفقاء الدرب والقلب.

إلى مهجتيّ هذا البيت وأمل الغد، إخوتي الروحيين الأقرب إلى قلبي **أماني وجواد**، الذين أضافوا لرحلتي بهجة وسروراً

إلى زميلتي الوفية في هذا الدرب **خديجة**، وإلى كل أصدقائي وصديقاتي بالخصوص **شيماء** وكل من يسكن قلبي .

أهديكم ثمرة جهدي وتخرجي.

الاهداء

بوجمعى خديجة

إلى الأعظم مقاماً في حياتي، من كان دعاؤهما سر توفيقي، وسندهما وقود كفاحي **..والداي العزيزين**، حفظهما الله ورعاهما.

الى اخوتي الأعزاء كل **من لؤي، نور الدين ، يقين و مجيد**.

إلى شريك حياتي ورفيق دربي، **زوجي الغالي**، الذي شاركني رحلة الطموح، وتحمل معي عناء السهر، وكان لي نعم السند والمشجع في كل خطوة خطوتها نحو النجاح.

وإلى رفيقة هذا الإنجاز وزميلتي الغالية **براءة**، وكل من أحبهم في الله.

أهديكم جميعاً ثمرة هذا النجاح والتفوق.

قائمة اهم المختصرات:

المختصر	الدلالة باللغة العربية
ق.ع	قانون العقوبات الجزائري
ق.إ.ج	قانون الإجراءات الجزائية الجزائري
إ.ج	إجراءات جزائية
م	مادة
ف	فقرة
ط	طبعة
ص	صفحة
د.ط	دون طبعة

مـــــقـــــدمـــــــة

مقدمة

يشهد المجتمع الدولي المعاصر طفرة تكنولوجية متسارعة أحدثت تحولاً جذرياً في بنيته الهيكلية، حيث نقلت الأنماط السلوكية والتعاملات البشرية من الحيز المادي التقليدي إلى فضاء سيبراني افتراضي عابر للحدود ومتحلل من قيود الزمان والمكان. وإذا كان هذا "التحول الرقمي" قد رفد الإنسانية بمزايا تنموية جليلة، إلا أنه أفرز في المقابل وجهاً مظلماً تمثل في بروز "الجريمة المعلوماتية المستحدثة"، وتتصدر **"جريمة الابتزاز الإلكتروني"** مشهد الإجرام المعاصر كإحدى أعقد المعضلات القانونية والتقنية؛ إذ تتمثل في قيام الجاني باستخدام الوسائط الرقمية والبرمجيات المتطورة كوسيلة للضغط النفسي والوعيد الموجه للضحية بقصد سلب إرادتها، وانتهاك حرمة حياتها الخاصة، أو استهداف ذمتها المالية تحت وطأة التهديد بنشر صور أو بيانات أو معلومات سرية.

إن جذور جريمة الابتزاز كفعل جرمي تمتد عميقاً في التاريخ التشريعي، حيث عرفتها القوانين الكلاسيكية كصورة من صور التهديد المصحوب بأمر السلب، وهو ما نظمه المشرع الجزائري تقليدياً في قانون العقوبات عبر أحكام جريمة التهديد. ومع مطلع الألفية الثالثة وتغلغل شبكة الإنترنت، شهدت هذه الجريمة قفزة نوعية؛ فتحولت من أسلوبها المادي التقليدي (الرسائل الورقية أو الاتصالات الهاتفية) إلى "الابتزاز السيبراني" بالتزامن مع ظهور وسائل التواصل الاجتماعي وتطبيقات المراسلة الفورية، مما دفع المشرع الجزائري إلى التدخل لمواكبة هذا التطور عبر تعديل قانون العقوبات بموجب القانون رقم 04-15 لحماية المعطيات والأنظمة الآلية، ثم تعزيز المنظومة الإجرائية بموجب القانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تكتسي هذه الدراسة أهمية بالغة تتبلور في شقين متكاملين:

- **الشق العلمي (النظري):** يكمن في رصد وتحليل التكييف القانوني والشرعي الذي أضفاه المشرع الجزائري على جريمة الابتزاز الرقمي، ومدى قدرة الموازنة التشريعية بين النصوص الكلاسيكية والنصوص المستحدثة لمجابهة السيولة التقنية للجريمة.
- **الشق العملي (التطبيقي الميداني):** ينبع من التنامي المطرد لمعدلات الجريمة في الواقع الجزائري، وظهور أنماط سلوكية خطيرة كاستدراج القُصّر عبر الألعاب الإلكترونية، واصطياد الحسابات المالية لمستخدمي تطبيق "بريدي موب"؛ وهو ما استدعى تدعيم هذه المذكرة بدراسة ميدانية تمثلت في **"استبيان إلكتروني"** وُجه لعينة من المجتمع للوقوف على المؤشرات الديموغرافية والتقنية الحقيقية للضحايا.

في ظل التحول الرقمي المتسارع، باتت جريمة الابتزاز الإلكتروني تُشكّل تهديداً حقيقياً للأمن الفردي والمجتمعي.

ومن هنا تبرز الإشكالية المحورية: كيف يواجه القانون الجزائري جريمة الابتزاز في بُعدها الرقمي؟

يتحدد نطاق هذا البحث موضوعياً بدراسة جريمة الابتزاز في شقها الإلكتروني الرقمي دون التطرق المفصل للابتزاز التقليدي إلا في حدود المقارنة الإيضاحية، كما يتحدد إقليمياً بالتركيز على المنظومة التشريعية والممارسات الإجرائية والقضائية في الجمهورية الجزائرية الديمقراطية الشعبية، مستهدفاً الفضاء الافتراضي والوسائط الرقمية الشائعة في المجتمع الجزائري حالياً.

اطلعنا على جملة من الدراسات الأكاديمية المقارنة والوطنية التي قاربت الموضوع، ومنها: دراسات ركزت على الجانب الموضوعي البحت لجرائم التهديد عبر الإنترنت، ودراسات أخرى ركزت على الأمن السيبراني وحماية المعطيات الشخصية بشكل عام. وتتميز دراستنا الحالية عن الدراسات السابقة بأنها لم تكتفِ بالتحليل النظري الجامد للنصوص القانونية، بل زاوجت بين الآليات الإجرائية المستحدثة (كالتحري الرقمي) ودراسة إحصائية ميدانية حية (الاستبيان) تسلط الضوء على واقع الجريمة المعاصر في البيئة الجزائرية.

يسعى هذا البحث إلى تحقيق جملة من الأهداف الأساسية:

- تبيان مدى مرونة واستيعاب القواعد الجنائية الموضوعية في الجزائر للأشكال المستحدثة للابتزاز الرقمي.
- تقييم كفاءة الصلاحيات الاستثنائية الممنوحة للضبطية القضائية في تتبع الأدلة الرقمية السائلة وسريعة المحو.

- استقراء المؤشرات الواقعية من خلال الاستبيان الميداني لتقديم توصيات وحلول تشريعية وتقنية عملية تساهم في وقاية المجتمع والضحايا من الوقوع في شرك المبتزين.

واجهت إعداد هذه المذكرة مجموعة من العقبات والصعوبات، أبرزها:

- الطبيعة الافتراضية واللامادية للجريمة مما يجعل رصد الأدلة وحصرها أمراً معقداً تقنياً.
- الطابع السري للجريمة وعزوف الكثير من الضحايا (خاصة النساء) عن التبليغ خوفاً من الفضيحة الاجتماعية، مما شكل تحدياً في جمع بعض البيانات الميدانية قبل التغلب عليه بالاستبيان الإلكتروني حامي الهوية.
- التسارع التقني الهائل الذي يجعل النصوص القانونية دائماً في حالة ملاحقة مستمرة ومجهدة للأساليب الجرمية المستحدثة كالذكاء الاصطناعي.

لمعالجة الإشكالية المطروحة، تم الاعتماد على **المنهج الوصفي التحليلي** لتفكيك النصوص القانونية المؤطرة للجريمة وإجراءاتها وتحليل معطيات الواقع، كما تم توظيف المنهج الميداني، **"الاستبيان" كأداة بحثية أساسية في الدراسة الميدانية**، حيث خضعت بيانات عينة الدراسة للتحليل الإحصائي المستفيض لصياغة مؤشرات كمية ونوعية تدعم المقاربة القانونية.

بناءً على مقتضيات الخطة المنهجية المعتمدة، تم تقسيم هذا البحث إلى فصلين رئيسيين:

- **الفصل الأول:** الإطار الموضوعي والإجرائي لجريمة الابتزاز الإلكتروني.
- **الفصل الثاني:** انعكاسات التحول الرقمي على جريمة الابتزاز الالكتروني.

الفصـــــــــل الأول

الاطـــــــار الموضوعي والاجـرائي لجريمة الابتزاز الالكتروني

تمهيد:

إن دراسة جريمة الابتزاز في بيئتها الرقمية المستحدثة تقتضي أولاً تفكيك معالمها المفاهيمية ورصد طبيعتها القانونية؛ بالنظر إلى أن الفضاء الافتراضي أضفى عليها أبعاداً مغايرة للجريمة التقليدية. ولما كان القانون الجنائي محكوماً بمبدأ الشرعية الصارم، فإن الإحاطة بهذه الظاهرة تستوجب تحديد تعريفها القانوني والتقني، واستظهار خصائصها الذاتية، ورصد أنواعها المتعددة، وصولاً إلى تبيان أركانها الجرمية (الشرعية، المادية، والمعنوية) التي استند إليها المشرع الجزائري لتجريم هذا السلوك.

ولا تكتمل الحماية القانونية للأفراد بمجرد التجريم الموضوعي، بل يتوقف أثرها على فاعلية المنظومة الإجرائية؛ بدءاً من آليات البحث والتحري الرقمي المعقدة التي تباشرها الضبطية القضائية، ووصولاً إلى حيازة الدليل الإلكتروني وتقييم حجيته ومدى مشروعيته أمام القضاء الجزائي.

وبناءً على ذلك، يسعى هذا الفصل إلى تشريح الإطارين الموضوعي والإجرائي لجريمة الابتزاز الإلكتروني، من خلال المخطط التالي:

- **المبحث الأول :**الإطار المفاهيمي والموضوعي لجريمة الابتزاز الإلكتروني (التعريف، الخصائص، الأنواع، والأركان).
- **المبحث الثاني :**الإطار الإجرائي لجريمة الابتزاز الإلكتروني وآليات إثباتها

المبحث الاول: ماهية الابتزاز واركانه

تعد جريمة الابتزاز الإلكتروني من أخطر الظواهر الإجرامية المستحدثة التي أفرزتها الثورة التكنولوجية، فهي لم تعد مجرد سلوك عدواني تقليدي، بل تحولت إلى معضلة قانونية وتقنية تتجاوز الحدود الجغرافية لتمس صلب الحياة الخاصة والذمة المالية للأفراد والكيانات. وللإحاطة بهذه الجريمة من كافة جوانبها، يقتضي الأمر أولاً سبر أغوار ماهيتها؛ وذلك من خلال تتبع جذورها اللغوية وتأصيلها الاصطلاحي، واستعراض كيفيات تناولها في الفقه القانوني والتشريعات المعاصرة التي حاولت وضع إطار جامع لتعريفها.

ولا تكتمل صورة هذه الماهية إلا بالوقوف على أنواع الابتزاز وتعدد أشكاله، واستخلاص الخصائص الجوهرية التي تمنحه طابعاً فريداً يميزه عن غيره من الأنماط الإجرامية، مع ضرورة رسم الحدود الفاصلة بينه وبين الجرائم المشابهة التي قد تلتبس معه في الوسيلة أو الغاية.

وبناءً على هذا التصور المفاهيمي، ننتقل في الشق الثاني من الدراسة إلى الجانب الهيكلي للجريمة عبر تحليل أركانها القانونية؛ بدءاً من الركن الشرعي الذي يمثل الغطاء القانوني للتجريم، مروراً بالركن المادي الذي يجسد السلوك الإجرامي المتمثل في التهديد والطلب، وصولاً إلى الركن المعنوي القائم على القصد الجنائي لدى الجاني، وذلك وفق التفصيل الذي سنعرضه في المطالب التالية.

المطلب الأول: مفهوم الابتزاز

يمكن تعريف الابتزاز بأنه زرع الخوف في النفس أو ذلك الفعل الذي يقوم به شخص بإنذار آخر بوعيده بالنشر، وهذا بالضغط على إرادة الشخص من ضرر سيلحقه به او سيلحق أشخاصاً أو أشياء له بها صلة أو بعبارة أخرى كل ضرراً سيتلقاه بشخصه او بماله أو بشخص أو مال غيره وهذا الإنذار سواء كان شفهياً او كتابياً او باي عبارة او شكل يمكن ان يزرع الرهبة في نفس الشخص المجني عليه والرعب او بمجرد ازعاجه وتخويفه من امر سيمس شخصه وماله.[1]

عموما يمكن تعريف الابتزاز بانه كل فعل غير مشروع يرمي الى منفعة غير مشروعة باي وسيلة كانت بحيث يطلب الجاني من المجني عليه او الشخص المبتز مبالغ مالية مقابل عدم نشر صور او محادثات سواء مرئية او صوتية كانت او رسائل كما يمكن ان يكون الابتزاز عبارة عن تهديد بسلب حياة شخص ما يعني للمجني عليه او ان يكون عبارة عن طلب الجاني للمجني اذ كانت فتاة بممارسة الأمور المخلة.

الفرع الأول: تعريف الابتزاز

لتحديد الذاتية القانونية لجريمة الابتزاز وإزالة الغموض الذي قد يحيط بمدلولها، يقتضي الأمر مناقشتها من عدة زوايا معرفية وتأصيلية. وبناءً على ذلك، لا يمكن استيعاب الأبعاد التشريعية والسيبرانية المستحدثة لهذه الجريمة دون التوقف أولاً عند أصلها الاشتقاقي في اللغة، ليكون منطلقاً ممهداً للغوص في ضبط ماهيتها في الاصطلاح الفقهي، وصولاً إلى التدقيق في التعريفات القانونية التي أفردها المشرع لمواجهتها؛ وهو ما سنفصله تباعاً وفق الآتي:

[1] حداد شيماء، جبلي سعيدة، جريمة الابتزاز عبر الوسائل الالكترونية في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، معهد الحقوق، جامعة عبد الحفيظ بو الصوف ميلة، 2025، ص7.

اولا: التعريف اللغوي للابتزاز

يعرف الابتزاز لغة بانه الوعيد والتخويف ، ويعرف أيضا بانه اخذ الشيء بجفاء وقهر ، وابتزه ،سلبه ، رمى به، ولم يرده .[1]

"وابتزت الشيء استلبته ومن ذلك جاء المثل (من عز بز) معنى ذلك من غلب سلب".[2]

ثانيا: التعريف الاصطلاحي للابتزاز

يعرف الابتزاز اصطلاحا بانه الحاق الأذى النفسي والجسدي باستعمال التهديد والترهيب، او الاضرار بسمعة الشخص اما بإلصاق التهم او نشر الاسرار و تلقيف الفضائح، هذا ما يجعل الشخص يجبر على الدفع للشخص الذي يبتزه .[3]

ومن منضور اخر يمكن تعريفه بانه تهديد شخص بكشف معلومات معينة عنه من شان هذه الأخيرة المساس بشرفه واعتباره ما لم يقم هو الاخر بالاستجابة الى طلبات الجاني وعادة ما يكون المجني عليه يحرص على إخفاء هذه المعلومات، ومنه يمكن القول انه ليس هنالك اختلاف كبير او تباين بين التعريف اللغوي والاصطلاحي فبالجمع بينهما يمكننا تعريف الابتزاز بانه الحصول على المال او منافع أخرى من شخص تحت التهديد وهذا يتم بفضح احد اسراره او المساس بقيمته وسمعته.[4]

ثالثا: التعريف الفقهي للابتزاز

تعددت التعريفات لدى الفقهاء فيما يخص الابتزاز، "فقد عرفه البعض على أنه الضغط الذي يباشره شخص على إرادة شخص آخر بجملة على ارتكاب جريمة معينة.

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

وفي تعريف آخر فقد عرف الابتزاز الإلكتروني بأنه الحصول على وثائق، وصور، ومعلومات عن الضحية من خلال وسائل الكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عن طريق استخدام الوسائل الإلكترونية لتحقيق أهداف يسعى لها المبتز.

من خلال التعاريف السابقة للابتزاز نجد أنها تخرج على اعتبار الابتزاز وسيلة ضغط أو تهديد يمارسه المبتز على إرادة المجني عليه بهدف الوصول إلى تحقيق مراده لان الابتزاز مرتبط بالتهديد فدون هذا الأخير لا يتحقق الابتزاز كما نستطيع القول أن الابتزاز الإلكتروني يمثل سلوك غير مشروع أو غير أخلاقي ويعد من الجرائم التي تقع عن طريق الشبكة المعلوماتية."[5]

---

[1] سليمان بن عبد الرزاق الغديان [واخرون...]، صور جرائم الابتزاز الالكتروني ودوافعها واثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسين، مجلة البحوث الأمنية، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد27، العدد69، يناير2018، ص66.

[2] بوشعير الحسن، حداد شعيب، جريمة الابتزاز الالكتروني _دراسة مقارنة_ ، مذكرة ماستر، تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي _برج بوعريرج_ ، 2023، ص9.

[3] المرجع نفسه، ص10.

[4] حداد شيماء، جبلي سعيدة، جريمة الابتزاز عبر الوسائل الالكترونية في التشريع الجزائري، ص8.

[5] بوشعير الحسن، حداد شعيب، جريمة الابتزاز الالكتروني _دراسة مقارنة_ ، ص ص10 11.

رابعا: التعريف القانوني للابتزاز

في الأصل ان المشرع لا يقوم بوضع تعريفات وانما يضع احكاما تحدد الموضوع المجرم ويترك امر التعريف للفقه، ولكن في بعض الأحيان قد يضع المشرع تعريفات وهدا لتفادي الوقوع في لبس وتبيان السلوك الاجرامي والمراد منه.

" لم يَتطرق المشرع الجزائرُي لجرَيمة الابتزاز وإنما تناولها من خلال النصوص العامة لجرَيمة التهدَيد، ومَيز المشرع الجزائريٌ بَين نوعَين من التهدَيد :

1. **التهدَيد المجرد:** وَيقتصر فَيه الجاني بإلقاء الرعب والخوف في نفس الضحَية وَيعاقب علَيه بالمادة 285ق ع.
2. **التهدَيد المصحوب بطلب أو تكلَيف بأمر أو امتناع عن فعل:** وهو أشد خطورة من التهديَد المجرد وهو ما َيدخل في مفهوم الابتزاز فهو َيدر نفعا مادَيا للمبتز، َعاقب علَيه بالمواد 371-286-284 ق ع."[1]

في نفس السياق عرف المشرع الفرنسي الابتزاز على انه كل فعل َتم عن طرَيق العنف أو التهدَيد بالعنف أو اكراه من أجل الحصول علً توقَيع أو تعهد أو تنازل او إفشاء سر أو تسلَم أموال أو ممتلكات، وهذا من خلال المادة 312-1 وقد نظم المشرع الفرنسِي الابتزاز في المواد 312-1 الَى 312-9.[2]

"من خلال التعرَيفات َيمكن الاستنتاج بأن الابتزاز َيعد صورة متقدمة عن التهدَيد حَيث َيتطلب فَيه الحصول علىً مقابل من الضحَية وَيكون هذا المقابل فِي شكل منفعة مادَية أو معنوَية أو مبالغ مالَية، علاقة غير اخلاقية... .

فهو بالمفهوم الدقَيق استخدام المبتز(الجانِي) شخصا كان أم تنظَيما أسلوبا من أسالَيب الضغط المادٌي أو المعنوٌي لدفع الضحيَة لنهج سلوك معين َيجلب المنفعة للجهة المبتزة".[3]

خامسا: تعريف الابتزاز الالكتروني

تمثل جريمة **الابتزاز الإلكتروني** الوجه المظلم لسوء استخدام التقنية، وهي سلوك إجرامي يعتمد على توظيف الإنترنت كأداة للضغط والترهيب. وتتجسد هذه الظاهرة في قيام الجاني (المبتز) بمحاصرة الضحية وتهديدها بنشر محتوى حساس سواء كان صوراً، مقاطع فيديو، أو بيانات سرية لإجبارها على الانصياع لمطالب غير مشروعة ، وهنا تختلف مآرب المبتزين باختلاف شخصياتهم والظروف المحيطة بهم، ويمكن حصرها في ثلاثة مسارات رئيسية:

- **دوافع مادية :**السعي للحصول على أموال مقابل الصمت وعدم النشر.
- **دوافع معنوية أو غير اخلاقية :**استهداف الجانب النفسي للضحية أو استدراجها لتقديم تنازلات غير أخلاقية.
- **استغلال مهني :**إرغام الضحية على إفشاء أسرار عملها أو القيام بأعمال غير قانونية تخدم مصالح المبتز.

[1] بن عمر ياسين، الابتزاز الالكتروني للأطفال في التشريع الجزائري، المجلد16، العدد2، دفاتر السياسة والقانون، الجزائر، جوان 2024، ص172.
[2] بن عمر ياسين، المرجع السابق، ص172.
[3] المرجع نفسه، ص ص172 173.

بحيث تستغل هذه الجرائم الانتشار الهائل لمنصات التواصل الاجتماعي **(مثل فيسبوك، تويتر، وإنستغرام والبريد الإلكتروني...)**، حيث توفر هذه الوسائل بيئة خصبة للمبتزين لتصيد ضحاياهم، مستغلين التزايد المستمر في عدد المستخدمين وسهولة الوصول إلى البيانات الشخصية عبر هذه البرامج المختلفة[1].

الفرع الثاني: أنواع الابتزاز الالكتروني

تتسم جريمة الابتزاز الإلكتروني بتعدد صورها وتنوع أنماطها الإجرامية، فهي ليست نمطاً ثابتاً، بل تتشكل وفقاً لعدة معايير؛ فتارةً تختلف باختلاف الضحية المستهدفة، وتارةً أخرى تتبع الغاية المرجوة أو المنفعة التي يسعى المجرم لتحقيقها من وراء فعله.

ونتيجة لهذا التداخل، يمكن تصنيف أنواع الابتزاز الإلكتروني إلى ثلاثة أقسام رئيسية، تُعد الأكثر شيوعاً وبروزاً في سجلات البلاغات الرسمية. وقد أثبتت الوقائع أن غالبية هذه الجرائم تقع عبر منصات التواصل الاجتماعي وتطبيقات الدردشة المختلفة، نظراً لسهولة الوصول للضحايا من خلالها.[2] وتتمثل أبرز هذه الأنواع في:

أولا : جريمة الابتزاز بالنظر للشخص الضحية

تختلف صور جرائم التهديد والابتزاز الإلكتروني باختلاف شخصية المجني عليه الذي يقع في شباك الجاني:

أ. **الشخصية الاعتبارية:** تستهدف بعض جرائم الابتزاز الإلكتروني الشخصيات الاعتبارية كالحكومات، والشركات، والمؤسسات؛ حيث ترتكز الجريمة على اختراق الخصوصية والحصول على بيانات سرية وحساسة. تبدأ هذه العمليات غالباً بتسلل إلكتروني إلى المواقع أو الأنظمة الحيوية، ثم تتطور إلى تهديد صريح بنشر تلك المعلومات للعامة أو للمنافسين. وما يدفع الجاني للاستمرار في هذا المخطط هو يقينه بملاءة الضحية المالية وقدرتها على الدفع لحماية سمعتها أو أسرارها التجارية، وقد يصل الأمر إلى السطو الكامل على المواقع الإلكترونية والسيطرة عليها لإحكام عملية الابتزاز.[3]

ب. **الاحداث:** تتباين التشريعات والأنظمة في تعريف (الأحداث) تَبَعاً لاختلاف تحديد سن التمييز والرشد، وهو تباين تفرضه العوامل الطبيعية والاجتماعية والثقافية المتفردة لكل مجتمع. وتتصاعد وتيرة الابتزاز الإلكتروني الموجه ضد هذه الفئة عبر ممارسة الضغوط والتهديد بنشر صور أو تسجيلات مرئية أو محادثات خاصة، تهدف في مجملها إلى الحط من قدر الحدث أو تشويه صورته أمام أهله ومجتمعه. وغالباً ما تستهدف هذه الجرائم استغلال الأحداث لتحقيق مآرب غير اخلاقية أو للحصول على معلومات عائلية حساسة؛ حيث يستغل الجاني حداثة سن الطفل وضعف خبرته في التصرف، متسللاً إلى إدراكه عبر شغفه بالتكنولوجيا. ولعل كون الأحداث الفئة الأكثر اتصالاً بالفضاء الرقمي ومنصات التواصل الاجتماعي التي باتت تستقطع جزءاً كبيراً من يومهم هو ما يجعلهم الصيد الأسهل والمستهدف الأول لهذه الجرائم.[4]

ت. **النساء:** يُعد ابتزاز النساء النمط الأكثر شيوعاً وانتشاراً في فضاء الجرائم الإلكترونية، حيث يمثل النموذج التقليدي لهذا النوع من الانتهاكات، لاسيما حين يكون الجاني رجلاً والضحية امرأة. ترتكز

---

[1] بوشعير الحسن، حداد شعيب، جريمة الابتزاز الالكتروني_دراسة مقارنة_، ص ص 16 17.

[2] نفس المرجع، ص17.

[3] عراب مريم، جريمة التهديد والابتزاز الالكتروني، المجلد07، العدد01، مجلة الدراسات القانونية، الجزائر، جوان 2021، ص 1210.

[4] عراب مريم، المرجع السابق، ص 1210.

هذه الجريمة غالباً على استغلال مواد حساسة مثل الصور الشخصية، أو المحادثات الخاصة، أو التسجيلات المرئية التي توثق علاقات سابقة، واستخدامها كأداة ضغط وتهديد. [1]
وفي كثير من الأحيان، تكون هذه الجرائم نتاج تخطيط مسبق من المبتز، وتزداد خطورتها حين تستهدف القاصرات (الأحداث)؛ حيث تندفع الضحية غالباً للاستجابة لمطالب المبتز رضوخاً لترهيبه، وخوفاً من الوصمة الاجتماعية أو ما يُعرف بـ 'العار'، وهو ما يستغله الجاني لإحكام سيطرته وضمان انصياع الضحية لطلباته.

ث. **الرجال:** لا ينجو الرجال من شباك الابتزاز الإلكتروني، حيث يقعون ضحايا لهذه الجرائم لاعتبارات عدة؛ فقد يُستهدف الرجل لكونه ميسور الحال من قبل محترفات الاستدراج عبر المواقع الإلكترونية، اللواتي يستخدمن صوراً أو مقاطع مصورة كوسيلة ضغط لتهديد مركزه الاجتماعي والوظيفي. وعلاوة على ذلك، قد تطال جرائم الابتزاز الرجل بسبب حيازته لأسرار مهنية أو عائلية حساسة، أو أي معلومات يرى أن الكشف عنها قد يلحق ضرراً بالغا بـ شرفه وسمعته.
فالمبتز في هذه الحالة يستغل خشية الضحية من الفضيحة الاجتماعية أو الخسارة المادية لفرض إملاءاته، مما يجعل الرجل عرضة للاستغلال الممنهج بناءً على نقاط ضعفه الشخصية أو المهنية.[2]

ثانيا: جريمة الابتزاز بالنظر الى الهدف المرجو من الجاني

تتنوع المقاصد الغائية التي يسعى المبتز لتحقيقها تبعاً لطبيعة كل جريمة وظروفها، ويمكن تصنيف هذه الأهداف على النحو الآتي:

أ. **هدف مادي:** تتصدر المنفعة المادية قائمة الدوافع المحركة لمرتكبي جرائم الابتزاز الإلكتروني؛ إذ يهدف الجاني من خلال ضغوطه وتهديداته إلى إحداث أثر مباشر في الذمة المالية للمجني عليه عبر إجباره على تقديم مبالغ نقدية أو قيم عينية ثمينة. وتتخذ صور هذا الاستغلال المادي مسارين إجرائيين: التحصيل المباشر: ويتمثل في مطالبة الضحية بنقل ملكية أموال أو أصول مالية للجاني مباشرة تحت وطأة الترهيب. التحصيل غير المباشر (تسوية الالتزامات): وهو نمط التفافي يُسخّر فيه الجاني ضحيته لسداد أعباء مالية مترتبة عليه تجاه الغير؛ كإلزامه بدفع أقساط قروض بنكية، أو تسوية ديون شخصية، أو الوفاء بالتزامات مادية لمصلحة المبتز، وذلك كشرط لعدم تنفيذ التهديد.[3]

ب. **هدف انتقامي:** يلعب الجانب النفسي دوراً محورياً في جرائم الابتزاز ذات الطابع الانتقامي؛ حيث يستهدف الجاني زعزعة الاستقرار النفسي للمجني عليه وإدخاله في صراع داخلي مرير، يقتات على الخوف المستمر من لحظة تنفيذ التهديد. وفي هذا النمط، لا يبحث المبتز عن منفعة مادية بالضرورة، بل ينصبُّ تركيزه على إذلال الضحية وتدمير سمعتها عبر فضاء الإنترنت. وتتجلى سادية الجاني في الاستمتاع بحالة العجز التي يعيشها المجني عليه، والتلذذ بتوسلاته رضوخاً للفضيحة المحتملة.
وما يزيد المشهد قتامة هو قيام المبتز بتوثيق هذا الانكسار عبر تسجيلات مرئية أو استدراج الضحية للإفصاح عن بيانات حساسة تزيد من إحكام السيطرة عليه. إن المحرك الأساسي هنا هو 'التشفي'، حيث يسعى الجاني بكل طاقته لإلحاق أقصى درجات الضرر الأدبي والاجتماعي بالضحية، متبعاً منهجية انتقامية تهدف إلى اغتيال الشخصية معنوياً أمام المجتمع[4].

ت. **هدف غير أخلاقي:** يبرز هذا الهدف بوضوح كأحد أكثر الدوافع شيوعاً في جرائم الابتزاز الإلكتروني، لاسيما عندما تكون الضحية من النساء أو فئة الأحداث (القاصرين)، وتتضاعف خطورة

[1] نفس المرجع، ص1211.
[2] عراب مريم ، المرجع السابق، ص 1211.
[3] بوشعير الحسن، حداد شعيب، جريمة الابتزاز الالكتروني_دراسة مقارنة_، ص20.
[4] بوشعير الحسن، حداد شعيب، المرجع السابق، ص20.

الجريمة وتأثيرها حين تجتمع هاتان الصفتان في المجني عليه. ويتحقق مأرب المبتز في هذا النمط حين يشترط نيل تنازلات أو ممارسات غير اخلاقية مقابل كتمان أسرار الضحية وعدم فضحها. ولا تقتصر مطامع الجاني على استغلال الضحية لنفسه فحسب، بل قد يمتد الإكراه ليشمل إجبار المجني عليه على القيام بممارسات مع أطراف أخرى. وتتفاوت وتيرة هذا الابتزاز بين طلب عارض لمرة واحدة أو استغلال متكرر وممنهج تفرضه ظروف كل واقعة؛ حيث تظل النساء الفئة الأكثر استهدافاً وتضرراً من هذا النوع.

وفي الفضاء الرقمي، يظهر المبتز كـ 'مجرم خفي 'يتخفى خلف الشاشات، مسخراً وسائل الاتصال والإنترنت للتسلل إلى خصوصيات الضحايا وجمع معلوماتهم الحساسة لاستخدامها كأداة ضغط لتحقيق نزواته[1].

ث. **هدف نفعي:** تكتمل أركان جريمة الابتزاز الإلكتروني حين ينجح الجاني في إخضاع إرادة الضحية لتحقيق مآرب معينة مقابل عدم إفشاء أسراره أو المساس بسمعته. ولا تقتصر هذه المنفعة على الكسب المادي فحسب، بل تمتد لتشمل إجبار المجني عليه على القيام بأفعال مادية أو قانونية قسراً؛ كارتكاب جرائم لصالح المبتز (مثل السرقة أو ترويج المواد المخدرة)، أو استغلال نفوذه للتوسط في إنهاء معاملات معينة.

وسواء كان العمل المطلوب من الضحية مشروعاً في أصله أو غير مشروع، فإن الجريمة تظل قائمة ومكتملة الأركان طالما كان الفعل قد أُنجز تحت وطأة التهديد وضد إرادة المجني عليه الحرة، مما يحول الضحية إلى أداة مطيعة في يد المبتز لتنفيذ جريمته وتحقيق منفعته.[2]

ثالثا : جريمة الابتزاز الالكتروني بالنظر الى وسائلها

أ. الابتزاز المادي: تعتمد جريمة الابتزاز الإلكتروني في جوهرها على استغلال الجاني لوسائط مادية ملموسة، مثل المستندات أو الصور والمقاطع المرئية، للضغط على الضحية وتهديدها. ويتحقق هذا التهديد من خلال توظيف الاتصالات الإلكترونية بمختلف أشكالها، سواء كانت عبارة عن إشارات، نصوص مكتوبة، رموز، أو بيانات صوتية ومعلوماتية يتم تداولها رقمياً. وتنتقل هذه الوسائط عبر قنوات تقنية متطورة تشمل الكابلات الضوئية (الألياف البصرية) أو الموجات الكهرومغناطيسية، مما يضفي على فعل التهديد صبغة مادية ملموسة رغم طبيعته الرقمية.[3]

ب. الابتزاز المعنوي: يتخذ الابتزاز المعنوي شكلاً مغايراً يعتمد على التأثير النفسي بدلاً من الوسائط المادية، حيث يسعى الجاني إلى محاصرة الضحية عبر توظيف عبارات هجومية ولغة تهديد حادة. ويتمحور هذا النوع من الابتزاز حول التلويح بكشف الأسرار أو فضح الشؤون الخاصة للمجني عليه، مستهدفاً بذلك إرباك استقراره النفسي وإرضاخه للمطالب عبر ممارسة ضغط لفظي مباشر يفتقر للأدلة الملموسة لكنه يحمل قوة ترهيبية عالية.

الفرع الثالث: تمييز جريمة الابتزاز الالكتروني عما يشابهها من جرائم

تتقاطع جريمة الابتزاز الإلكتروني مع عدة جرائم أخرى في جوانب معينة، إلا أنها تنفرد بخصائص تميزها عن الابتزاز التقليدي وجرائم المساس بالحياة الخاصة، ويمكن توضيح ذلك وفق الآتي:

أولاً: الفرق بين التهديد التقليدي والتهديد الإلكتروني:

رغم اشتراك كلا النمطين في كونهما تهديداً بإلحاق ضرر مقابل نيل مكاسب (مادية، معنوية، أو غير اخلاقية)، إلا أنهما يختلفان في الجوانب التالية:

[1] عراب مريم، المرجع السابق، ص 1211.
[2] المرجع نفسه.
[3] بوشعير الحسن، حداد شعيب، المرجع السابق، ص22.

- نطاق الضرر وامتداده: يتميز الابتزاز الإلكتروني بضرر عابر للحدود وواسع الانتشار؛ إذ يمكن للفضيحة أن تطال آلاف الأشخاص في ثوانٍ معدودة، بخلاف الابتزاز التقليدي الذي غالباً ما يكون محدود الأثر في نطاق جغرافي وضيق.
- صعوبة الإثبات الرقمي: يسهل في البيئة الرقمية محو آثار الجريمة وإخفاء الأدلة أو طمس هوية الجاني، مما يجعل اكتشاف الجريمة وإثباتها وتحديد فاعلها أمراً معقداً مقارنة بالابتزاز التقليدي الذي يترك خلفه آثاراً مادية ملموسة.
- طبيعة الجريمة والعائد المادي: يُصنف الابتزاز الإلكتروني ضمن "الجرائم الناعمة" التي تدر أرباحاً طائلة على مرتكبيها، خاصة عند استهداف الكيانات الكبرى والشركات أو الشخصيات الثرية، وهو ما يفوق بمراحل العوائد المحتملة في الابتزاز التقليدي.[1]

ثانياً: التمييز بين الابتزاز وجرائم المساس بالحياة الخاصة:

يوجد خيط رفيع يربط بين هاتين الجريمتين، ويتجلى الفرق بينهما في النقاط الآتية:

- أوجه التشابه: تلتقي الجريمتان في حيازة الجاني لمعلومات حساسة (صور، تسجيلات، مقاطع فيديو) تخص خصوصية المجني عليه، وتُستخدم كوسيلة للضغط أو التشهير.
- أوجه الاختلاف (نطاق محل الجريمة):
  - في جرائم الحياة الخاصة: ينصب التركيز حصراً على ما يمس أسرار الفرد الشخصية والعائلية.
  - في جريمة الابتزاز: نجد أن "محل الابتزاز" أوسع نطاقاً؛ فالجاني قد لا يكتفي بالمعلومات الخاصة، بل قد يستخدم وثائق مهنية، أسراراً سياسية، أو وقائع رسمية تؤدي في حال إفشائها إلى الإضرار بسمعة الضحية. وبذلك، فإن الابتزاز يتجاوز حرمة الحياة الخاصة ليشمل أي معلومة يمكن استغلالها كأداة ضغط لتحقيق مآرب الجاني.[2]

الفرع الرابع: خصائص جريمة الابتزاز

تنبثق عن كل نمط إجرامي مستحدث سمات خاصة تفرقه عن الجرائم التقليدية، وهو ما ينطبق جلياً على الابتزاز الإلكتروني الذي أفرز نموذجاً فريداً من الجناة؛ فالمجرم المعلوماتي لا يعتمد على القوة العضلية أو العنف المادي، بل يرتكز في نشاطه على الذكاء والاحترافية التقنية داخل البيئة الرقمية. وقد أدى التطور المتسارع في شبكات التواصل الاجتماعي إلى ظهور جاني يتميز بهدوء الطباع والقدرة على التخفي خلف الشاشات، مستعيناً بمؤهلاته المعرفية بدلاً من السلوك العدواني المباشر، وهو ما يستوجب تسليط الضوء على الخصائص العامة لهذا السلوك والسمات الشخصية لمرتكبه وفقاً للآتي[3]:

1. الطابع العابر للحدود (العالمية):

لا تتقيد هذه الجريمة بالحدود السياسية للدول؛ إذ يمكن للجاني ارتكابها من قارة والمجني عليه في قارة أخرى. وقد تباينت المعالجات القانونية لهذه الخاصية فبالنسبة للمشرع الجزائري: يميل قانون العقوبات

[1] بن عمر ياسين، المرجع السابق، ص 174.
[2] بن عمر ياسين، المرجع السابق، ص 174.
[3] بوشعير الحسن، حداد شعيب، المرجع السابق، ص23.

الجزائري إلى مبدأ السريان الإقليمي (داخل أراضي الجمهورية)، وهو ما قد يطرح تحديات في ملاحقة الجرائم المرتكبة كلياً خارج الإقليم.[1]

2. المساس بحرمة الحياة الخاصة والحريات:

تعد هذه الجريمة اعتداءً مباشراً على الحقوق الدستورية المتعلقة بالخصوصية، حيث تتشابه مع جرائم التشهير والقذف؛ إذ يستغل الجاني بيانات أو صوراً شخصية تم الحصول عليها دون علم المجني عليه للضغط عليه وتهديده.

3. الاعتماد الكلي على الوسائل التقنية:

تتطلب الجريمة وجود بيئة رقمية (حاسوب، هاتف محمول، إنترنت) ومعرفة تقنية لدى الجاني تمكنه من اختراق خصوصية المجني عليه أو الحصول على بياناته واستخدام برامج التواصل كمنصة للتنفيذ.

4. الخطورة البالغة والأبعاد الأمنية:

تتجاوز خطورتها الأفراد لتصل إلى المؤسسات والدول؛ فالشركات قد تخفي تعرضها للابتزاز خشية انهيار أسهمها، كما اعتبر المشرع الإماراتي ارتكابها لمصلحة جهات أجنبية أو إرهابية ظرفاً مشدداً، مما يعكس تأثيرها على الأمن القومي.[2]

5. تعقيد الإثبات الجنائي:

يصعب إثبات هذا النوع من الجرائم نظراً لسهولة طمس الأدلة الرقمية ومحو آثار الجريمة في وقت قياسي، فضلاً عن إحجام الضحايا عن التبليغ أو تواجد الجاني في ولاية قضائية مختلفة.[3]

6. الصبغة "الناعمة" للجريمة:

تُصنف كجريمة "ناعمة" لخلوها من العنف المادي الملموس (كالقتل أو الضرب)؛ حيث يعتمد الجاني كلياً على الضغط النفسي والوعيد من خلف الشاشات لتحقيق مآربه.[4]

7. طبيعتها كجريمة أموال:

تكتسي طابعاً مالياً عندما يكون الهدف منها الحصول على مكاسب نقدية أو بيانات تجارية وبراءات اختراع، وفي هذه الحالة يتحول محل الاعتداء من الشخص إلى الذمة المالية للمجني عليه.[5]

المطلب الثاني: وسائل جريمة الابتزاز الالكتروني واركانها

تنفرد جريمة الابتزاز الإلكتروني بتعدد أساليبها وتطور وسائلها التقنية، حيث يختار الجاني الأداة الأكثر فاعلية للوصول إلى بيانات الضحية وإحكام السيطرة عليها. وسنتناول في هذا المطلب الأدوات المادية والبرمجية التي تشكل المسرح العملياتي لهذه الجريمة وكذا الأركان التي تنشئ عليها وفق الآتي:

[1] يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، د.ط، دار الجامعة الجديدة، الإسكندرية،2019، ص80.
[2] بوشعير الحسن، حداد شعيب، المرجع السابق، ص26.
[3] عراب مريم، المرجع السابق، ص 1222.
[4] يزيد بوحليط، المرجع السابق، ص83.
[5] عراب مريم، المرجع السابق، ص1222.

الفرع الأول: وسائل الابتزاز الالكتروني واثاره

لا تقتصر خطورة جريمة الابتزاز الإلكتروني على طبيعتها الجرمية فحسب، بل تمتد لتشمل ذكاء الوسائل المستخدمة في تنفيذها وعمق الآثار التي تتركها في وجدان الضحية وكيان المجتمع. فبقدر ما وفرت التكنولوجيا من أدوات تقنية سهلت للجاني الوصول إلى أدق تفاصيل الحياة الخاصة، بقدر ما أفرزت تداعيات مدمرة تتجاوز الضرر المادي لتطال الجوانب النفسية والاجتماعية والشرعية؛ وهو ما يستوجب منا تسليط الضوء على هذه الوسائل وكذا تحليل الاثار الناجمة عن الابتزاز وفق الآتي:

أولا: وسائل الابتزاز

تتنوع الوسائل التقنية التي يتكئ عليها المجرم المعلوماتي لتنفيذ مآربه، وتختلف باختلاف مستوى احترافية الجاني ونوع البيانات المستهدفة، ومن أبرز هذه الوسائل:

1: الحاسب الآلي

يُعد الحاسب الآلي الركيزة الأساسية في منظومة الجرائم المعلوماتية؛ فمن الناحية اللغوية اشتق مصطلح "الكمبيوتر" من الفعل الإنجليزي (To Compute) أي الحساب أو العدّ. أما اصطلاحاً، فهو منظومة إلكترونية متكاملة صُممت لاستقبال البيانات (المعطيات) ومعالجتها وتخزينها ثم استرجاعها بدقة وسرعة فائقة وبأدنى تدخل بشري. ويمثل الحاسب في جريمة الابتزاز إما "أداة" لتخزين البرامج الاختراقية، أو "مستودعاً" للبيانات المسروقة التي يُهدد بها المجني عليه.[1]

2: البرمجيات والنظم

تمثل البرامج الروح المحركة للحاسوب، وهي عبارة عن حزمة من الأوامر والتعليمات المكتوبة بلغات برمجية دقيقة تهدف لتوجيه الجهاز لأداء وظائف محددة. وفي سياق الابتزاز، يستغل الجاني هذه البرامج كواجهة تفاعلية للوصول إلى ملفات الضحية، أو توظيف برمجيات خبيثة لاختراق الخصوصية والحصول على الصور والمستندات دون وجه حق، إذ لا يمكن للجهاز المادي أداء أي دور تخريبي دون هذه الوسائط البرمجية.[2]

3: الشبكة المعلوماتية

تُعتبر الإنترنت الفضاء الرحب الذي أحدث ثورة في الاتصال الكوني، وهي شبكة عنكبوتية عالمية تربط ملايين الحاسبات عبر كوابل الألياف البصرية أو الأقمار الصناعية والموجات الكهرومغناطيسية. وتتجلى خطورة الإنترنت في الابتزاز من خلال خدمتين أساسيتين:

- **البريد الإلكتروني:** الذي يُعد الوسيلة الرقمية البديلة للمراسلات التقليدية، ويُستخدم لإرسال رسائل التهديد المباشرة المرفقة بالوسائط الفاضحة.
- **تطبيقات الدردشة والتواصل الفوري:** التي تتيح للجاني التفاعل المباشر واللحظي مع الضحية، مما يسهل عملية الضغط النفسي والمساومة.[3]

4: الهاتف النقال

لم يعد الهاتف مجرد وسيلة اتصال صوتي، بل استحال إلى جهاز حاسوبي مصغر عالي الكفاءة مرتبط بشبكات لاسلكية ورقمية. ويُعد الهاتف من أخطر وسائل الابتزاز نظراً لملازمته الدائمة للمجني عليه

[1] حداد شيماء، جبلي سعيدة، المرجع السابق، ص13.
[2] حداد شيماء، جبلي سعيدة، المرجع السابق ، ص14.
[3] - ضياء مصطفى عثمان، السرقة الإلكترونية، دراسة فقهية، ط1، دار النفاس للنشر والتوزيع ،2011، ص25.

واحتوائه على ملحقات حساسة كالكاميرا عالية الدقة وآلات التسجيل. ويستخدم المبتز تطبيقات التواصل المثبتة على الهاتف (مثل واتساب، فيسبوك...) للوصول إلى خصوصيات الضحية أو ممارسة التجسس التقني، مما يجعله أداة طيعة لارتكاب الجريمة بسرعة فائقة وتأثير مباشر.[1]

ثانيا : الاثار المترتبة عن الابتزاز

تتجاوز جريمة الابتزاز الإلكتروني في أبعادها مجرد السلوك الإجرامي العابر، لتلقي بظلال قاتمة وآثار مدمرة تطال الفرد والأسرة والمجتمع على حد سواء. ويمكن إجمال هذه الآثار في المحاور الآتية:

1: الآثار الشرعية (الدينية)

تُعد جرير الإثم الديني أولى وأخطر الآثار التي تلاحق الجاني، إذ إن الابتزاز بكافة صوره محرم شرعاً ويستوجب سخط الخالق عز وجل. وقد استدل الفقهاء على ذلك بآيات الذكر الحكيم التي تنهى عن استغلال الضعف البشري للإيقاع بالغير، كما في قوله تعالى على لسان امرأة العزيز في سورة يوسف: (وَلَقَدْ رَاوَدتُّهُ عَن نَّفْسِهِ فَاسْتَعْصَمَ ۖ وَلَئِن لَّمْ يَفْعَلْ مَا آمُرُهُ لَيُسْجَنَنَّ وَلَيَكُونًا مِّنَ الصَّاغِرِينَ)[2]، حيث يظهر الوعيد والابتزاز كوسيلة للإكراه.

كما زخرت السنة النبوية الشريفة بالأحاديث التي تحذر من تتبع عورات المسلمين، ومنها قوله ﷺ: "يا معشر مَن أسلم بلسانه ولم يفضِ الإيمان إلى قلبه، لا تؤذوا المسلمين ولا تعيروهم ولا تتبعوا عوراتهم، فإنه من يتبع عورة أخيه المسلم يتتبع الله عورته، ومن يتبع الله عورته يفضحه ولو في جوف رحله"[3]. وهذا يؤكد أن المبتز يضع نفسه في مواجهة مباشرة مع الوعيد الرباني بالفضيحة في الدنيا والآخرة.

2: الآثار النفسية

تمثل الصدمة النفسية للضحية أحد أكثر الآثار تعقيداً واستمرارية؛ إذ غالباً ما تؤدي جريمة الابتزاز إلى فقدان المجني عليه الثقة بذاته وبالآخرين. وقد تتفاقم هذه الاضطرابات لتصل إلى حالات مرضية مستعصية مثل الاكتئاب الحاد، القلق المزمن، والانهيار العصبي. وفي حالات الابتزاز الغير اخلاقي، قد يشعر الضحية بالعجز التام عن مواصلة الحياة الطبيعية، مما يولد رغبة انتقامية أو اندفاعاً نحو إنهاء الحياة (الانتحار) هرباً من الضغوط النفسية الهائلة والوصمة التي تلاحقه ولا يقتصر هذا على الضحية فقط بل حتى عائلتها.[4]

3: الآثار الأمنية

تؤدي شيوع جرائم الابتزاز إلى خلخلة السلم المجتمعي وزعزعة الشعور بالأمن والأمان، مما يحول المجتمع إلى بيئة يسودها الحذر والخوف. وبما أن الأمن هو الركيزة الأساسية للحكم على رقي المجتمعات، فإن تنامي هذه الجرائم يؤدي إلى انهيار منظومة القيم والأخلاق، وانتشار الرذيلة، وفقدان الأفراد لخصوصيتهم، مما يزعزع أركان الدولة ويشتت جهود الأجهزة الأمنية في ملاحقة مجرمين يتخفون خلف الستار الرقمي.[5]

4: الآثار الاجتماعية

تعتبر هذه الجريمة معول هدم للروابط الأسرية، لاسيما في المجتمعات المحافظة كالمجتمع العربي والجزائري، حيث يرتبط الابتزاز بقضايا "العرض والشرف" التي تُمثل وصمة عار قد تلاحق العائلة لأجيال. وقد تؤدي هذه الجريمة إلى تشتت الأسر ووقوع حالات الطلاق، وفي حالات متطرفة قد تدفع نحو ارتكاب "جرائم الشرف" أو قتل الضحية. كما أن تشويه سمعة الضحايا (خاصة الأمهات) يؤثر بعمق على

---

[1] عراب مريم، المرجع السابق، ص1213.
[2] القرءان الكريم، سورة يوسف، الاية32 .
[3] حداد شيماء، جبلي سعيدة، المرجع السابق، ص16.
[4] نفس المرجع.
[5] - سليمان عبد الرزاق الغديان، المرجع السابق، ص179.

تنشئة الأجيال القادمة ويحطم البنيان الاجتماعي من الداخل، مما يجعلها جريمة ذات آثار مدمرة بكل ما تحمله الكلمة من معنى.[1]

بناءً على هذا يتضح جليا أن الابتزاز الإلكتروني ليس مجرد اعتداء تقني، بل هو اعتداء شامل يمس العقيدة، والنفس، والأمن، والاجتماع، مما يستوجب تظافر الجهود القانونية والتربوية للحد من تداعياته.

الفرع الثاني: اركان جريمة الابتزاز الالكتروني

تعد الجريمة الإلكترونية ظاهرة إجرامية مستحدثة تتسم بخصوصية تقنية عالية، إلا أنها ومن الناحية القانونية لا تخرج عن القواعد العامة للنظرية العامة للجريمة، حيث يتوقف قيامها على توافر أركانها الثلاثة الأساسية. ففي بادئ الامر لا بد من وجود " الركن الشرعي" الذي يجسد مبدأ المشروعية من خلال النصوص التي استحدثها المشرع الجزائري في قانون العقوبات لمواجهة الاعتداءات على أنظمة المعالجة الآلية للمعطيات. ويلي ذلك " الركن المادي" الذي يتخذ طابعاً رقمياً يتمثل في السلوك الإجرامي، سواء كان إيجابياً كالدخول غير المشروع أو البقاء العمدي داخل النظام، أو سلبياً بالامتناع، مما يترتب عليه مساس بسلامة المعطيات. وصولاً إلى "الركن المعنوي" الذي يشكل المحرك الإرادي لهذه الأفعال، حيث لا تقوم هذه الجرائم في الغالب إلا بتوافر القصد الجنائي القائم على علم الجاني بمشروعية النظام الذي يخترقه وتوجه إرادته لتحقيق النتيجة الإجرامية، وهو ما يضفي على هذه الجرائم صبغتها العمدية[2].

اولا: الركن الشرعي لجريمة الابتزاز

لقد أحاط المشرع الجزائري الخصوصية الشخصية للأفراد بسياج متين من الحماية القانونية، إدراكاً منه لخطورة الاعتداء عليها وما يخلّفه من أضرار جسيمة تصيب كيان المجني عليه ومكانته. وتتجلى خطورة الابتزاز الإلكتروني في استهدافه المباشر للجانب الأخلاقي، وهو ما يمثل تهديداً للهوية القيمية للمجتمع الجزائري المتمسك بمبادئه الفاضلة؛ إذ إن آثار هذه الجريمة لا تتوقف عند حدود الفرد، بل تمتد لتهدم كيان الأسرة وتفقدها كرامتها واستقرارها المجتمعي.

وقد استمدت هذه الحماية قدسيتها من الدستور الجزائري، وتحديداً في المادة 39 التي كفلت حرمة الحياة الخاصة وشرف المواطن، وأقرت ضمان سرية المراسلات والاتصالات بكافة أشكالها تحت حماية القانون.[3]

وتماشياً مع التوجهات التشريعية الحديثة، اعتمد المشرع الجزائري منهجاً شمولياً في مكافحة الإجرام المعلوماتي من خلال القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. حيث يستنبط من نص المادة الثانية من هذا القانون سعي المشرع لتجريم كافة الأفعال المرتكبة عبر الوسائط التقنية، ومن ضمنها جريمة الابتزاز الإلكتروني؛ وذلك استناداً إلى "عمومية النص" التي تفتح المجال لتطبيق القواعد القانونية الكلاسيكية المتعلقة بجريمة التهديد على هذه الأنماط المستحدثة.[4]

وبناءً عليه، يمكن اعتبار الابتزاز الإلكتروني ما هو إلا امتداد رقمي وصورة مطورة لجريمة التهديد والابتزاز التقليدية المنصوص عليها في المادة 371 من قانون العقوبات الجزائري، مما يضمن عدم إفلات الجاني من العقاب برغم حداثة الوسيلة المستخدمة.[5]

---

[1] حداد شيماء، جبلي سعيدة، المرجع السابق، ص17.

[2] محمد علي احمد ابو علي، جريمة الابتزاز الإلكتروني في التشريع الفلسطيني، مذكرة استكمال متطلبات درجة الماجيستر في تخصص العلوم الجنائية، كلية الدراسات العليا، الجامعة العربية الأمريكية، 2022، ص22.

[3] أنظر المادة 39 من دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 7 ديسمبر،1996 الجريدة الرسمية رقم 76 المؤرخ في: 8 ديسمبر،1996 المعدل.

[4] قانون رقم 04-09 المؤرخ في 14 شعبان عام1430ه ال موافق5غشت سنة ،2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد ،47 الصادر بتاريخ 25 شعبان عام 1430ه، الموافق16 غشت سنة 2009,

[5] بوشعير الحسن، حداد شعيب، المرجع السابق، ص53.

ثانيا: الركن المادي لجريمة الابتزاز

تقتضي القواعد العامة في القانون الجنائي عدم بسط العقاب على مجرد الأفكار أو النوايا الكامنة في النفس مهما بلغت درجة خطورتها، ما لم تتجسد في سلوك خارجي ملموس يخرجها إلى حيز الوجود؛ وهو ما يُعرف بـ "الركن المادي للجريمة".

ويتشكل البنيان المادي للجريمة التامة من ثلاثة عناصر جوهرية هي: السلوك الإجرامي الصادر عن الجاني، والنتيجة الضارة التي تتولد عن هذا السلوك، بالإضافة إلى رابطة السببية التي تجمع بينهما. ومع أن هذه العناصر ثابتة في أصلها، إلا أن طبيعتها تختلف باختلاف نوع الجريمة.

وفي هذا السياق، يبرز تحدي قانوني عند تحديد ماهية الركن المادي في الجرائم الإلكترونية؛ نظراً لخصوصية مسرح الجريمة الرقمي، حيث يتمثل السلوك الإجرامي في التعامل مع "الحاسوب" بوصفه أداة لتنفيذ المخطط الإجرامي، أو بكونه هدفاً ومحلاً للاعتداء في حد ذاته ، فلا تقوم الجريمة قانوناً بمجرد النوايا الكامنة، بل لا بد من تجسدها في سلوك إجرامي يمثل الركن المادي؛[1] وهو النشاط الخارجي الذي يحدث تغييراً في العالم الواقعي أو الرقمي. وينقسم هذا السلوك في القواعد العامة إلى صورتين:

أ- **السلوك الإيجابي:** وهو الحركة العضوية الإرادية الهادفة لارتكاب فعل محظور، وقد يكون بسيطاً (كفعل واحد) أو مستمراً أو متتابعاً.

ب- **السلوك السلبي (الامتناع):** ويتحقق بترك فعل أوجبه القانون، شريطة قدرة الشخص على القيام به وتوافر الإرادة لديه.[2]

1: خصوصية السلوك الإجرامي في البيئة الرقمية

تنفرد الجريمة الإلكترونية بركن مادي ذو طبيعة تقنية؛ فبينما يتطلب السلوك التقليدي مجهوداً عضلياً، يبدأ السلوك الرقمي بـ "ضغطة زر" أو "لمسة شاشة". ويظهر ذلك جلياً في الأفعال التالية:

- **الاحتيال وانتحال الصفة:** كالدخول للشبكة بهوية مزيفة (تاجر أو مستثمر) لاستدراج الضحايا.
- **التدمير البرمجي**: كإرسال فيروسات لتخريب البيانات أو تعطيل الأنظمة.
- **الاعتداء على الخصوصية:** كإرسال ملفات فيديو أو رسائل نصية تمس بكيان المتلقي.

2: الابتزاز الإلكتروني كصورة مستحدثة للركن المادي

يعتبر الابتزاز الإلكتروني نموذجاً مثالياً لتعقيد الركن المادي؛ فهو يجمع بين "السلوك التقني" و"النتيجة النفسية/المادية". يتمثل السلوك الإجرامي فيه في:

- **فعل الاختراق أو الاستدراج:** الحصول على صور أو بيانات حساسة عبر التسلل لأنظمة المعالجة الآلية أو عبر برامج المحادثة.
- **فعل التهديد الرقمي:** إرسال عبارات الوعيد عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي، وهو سلوك إيجابي يهدف إلى ترويع الضحية وحملها على تقديم تنازلات (مالية أو غير اخلاقية).

3: التكييف التشريعي في القانون الجزائري

[1] يزيد بوحليط، المرجع السابق، ص130.
[2] نفس المرجع، ص131.

أدرك المشرع الجزائري صعوبة حصر الركن المادي في هذه البيئة الافتراضية، فقام بموجب القانون رقم 04-15 بتعديل قانون العقوبات وإضافة القسم السابع مكرر (المساس بأنظمة المعالجة الآلية للمعطيات).

بحيث يمكن حصر مظاهر الركن المادي في التشريع الجزائري (المواد 394 مكرر وما بعدها) وفق الآتي:

- **جريمة الدخول أو البقاء غير المشروع:** نصت المادة (394 مكرر) على تجريم الولوج إلى النظام المعلوماتي "عن طريق الغش". ويتحقق الركن المادي هنا بمجرد "الدخول" (الولوج الذهني والتقني للمنظومة) أو "البقاء" (الاستمرار في التواجد داخل النظام رغم انتهاء التصريح أو انعدامه).
- **الصور المشددة للركن المادي:** يتضاعف العقاب إذا تجاوز السلوك مجرد الدخول إلى "تغيير أو حذف المعطيات" أو "تخريب نظام اشتغال المنظومة".[1]

4: استخلاص الركن المادي في الابتزاز

بناءً على ما سبق، يتحقق الركن المادي في جريمة الابتزاز الإلكتروني من خلال:

- **استخدام المنطق التقني**: توظيف برامج الاختراق أو "الهاكرز" للوصول إلى بيانات الضحية (وهو ما يندرج تحت المادة 394 مكرر).
- **النشاط الإجرامي المركب:** يبدأ بالدخول غير المشروع للنظام، ثم يتلوه فعل التهديد بالنشر (السلوك الإيجابي)، وصولاً إلى النتيجة الإجرامية وهي انصياع الضحية للمبتز، مع وجود رابطة سببية تربط بين الوسيلة التقنية المستخدمة والضرر الواقع على المجني عليه.[2]

وخلاصة القول ان المشرع الجزائري، من خلال حصر أفعال الدخول، البقاء، والتلاعب بالمعطيات، قد وضع الإطار المادي الذي يسمح بملاحقة المبتز إلكترونياً، معتبراً أن أي استخدام غير مشروع للتقنية يمس بسلامة البيانات أو إرادة الأفراد يشكل ركناً مادياً كافياً لقيام المسؤولية الجزائية.

ثالثا: الركن المعنوي لجريمة الابتزاز

لا تكتمل أركان جريمة الابتزاز الإلكتروني إلا بتوافر الركن المعنوي إلى جانب ركنيها المادي والشرعي، فهي تُصنف ضمن الجرائم العمدية التي تتخذ صورة القصد الجنائي القائم على عنصري العلم والإرادة. ويقتضي ذلك إدراك الجاني بأن حصوله على بيانات أو صور سرية وتهديد الضحية بها مقابل نيل منفعة هو فعل مجرم قانوناً، مع إدراكه التام بأن قوله أو كتابته الموجهة عبر الوسائط التقنية ستؤدي حتماً إلى ترويع المجني عليه وإرضاخه لمطالبه. ويُعد الركن المعنوي هنا مسلكاً نفسياً وذهنياً يربط إرادة الجاني بنتيجة سلوكه، مما يمهد لقيام مسؤوليته الجزائية وحق الدولة في معاقبته. وبناءً عليه، يتمحور القصد الجنائي لدى المبتز في اتجاه علمه وإرادته نحو الاعتداء على خصوصية الآخرين وابتزازهم، وهو ما يمكن تفصيله وفق الآتي:

1: القصد العام

يقوم القصد العام في هذه الجريمة على ركنين أساسيين:

أ- العلم: ويتمثل في إحاطة الجاني بكافة الوقائع المكونة للجريمة، فيجب أن يعلم يقيناً أن استخدامه للصور الفاضحة أو البيانات السرية كوسيلة للتهديد هو فعل محظور، وأن من شأن هذا السلوك إلحاق ضرر جسيم بالمجني عليه، فمتى انتفى هذا العلم انتفى القصد الجنائي.

[1] يزيد بوحليط، المرجع السابق ، ص ص133 132.
[2] نفس المرجع، ص ص134 133.

ب- الإرادة: وتتمثل في انصراف نية المبتز نحو تحقيق النتيجة غير المشروعة المتمثلة في المساس بمصلحة يحميها القانون. وتنقسم الإرادة هنا إلى "إرادة الفعل" بحيث يكون الجاني مختاراً ومدركاً لما يفعل دون إكراه، و"إرادة النتيجة" بحيث تتجه نيته الصريحة نحو تحصيل المنفعة (سواء كانت مادية أو غير أخلاقية). ولا عبرة هنا بالباعث على الجريمة، فيستوي أن يكون الهدف هو الانتقام أو تحقيق مصلحة شخصية، طالما توافر القصد الجنائي.[1]

2: القصد الخاص

نظراً لطبيعة الابتزاز الإلكتروني كجريمة تقنية تتطلب مهارات احترافية في التعامل مع تكنولوجيا المعلومات لضمان الوصول للبيانات وتنفيذ التهديد، فإنه لا يمكن تصور وقوعها عن طريق الخطأ أو الإهمال؛ فهي جريمة عمدية بامتياز يكتفي القانون فيها بتوافر القصد العام، دون اشتراط وجود قصد خاص يتجاوز إرادة التهديد وتحقيق المأرب غير المشروع.[2]

وكخلاصة لهدا المطلب نجد **ان** خطورة جريمة الابتزاز الإلكتروني تتجلى في كونها جريمة مركبة تقنياً ونفسياً، ولا تكتمل صياغتها القانونية إلا بتضافر ثلاثة أركان أساسية:

1. الركن الشرعي:

ويتمثل في مبدأ "لا جريمة ولا عقوبة إلا بنص"، حيث استند المشرع الجزائري إلى نصوص تقليدية مثل المادة **371 ق.ع**، وعززها بنصوص مستحدثة ضمن القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات (**المواد 394 مكرر وما بعدها**)، مما أضفى الصبغة الشرعية على تجريم هذا السلوك الرقمي.

2. الركن المادي:

وهو المظهر الخارجي للجريمة، ويقوم على:

- **السلوك الإجرامي:** فعل إيجابي يتمثل في التهديد باستخدام وسائط إلكترونية (صور، فيديوهات، بيانات) بعد الوصول إليها بطريقة غير مشروعة.
- **النتيجة الإجرامية:** حالة الرعب والضغط النفسي التي تسيطر على الضحية، أو انصياعها الفعلي لمطالب المبتز.
- **رابطة السببية:** أن يكون التهديد الإلكتروني هو السبب المباشر والوحيد الذي أدى إلى ترويع المجني عليه أو إرضاخه.[3]

3. الركن المعنوي:

باعتبارها جريمة **عمدية** بامتياز، لا يتصور وقوعها خطأً، وتتطلب توافر:

- **العلم:** إدراك الجاني بأن فعله يمس خصوصية الآخرين ويعاقب عليه القانون.
- **الإرادة:** انصراف نية الجاني بكل حرية واختيار نحو تحقيق نتيجة الابتزاز (الحصول على منفعة مادية أو معنوية)، مع عدم الاعتداد بالبواعث سواء كانت انتقاماً أو طمعاً.[4]

---

[1] بوشعير الحسن، حداد شعيب، المرجع السابق، ص62.
[2] نفس المرجع، ص63.
[3] فاطمة العرفي، حجية الدليل الرقمي في اثبات جريمة الابتزاز الالكتروني في القانون الجزائري، مجلد8، عدد خاص 2022، مجلة صوت القانون، ص498.
[4] نفس المرجع، ص499.

ومنه فإن جريمة الابتزاز الإلكتروني تتحقق قانوناً بمجرد توجيه التهديد المصحوب بطلب عبر الوسائط الرقمية، حتى لو لم تتحقق المنفعة فعلياً، إذ يكفي لتمسك أركانها أن تصل الرسالة التهديدية لعلم المجني عليه وتؤثر في إرادته، مما يجعلها من الجرائم التي تحاربها القوانين المعاصرة بحزم لحماية حرمة الحياة الخاصة.

المبحث الثاني :القواعد الاجرائية لجريمة الابتزاز الاليكتروني .

شهدت الجرائم تطور كبير على مر العصور مما استدعى امتدادها الى المواقع الاليكترونية ,"هدا ما جعلها تعتبر نوع مستحدث يختلف عن الجرائم التقليدية, تبعا لخصوصية التقنيات التى تتم خلالها ,الامر الدي استدعى تدخل المشرع الجزائري بانشاء نصوص تشريعية و احكام قانونية للحد من هده الجرائم الاليكترونية و ايجاد حلول "للاشكالات التى طرحتها."[1]

المطلب الاول :اجراءات البحث و التحري و تحريك الدعوى العمومية في جريمة الابتزاز الاليكتروني:

"وضع المشرع الجزائري اليات خاصة للتعامل مع هده الجرائم حيث نص ضمن القانون 09_04 سنة 2009 على القواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا و تتمثل هده القواعد في اجراءات التحري التى منحها المشرع الجزائري لضبطية القضائية في كل من قانون الاجراءات الجزائية و قانون الوقاية من الجرائم متصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ."[2]

الفرع الاول: تقديم شكوي.

يعتبر اجراء قانوني معتاد حيث يمكن للشخص المتضرر توجه "للجهات مختصة مثل الشرطة او الى الجهة القضائية المختصة بالجرائم معلوماتية و تقديم شكوى مع اصطحابه لكافة دلائل من رسائل او صور التي توضح ان الشخص وقع ضحية احدى جرائم (النصب ولاحتيال, دكاء اصطناعي و غيرها...), بعد اتمام هدا اجراء تقوم سلطة المختصة بفتح تحقيق حول الحادثة الواقعة على عائق ضحية و جمع بيانات دات صلة بها ,و لاجراء تحقيق لابد من تعاون مع جهات خاصة في مثل هده الجرائم و استخدام تقنيات رقمية حديثة و تحليل بيانات لازمة بناءا على الادلةالمتوفرة.

الفرع الثاني:اجراءات التحري في الجريمة الالكترونية

سنتطرق في هدا الفرع الى تعريف التحري و تعرف على وسائل المستخدمة في التحري و اساليبه.

أولا-التعريف القانوني : تنص المادة 2 في فقرتها الثانية من القانون الاجراءات الجزائية على انه :"ويناط بالضبط القضائي مهمة البحث عن الجريمة المقررة في القانون العقوبات و جمع الادلة فيها و البحث عن مرتكبيها ما دام لم يبدأ فيها بتحقيق قضائي " [3]

وبهدا يمكن بلورة العناصر الاساسية لعملية التحري في النقاط التالية:

- انها مجموعة من الاجراءات الجزائية.
- الاختصاص النوعي اي ينفدها اعضاء الضباط القضائي .
- النطاق الزمني و الوظيفي بمعنى انها تبدأ من لحظة وقوع الجريمة و تنتهي عند تدخل السلطة القضائية لتحريك دعوى .
- يرتكز مهام التحري على شقين , الاول مادي يتمثل في معاينة و جمع الادلة و القرائن و الثاني شخصي يتمثل في تتبع الجناة و تحديد هوياتهم .
- الهدف الاستراتيجي هو التمهيد لتحريك الدعوى العمومية و مباشرتها .[4]

---

[1] بومحراث ليندا، يوم دراسي حول الجريمة السيبيرانية المعنون ب(اجراءات التحقيق الخاصة بالجرائم السيبرانية)،المنعقد يوم 20افريل 2022، بجامعة الامير عبد القادر للعلوم الاسلامية قسنطينة،ص2.

[2] المرجع نفسه، ص48.

[3] المادة 12ا لفقرة 3من الامر رقم 66_155 المؤرخ في 8جوان 196 المتضمن قانون الاجراءات الجزائية المعدل و المتمم بالامر رقم 11_02 المؤرخ في 23فيفري2011 ج.ر،ج ج.د.ش، العدد12المؤرخ في 23 فيفري 2011.

[4] حمزة قريشي، الوسائل الحديثة للبحث و التحري في ضوء القانون الجزائري، دراسة مقارنة،ط1،منشورات السائحي،الجزائري،2017،ص18.

ثانيا:الوسائل المستخدمة في التحري و جمع الادلة .

أ. الوسائل المادية:

تعتمد عملية الاستدلال في الجرائم المعلوماتية على مجموعية من الاليات و الوسائط التقنية التي تساهم في توثيق الدليل الرقمي و تتمثل اهم هده الوسائل في:[1]

1) الخوادم الوسيطة Proxy Severs:

تعد حجز الزاوية في ادارة تدفق البيانات بين الشبكة الداخلية و المستخدمين ,فالى جانب دورها في تحسين الاداء عبر نضام الداكرة المخبئية Cache Memory, فهي تعمل كأداة رقابية تتيح للمؤسسات و مزودي الخدمة تتبع سجلات الدخول و الخروج, مما يسهل عمليات الشبهات التقنية و الضمان أمن الشبكة.

2) برمجيات التتبع و التعقب :

هي ادوات تقنية متخصصة في رصد و تحليل محاولات الاختراق غير المشروعة تتميز هده البرامج بقدرتها على توليد تقارير تتضمن:

- التوثيق الزمني للواقعة (تاريخ ووقت الحدث)
- تحديد العنوان البروتوكوليIP Addres للمخترق .
- كشف هوية مزود خدمة الانترنت (ISP) الدي استخدمه الجاني ,و تحديد منافد العبور الرقمية المستخدمة ,مما يوفر خيطا استدلاليا قويا لرجال الضبط القضائي .

3) انظمة كشف التسلل :

تمثل هده الانظمة "الحارس الرقمي "للشبكة ,حيث تقوم بمراقبة مستمرة و تحليل لكافة الانشطة و العمليات التي تجري على الاجهزة . تكمن قيمتها الاجرائية في قدرتها على استشعار الانماط غير الطبيعة او السلوكيات التي تشير الى وجود تهديد أمني , مما يسمح بتوثيق محاولة الابتزاز او الاختراق في مهدها .

4) المعرفات الرقمية ووسائط الاتصال :

و تشمل العناوين البروتوكولية (IP Addresses),وصناديق البريد الاليكتروني ,وسجلات منصات المحادثة الفورية . تعد هده العناصر بمثابة البصمة الرقمية التي لا غنى عنها في اثبات نسبة الجريمة لفاعلها , حيث تتيح الربط المادي بين الفعل الاجرامي و الجهاز المستخدم في تنفيده.[2]

ب. الرسائل الاجرامية:

و يقصد بها الاجراءات التي باستخدامها يتم تنفيد طرق التحقيق الثانية و المحددة و المتغيرة وغير المحددة التي تثبت وقوع الجريمة و تحدد شخصية مرتكبها ومنها :

1) تقصي الاثر الرقمي:

[1] بوديسة بجاد عبد الرؤوف، اليات التحري عن الجريمة الالكترونية في القانون الجزائري، مدكرة ماستر مهني تخصص قانون الاعلام الالي و الانترنت، جامعة محمد البشير الابراهيمي برج بو عريريج، كلية الحقوق و العلوم السياسية، السنة 2022، ص42.

[2] عثماني عزالدين، اجراءات التفتيش و التحقيق في الجرائم الماسة بانظمة الاتصال المعلوماتية، مجلة دائرة البحوث و الدراسات القانونية السياسية، مخبر المؤسسات الدستورية و النظم السياسية، جامعة تبسة، العدد4، جانفي 2018 .

تعتمد هده الوسيلة على ملاحقة المسارات الالكترونية التي يتركها الجاني و تتم عبر تتبع المراسلات خلال مراقبة مسار البريد الالكتروني و تتبع العتاد عبر تحديد البصمة الرقمية للجهاز المستخدم في الولوج غير المغير المشروع او عملية الاختراق مثل عنوان الIP.

2) فحص النظم المعلوماتية و بروتكولات :

يتضمن هدا الاجراء النفاد الى سجلات النظام لتحليل كيفية عمله ,و فهم الثغرات التي استغلها المجرم و دراسة اسلوب التشفير او الحماية المطبق .

3) التوظيف الجنائي للدكاء الاصطناعي :

تعتمد هده الوسيلة على استخدام برمجيات حسابية متطورة مصممة خصيصا للتحقيق الجنائي ,حيث تقوم بتحليل كميات ضخمة من البيانات الرقمية و استنباط النتائج بناءا على خوارزمية دقيقة .[1]

4) مراقبة الاتصالات الالكترونية :

تعتبر من الوسائل التحقيقية المعقدة التى تثير جدلا كما نجد المشرع الجزائري لم يعرف عملية مراقبة الاتصالات الالكترونية على عكس بعض التشريعات التي عرفتها مثل التشريع الامريكي.

ثالثا_اساليب التحري في الجريمة الالكترونية .

إن الخصائص الاستثنائية التي تتميز بها الجريمة الإلكترونية ـــوعلى رأسها الطبيعة اللامادية والافتراضية للأدلة الرقمية وسرعة تلاشيهاـــ جعلت من القواعد التقليدية للتحري والبحث عن الجرائم تقف عاجزة في كثير من الأحيان عن كشف هوية الجناة أو ضبط معالم الجريمة. وأمام هذا التحدي الإجرائي، كان لزاماً على المنظومة القانونية المعاصرة التخلي عن النمطية، والبحث عن آليات بديلة تتلاءم مع البيئة الرقمية؛ وهو ما دفع المشرع إلى إقرار وتفعيل طائفة من أساليب التحري والبحث المستحدثة والمتطورة تقنياً، والتي نبرز أهمها في الآتي:

1. اساليب التحري المستحدثة في الجريمة الالكترونية:

سنقتصر في اجرأين اساسين:

- **المراقبة الالكترونية:**

تبنى المشرع الجزائري في القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و اتصال و مكافحتها توجها حديثا يتيح اختراق حاجز السرية الرقمية لأغراض قضائية .فبموجب المادة3 منه ,صار من الممكن اخضاع الاتصالات الالكترونية للمراقبة القنية و التسجيل الفوري لمحتواها , كاجراء استثنائي تمليه ضرورة الكشف عن الجرائم الرقمية , بشرط التقيد بالضوابط المنصوص عليها في قانون اجراءات الجزائية لضمان عدم المساس بالحقوق و الحريات .[2]

أ.شروط المراقبة الاليكترونية:

برجوع الى المادة 04من قانون 09-04 احاطة المشرع الجزائري اجراءات المراقبة الالكترونية بضمانات اجرائية صارمة تتمثل في:

- التبعية للسلطة القضائية (الرقابة قضائية)
- الحصول على الادن المسبق.

[1] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص43

[2] المادة 3 من القانون 09_04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكافحتها، جريدة رسمية.

- معيار الضرورة والتبعية حيث اقر المشرع مبدأ الضرورة الاجراءات.
- معيار الفعالية و توقع النجاح .[1]

- **الحفظ و افشاء الفوري للمعطيات الالكترونية:**

يعد اجراء الحفظ و الافشاء العاجل للمعطيات المعلوماتية من أبرز الاليات الاجرائية المستحدثة التي اقرها المشرع الجزائري في المادة 04-09,[2] لمواجهة الطبيعة غير المادية للجريمة الاليكترونية , و يقع عبئ هدا الاجراء بصفة اساسية على عاتق مقدمي الخدمات , الدين يلتزمون تقنيا بحفظ و تخزين البيانات المتداولة عبر انظمتهم لضمان عدم ضياعها او العبث بمحتواها او تغييرمعالمها الاصلية ,وتتجلى الغاية من هدا الالتزام في تمويل جهات التحقيق و التحري ب الدليل الرقمي فور طلبه .[3]

2.اساليب التحري العامة على الجريمة الالكترونية:

بناءا على الخصوصية موضوع الجريمة الرقمية , سنقتصر في دراستنا للاجراءات التحقيق على محوري المعاينة و التفتيش , كونهما الاكثر تفاعلا مع بيئة الرقمية وهو ما سنفصله .

اولا_المعاينة:

بالرغم من خلو التشريع الجزائري من تعريف جامع للمعاينة , الا ان المشرع كرسها كاجراء جوهري من اجراءات التحقيق بموجب المادة 79من القانون الاجراءات الجزائية و التي منحت القاضي صلاحية الانتقال الى المسرح الجريمة لمباشرة المعاينات اللازمة والوقوف على الاثار المادية[4].

_كما تعددت المقاربات الفقهية في تعريف عملية المعاينة، إلا أنها تقاطعت جميعها في اعتبارها إجراءً تحقيقياً مادياً وبصرياً؛ حيث يُمكن استعراض أبرز هذه التوجهات فيما يلي[5]:

- **باعتبارها أداة إثبات مادية** عُرّفت المعاينة بأنها الفحص البصري المباشر الذي يجريه المحقق على الأشخاص أو الأماكن أو الأشياء، بهدف توثيق حالتها الراهنة واستخلاص الأدلة المادية التي تساهم في اجلاء الحقيق.[6]
- **باعتبارها إجراءً انتقالياً كاشفاً** :

كما نُظر إليها كإجراء جوهري يقتضي انتقال السلطة المختصة إلى مسرح الجريمة للمشاهدة الفعلية وجمع الآثار المادية المتبقية، فهي بمثابة "التصوير الواقعي" لمجريات الحادث، حيث تهدف إلى الربط المنطقي بين كيفية وقوع الجريمة وبين مرتكبيها من خلال معاينة الوجود المادي للجريمة وفك الغموض المحيط بها، وتكتسي المعاينة أهمية خاصة تمليها طبيعة الجريمة محل البحث، حيث يبرز التمايز الواضح بين المعاينة في الجرائم الكلاسيكية والمعاينة في البيئة الرقمية. ففي جرائم النظم المعلوماتية، غالباً ما تغيب الأدلة المادية المحسوسة، كما يزداد خطر تلوث الأدلة الرقمية نتيجة تردد مستخدمين كثر على النظام[7]. وبناءً عليه، يتوقف نجاح التحقيق في هذه الجرائم على تقدير مدى سلامة مسرح الجريمة من الناحية التقنية، والالتزام بضوابط المعاينة الفنية المتخصصة لكشف الحقيقة".

---

[1] بومحراث ليندا، مرجع السابق، ص20.
[2] القانون رقم 09_04المؤرخ في 5 أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال ومكفحتها، المرجع السابق.
[3] بومحراث ليندا، المرجع السابق، ص11.
[4] المرجع نفسه.
[5] المرجع نفسه.
[6] فؤاد كروم، اجراءات المعاينة التقنية لمسرح الجريمة، مدكرة ماستر في القانون الجنائي، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2018م، ص26_27.
[7] بومحراث ليندا، مرجع السابق، ص12.

أ_معاينة الوسط المادي المحيط بالجريمة المعلوماتية:

تتمحور المعاينة في مسرح الجريمة التقليدي حول ضبط العناصر ذات الكيان المادي الملموس المرتبطة بالفعل الإجرامي؛ حيث تشمل المكونات الصلبة للحاسب الآلي وملحقاته، ووسائط الحفظ الخارجية، وكافة التجهيزات الإلكترونية والتقنية المستخدمة في ارتكاب الجريمة. وتتميز المعاينة في هذا النطاق باليسر الإجرائي، نظراً لأن محل الضبط هو أشياء مادية يسهل التعامل معها إجرائياً وفنياً من قِبل جهات الضبط الجنائي، مما يسهل عملية التحفظ على هذه الأدلة وتوظيفها لربط الجريمة بفاعلها بطريقة مادية مباشرة لا تثير تعقيدات تقنية كبرى مقارنة بالمسرح الافتراضي[1].

ب_خصوصية المسرح الافتراضي (البيئة الرقمية):

يُمثل المسرح الافتراضي ذلك الفضاء الرقمي أو النطاق المعلوماتي غير الملموس الذي شهد تنفيذ العمليات الإجرامية أو استُخدم كأداة لتحقيق مآرب الجاني. وخلافاً للمسرح التقليدي، فإن الولوج إلى هذا المسرح واستنطاق أدلته يخرج عن نطاق المهارات التقليدية لرجال الضبط الجنائي؛ إذ يتطلب كفاءة تقنية عالية وقدرة على التعامل مع البرمجيات والأنظمة المعقدة. ومن خلال هذه المعاينة الفنية، يتم استخراج "الأدلة الرقمية "والحجج المعلوماتية التي تُشكل الدعامة الأساسية لإثبات الجريمة وإسنادها مادياً ومعنوياً إلى مقترفها في بيئة تتسم بالسيولة والتخفي[2].

د _اجراءات الانتقال إلى المسرح الرقمي وضوابط تأمينه:

لا تختلف الجريمة السيبرانية عن نظيرتها التقليدية في ضرورة "الانتقال" لمعاينة الآثار، إلا أن هذا الانتقال يتخذ طابعاً افتراضياً يتجاوز الحدود المادية. ولضمان سلامة هذه المعاينة، يتعين على المحقق اتخاذ سلسلة من التدابير الاحترازية والفنية قبل المباشرة في استنطاق الأدلة، وتتمثل في[3]:

- **الاستطلاع التقني المسبق :**جمع معلومات دقيقة حول الطوبولوجيا الرقمية لمسرح الجريمة، بما يشمل تحديد نوعية الأنظمة، عدد الأجهزة المرتبطة، والشبكات المحلية أو الطرفية المستهدفة بالمعاينة.

- **التجهيز اللوجستي التخصصي :**إعداد العتاد البرمجي والمادي اللازم (كالبرامج المتخصصة في الاستنساخ الجنائي وأقراص التخزين المؤمنة) لضمان فحص وضبط البيانات دون المساس بسلامتها الأصلية.

- **تأمين البيئة الطاقوية :**ضمان استمرارية التيار الكهربائي واستقراره، للحيلولة دون ضياع البيانات المتطايرة(RAM) أو تعرض النظام للتلف العمدي أو التخريب الرقمي الناتج عن الانقطاع الفجائي .

-**تحييد المؤثرات الخارجية :**عزل مسرح الجريمة عن أي مجالات مغناطيسية أو موجات اتصال قد تؤدي إلى محو المعطيات أو إتلاف الأدلة الرقمية الحساسة.

-**ضبط الملحقات المادية وحجية البصمات :**لا تقتصر المعاينة الرقمية على الأجهزة فحسب، بل تمتد لتشمل التحفظ على المخرجات الورقية وسلال المهملات، بهدف استخراج الأدلة التقليدية (كالبصمات الحيوية) التي قد توجد على هذه الأوساط، مما يعزز من قوة الإثبات الجنائي في مواجهة المتهم.

الاستعانة بالمساعدة الفنية المتخصصة :إشراك ذوي الخبرة والكفاءة في تقنيات الإعلام الآلي ضمن إجراءات المعاينة، لضمان التعامل السليم مع الأنظمة الرقمية المعقدة، وحماية الأدلة من التلف أو الفقد أثناء عملية الفحص والتحليل.بتالي تُمثل المعاينة الحجر الزاوية في مستهل إجراءات التحقيق في الجرائم السيبرانية؛ فهي الإجراء الأول الذي ينصبُّ على فحص 'مسرح الجريمة' بشقَّيه المادي والافتراضي. ونظراً

[1] خالد مرزوق سراج العتيبي، الجوانب في الشروع في الجريمة السيبيرانية، مكتبة القانون والاقتصاد، المملكة العربية السعودية،2014، ص64.
[2] خالد مرزوق سراج العتيبي، المرجع نفسه،ص64.
[3] بومحراث ليندا، المرجع السابق، ص13.

لخصوصية الأدلة الرقمية، فقد أحاطها المشرع بحزمة من الضوابط الإجرائية والشروط الفنية التي يتعين على مأموري الضبط القضائي التقيد بها، بدءاً من لحظة الانتقال الفعلي إلى موقع الجريمة، وصولاً إلى بسط السيطرة الأمنية والتقنية عليه، بما يضمن حماية الآثار الرقمية من أي عبث أو تدمير قد يطال محتواها.

ثانيا: التفتيش

يستمد التفتيش خطورته من كونه إجراءً اقتحامياً يهدف إلى ضبط الأدلة الجنائية تحت إشراف وضوابط قانون الإجراءات الجزائية أو القوانين الخاصة. وفي ظل التحول الرقمي، اكتسب هذا الإجراء أبعاداً جديدة تتجاوز النطاق التقليدي، لتستهدف 'المحتوى المعلوماتي' داخل أجهزة الحاسب الآلي. وباعتبار أن هذه الأجهزة أصبحت مستودعاً لأسرار الأفراد وخصوصياتهم، فإن تفتيشها في الجرائم السيبرانية يمثل تحدياً قانونياً يستلزم دقة متناهية في التنفيذ لضمان مشروعية الأدلة المستخلصة وعدم إهدار الحريات الرقمية[1].

أ_ تعريف التفتيش:

" تعددت التعريفات الفقهية للتفتيش، وجميعها لا تخرج عن كونه :إجراء من إجراءات التحقيق، يباشر من مختصين عند وقوع جناية أو جنحة للبحث عن أدلة الجريمة متى استلزمت ضرورة التحقيق ذلك، ويباشر في محل له حرمة سواء رضي به من يباشر حياله أم لم يرضى. كما أنه عرف على أنه:" إجراء من إجراءات التحقيق تقوم به سلطة مختصة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بلحرمة".[2]

ب _لضوابط القانونية لتفتيش النظم المعلوماتية:

نظراً لما ينطوي عليه التفتيش من مساس بالحرية الشخصية، فقد أخضعه المشرع لرقابة قانونية صارمة عبر مجموعة من الشروط والضمانات التي لا يجوز الحياد عنها. وتتجلى الحكمة التشريعية من هذه القيود في كفالة التوازن بين مصلحة المجتمع في ملاحقة مرتكبي الجرائم الإلكترونية وبين حماية الفضاء الخاص للأفراد. وتتنوع هذه الضمانات بين شروط **موضوعية** ترتبط بجدية الاتهام ووجود قرائن قوية، وشروط **شكلية** توجب اتباع قوالب قانونية محددة عند صدور الأمر بالتفتيش أو أثناء تنفيذه[3].

1- الضوابط الشكلية :

تتمثل في:

- **الحضور الوجوبي في التفتيش الرقمي:**

يُعد حضور أشخاص معينين أثناء عملية التفتيش من أهم الضمانات الشكلية التي كفلها القانون لصون حقوق المتهم وحماية من البطلان. وتتمثل هذه الضوابط فيما يلي[4]:

أصل العام (حق الحضور):وجب القانون حضور المتهم بصفته المعني الأول بالإجراء، وفي حال تعذر ذلك (خاصة عند تفتيش مسكنه)، منحه المشرع حق إنابة من يمثله، أو استدعاء شاهدين لحضور المعاينة والضبط. كما يمتد هذا الحق ليشمل المحامي لمؤازرة المتهم، وكذا حائز المكان (غير المتهم) ضماناً لمصالحه، بالإضافة إلى حق النيابة العامة في الحضور إذا كان الإجراء من اختصاص قاضي التحقيق.

---

[1] بومحراث ليندا، المرجع نفسه، ص14.

[2] عبد الله ماجد العكالية، الاختصاصات القانونية لمامور الضبط القضائي في الاحوال االعادية و الاستثنائية، دار الثقافة، ط1، الاردن، 2010، ص ص501 500.

[3] عبد الله ماجد العكالية، مرجع نفسه، ص ص511 516.

[4] عبد الله ماجد العكالية، مرجع نفسه، ص ص 515 516.

الخصوصية الإجرائية في القانون الجزائري : بالرجوع للمادة **45/1**من قانون الإجراءات الجزائية، نجد أن المشرع كرس هذه الضمانات، لكنه استدرك في الفقرة الأخيرة بوضع **استثناء جوهري** يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات (وهي الجرائم التي يندرج ضمنها الابتزاز الرقمي)

علة الاستثناء :برر المشرع التخلي عن بعض هذه القيود الشكلية في الجرائم المعلوماتية نظراً لطبيعتها التقنية المعقدة؛ إذ يتطلب الأمر سرعة فائقة في التدخل لضبط الأدلة الرقمية والحيلولة دون محوها أو تشفيرها، وهو ما يفرض تقديم "الفعالية الإجرائية" على بعض الشكليات التقليدية في هذا النطاق الضيق.

- **النطاق الزمني لتفتيش النظم المعلوماتية:**

تباينت السياسات الجنائية في التشريعات الإجرائية المعاصرة بشأن تحديد التوقيت القانوني لمباشرة تفتيش الأنظمة المعلوماتية، ويتوزع هذا التباين على ثلاثة اتجاهات رئيسية[1]:

1. **اتجاه تقييدي :**يحظر التفتيش في أوقات معينة (كالفترة الليلية) صوناً لحرمة المساكن وحمايةً للسكينة الخاصة.
2. **اتجاه توفيقي :**يربط التفتيش بمواقيت محددة سلفاً، بهدف تضييق نطاق المساس بالحقوق والحريات الفردية
3. **اتجاه إطلاقي :**يمنح السلطة المختصة بالتفتيش صلاحية تقديرية واسعة لمباشرة الإجراء في أي وقت (ليلاً أو نهاراً)، استجابةً للطبيعة الخاصة للجريمة الرقمية التي لا تعترف بالحدود الزمانية.

و اما بالنظر إلى موقف **المشرع الجزائري**، فقد نظم هذه المسألة بموجب المادة **47**من قانون الإجراءات الجزائية، والتي وضعت القواعد العامة والخاصة لمواعيد التفتيش، موازنةً بين مقتضيات الفعالية الأمنية وضمانات الحماية الدستورية للمسكن..

2-لضوابط الموضوعية لصحة التفتيش الرقمي:

تمثل الشروط الموضوعية الركائز الجوهرية التي يستند إليها مشروعية التفتيش؛ فهي الضمانات التي تسبق التنفيذ المادي للإجراء لضمان عدم الانحراف بالسلطة. ويمكن حصر هذه الضوابط في ثلاث ركائز أساسية تشكل في مجموعها "النظام الموضوعي" للتفتيش، وهي :**السبب المشروع** الذي يبرر الاقتحام، **المحل القانوني** الذي ينصب عليه التفتيش، و**الاختصاص الوظيفي** للسلطة القائمة به. وفيما يلي تفصيل لهذه الشروط..[2]

- **سبب التفتيش :**

يُمثل السبب "الواقعة المنشئة" التي تمنح السلطة المختصة الحق القانوني في إصدار أمر التفتيش ومباشرته؛ فلا يُبنى التفتيش في البيئة الرقمية على التخمين، بل يتطلب وجود جريمة (جناية أو جنحة) قد وقعت فعلاً، مع توافر أدلة أو قرائن كافية تُرجح أن عملية التفتيش ستؤدي إلى ضبط وسائط أو بيانات معلوماتية ساهمت في ارتكاب الجريمة أو إثباتها[3].

- **محل التفتيش (النطاق الموضوعي):**

[1] عبد اللطيف دحية و اخرون، المواجهة الاجرائية لجرم المعلوماتية، مدكرة ماستر في القانون الجنائي، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، مسيلة، الجزائر،2019م، ص46.
[2] بومحراث ليندا، المرجع السا بق، ص16.
[3] عبد الله ماجد العكالية، المرجع السابق، ص512_513.

يشترط لصحة التفتيش أن ينصب على محل مشروع ومحدد بدقة نافية للجهالة، سواء كان ذلك المحل **مادياً** كالحواسيب، الهواتف الذكية، والوسائط التخزينية أو **معنوياً** كالبيانات، البرامج، وقواعد المعطيات. ونظراً لأن الوسائل الرقمية لا توجد في فراغ، فإن تفتيشها يرتبط حتماً بمكانها (كمسكن المتهم) أو الشخصي (كحائز الجهاز)[1]

ويتوجب في هذا الصدد مراعاة ضابطين جوهريين:

- **التخصيص :**يجب تحديد الأجهزة أو النظم المستهدفة بدقة، فلا يجوز التفتيش العشوائي لكافة أجهزة منشأة أو عائلة ما دون صلة مباشرة بالجريمة، وذلك صوناً لحرمة الخصوصية.
- **الحصانة القانونية :**يُحظر التفتيش إذا صادف محلاً يتمتع بحصانة قانونية (كدور البعثات الدبلوماسية، الهيئات النيابية، أو مكاتب المحامين)، حيث يترتب على مخالفة ذلك بطلان الإجراء وما يسفر عنه من أدلة[2].

- **سلطة المختصة بالتفتيش الرقمي:**

نظراً لأن صدور إذن التفتيش عن جهة غير مختصة يترتب عليه البطلان المطلق، حصر المشرع الجزائري هذه السلطة وفقاً للمادة **05من القانون 09-04**)المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها) في جهتين أساسيتين:

- **السلطة القضائية المختصة :**وهي صاحبة الولاية الأصلية في الأمر بالتفتيش (قاضي التحقيق أو النيابة العامة حسب الحال).
- **ضبطية قضائية متخصصة :**أجاز القانون لضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية، تنفيذ عمليات التفتيش والدخول إلى الأنظمة المعلوماتية أو وسائط التخزين، ولو عن بعد.[3]

الفرع الثالث: تحريك الدعوى العمومية:

تعد النيابة العامة صاحبة الاختصاص أصيل في تحريك الدعوى العمومية، فهي تنوب عن الشعب في المطالبة وتتبع كل من يرتكب فعل يجرمه القانون لتسليط الجزاء المناسب عليه أمام الجهة القضائية المختصة، يتم تحيك دعوى العمومية في الجرائم الالكترونية عبر مسارين (نيابة العامة الالكترونية و شخص مضرور).

اولا_ الجهة المختصة بتحريك الدعوى العمومية:

لتعريف النيابة العامة الالكترونية يستوجب علينا التعرف على النيابة العامة بشكلها التقليدي [4]،تختص النيابة العامة في تحريك الدعوى العمومية في الجرائم التقليدية بمجردوصول علم الجريمة اليها عبر البلاغات الشكاوى,او المحاضر الضبطية القضائية ,كما تمارس أعضاء النيابة العامة مهامهم ضمن

[1] بومحراث ليندا، المرجع السابق، ص17.
[2] بومحراث ليندا، المرجع نفسه،ص17.
[3] القانون رقم 09_04 المؤرخ في14شعبان 1430 الموافق ل16 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.
[4] بن عنطر سيهام، التحقيق الجنائي في الجرائم الالكترونية، مدكرة ماستر في القانون تخصص القانون الجنائي و العلوم الجنائية، جامعة مولود معمري، كلية الحقوق، تيزي وزو، ، ص49،السنة2023.

النطاق الإقليمي للمحاكم التابعين لها، مع تمتع النائب العام (أو من ينوب عنه) بصلاحية ممارسة هذه الاختصاصات عبر كامل دائرة اختصاص المجلس القضائي. وتتمثل أبرز هذه المهام في:

1. **الاستدلال والتلقي :**استلام المحاضر والشكاوى والبلاغات وفحصها لتحديد الإجراء القانوني المناسب بشأنها.
2. **تحريك الدعوى العمومية** :مباشرة الخصومة الجنائية ومتابعتها أمام الجهات القضائية المختصة.
3. **البحث والتحري** :الإشراف على إجراءات التقصي عن الجرائم، وإحالة القضايا إلى جهات التحقيق أو المحاكمة، أو إصدار قرارات "الحفظ" (وهي قرارات إدارية مؤقتة قابلة للإلغاء حال ظهور أدلة جديدة).[1]

1. النيابة العامة الالكترونية:

أ. تعريف النيابة العامة الالكترونية :

هي نظام قضائي معلوماتي جديد يتيح للشخص طبيعي كان أو معنوي أو لوكيله إيداع شكوى على مستوى مصالح وكيل الجمهورية المختص أو النائب العام عبر الأنترنت وهذا الأخير ملزم قانونا بالرد عبر الأنترنت على تلك الشكوى أو العريضة .يظهر جليا من خلال ما سبق بأن هذا النظام يحقق فوائد كبيرة لما فيه من اختصار للوقت والجهد والمال ولاسيما بالنسبة لأفراد الجالية الوطنية بالمهجر.[2]

ب .الخصائص الجوهرية للنيابة العامة الإلكترونية

تنفرد النيابة العامة الإلكترونية بسماتٍ تميزها عن النمط التقليدي للادعاء العام، حيث نقلت العمل القضائي من الحيز المادي إلى الحيز الرقمي، وتتجلى أبرز خصائصها فيما يلي[3]:

- **لتخلي عن النظام الورقي** : تنفرد النيابة العامة الإلكترونية بإلغاء التعامل بالوثائق المادية في كافة مراحل الإجراءات، حيث يتم تبادل البيانات ومعالجتها رقمياً. ويحقق هذا التحول عدة مزايا استراتيجية منها التخلص من تراكم الملفات الضخمة وما يصاحبها من أعباء إدارية,الحفظ المنظم, سرعة النفاذ للمعلومة.
- **اعتماد على الوسيط الالكتروني:**تتطابق النيابة العامة الإلكترونية مع نظيرتها التقليدية من حيث الموضوع وأطراف الخصومة، إلا أن وجه الاختلاف يكمن في **الإجراءات؛** حيث تعتمد الأولى على الوسائط الرقمية والحواسب المرتبطة بالشبكة العالمية كآلية أساسية لتحريك الدعوى وتقديم الشكاوى.
- **سرعة التنفيذ:** ساهم التقاضي الإلكتروني في تحقيق **السرعة الإجرائية؛** من خلال إتاحة إيداع الشكاوى والمستندات رقمياً، مما يلغي حتمية الانتقال المادي لأطراف الخصومة ويضمن استثماراً أفضل للوقت والجهد.
- **جودة الخدمة للمتقاضين:** تضمن النيابة الرقمية للمتقاضين حق **المتابعة الفورية** للإجراءات دون عناء التنقل، مما يرفع من جودة الأداء القضائي، وإن كانت فعاليتها لا تزال مرهونة بتجاوز بعض الصعوبات الهيكلية والتقنية.

ج .اساليب تحريك دعوى من طرف النيابة:

[1] بن عنطر سيهام، المرجع نفسه، ص49.
[2] المرجع نفسه.
[3] بن عنطر سيهام، المرجع نفسه، ص49_50.

قد تفترض ممارسة الدعوى سلسلة من الاجراءات منذ تحريك الدعوى العمومية حتى استعمال طرق الطعن عند الحكم الجزائي، وكون هذه الأخيرة تتعلق بشق مباشرة الدعوى العمومية فسنلتزم في دارستنا على أن نقتصر بذكرنا للأساليب المختلفة التي تملكها النيابة العامة في تحريكها للدعوى العمومية فقط وهي[1]:

- **الاخطار:** تنص المادة 114 من قانون إ.ج:" الإخطار المسلم بمعرفة النيابة العامة يغني عن التكليف بالحضور إذا تبعه حضور الشخص الموجه إليه الإخطار بإرادته...[2]".

"نص القانون الذي يعاقب ويتعين أن يشير هذا الإخطار للجريمة محل المتابعة لى عليها، ويجوز أن يوجه سواء على متهم طليق أو محبوس احتياطيا، وبينما يفترض في الحضور الطوعي للمتهم الطليق رضاؤه بأن يحاكم، فإن حضور المتهم المحبوس لا يعتبر قبولا من طرفه بأن يحاكم إلا إذا ثبت ذلك بحكم المادة 114 من قانون إ.ج، وعلى العموم إذا دعي المدعي عليه ولم يستوجب للدعوى من تلقاء نفسه يتعين على النيابة العامة أن تلجأ إلى أسلوب التكليف بالحضور"[3].

- **التكليف بالحضور المباشر** :"وينطوي ذلك على تكليف المدعي عليه أو المتهم للحضور مباشرة أمام المحكمة وهذا الأسلوب يتبع في جرائم الجنح والمخالفات دون الجنايات ألن في هذه الأخيرة يكون التحقيق إجباريا طبقا للمادة 11 من قانون إ.ج" .[4]

" ويعد ذلك اسلوب أي تكليف المتهم بالحضور المباشر بمثابة الأسلوب العادي الذي تلجأ إليه عادة النيابة العامة وذلك ما لم يطلب وكيل الجمهورية إجراء التحقيق طبقا النص المادة 11 فقرة 7 من قانون إ.ج، ويجوز لوكيل الجمهورية أيضا الاتجاه إلى أسلوب التكليف بالحضور المباشر في الجنح، إلا إذا كان مرتكب الجنحة مجهولا فهنا يتعين عليه أن يطلب فتح التحقيق 1ضد مجهول أو إذا كان مرتكب الجنحة حدث طبقا لنص المادة 461 من قانون إ. ج "[5] وا كانت الجنايات أو الجنح المرتكبة يتطلب القانون فيها إجراء تحقيق، فيتعين على النيابة العامة الاتجاه إلى الأسلوب الثالث لتحريك الدعوى العمومية والمتمثل في الطلب الافتتاحي والذي يتم توجيهه إلى القضاء.

- **الطلب الافتتاحي :**

"إن الطلب الافتتاحي أو كما يسمى أيضا طلب إجراء التحقيق هو الطلب المكتوب موجه من النيابة العامة إلى قاضي التحقيق أو غرفة الاتهام بإجراء التحقيق وذلك طبقا للمادة 11 من 2قانون إ. ج ويبين فيه الوقائع الان المتابعة تجري على أساس الافعال بمعنى أن قاضي التحقيق يضع يده على القضية بصفة واقعية من ناحية الافعال لاعلى الاشخاص المعينين في الادعاء وتكييفها القانوني واسم مرتكب الافعال إن كان معروفا والا يطلب فتح تحقيق ضد مجهول، ويتعين أن يكون مؤرخا وهذا أمر هام بالنسبة الموضوع قطع التقادم وأخيرا يجب أن يحمل اسم وتوقيع وكيل الجمهورية أو نائبه الذي حرر الطلب ويستوجب على النيابة العامة اللجوء إلى هذا الاسلوب لتحريك الدعوى العمومية في الجرائم التي يكون فيها التحقيق إجباريا كالجنايات وبعض الجرائم الجنحية كما يجوز استعمال أيضا 1في الجرائم التي يكون فيها التحقيق اختياريا و المخالفات "[6].

المطلب الثاني: قواعد الاثبات الجنائي (الدليل):

لقد أحدثت الطفرة التكنولوجية المعاصرة تحولاً جوهرياً في بنية الجريمة، حيث انتقل **المسرح الجنائي** من حيزه المادي التقليدي إلى فضاءات رقمية افتراضية لا تعترف بالحدود الجغرافية. وفي هذا السياق،

---

[1] بنوخ حبيب، تحريك دعوى العمومية، مدكرة ماستر، ميدان حقوق و علوم سياسية، تخصص علم الاجرام و العلوم الجنائية، جامعة عبد الحميد بن بديس، كلية الحقوق و العلوم السياسية، سنة 2019، ص14

[2] ينظر المادة 11 من قانون الإجراءات الجزائية الجزائري.

[3] بن نوخ حبيب، المرجع السابق، 15.

[4]- ينظر المادة 67 من قانون الإجراءات الجزائية الجزائري.

[5] لمادة416 من قانون الإجراءات الجزانية الجزائري.

[6] ينظر المادة 435 من قانون الإجراءات الجزائية الجزائري.

برزت **جريمة الابتزاز الإلكتروني** كواحدة من أخطر الظواهر المستحدثة التي استغلت التقنية للنيل من ذمة الأفراد المالية وحرمة حياتهم الخاصة. وتبعاً لهذا التحول، لم يعد الدليل المادي الكلاسيكي كافياً لفك شفرات هذه الجرائم، مما أدى إلى بروز **'الدليل الرقمي '**كركيزة إثباتية جوهرية ووسيلة فنية وقانونية لا غنى عنها لملاحقة الجناة في البيئة الافتراضية، وهو ما يفرض على المشرع والقاضي الجنائي تبني آليات إجرائية تتناسب مع طبيعة هذه الأدلة اللامادية.[1]

الفرع الاول: تعريف الدليل الالكتروني:

يُشكل الدليل في المادة الجزائية الركيزة الأساسية التي يبني عليها القاضي عقيدته الصائبة لإدانة المتهم أو تبرئته، وبناءً عليه، يستوجب منا تسليط الضوء على المقصد القانوني للدليل بصفة عامة قبل الولوج إلى خصوصيته الرقمية، وفق ما يلي:

اولا_ تعريف الدليل بصفة عامة:

"الوسيمة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى [2] الحقيقة، و لم يأتي قانون 07/18 المتعمق بحماية الشخاص الطبيعيين في مجال معالجة المعطيات ذات [3] الطابع الشخصي بأي تعريف للدليل الالكتروني لكن يمكن استخلاص بعض التعريفات الفقهية، حيث تعرف على أنه: :"الدليل المأخوذ من أجهزة الحاسب آلي ويكون في شكل مجالات أو نبضات مغناطيسية أو، كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، لتظهر في شكل صور أو [4] تسجيلات صوتية أو مرئية".

"او هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية أجهزة ومعدات وأدوات الحاسب الالي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، تقديمها للقضاء بعد تحليلها عمليا و تفسيريا في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات لاثبات وقوع الجريمة ولتقرير البراءة أو الادانة فيها" [5].

ثانيا: خصائص الدليل الرقمي: تتمثل خصائص الدليل الرقمي في مايلي:

1. الدليل دو طابع علمي:

يتسم الدليل الرقمي بطابع علمي محض، كونه أثراً تكنولوجياً يتمثل في بيانات مشفرة لا تدرك إلا من خلال وسيط إلكتروني. ونظراً لارتباط هذا الدليل بالبيئة الافتراضية التي نشأ فيها، فإن الكشف عن محتواه الجنائي يظل رهيناً باستخدام مناهج البحث العلمي الرقمي وأدوات التحليل التقنية المتطورة، وهو ما يخرجه من نطاق الأدلة التقليدية التي يمكن معاينتها مباشرة[6].

2. الدليل دو طابع تقني:

"إن الطبيعة التقنية للدليل الالكتروني أنه اكتسب مميزات من حيث قابليته للنسخ، أي يمكن استخراج نسخ من الادلة الالكترونية مطابقة للاصل ولها نفس القيمة العلمية وهذه الخاصية لا

---

[1] ديب اكرم، بن عبد الله نورة، دور الدليل الرقمي الجنائي في إثبات الجريمة الابتزاز الاليكتروني، مجلة الحقوق و العلوم الانسانية، جامعة باتنة1، كلية الحقوق و العلوم السياسية، المجلد16، العدد1، سنة 2023، ص400.

[2] عائشة بن قارة، حجية الدليل الالكتروني في مجال الاثبات الجنائي، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، سنة2010 ،ص5.

[3] قانون رقم 07/18 ،المؤرخ في 2018/06/10 ،المتعمق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية العدد: 34.

[4] سوزان نوري عمي محمد، الاثبات في مجال الانترنت في القانون العراقي المقارن، رسالة دكتوراه في الحقوق، جامعة المنصورة، مصر، 2015 ،ص44.

[5] محمد الامين البشري، التحقق في الجرائم المستحدثة، جامعة نايف للعلوم الامنية، الرياض، الطبعة1 ،2002 ، ص234.

[6] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كمية 13 الحقوق، جامعة باتنة، 2013 ،ص62.

تتوفر في الدليل المادي العادي مما يشكل ضمانة شديدة الفعالية ويمكن الحفاظ عليها ضد التلف أو التغيير أو الحذف".[1]

3. الدليل سهل الاخفاء:

" إن التخلص من الدليل الالكتروني قد يقابله مسألة أخرى ذات علاقة بمسألة التطور المستمر في تكنولوجيا المعلومات، وهي أن الدليل الالكتروني نتيجة لمرونته فإنه يسهل فقدانه بسبب إتلافه أو إضاعته أو إلغاءه."[2]

"كما يتميز الدليل الرقمي أنو دليل ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات اتصال متعدية الزمان والمكان[3]."

ثالثا: الاشكال الدليل الاليكتروني:

"يتمتع الدليل الرقمي باشكال مختلفة"[4]:

1) صورة رقمية:

تعتبر الصور الرقمية توثيقاً بصرياً وتقنياً للمعطيات المرتبطة بالواقعة الإجرامية؛ فهي بمثابة دليل مادي افتراضي يتم استخراجه من الأوساط الإلكترونية، وتتخذ هذه الصور مظهرين في التعامل القضائي: إما شكلاً مادياً بعد إفراغها في دعامة ورقية، أو شكلاً تقنياً من خلال عرضها عبر الوسائط الرقمية، مع احتفاظها بكافة خصائصها البيانية التي تسمح للقضاء بمعاينة مسرح الجريمة الافتراضي.[5]

2) التسجيلات الصوتية:

" يمكن تعريفيا على أنها:" عبارة عن ترجمة لتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة، ويكون التسجيل عادة بواسطة الة تترجم موجات الصوت ، وتكون التسجيلات هي التي يتم كتابتها بواسطة الالة الرقمية ومنها الرسائل عبر البريد الالكتروني والبيانات المسجلة بأجهزة الحاسب الالي."[6]

"وتتخذ أدوات التسجيل الصوتي أنواع عديدة منيا أجهزة الاتصال السمكي الخارجي أو اللاسلكي والميكروفونات الصغيرة التي ال يتعدى حجميا عود ثقاب، وميكروفونات الميزر وكذلك الميكروفونات المسمارية."[7]

3) -النصوص المكتوبة:

" وتشمل النصوص التي يتم كتابتها بواسطة الة الرقمية ومنها الرسائل عبر البريد الالكتروني والبيانات المسجلة بأجهزة الحاسب الالي ووفقا لما قررت وزارة العدل الامريكية سنة 2002 فإن الدليل الالكتروني يمكن أن يأخذ الأشكال التالية:"[8]

أ. تصنيف السجلات الرقمية كأدلة جنائية:

---

[1] عمر بن يونس، الدليل الرقمي، بدون دار نشر، الطبعة 1 ،مصر، 2008 ،ص4.

[2] فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية لمجتمع المعلوماتي، 14 بدون طبعة، دار النهضة العربية، القاهرة، 2010 ،ص653.

[3] عبد الناصر محمد محمود فرغمي، عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، ورقة بحثية مقدمة لمؤتمر العربي الأول لعموم الأدلة الجنائية والطب الشرعي، المنعقد بالرياض، 12/ 14 نوفمبر2008، ص13

[4] ايت حمودة كاهنة، اليات البحث و التحري الجنائي في مسرح الجريمة الالكترونية، مجلة الفكر القانوني السياسي، جامعة حسيبة بن بو علي، الشلف، المجلد السابع، العدد الاول، سنة 2023، ص184.

[5] ايت حمودة كاهنة، المرجع نفسه، ص184.

[6] صالح عبد الزبرة الحسون، أحكام التفتيش وآثاره في القانون العراقي، دراسة مقارنة، الطبعة1 ،بدون دار نشر، 16 جامعة بغداد، 1989 ،ص125.

[7] ايت حمودة كاهنة، المرجع السابق،ص184.

[8] ايت حمودة كاهنة، المرجع نفسه، ص185.

- **السجلات الرقمية ذات المصدر البشري (المخزنة):**

تتمثل في الوثائق والمراسلات التي اتخذت من الوسيط الإلكتروني مستودعاً لها بعد أن قام العنصر البشري بإنشائها وتدوينها؛ ومن أبرز أمثلتها المحررات الإلكترونية الصادرة عن برامج معالجة النصوص، ومحتوى البريد الإلكتروني، وسجلات المحادثات الفورية .(Chat Logs) وتستمد هذه السجلات قيمتها القانونية من كونها تعبيراً عن إرادة أو واقعة أفرغها المستخدم في قالب رقمي.

- **سجلات الرقمية ذات المصدر التقني الخالص (المولّدة آليا):**

وهي المخرجات المعلوماتية التي يتم إنشاؤها وتلقائيًا بواسطة أنظمة الحاسوب وبرمجياته دون تدخل أو معالجة بشرية مباشرة. وتعتبر هذه السجلات بمثابة 'آثار تقنية صماء' ترصد نشاط النظام أو الجهاز، مثل سجلات الدخول والخروج(Log Files) ، وعناوين البروتوكولات(IP Addresses) ، وتتجلى أهميتها في كونها أدلة تقنية محايدة بعيدة عن احتمالات التزيف البشري اليدوي.

- **سجلات الرقمية المختلطة (المعالجة تقنيا):**

وهي السجلات التي تشترك في تكوينها الإرادة البشرية مع القدرة المعالِجة للحاسوب؛ حيث يقوم المستخدم بإدخال بيانات أولية(Data Entry) ، ثم يتولى النظام معالجتها أو إجراء عمليات حسابية ومنطقية عليها عبر برامج متخصصة (مثل تطبيقات الجداول الحسابية وقواعد البيانات). ويخضع هذا النوع من السجلات لرقابة مزدوجة لضمان صحة البيانات المدخلة وسلامة العمليات البرمجية التي أجريت عليها[1].

كما يمكن أن تتخذ انواع التالية :

- ❖ اقراص المرنة واقراص الصلبة.
- ❖ أشرطة تخزين المعلومات التي تستخدم لحفظ النسخ الاحتياطية .
- ❖ أدلة ورقية مثل الرسوم ومخرجات الطابعة.
- ❖ أجهيزة المودم وتسجيلات الكابلات المتصلة .
- ❖ جهاز الحاسوب وملحقاته.[2]

سنتفصل فيها كمايلي:

- **اقراص المرنة و الاقراص الصلبة :**

وتتمثل في الأقراص الصلبة (Hard Disks) والوسائط القابلة للنقل (الأقراص المرنة سابقاً والذاكرة الوميضية حالياً)، بالإضافة إلى أشرطة النسخ الاحتياطي؛ وتكمن أهميتها في كونها المستودع الدائم للبيانات والملفات التي قد تشكل مادة الابتزاز أو أثراً لجريمة وقعت.[3]

- **اشرطة تخزين المعلومات التي تستخدم لحفظ النسخ الاحتياطية:**

[1] بصائر عمي محمد، مروى عبد الواحد حسن، الدليل الالكتروني في مجال الاثبات الجنائي، مجلة لارك للفلسفة 17 واللسانيات والعلوم الاجتماعية، العدد 27 ،سنة2017 ،ص277.

[2] بن فريحة رشيد، ميهوب يوسف، التحري الجنائي في مسرح الجريمة الإلكترونية، مجلة جامعة القدس المفتوحة 18 لألبحاث والدراسات، العدد 42 ،2017 ،ص5.

[3] بن فريحة رشيد، ميبوب يوسف ،المرجع السابق، ص5.

وتتمثل في الأشرطة والوحدات التقنية المخصصة للاحتفاظ بنسخ احتياطية من البيانات (Backup Tapes)؛ وتتجلى أهميتها الجنائية في كونها مخزناً تاريخياً يتيح لخبراء التحقيق الرقمي استرجاع الملفات أو المراسلات الابتزازية التي قد يعمد الجاني إلى حذفها من القرص الصلب لتضليل العدالة[1].

- **أدلة ورقية (الرسوم ومخرجات الطابعة):**

وهي الأدلة التي انتقلت من طورها الرقمي إلى طور الإدراك المادي، مثل المخرجات الورقية، الرسوم، والوثائق المطبوعة، والتي تمنح القاضي تصوراً حسياً مباشراً لمحتوى الجريمة[2].

- **أجهزة المودم وتسجيلات الكابلات المتصلة:**

تضم أجهزة المودم (Modems) وكافة الوسائط الكبلية المسؤولة عن نقل البيانات؛ حيث تكمن قيمتها الإثباتية في قدرتها على تعقب مسارات تدفق المعلومات وتحديد نقاط الاتصال الجنائي[3].

- **جهاز الحاسوب وملحقاته:**

وتشمل جهاز الحاسوب بكامل مكوناته وتوابعه التقنية، باعتباره 'أداة الجريمة' والبيئة التي تمت فيها معالجة البيانات وتوجيه التهديدات الابتزازية. [4]

الفرع الثاني: القيمة الثبوتية للدليل الالكتروني:

" تعتبر مشكلة تقدير أدلة الاثبات و الاقتناع بها من أعظم المشاكل التي تقع على عاتق القاضي الجنائي، فالقاضي قبل أن يصدر حكمه يقوم بالبحث والتثبت حتى يتبين وجه الحق في الدعوى وهو في سبيل ذلك يقوم بفحص ادلة المختلفة ويطرحها في الجلسة ليتناولها الخصوم بالفحص والتنفيذ سعيا للوصول إلى الحقيقة التي ترضي ضميره وتكون اقتناعه الشخصي بهد ف تحقيق العدالة، وفي وسط الوسائل العلمية المرتكزة على وسائل البحث والتحري الحديثة التي جاءت بسبب عجز ادلة الكلاسيكية التي تعتمد على أساليب بسيطة ومكلفة للوقت لكشف الجريمة، وتتمثل معالم هذا النظام في استخدام وسائل علمية حديثة تساير وتيرة مواجهة الجريمة المتصاعدة والمتشابكة في العصر الحديث لتغب على كل محاولات المتهم في تضليل العدالة، وفي نطاق الجريمة الالكترونية ونظرا لطبيعة الدليل الالكتروني من إمكانية تعرضه للتلف أو التغيير والعبث يجب أن تكون لهذا الدليل حجية معترف بها حتى يتمكن القاضي الحكم على أساسها."[5]

اولا_ الاحكام الخاصة للدليل الرقمي في الاثبات الجنائي:

"يرتكز الاثبات الجنائي بألادلة الرقمية على مراعاة أسس ومعايير، فمجرد وجود دليل على و قوع جرمية ما ليس معناه إدانة مرتكبها، وإّنما يتوقف ذلك على مراعاة ضوابط إجرائية يشترك في احترامها المكلفين بالتحقيقات الجنائية والقاضي الجزائي وفقا لسلطته التي يتمتع بها، وهو ما سنحاول التفصيل فيه."[6]

1. المتطلبات الاجرائية الواجب توفرها لقبول الدليل الرقمي:

"ان حديث عن مقبولية الدليل الرقمي أمام القضاء الجزائي مرهون بتوافر عدة ضوابط تعد بمثابة حجر الاساس في صحة الاجراءات المتخذة الاستخلاص الدليل الرقمي الجنائي من رحم النظم المعلوماتية والحاسب الالي، أو مختلف تقنيات التكنولوجيا والاتصال الحديثة، و يسبق توافر هذه

[1] ممدوح عبد الحميد عبد المطلب، "البحث الجنائي الرقمي وجمع الأدلة في جرائم الكمبيوتر والإنترنت، دار النهضة العربية، القاهرة، ص120.
[2] طوني ميخائيل، الدليل الرقمي مفهومه وحجيته في الإثبات الجنائي، منشورات الحلبي الحقوقية، بيروت، ص25.
[3] خالد ممدوح إبراهيم، التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ص153.
[4] طوني ميخائيل، المرجع السابق، ص25.
[5] ايت حمودة كاهنة، المرجع السابق، ص193.
[6] ديب اكرم، بن بو عبد الله نورة، المرجع السابق، ص408

الضوابط الاجرائية حتمية الخواص في الاساس الذي يستند إليه هذا الدليل حسب نظام الاثبات السائد في الدولة، و هو ما يفرض علينا تحديد أساس قبول الدليل الرقمي الجنائي في الاثبات الجنائي أولا، انطلاقا من تبيني موقف التشريعات المقارنة و المشرع الجزائري من الدليل الرقمي الجنائي، لنتطرق بعدها الى شروط قبول الدليل الرقمي أمام القضاء الجزائي ثنيا."[1]

أ. اساس القبول الدليل الرقمي الجنائي في الأثبات الجنائي:

يمثل الإثبات الجنائي المحور الذي يدور حوله الحكم الجزائي، وتتفاوت قدرة التشريعات على قبول الأدلة الرقمية تبيعاً لنظام الإثبات المتبع، إذ يوفر النظام الحر بيئة خصبة لقبول مخرجات التكنولوجيا الحديثة طالما اطمأن إليها ضمير القاضي. وفي المقابل، تظهر إشكاليات القبول في نظام الإثبات المقيّد الذي يضع ضوابط صارمة تُحجّم دور القاضي في تقدير قيمة الدليل، مما يشكل عائقاً أمام إثبات الجرائم المعاصرة كالابتزاز الإلكتروني.[2]

و استثناءً من القواعد التقليدية لنظام الإثبات المقيّد، تبنت بعض التشريعات المقارنة توجهاً مرناً يقر بالحجية القانونية للدليل الرقمي استناداً إلى معيار الأصالة، فقد أقر المشرع الأمريكي في المادة (3/1001) من قانون الإثبات إمكانية الاعتداد بالمخرجات الرقمية كأدلة أصلية، متى ثبتت دقتها الفنية وأفرغت في قالب مادي مقروء بصرياً، وعلى ذات النهج، ربط المشرع الإنجليزي في المادة 69 من قانون الشرطة والأدلة الجنائية لعام 1984 (المعدل) قبول مخرجات الحاسوب كدليل إثبات باستيفائها حزمة من الضوابط القانونية والتقنية التي تضمن سلامتها وموثوقيتها.[3]

كما بنت المنظومات القانونية اللاتينية صياغة مرنة للإثبات الجنائي تقوم على دعامة الاقتناع اليقيني للقاضي، مما مهد الطريق لقبول الأدلة الرقمية دون حاجة لنصوص خاصة بكل نوع منها. ويظهر ذلك جلياً في المادتين (427 فرنسي) [4]و(212 جزائري) [5]اللتين جعلتا من حرية الإثبات أصلاً ثابتاً. ولإزالة أي لبس فقهي حول طبيعة الأدلة المستحدثة، تدخل المشرع الجزائري عبر القانون 09-04، حيث نص في مادته السادسة على شرعية الدليل الإلكتروني في الخصومة الجنائية، مخضعاً إياه لذات الضوابط الإجرائية التي تحكم الأدلة التقليدية.

ب. ضوابط قبول الدليل الرقمي أمام القضاء الجزائي:

تظل القيمة القانونية للدليل الرقمي معلقة على شرطين متكاملين؛ أحدهما شكلي يتمثل في **المشروعية الإجرائية** عند الضبط والتفتيش، والآخر موضوعي يتمثل في **اليقينية الثبوتية** وقابلية الدليل للمناقشة القضائية، فبدون توافر هذه الضوابط، يفقد الدليل الرقمي أصالته ويصبح عاجزاً عن تكوين عقيدة القاضي اليقينية، نظراً لخصوصية الأدلة الجنائية التي لا تُبنى إلا على الجزم واليقين[6]، كما يُشترط لقبول الدليل الرقمي في الخصومة الجنائية أن يكون وليد إجراءات صحيحة تتفق وصحيح القانون؛ حيث يلتزم المكلفون بالبحث والتحري بمباشرة مهام التفتيش والضبط الرقمي تحت مظلة المشروعية القانونية وبما لا ينتهك حرمة الحياة الخاصة[7]، وإن أي إخلال بهذه القواعد الإجرائية الآمرة من شأنها تجريد الدليل من فاعليته القانونية أمام القضاء؛ إذ يترتب على مخالفة الأصول الجوهرية للتحقيق الجنائي **بطلان الدليل وفقدان أثره في الإثبات**، مهما بلغت درجة يقينيته الفنية، حمايةً لسيادة القانون وتكريساً لعدالة المحاكمة، ،و لا يرتب على ذلك بطلان الاجراءات و عدم صحتها و فقدان الدليل لقيمته أمام القضاء، و من قبيل ذلك الحصول على الدليل

[1] المرجع نفسه، ص408.
[2] المرجع نفسه، ص409.
[3] ديب اكرم، عبدالله نورة، المرجع السابق، ص.409.
[4] المرجع نفسه، ص409.
[5] الامر رقم 66-155 المؤرخ في8 يونيو سنة 1966 المتضمن قانون إجراءات الجزائية، المعدل بقانون رقم 19-10 مؤرخ في11 ديسمبر سنة 2019 ،طبعة حمينة، دار بلقيس للنشر، الدار البيضاء، الجزائر، سنة 2020 ،ص124.
[6] ديب اكرم، بن عبد الله نورة، المرجع السابق، ص409.
[7] بن طالب ليندا، الدليل الإلكتروني ودوره في الاثبات الجنائي دراسة مقارنة، أطروحة دكتوراه علوم، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، سنة 2019.

الرقمي عن طريق التدليس و الغش أو الضغط أو إكراه المشتبه فيه أو التحريض ، فكل ذلك يقع تحت طائلة البطلان و العقوبات الجزائية المنصوص عليها في المادة 107 من قانون العقوبات الجزائري و المادة85 من قانون الاجراءات الجزائية.[1]

وتجسيداً لضمانات المحاكمة العادلة، يلتزم القاضي الجزائي بطرح كافة الأدلة الرقمية للمناقشة الوجاهية بين الخصوم، عملاً بالمادة (2/212) من قانون الإجراءات الجزائية. فلا يجوز بناء الأحكام على قناعات شخصية أو أدلة لم يتم تمحيصها علناً؛ إذ تظل قيمة الدليل الرقمي رهينةً بطرحه للنقاش والرد، لضمان استقامته كأصل ثابت في أوراق الدعوى.[2]

ويضاف الى شروط سابقة انه لا يصلح الدليل الرقمي دليلاً للإدانة وهدماً لقرينة البراءة إلا إذا بلغ مرتبة **الجزم واليقين**[3]؛ وبخلاف الأدلة التقليدية التي يسهل على القاضي تمحيصها حسياً، يتوقف اليقين في الدليل الإلكتروني على **الخبرة الفنية** .فالمعرفة التقنية المتخصصة هي وحدها الكفيلة بالتأكد من سلامة الدليل وعدم تعرضه للعبث أو التغيير، مما يمنح القاضي تصوراً جازماً بصحة الواقعة[4].

ت. السلطة القاضي الجزائي الجزائي في تقدير الدليل الالكتروني:

"إن الغاية الاساسية من الاثبات الجنائي هو معرفة الحقيقة الواقعية المرتبطة بما حدث بالعالم الخارجي من وقائع إجرامية ومدى ثبوتها، وباعتبار أن للقاضي الجزائي سلطة تقديرية في تقدير الادلة الجنائية بغية الوصول إلى الحقيقة الواقعية، ومن جانب آخر أيضا فإن مبدأ الاقتناع القضائي من أبرز المبادئ الاساسية التي يقوم عليها الاثبات الجنائي ويعني هذا الاخير أن يتوفر أمام القاضي الجزائي مجموعة من الادلة المطروحة أمامه تكفي لتسبيب اعتقاده بثبوت الوقائع أو نفيها كما أوردها في حكمه ونسبها إلى المتهم[5]".
و تُمثّل عملية **تقدير الأدلة** الركيزة الجوهرية لمرحلة النطق بالحكم؛ إذ لا يستقيم القضاء النهائي إلا بممارسة القاضي لسلطته التقديرية الكاملة على سائر الأدلة، ماديةً كانت أم معنوية. وفي هذا السياق، لا يتمتع الدليل الإلكتروني بخصوصية استثنائية تعزله عن القواعد العامة للإثبات، بل يخضع لذات المعايير القانونية والمنطقية التي تحكم باقي الأدلة، حيث يتولى القاضي وزنه واستخلاص قيمته التدليلية وفقاً لاقتناعه الوجداني.

" ولقد أشار المشرع الجزائري إلى هذه المسألة بنصه على مبدأ الاقتناع الجزائي في المادة307 من قانون الاجراءات الجزائية التي تنص على إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الاخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص في ضمائرهم في أي تأثير قد أحدثته في إدراكهم الادلة المستندة إلى المتهم وأوجه الدفاع، وفي إطار إعمال مبدأ الإقناع القضائي يترتب عن ذلك: حرية القاضي في قبول و تقدير الدليل الالكتروني"[6]

- **حرية قاضي الجزائي في قبول و تقدير الدليل الرقمي:**

يتسهل القاضي الجزائي فحص الخصومة بتقرير مدى مقبولية الدليل الرقمي، وهي عملية إجرائية تليها مرحلة التقييم الموضوعي المستندة إلى السلطة التقديرية للمحكمة. إن جوهر هذه السلطة يكمن في إعمال مبدأ

[1] الامر رقم 66-156 مؤرخ في8 يونيو 1966 ،المتضمن قانون العقوبات، ج ر 49 المؤرخة في 11 جوان 1966 المعدل القانون رقم 16-02 2 المؤرخ في 19 يونيو سنة 2016، ج ر 37، المؤرخة في 22 يونيو سنة 2016، دار بلقيس للنشر، الجزائر، سنة 2019 ،ص 5.
[2] ديب اكرم، بن عبد الله نورة، المرجع السابق، ص410.
[3] مروة صالح الدين محمد، الدليل الكرتوني ومدى حجيته في الإثبات الجنائي، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية ، القاهرة، مصر، سنة 2021، ص 120.
[4] ديب اكرم، بن عبد الله نورة، المرجع السابق، ص410.
[5] عيدة بمعابد، الدليل الرقمي بين حتمية الاثبات الجنائي والحق في الخصوصية المعلوماتية، ملمة آفاق علمية، المجلد11، العدد1،السنة2019، ص137.
[6] ايت حمودة كاهنة، المرجع السابق، ص193.

الاقتناع القضائي، الذي يتيح للقاضي تطويع وسائل الإثبات وتنسيق جهود البحث عما يخدم الحقيقة اليقينية. وعليه، فإن هذا المبدأ لا يحكم مشروعية الوسيلة' فحسب، بل يُعد المعيار الأساسي لتقدير **القوة التدليلية** الكامنة في الدليل الرقمي ومقدار الثقة التي يوليها له القاضي،[1] بالتالي إن إطلاق سلطة القاضي في تقدير وسائل الإثبات يجد تبريره في غاية القانون الجنائي وهي **إصابة الحقيقة**؛ وبناءً عليه، يتمتع القاضي الجزائي بمركز إيجابي يتيح له وللخصوم طرح كافة الأدلة وتداولها بحرية تامة. وتعكس هذه الصلاحية 'ذاتية قواعد الإثبات الجزائي' التي ترفض الجمود وتفارق المسلك السلبي للقاضي المدني، مما يجعل من الخصومة الجنائية ساحة للبحث النشط عن الحقيقة وليس مجرد صراع شكلي على الأدلة.[2]

موقف المشرع الجزائري من الأخذ بحجية الدليل الالكتروني:

رغم خلو التشريع الجزائي من نص صريح يقر بمقبولية الدليل الإلكتروني، إلا أن الأساس القانوني للاعتداد به يجد مرجعيته في المادة 212من قانون الإجراءات الجزائية، التي تكرس مبدأ حرية الإثبات في المواد الجنائية. ويتناغم هذا التوجه مع نظيره في التشريع الفرنسي المادة 427، حيث يُسمح بإثبات الجرائم بكافة الوسائل ما لم ينص القانون على خلاف ذلك. وبناءً عليه، يمتلك القاضي سلطة بناء حكمه وفقاً لاقتناعه الخاص، شريطة أن يستند في ذلك إلى أدلة طُرحت للمناقشة الوجاهية والعلنية أثناء المحاكمة.[3]

_ان إدراج المشرع الجزائري لهذه المادة ضمن الأحكام المشتركة لوسائل الإثبات يقطع دابر الشك حول شمولية تطبيقها أمام كافة الجهات القضائية؛ حيث كرس نظام الأثبات المقيد كأصل عام، مع الإبقاء على نظام الإثبات المقيد كاستثناء تمليه بعض النصوص الخاصة[4]. وبذلك، يكون المشرع قد انخرط في التوجه العالمي الرامي إلى تعزيز الحجية القانونية للأدلة الرقمية بكافة صورها، بدءاً من المحررات ذات الشكل الإلكتروني،[5] وصولاً إلى التوقيع والتصديق الإلكترونيين،[6] إضفاءً للصبغة القانونية على المعاملات والجرائم المستحدثة.

_ كدلك عزز المشرع الجزائري منظومة الإثبات الرقمي بفرض تدابير إجرائية صارمة تتعلق بـ **مراقبة الاتصالات الإلكترونية** وحفظ بيانات حركة السير(Traffic Data) ، وقد ألقى المشرع على عاتق مؤدي الخدمات التزاماً قانونياً بحفظ الأدلة الرقمية وضمان سلامتها، مع إتاحة المجال للجهات القضائية للاستعانة بـ **ذوي الخبرة والمؤهلات التقنية**؛ وذلك لتقديم الدعم الفني اللازم لاستخلاص الأدلة وتفسيرها، بما يخدم مقتضيات التحقيق الجنائي الحديث.[7]

كما يتضح جلياً أن المنظومة التشريعية في الجزائر قد أقرّت بصلاحية الأدلة الرقمية كركيزة للإثبات الجنائي، إدراكاً منها بضرورة تفعيل آليات مكافحة الجريمة الإلكترونية. ويتجلى هذا المنحى في الاعتراف المتزايد بحجية الوسائط الرقمية بمختلف صورها التقنية، مع مساواة التوقيع الرقمي نظيره الفيزيائي في القوة التدليلية. بيد أن هذا التحول نحو البيئة التقنية لم يأتِ على حساب المبادئ الجوهرية للتقاضي؛ إذ يظل العلني، وضمان حصانته التقنية ضد أي تزوير أو تعديل[8].

---

[1] سالمة محمد لمنصوري، تطبيق مبدأ الاقتناع القضائي على الدليل الالكتروني، أطروحة لنيل الماجستير، جامعة 47 الامارات العربية المتحدة، ص81.

[2] المرجع نفسه، ص82.

[3] المادة 212 من قانون الاجراءات الجزائية الجزائري.

[4] بوحميط يزيد ، السياسة الجنائية في مجال مكافحة الجرائم الالكترونية في الجزائر أطروحة دكتوراه ، كلية الحقوق ، 50 قسم القانون الخاص، جامعة باجي مختار، عنابة، 2016 ،ص285.

[5] المادة 323 مكرر 1 من الامر رقم 75-58 المؤرخ في 1975/09/26 و المتضمن القانون المدني و التي 51 تنص على " يعتبر الاثبات بالكتابة في الشكل الالكتروني كالأثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون معدة ومحفوظة في ظروف تضمن سالمتها".

[6] لمادة 2 الفقرة أولى من القانون رقم 04/15 ،المؤرخ في 2015/02/01 ،المحدد لقواعد العامة المتعمقة 52 بالتوقيع والتصديق الالكترونيين، جريدة رسمية العدد: 06.

[7] المواد 4-12 من القانون رقم 04/09.

[8] بوحميط يزيد ، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر أطروحة دكتوراه ، كمية الحقوق ، 50 قسم القانون الخاص، جامعة باجي مختار، عنابة، 2016 ،ص285.

استناداً إلى القواعد العامة المقررة في قانون الإجراءات الجزائية، لا يجد القاضي الجزائي عائقاً في الأخذ بالدليل الإلكتروني، نظراً لسيادة مبدأ حرية الإثبات الذي يميزه عن نظيره في المادة المدنية. وبموجب هذه السلطة التقديرية، يصبح الدليل الرقمي وسيلة مقبولة لبناء عقيدة المحكمة[1].

[1] ايت حمودة كاهنة، المرجع السابق، ص195.

الفصـــــــــل الثانـــــي
انعكاســـــات التحـــــــول الرقـــمي على جريمة الابـــتزاز الالكتروني

تمهيد

لم يكن التحول الرقمي مجرد طفرة تكنولوجية تيسّر سبل الاتصال، بل أفرز واقعاً موازياً أعاد تشكيل البنية الهيكلية للجريمة وأنماط مرتكبيها. فقد أدى التطور التقني المتسارع والاعتماد الكلي على الشبكات الافتراضية إلى بروز جيل سيبراني من الجناة يمتلكون أدوات تخفٍّ واختراق فائقة، مما جعل الأفراد والمؤسسات على حد سواء عرضة لاستهداف ممنهج. إن هذا التحول فرض صوراً واقعية وخطيرة للابتزاز لم تكن معهودة في الإجرام التقليدي؛ مما يفرز تداعيات حتمية تمس عمق الحماية الجنائية المقررة في التشريع الجزائري والمقارن .ومن هذا المنطلق، يخصص هذا الفصل لبحث تجليات هذا التحول؛ حيث نسلط الضوء في المبحث الأول على المظاهر المستحدثة للجناة والضحايا والأشكال الواقعية لهذه الجريمة، لننتقل في المبحث الثاني إلى تحليل الآليات القانونية والتقنية المعتمدة للوقاية من هذا الإجرام العابر للحدود ومكافحته

المبحث الأول: المظاهر المستحدثة للجريمة الابتزاز الالكتروني (الجناة والضحايا)

أدى التحول الالكتروني المتسارع إلى ظهور جيل جديد من المجرمين الذين يمتلكون مهارات تقنية عالية، كما وسع من دائرة الاستهداف لتشمل الأفراد والمؤسسات على حد سواء. وسنحاول من خلال هذا المبحث تسليط الضوء على هؤلاء الفاعلين (المبتزين) وصور الاعتداءات التي يمارسونها ضد الأشخاص الطبيعيين والمعنويين.

المطلب الأول: الأشكال الواقعية للجناة والضحايا في جريمة الابتزاز

يتطلب فهم جريمة الابتزاز الإلكتروني الخروج من الإطار النظري الضيق لدراسة أشكالها وصورها الحقيقية كما تحدث في الواقع المعاش؛ إذ يتنوع المبتزون في أساليبهم وأهدافهم تَبَعاً لطبيعة الضحية المستهدفة. وبناءً على ذلك، سنقوم في هذا المطلب بتسليط الضوء على أنواع المبتزين، ثم نستعرض أمثلة ونماذج واقعية لهذه الجريمة، مقسمين إياها بحسب نوع الضحية؛ حيث نبدأ بالشخص الطبيعي (الأفراد) وما يتعرض له من ابتزاز عاطفي، وغير اخلاقي، أو استغلال للأطفال وعبر الألعاب الإلكترونية، ثم ننتقل إلى الشخص المعنوي (الشركات والمؤسسات) لنبين كيف يتم استهدافها ومساومتها عبر البريد الاحتيالي، أو تعطيل موزعي الخدمة، وتشفير البيانات والمطالبة بالفدية المالية.

الفرع الأول: التصنيف النوعي للمبتزين وصور الابتزاز الالكتروني على الأشخاص الطبيعيين

يعد الشخص الطبيعي الحلقة الأضعف والأكثر استهدافاً في الفضاء الالكتروني، نظراً للعفوية في استخدام الوسائط الإلكترونية. إلا أن فهم كيفية وقوع هذا الاعتداء يتطلب أولاً تسليط الضوء على هوية القائم به؛ إذ يتنوع الجناة بين مراهقين يقودهم الفضول الرقمي، وبين محترفين يمتلكون مهارات الاختراق والبرمجة (الهاكرز والكراكرز) الذين يسخرون قدراتهم لسلب إرادة الضحايا وتطويعهم، تمهيداً لممارسة صور شتى من الابتزاز، تتراوح بين ما هو غير اخلاقي وعاطفي، وبين ما يمس السلامة النفسية والمالية للأطفال والمستخدمين.

البند الأول: الأنماط الإجرامية للمبتزين في البيئة الرقمية

لا يمكن فهم الركن المادي لجريمة الابتزاز الإلكتروني بمعزل عن دراسة "الجاني" (المبتز)، إذ أن طبيعة الوسيلة التقنية المستخدمة في التهديد تفرض وجود تفاوت في المهارات الإجرامية. فالمبتز في الفضاء الرقمي ليس نمطاً واحداً، بل تتعدد شخصياته الإجرامية وفقاً لدرجة الاحترافية والدوافع التقنية، وبما اننا قد عرجنا سابقا للركن المادي لجريمة الابتزاز أصبح من الواجب التعرج لأنماط المجرمين، ويمكن تقسيمهم إلى ثلاثة أنماط رئيسية:

أولاً: المبتز الهاوي او الشخص العادي

يتمثل هذا النمط غالباً في فئة الشباب أو المراهقين الذين يمتلكون مهارات تقنية بسيطة، ويقودهم الفضول الرقمي لاستخدام برامج جاهزة لاختراق الحسابات الشخصية. غالباً ما يكون دافعهم هو حب الاستطلاع أو إثبات الذات تقنياً، ولكن سرعان ما يتحول هذا الفضول إلى جريمة ابتزاز عند العثور على بيانات أو صور خاصة للضحية، حيث يبدأ الجاني في مساومتها مقابل مبالغ زهيدة أو تنازلات معنوية. يضم هذا النمط الطائفة الأوسع من مرتكبي جريمة الابتزاز في الفضاء الرقمي، ويتميز هؤلاء الجناة بكونهم لا يمتلكون بالضرورة مهارات برمجية عميقة، بل يعتمدون على "الهشاشة النفسية" للضحية أو "الثغرات الأمنية البسيطة" في الحسابات الشخصية، وينقسمون إلى فئتين:

1. **المبتز التقليدي (الاجتماعي) :**وهو الجاني الذي لا تربطه بالتقنية صلة احترافية، بل يستمد قوته الإجرامية من **"رابطة الثقة "**التي كانت تجمعه بالضحية (كعلاقة زمالة، قرابة، أو صداقة). يحصل هذا المبتز على المادة محل التهديد (صور، مقاطع فيديو، محادثات سرية) بطريقة مشروعة في

بدايتها نتيجة الثقة المتبادلة، أو بطريقة غير مشروعة بسيطة (كاستراق النظر أو استغلال ترك الجهاز مفتوحاً)، ثم يوظف الوسائط الالكترونية (مثل "واتساب" أو "فيسبوك") كأداة ضغط لمساومة الضحية لتحقيق مآرب مادية أو معنوية بعد انهيار تلك الرابطة[1].

2. **المبتز الهاوي (الفضولي) :**ويمثل جيل الشباب المولع بالتكنولوجيا دون الوصول لدرجة الاحتراف (الهاكرز). يعتمد هذا الجاني على استخدام تطبيقات جاهزة، أو روابط "اصطياد" بسيطة، أو استغلال كلمات المرور الضعيفة لاختراق الحسابات الشخصية. دافعه الإجرامي غالباً ما يكون "وليد الصدفة"؛ حيث يبدأ بفضول الاختراق والاطلاع على أسرار الغير، وبمجرد عثوره على محتوى حساس، يتولد لديه القصد الجنائي لممارسة الابتزاز. تكمن خطورته في كونه غالباً ما يتحرك بدافع التباهي أو الرغبة في الكسب السريع دون إدراك تام للتبعات الجزائية لفعلته.

ثانياً: المجرم المعلوماتي

" إن المجرم المعلوماتي هو شخص يختلف عن المجرم العادي فال يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية حيث يكون على أتم الاطلاع بمختلف التقنيات المتعلقة بالإعلام الآلي وبشبكة الأنترنت ولهم خبرة في التعامل مع البرامج ولغات البرمجة حيث نميز ثالثة أنواع بارزة لهؤلاء المجرمين أو بالأحرى ثالث تصنيفات سنوجزها كما يلي :

1. **الهاكرز:** هو شخص فضولي في بعض الأحيان، يكون عادة من المراهقين المولعين بالشبكة العنكبوتية، حيث يدفعهم الفضول إلى معرفة كلمة سر بعض الأشخاص و الدخول على نظامهم المعلوماتي، والعبث بالمعلومات والبيانات الشخصية، ومحاولة استعمالها ضده بغرض تجريب طرق الولوج غير المصرح به، حيث يقوم هذا الشخص بإخفاء نواياه الحقيقية حتى يستطيع كسب ثقة الفرد الذي يكون معه على اتصال غما في منتدى عام أو خاص أو موقع للدردشة أو موقع من مواقع التواصل الاجتماعي مثل الفيسبوك أو التويتر أو غيرهما،... حيث يعتمد "الهاكرز "على استخدام برامج خبيثة تحمل في طياتها صفات الجوسسة ومن ثم يقوم بإرسال هذه البرامج أو أحدها إلى الضحية عن طريق برنامج مموه وغير قابل للكشف من طرف برنامج مكافحة الفيروسات، ومن ثم فإنه وبعد تلقي البرنامج المموه فإن "الهاكرز" يقوم بتنفيذ خططه بدء بالسطو على كل ما يحتويه جهاز الضحية من ملفات وصور وفيديو وغيرها، أو قد يذهب إلى أبعد من ذلك حيث يستطيع أن يصل إلى كل كلمة سر قد قامت الضحية بكتابتها على جهازها، وبالتالي يمكنه أن يستعمل كل ما تم الكشف عنه ضد الضحية مطالبا أبعدً إياها بتلبية بعض المطالب سواء كانت مالية بحتة أو حتى من ذلك كأن يطلب من الضحية - إذا كانت أنثى – الخروج معها في معود الغرض منه الاعتداء الغير اخلاقي بطبيعة الحال.
2. **الكراكرز:** هم أشخاص متسللون يتابعون عن كثب آخر الأخبار او برامج الحماية الأمنية للأجهزة والمعلومات، إلى حد أنهم ينشئون النوادي لتبادل المعلومات .وهؤلاء المجرمون يستطيعون الاجتياز- التخطي - الأمني لمختلف المواقع بقصد التخريب و الاختلاس و التزوير، و من أهم هذه الجماعات هي جماعة القراصنة الروس الذين يعتبرون الأفضل على الإطلاق، ففي استطلاع للأراء أكد أنهم متمكنون من الخرق الآلي للأنظمة بنسبة 82%حتى أن الولايات المتحدة الأمريكية وجهت الاتهام لروسيا بمحاولة سرقة برامج نظام تمركز الصواريخ العالي، ألن بعض الهاكرز الروس قاموا بمهاجمة موقع حلف الأطلسي ومواقع تابعة للعديد من الحكومات. و للعلم فإن هناك بعض المجلات

[1] عمر خوري، الحماية الجنائية للحياة الخاصة في ظل تكنولوجيا المعلومات والاتصال، دار الجامعة الجديدة، الإسكندرية، 2014، ص 88.

التي تصدر مهمتها الدفاع عن هذه الفئة التي ال تعتبرها مجرمة بل تقول انهم يبلون حسنا، و أنهم يكتشفون الثغرات الأمنية في الأنظمة المعلوماتية".[1]

3. **مصممو المواقع الخطيرة:** وتسمى المنظمات الاجرامية السيبرانية وهي تلك المواقع التي تروج للفكر الإرهابي و الإباحي و حتى الوهمية لجلب الأفراد المهتمين بالتسوق مثال من اجل معرفة شفرة بطاقة الائتمان (البطاقات البنكية، البريدية، ...)، و استعمالها لحاجات شخصية ، مع الإشارة الى ان هذه الجماعات تتخذ الابتزاز نشاطا منظما وعابرا للحدود ، و لكن الملاحظ ان هذه الفئة اقل خبرة من الفئة السابقة الذكر . وتجدر الإشارة إلى أن المشرع الجزائري قد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.[2]

البند الثاني: أمثلة واقعية عن صور الابتزاز المسلطة على الأشخاص الطبيعيين

بعدما عرفنا أنواع الابتزاز في الفصل الأول من الناحية النظرية، سنحاول في هذا الفرع تقديم **أمثلة واقعية** توضح كيف تقع هذه الجرائم في الحقيقة. فالهدف هنا ليس إعادة التعريف، بل إظهار الطرق التي يستخدمها المجرمون للوصول إلى ضحاياهم من الأفراد العاديين، وسوف نعرض هذه الأمثلة في ثلاث نقاط أساسية:

أولاً: أمثلة عن الابتزاز ذو الطابع الشخصي (الغير اخلاقي والعاطفي).

ثانياً: أمثلة عن الابتزاز عبر منصات التواصل والألعاب الإلكترونية (استهداف الأطفال).

ثالثاً: أمثلة عن الابتزاز المالي عبر البريد الإلكتروني (تقنيات الاصطياد).

أولاً: الابتزاز ذو الطابع الشخصي (الابتزاز الغير اخلاقي والعاطفي)

تعتبر هذه الصورة من أخطر أنواع الابتزاز لأنها تمس شرف الإنسان وخصوصيته. وبما أننا سبق وعرّفنا هذا النوع من الجانب النظري في الفصل الأول، سنقوم هنا بتقديم مجموعة من الأمثلة والحالات الواقعية التي تبرز كيف يتم استغلال المشاعر أو الصور الخاصة للضغط على الضحية وإجبارها على تنفيذ طلبات الجاني، سواء كانت هذه الطلبات مالية أو غير ذلك.

من خلال تحليل الحالات الواقعية، يتضح أن الابتزاز الشخصي لا يقتصر فقط على طلب مبالغ مالية، بل يمتد ليشمل طلب "تنازلات أخلاقية" أو القيام بأفعال مخلة بالحياء تحت ضغط التهديد بالفضيحة، وهو ما يظهر في النماذج التالية:

1. نموذج الابتزاز العاطفي (استغلال الثقة):

يحدث هذا عندما يستغل الجاني مشاعر الضحية أو "رابطة الثقة" السابقة (كالوعد بالزواج) للحصول على صور خاصة. وبمجرد انتهاء العلاقة، يبدأ الجاني في تهديد الضحية بنشر هذه الصور لإجبارها على العودة إليه أو الاستمرار في علاقة غير شرعية رغماً عنها.

[1] سعيد زيوش، ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها - قراءة سوسيولوجية وأراء نظرية- ، العدد 22، مجلة العلوم الاجتماعية، جانفي 2017، ص ص75 76.

[2] قانون العقوبات الجزائري، القسم السابع مكرر، الفصل الثالث، القانون رقم05-04 المؤرخ في 10 نوفمبر 2004.

- مثال: حالة "مريم" (الموظفة) التي تعرضت للتهديد بنشر صور ذكرياتها السابقة من طرف صديق سابق، حيث كان الهدف هو الضغط النفسي عليها ومساومتها مادياً ومعنوياً.[1]

2. نموذج الابتزاز الغير اخلاقي مقابل "أفعال مخلة" (بدل المال):

في هذه الحالة، يكون غرض المبتز هو إشباع رغباته الدنيئة وليس الحصول على المال. حيث يهدد الضحية بنشر فيديوهات أو صور فاضحة لها ما لم تستجب لطلبه باللقاء أو ممارسة أفعال غير اخلاقية.

الواقعة: تشير التقارير الأمنية إلى أن الكثير من الفتيات يقعن في "فخ الاستدراج"، حيث يطلب المبتز "صوراً أكثر جرأة" أو "لقاءات غير اخلاقية" مقابل مسح ما لديه من صور قديمة، وهو ما يُغرق الضحية في سلسلة لا تنتهي من التنازلات خوفاً من الفضيحة.

3. نموذج الابتزاز عبر "المونتاج" والتزييف:

لا يشترط أن تكون المادة حقيقية، بل قد يلجأ الجاني (مثل زميل الدراسة أو العمل) إلى تركيب وجه الضحية على محتوى غير اخلاقي.

- مثال: قضية الطالبة "نسرين" التي حاول زميلها ابتزازها بمبلغ مالي (100 ألف دينار) مقابل عدم نشر صور مفبركة لها، وهو ما يثبت أن الجاني قد يكون شخصاً "عادياً" أو "هاوياً" كما ذكرنا سابقاً، ولكنه يستخدم وسائل تقنية مخربة.[2]

ثانياً: الابتزاز عبر منصات التواصل والألعاب الإلكترونية (استهداف الأطفال والمراهقين)

تعتبر فئة القصر والمراهقين من أكثر الفئات عرضة للابتزاز الإلكتروني نظراً لنقص خبرتهم وسهولة استدراجهم عاطفياً وتقنياً. فالمجرمون هنا لا يستخدمون القوة، بل يستخدمون "أسلوب الإغراء" أو "المصادقة" داخل بيئات تبدو في ظاهرها ترفيهية، وسنوضح ذلك من خلال الأمثلة التالية:

1. **نموذج الابتزاز عبر الألعاب القتالية (مثل PUBG وFree Fire):**

أصبحت غرف الدردشة داخل الألعاب الجماعية مكاناً سهلاً للمبتزين للتقرب من الأطفال، وعند تحليل ظاهرة ابتزاز الأطفال عبر الألعاب الإلكترونية، يشير **دليل التوعية ضد مخاطر الابتزاز (#لا_تغفل_عنها)** إلى أن المجرمين يستخدمون استراتيجية "التدريج في الاستدراج" (Grooming)حيث تبدأ العلاقة تحت غطاء اللعب الجماعي، ثم تنتقل إلى محاولة عزل الطفل عن رقابة والديه من خلال:

1. **بناء الثقة الوهمية :**عبر منح الطفل مكافآت داخل اللعبة أو إظهار اهتمام مبالغ فيه بهواياته.
2. **استغلال البراءة :**دفع الطفل للقيام بأفعال تبدو بسيطة (مثل تصوير غرفته أو ملابسه) ثم استخدام تلك الصور كأوراق ضغط وتهديد.

---

[1] توفيق بوقعدة، الجزائر: عصابات تستغل وسائل التواصل الاجتماعي للابتزاز، مقال منشور بموقع(DW عربية)، بتاريخ 17 أبريل 2016، متاح على الرابط: [https://www.google.com/search?q=https://www.dw.com/ar/a-19177395]، تاريخ الاطلاع: (2026/5/6 الساعة21:28).

[2] "نلاحظ من هذه الأمثلة أن المشرع الجزائري من خلال المادة 303 مكرر وما بعدها، والمادة 371 من قانون العقوبات، يحمي حرمة الحياة الخاصة بصرف النظر عن وسيلة التهديد أو الغرض منه، سواء كان الغرض الحصول على مبالغ مالية أو إجبار الضحية على القيام بأفعال مخلة بالحياء."

- **العامل النفسي :**يعتمد المبتز هنا على خوف الطفل من العقاب؛ حيث يُوهمه بأن والديه سيعاقبانه إذا اكتشفا صوره أو محادثاته، مما يجبر الطفل على الرضوخ لمطالب المبتز (سواء كانت مالية أو غير اخلاقية) خوفاً من الفضيحة.[1]
- مثال: يبدأ الجاني باللعب مع الطفل وتقديم "هدايا مجانية" أو "ترقية لمستوى اللعب"، وبعد كسب ثقة الطفل، يطلب منه الانتقال للتواصل عبر تطبيقات أخرى (مثل واتساب) وإرسال صور خاصة أو صور لأفراد عائلته أو بيانات بنكية خاصة بوالديه، ثم يبدأ بتهديد الطفل بحرمانه من اللعبة أو نشر صوره إذا لم ينفذ طلباته.

"تجسد هذه الصورة عملياً في قضية عالجتها مصالح الأمن المختصة، وتتلخص وقائعها فيما يلي:

قام شخص بالغ بانتحال صفة مراهق عبر لعبة قتالية مشهورة (لعبة Free Fire)، حيث بدأ باللعب مع طفل قاصر وتوطيد العلاقة معه من خلال منحه هدايا افتراضية داخل اللعبة (شحن جواهر أو أسلحة مجانية).

بعد كسب ثقة الطفل، أقنعه الجاني بالانتقال للتحدث عبر تطبيق "فايبر" ، وهناك طلب منه تصوير نفسه و تصوير "البطاقة البنكية" لوالديه مقابل منحه ميزات أكبر في اللعبة. وبمجرد حصول الجاني على صور خاصة للطفل و لبيانات عائلته، بدأ بتهديده بنشر تلك الصور أو إخبار عائلته بأنه "سارق" إذا لم يقم الطفل بإرسال مبالغ مالية (عن طريق تعبئة أرصدة هاتفية أو تحويلات ماليّة).

وتوضح هذه الواقعة كيف تتحول الوسيلة الترفيهية إلى فخ لاستدراج القصر وابتزازهم."[2]

2. **نموذج "تحديات" منصات التواصل (مثل TikTok وSnapchat):**

يستغل المبتزون رغبة المراهقين في الشهرة أو الحصول على "متابعين"، فيقوم الجاني بانتحال صفة "مدير أعمال" أو "مؤثر مشهور".

- مثال: إقناع مراهقة بالمشاركة في "تحدي" يتطلب القيام بحركات معينة أو ارتداء ملابس معينة أمام الكاميرا، ليقوم الجاني بتسجيل هذه اللقطات واستخدامها لاحقاً لابتزازها مادياً أو إجبارها على القيام بأفعال مخلة بالحياء خوفاً من إرسال الفيديو لأهلها.

3. **نموذج انتحال الشخصية (البروفايل الوهمي):**

كثير من المبتزين ينشئون حسابات بأسماء وصور فتيات للتقرب من مراهقين، أو العكس، بهدف الحصول على أسرار عائلية أو صور خاصة.

- الواقعة: أثبتت التقارير الأمنية أن الكثير من المراهقين وقعوا ضحايا لمبتزين أوهموهم بالحب والصداقة، ليتضح في النهاية أن خلف الشاشة "عصابة" تهدف لابتزاز العائلة مالياً من خلال استغلال خصوصية أبنائهم.[3]

ثالثاً: الابتزاز المالي عبر البريد الإلكتروني(تقنيات الاصطياد)

واقعة حقيقية: الابتزاز المالي عبر انتحال صفة هيئة رسمية (تطبيق بريدي موب)

شهدت الساحة الوطنية في الآونة الأخيرة موجة واسعة من عمليات الاحتيال والابتزاز التي استهدفت مستخدمي تطبيق "بريدي موب .(BaridiMob) "وتعتبر هذه الواقعة نموذجاً حياً لما يسمى بـ "الهندسة الاجتماعية" والاصطياد الإلكتروني، وتتلخص وقائعها فيما يلي:

---

[1] انظر في هذا الصدد: منظمة الإنتربول عملية (Strikeback)، وراجع أيضاً: المركز الوطني للوقاية من الجريمة، **دليل التوعية ضد مخاطر الابتزاز الإلكتروني (#لا_تغفل_عنها)**، ص 12-14.

[2] محمد الأمين بن ميسرة، الحماية الجنائية للطفل من الجرائم المعلوماتية في التشريع الجزائري، مجلة البحوث والدراسات القانونية والسياسية، العدد12، جامعة البليدة 2، ص 145.

[3] "المشرع الجزائري أفرد حماية خاصة للقصر في قانون العقوبات وفي القانون رقم 15-12 المتعلق بحماية الطفل، حيث تُشدد العقوبة إذا كان ضحية الابتزاز الإلكتروني قاصراً، نظراً لضعف إدراكه وعدم تقديره للعواقب."

1. **أسلوب الخداع :**يتلقى الضحية رسالة نصية (SMS) على هاتفه المحمول، تظهر في صندوق الرسائل تحت اسم "BaridiMob" أو "Algérie Poste" لإيهام الضحية برسميتها. تخبره الرسالة بأن "حسابه البريدي محظور" أو "يجب تحديث البيانات لتفادي قطع الخدمة"، مع وضع رابط إلكتروني مشبوه.
2. **الفخ التقني :**بمجرد ضغط الضحية على الرابط، ينتقل إلى صفحة مزورة تشبه تماماً الواجهة الرسمية للتطبيق، ويُطلب منه إدخال "اسم المستخدم"، "كلمة المرور"، و"رقم البطاقة الذهبية."
3. **مرحلة الابتزاز والسرقة :**بمجرد حصول الجناة على هذه البيانات، يقومون بسحب الرصيد المالي للضحية. وفي حالات أخرى، يتم ابتزاز الضحية؛ فإذا كانت المبالغ الموجودة في الحساب قليلة، يقوم الجاني بالاتصال بالضحية وتهديده باستخدام بياناته البنكية في عمليات غير قانونية أو حرمان صاحب الحساب من استرجاعه إلا مقابل دفع مبالغ مالية (فدية).

أصدرت مؤسسة بريد الجزائر والمصالح الأمنية (الأمن الوطني والدرك الوطني) عدة بيانات تحذيرية رسمية تؤكد فيها أن الإدارة لا تطلب أبداً الأرقام السرية عبر الرسائل النصية، ودعت المواطنين لعدم الضغط على الروابط المجهولة[1].

ولمواجهة هذه الموجة من الابتزاز المالي، قامت مؤسسة **بريد الجزائر** بتغيير سياستها التواصلية، حيث أصبحت ترسل رسائل نصية تحذيرية دورية لكافة زبائنها، تنبههم فيها بضرورة الحفاظ على سرية المعلومات وعدم الانسياق وراء الروابط المشبوهة التي تنتحل صفة تطبيق (بريدي موب).

ويعتبر هذا الإجراء دليلاً على استفحال الجريمة وتطور أساليب المبتزين الذين لم يعودوا يستهدفون الأفراد بشكل عشوائي فحسب، بل أصبحوا ينتحلون صفة هيئات رسمية لكسب الثقة، وهو ما دفع المصالح الأمنية والمؤسسات المالية لتكثيف الحملات التحسيسية للحد من عدد الضحايا.

قد يبدو للوهلة الأولى أن الأمثلة المتعلقة بانتحال صفة المؤسسات الرسمية – مثل مؤسسة بريد الجزائر – تنتمي إلى الابتزاز المسلط على الشخصية المعنوية، إلا أننا آثرنا إدراجها ضمن هذا المطلب (الأشخاص الطبيعيين) لسبب جوهري؛ وهو أن **المستهدف الحقيقي** من وراء هذه الهجمات هو **المواطن البسيط** في ذمته المالية وأمنه الشخصي، حيث تُستخدم أسماء المؤسسات هنا كـ **"وسيلة تدليسية "**فقط للوصول إلى الشخص الطبيعي وابتزازه، وليس للإضرار بنظام المؤسسة في حد ذاته.

رابعاً: الابتزاز الغير اخلاقي العابر للحدود (قضية "الإنتربول" والشبكات المنظمة)

لا يتوقف الابتزاز الإلكتروني عند حدود الدولة الواحدة، بل قد يدار من قبل عصابات دولية منظمة تستهدف الضحايا عبر القارات. ومن أبرز الحالات الواقعية التي وثقتها منظمة الشرطة الجنائية الدولية (الإنتربول) نذكر:

1. قضية عملية الضربة المضادة(Strike back):

تعتبر هذه العملية من أشهر القضايا الدولية التي استهدفت شبكات "الابتزاز الغير اخلاقي" (Sextortion) ، حيث تم تفكيك شبكة إجرامية في الفلبين كانت تدير مكاتب تشبه "مراكز الاتصال" (Call Centers) لكن مهمتها كانت استدراج الضحايا من مختلف دول العالم (المملكة المتحدة، الولايات المتحدة، آسيا...) عبر الإنترنت.

[1] انظر: البيانات التحذيرية الصادرة عن مؤسسة بريد الجزائر عبر صفحاتها الرسمية حول حملات الاحتيال والابتزاز الإلكتروني، فيفري/مارس 2026. انظر أيضاً: منشورات "خلية مكافحة الجريمة المعلوماتية" للأمن الوطني الجزائري حول حماية البيانات البنكية.

- **أسلوب الجريمة:** كان أفراد هذه العصابة يتلقون تدريبات وحوافز مالية مقابل بلوغ "أهداف مالية" محددة من خلال ابتزاز الضحايا بصور أو فيديوهات حميمية، وتراوحت المبالغ المطلوبة بين 500 و15000 دولار أمريكي.
- **النتائج المأساوية:** أدت هذه الشبكة إلى انتحار مراهق (دانيال بيري) في اسكتلندا بعد وقوعه ضحية لابتزازهم، مما يبرز الأثر القاتل لهذه الجرائم على الحالة النفسية للأفراد.

2. استدراج القصر عبر انتحال الشخصية:

أشار تقرير الإنتربول في هذه الواقعة إلى أسلوب "طلب المشاهد الحية" (Livestreaming)، حيث ينتحل المبتزون شخصية أطفال أو مراهقين لكسب ثقة أقرانهم، ثم يصورونهم في أوضاع مخلة لاستخدامها كأداة ضغط مستمر للحصول على مزيد من الصور أو المال.[1]

خامسا: الآثار الاجتماعية والنفسية الوخيمة (الحق في الحياة والسمعة)

لا تتوقف خطورة الابتزاز الإلكتروني عند حدود الضرر المالي أو النفسي العابر، بل قد تمتد لتشكل تهديداً مباشراً لـ **'الحق في الحياة'**، خاصة في المجتمعات العربية التي تتسم بحساسية مفرطة تجاه قضايا الشرف والسمعة.

ويبرز **النموذج العراقي** كواقعة مأساوية ومعاصرة في هذا السياق؛ حيث تشير التقارير الحقوقية والإعلامية الدولية (مثل تقرير مؤسسة **DW**) إلى تصاعد ظاهرة انتحار النساء والفتيات نتيجة وقوعهن ضحايا لشبكات الابتزاز الإلكتروني. فالمبتز هنا لا يكتفي بالتهديد بنشر المحتوى الحميمي، بل يعمد إلى استغلال 'الوصمة الاجتماعية' كأداة ضغط قاتلة، مما يضع الضحية أمام خيارات أحلاها مرّ؛ إما الرضوخ لمطالب المبتز اللامتناهية، أو مواجهة مصير اجتماعي قد يصل إلى حد التعرض لجرائم الشرف أو الإقصاء الأسري التام.

إن هذا المثال الواقعي يفرض على المشرع ضرورة عدم التعامل مع الابتزاز كجريمة معلوماتية بسيطة، بل كجريمة مركبة تمس أمن الفرد وحياته، مما يستوجب توفير آليات حماية تتجاوز العقوبات الزجرية لتشمل الدعم النفسي والاجتماعي وتأمين سرية البلاغات.[2]

سادسا: إشكالية "الرضا المسبق" وعلاقتها بالتكييف القانوني لجريمة الابتزاز

تثور في الواقع العملي والقضائي إشكالية قانونية دقيقة تتعلق بمدى تأثير السلوك المسبق للضحية على قيام جريمة الابتزاز؛ ففي كثير من حالات الابتزاز العاطفي أو الغير اخلاقي، تبدأ العلاقة "برضا" الضحية (كإرسال صور أو فيديوهات طواعية في سياق ثقة متبادلة). وهنا يطرح التساؤل القانوني التالي: **هل يعتد برضا الضحية الأولي كسبب لانتفاء الركن المادي للجريمة؟ وهل يسقط حق الضحية في الحماية القانونية إذا كان قد ساهم بسلوكه في تمكين المبتز من المادة محل التهديد؟**

للإجابة على هذه الإشكالية، يجب التفرقة بين "الفعل التمهيدي" وبين "فعل الابتزاز" بذاته، وذلك وفق النقاط التالية:

- **استقلال جريمة الابتزاز:** إن الرضا بالارتباط أو بمشاركة المحتوى في البداية لا يعني إطلاقاً الرضا بالتعرض للابتزاز لاحقاً. فجريمة الابتزاز تكتمل أركانها بمجرد صدور **"التهديد"** المقترن بطلب

---

[1] منظمة الشرطة الجنائية الدولية (الإنتربول)، **عملية ينسقها الإنتربول تستهدف شبكات الابتزاز الغير اخلاقي**، مقال منشور بتاريخ 02 ماي 2014، متاح على الموقع الرسمي للإنتربول[www.interpol.int]، تاريخ الاطلاع 2026/5/7الساعة 12:57.

[2] امل صقر، (DW) **الابتزاز الإلكتروني.. جريمة تودي بحياة عراقيات فأين القانون؟**، مقال منشور بتاريخ2025/12/21، متاح على الرابط: [https://www.dw.com/ar/a-75255264]، تاريخ الاطلاع: 08 ماي 2026الساعة15:24.

(مال أو منفعة)، حيث تتحول إرادة الضحية من "إرادة حرة" إلى **"إرادة مسلوبة"** تحت وطأة الخوف من الفضيحة.

- **حماية الإرادة لا السلوك:** القانون الجنائي يحمي "إرادة الشخص" من الإكراه؛ فالمبتز الذي يستغل ثقة الضحية أو "زلة" معينة ارتكبتها، لا يكتسب أي شرعية لفعلته. بل على العكس، يرى الفقه القانوني أن استغلال "الاستدراج العاطفي" للوصول إلى غاية إجرامية يعد ظرفاً يثبت **"القصد الجنائي"** لدى المبتز.
- **التكييف القضائي:** استقر الاجتهاد القضائي على أن خطأ الضحية (المشاركة الطوعية للمحتوى في البداية) لا يبرر فعل المبتز ولا يمنع من عقابه، لأن المصلحة المحمية هنا هي "حرية الشخص وسلامته المعنوية"، وهي حق أصيل لا يسقط بسلوك مسبق خاطئ.

بناءً على ما تقدم، نخلص إلى أن إشكالية الرضا لا تعيق قيام الجريمة، بل تضع على عاتق أجهزة التحقيق ضرورة التمييز بين "الضحية" التي تعرضت للتلاعب وبين "الجاني" الذي خطط للاستدراج، مما يجعل من الابتزاز جريمة قائمة بذاتها بمجرد بدء التهديد.[1]

الفرع الثاني: الابتزاز الإلكتروني المسلط على الشخصية المعنوية

تتخذ جريمة الابتزاز الإلكتروني الموجهة ضد الشخصية المعنوية أبعاداً أكثر تعقيداً من تلك الموجهة للأفراد، نظراً لتعدد الجهات الفاعلة وتنوع المصالح المستهدفة؛ إذ لم يعد المبتز مجرد هاوٍ يبحث عن منفعة عابرة، بل استحال في كثير من الأحيان إلى "كيان إجرامي" أو "خصم استراتيجي" يستهدف عصب المؤسسة. وتتجلى أولى صور هذا الابتزاز في ذلك الخطر القادم من داخل أسوار المؤسسة ذاتها، حيث يبرز **"الموظف"** أو العامل السابق كواحد من أخطر المبتزين. فالموظف، بحكم وظيفته وصلاحيات الوصول الممنوحة له، يمتلك القدرة على تجاوز الحواجز الأمنية الرقمية التي قد تستعصي على الغرباء. وغالباً ما يتحرك هذا المبتز بدافع الانتقام الوظيفي أو الطمع المادي، حيث يقوم بالاستيلاء على "الأسرار المهنية" أو "قواعد بيانات الزبائن" ويهدد بتسريبها للمنافسين أو مسحها نهائياً ما لم تستجب الإدارة لمطالبه المالية. وتبرز الخطورة القانونية هنا في أن هذا الفعل يشكل "خيانة أمانة رقمية" مضاعفة، يشدد فيها المشرع الجزائري العقوبة نظراً لاستغلال الجاني لثغرات نظامٍ اؤتمن على حمايته أو العمل من خلاله.

وفي سياق متصل، لا يقتصر التهديد على الداخل، بل يمتد ليشمل **"الابتزاز التنافسي"** الذي تمارسه بعض الشركات أو الجهات المنافسة في السوق. ففي ظل الاقتصاد الرقمي، أصبحت "المعلومة" هي رأس المال الحقيقي، وهو ما جعل من "التجسس الصناعي" المقترن بالابتزاز أداة لتحطيم الخصوم. ويتم ذلك عبر اختراق أنظمة الشركة المنافسة وسرقة براءات اختراع قيد التطوير أو خطط تسويقية سرية، ثم مساومة الشركة الضحية بين دفع مبالغ طائلة أو خسارة ميزتها التنافسية في السوق. إن هذا النوع من الابتزاز لا يهدف للربح المالي الفوري فحسب، بل يهدف إلى إحداث شلل استراتيجي في الكيان المعنوي المنافس، مما يؤدي إلى انهيار قيمته السوقية وفقدان ثقة المستثمرين والزبائن على حد سواء. وهنا يتقاطع قانون العقوبات مع قانون المنافسة، ليضع القاضي أمام جريمة مركبة تمس بالنظام العام الاقتصادي للدولة.

أما الصورة الأكثر حداثة وعولمة في هذا المطلب، فتتمثل في الهجمات المنظمة التي تشنها عصابات دولية غرضها **"الربح المادي البحت"** عبر تقنية "برمجيات الفدية" (Ransomware)[2]، وفي هذه الحالة، لا يوجد رابط سابق بين الجاني والمؤسسة الضحية، بل يتم استهدافها لكونها "مليئة مالياً". وتعتمد هذه

---

[1] ريطاب عز الدين ، صدراتي نبيلة، الطبيعة القانونية لفعل التشهير الإلكتروني عبر أدوات الذكاء الاصطناعي، المجلة الجزائرية للحقوق والعلوم السياسية ، المجلد 09 ، العدد 01،ص ص933 950.

[2] موقع **no more ransom**، الرابط [https://www.nomoreransom.org/ar/index.html]تاريخ الزيارة2026/5/11 الساعة20:43.

الجريمة على تشفير كامل لبيانات المؤسسة الحيوية، مما يؤدي إلى توقف "المرفق العام" أو "النشاط التجاري" كلياً. وهنا تبرز الأهمية القصوى لمبادرات دولية مثل **"No More Ransom"**، التي كشفت تقاريرها أن المؤسسات غالباً ما تجد نفسها في مأزق قانوني وأخلاقي؛ فالتوقف عن العمل يكلفها خسائر يومية تفوق قيمة الفدية المطلوبة، وهو ما يشجع المجرمين على الاستمرار.[1] إن هذا النوع من الابتزاز العابر للحدود يضع الشخصية المعنوية في مواجهة مجرمين مجهولي الهوية يستخدمون العملات المشفرة لتلقي الأموال، مما يجعل من تتبع الأثر المالي أمراً في غاية الصعوبة، ويفرض على المؤسسات ضرورة تبني استراتيجيات دفاعية تقنية وقانونية استباقية تتجاوز الحدود الوطنية لتصل إلى مستوى التعاون الأمني الدولي.[2]

وعند الغوص في الآليات التقنية التي تعتمدها هذه الجهات المبتزة (سواء كانت موظفين أو منافسين أو عصابات)، نجد أن الابتزاز لا يتوقف عند تشفير البيانات فحسب، بل يمتد ليشمل أساليب أكثر هجوماً وتعقيداً. ومن أبرز هذه الصور **'هجمات حجب الخدمة الموزعة' (DDoS Attacks)**؛ حيث يقوم المبتز بتهديد المؤسسة بإغراق موقعها الإلكتروني أو أنظمتها الرقمية بطلبات وهمية تؤدي إلى انهيار النظام وتوقفه عن العمل، مما يكبد المؤسسة خسائر فادحة نتيجة انقطاع الخدمة عن الزبائن، ولا يتوقف الهجوم إلا بدفع الفدية المطلوبة.

كما يبرز نوع آخر شديد الخطورة وهو **'الابتزاز عبر البريد الإلكتروني' (Email-based Extortion)**، حيث يتم استهداف كبار التنفيذيين في الشركة عبر رسائل تصيد احتيالي تحتوي على برمجيات خبيثة، أو تهديدهم بنشر محادثات إدارية سرية تم الاستيلاء عليها. إن هذا التعدد في الوسائل التقنية – كما تشير إليه تقارير شركة **Fortinet** العالمية – يبرهن على أن الابتزاز الإلكتروني للشخصية المعنوية أصبح يعتمد على 'الهندسة الاجتماعية' الممزوجة بالقدرة التقنية العالية، مما يجعل من الدفاع السيبراني للمؤسسات ضرورة قانونية وإدارية لحماية أصولها المعنوية والمادية.[3]

أولاً: تعريف الابتزاز عبر برمجيات الفدية (Ransomware) وطبيعته القانونية

تُعد برمجيات الفدية نوعاً متطوراً من البرامج الخبيثة (Malware) التي تُستخدم كأداة لاحتجاز البيانات الرقمية كـ "رهينة". وتتمثل الخطورة الإجرامية لهذا الفعل في قيام الجاني بسلب سيطرة الشخصية المعنوية على أصولها المعلوماتية وتشفيرها، مانعاً إياها من الوصول إلى بياناتها الحيوية (مثل الحسابات المالية، أسرار التصنيع، وبيانات الموظفين)، ولا يتم الإفراج عن هذه البيانات إلا بعد الانصياع لمطالب المبتز المالية. ووفقاً لتقارير الأمن السيبراني لعام **2026**، فإن هذا النوع يمثل ثالث أكثر طرق الهجمات استخداماً على مستوى العالم، حيث يتجاوز كونه مجرد اختراق تقني ليصبح جريمة "ابتزاز أموال" كاملة الأركان، تعززها سرية المعاملات عبر العملات الرقمية التي تسهل للمجرمين استلام الفدية بعيداً عن الرقابة المالية التقليدية[4].

---

[1] تقرير مبادرة **No More Ransom(لا لمزيد من الفدية)**، "برمجيات الفدية: التهديد المتزايد للمؤسسات"، متاح على الموقع الرسمي للمبادرة بالتعاون مع اليوروبول(Europol) ، الرابط [https://www.nomoreransom.org] ، تاريخ الاطلاع: 09 ماي 2026الساعة11:35.

[2] تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا، الإصدار الثالث، متاح على الموقع الرسمي للانتربول الرابط[file:///C:/Users/RouibaTech/Downloads/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_AR_LR%20(1).pdf]، تاريخ زيارة الموقع2026/5/11 الساعة19:56.

[3] شركة فورتينت (Fortinet)، **دليل المفاهيم السيبرانية: ما هو الابتزاز الإلكتروني وأنواعه الشائعة؟**، متاح على الموقع الرسمي للشركة الرابط:[https://www.fortinet.com/resources/cyberglossary/cyber-extortion]، تاريخ الاطلاع2026/5/9 الساعة18:03.

[4] تعريف برمجيات الفدية متاح على الموقع الرسمي لشركة no more ransom، المرجع السابق.

المراحل الإجرائية لهجمة الابتزاز (دورة حياة الجريمة) لا تتم عملية الابتزاز ضد الشخصية المعنوية بشكل عشوائي، بل تتبع مساراً منظماً يبرز القصد الجنائي التصميمي لدى الفاعل، ويمكن تقسيم هذه الهجمة إلى مراحل ست أساسية:

1. **مرحلة الاستطلاع :(Reconnaissance)** وهي المرحلة التمهيدية التي يقوم فيها المبتز بدراسة نقاط الضعف في شبكة المؤسسة المستهدفة. تعد هذه المرحلة هي العقل المدبر للجريمة، حيث يقوم المبتز بجمع المعلومات حول "البنية التحتية" للمؤسسة الضحية. يبحث الجاني هنا عن الثغرات غير المرقعة في الأنظمة، أو يجمع معلومات عن الموظفين عبر منصات مثل (LinkedIn) لتحديد الأهداف السهلة. من الناحية القانونية، تمثل هذه المرحلة "الأعمال التحضيرية" التي تعكس سبق الإصرار والترصد الإجرامي لدى الفاعل.
2. **مرحلة العدوى :(Infection)** وتتم عبر التسلل إلى الشبكة، وغالباً ما يكون ذلك من خلال رسائل "التصيد الاحتيالي" أو الروابط الملغومة التي يفتحها الموظفون. هنا يبدأ التنفيذ المادي للجريمة، حيث يتم تسليم البرمجية الخبيثة للمؤسسة. الوسيلة الأكثر شيوعاً هي **"التصيد الاحتيالي الموجه " (Spear Phishing)**، عبر إرسال بريد إلكتروني يبدو رسمياً يحتوي على مرفق ملغوم. بمجرد فتح الموظف للمرفق، يتم تثبيت "برنامج نصي" خفي يبدأ بالعمل داخل جهاز واحد، وهي الثغرة التي تسمح للجاني بالدخول إلى حصون الشخصية المعنوية.
3. **مرحلة التصعيد :(Escalation)** حيث يسعى المبتز للحصول على صلاحيات "المسؤول " (Admin)للسيطرة الكاملة على خوادم المؤسسة. بمجرد الدخول إلى جهاز عادي، يدرك المبتز أن صلاحياته محدودة، لذا يبدأ في البحث عن ثغرات داخل النظام للانتقال من "مستخدم عادي" إلى **"مدير النظام .(Administrator)** "هذه المرحلة بالغة الخطورة قانوناً لأنها تمثل "الدخول غير المصرح به" وتجاوز تدابير الحماية، وهي الركن المادي الذي تشدد عليه المادة **394مكرر** من قانون العقوبات الجزائري.
4. **مرحلة المسح :(Scanning)** يقوم البرنامج الخبيث بمسح شامل للشبكة لضمان انتشار العدوى في كافة الأجهزة المرتبطة لضمان شلل تام للمؤسسة. بعد الحصول على صلاحيات المدير، يبدأ المبتز في التنقل "أفقياً" داخل شبكة المؤسسة. يقوم بمسح كافة الأجهزة المرتبطة، الخوادم(Servers) ، وقواعد البيانات الضخمة. الهدف هنا هو زرع "قنابل موقوتة" في كل ركن من أركان النظام لضمان أنه عند لحظة التشفير، لن تجد المؤسسة أي جهاز سليم لتشغيل عملياتها منه.
5. **مرحلة التشفير :(Encryption)** وهي الركن المادي الجوهري، حيث يتم قفل الملفات الحساسة باستخدام خوارزميات معقدة. هي المرحلة الحاسمة التي يتحقق فيها الضرر المادي. يقوم المبتز بتفعيل خوارزميات تشفير معقدة مثل(AES-256) تقوم بتحويل البيانات المنظمة إلى "رموز غير مفهومة". في هذه اللحظة، تفقد المؤسسة قدرتها على قراءة عقودها، بيانات موظفيها، أو حتى سجلاتها المالية. هنا يستولي الجاني فعلياً على "الأصول المعلوماتية" للمؤسسة دون نقلها مادياً، وهو ما يطرح إشكالية قانونية حول "طبيعة المال المستولى عليه" في الجريمة الإلكترونية.
6. **مرحلة المساومة :(Ransom)** وهي المرحلة النهائية التي تظهر فيها "رسالة الفدية"، ليبدأ المبتز في ممارسة ضغوطه النفسية والمالية على إدارة المؤسسة. هنا يخرج المبتز من الظل إلى العلن. تظهر رسالة على كافة شاشات المؤسسة تُعلمهم بالهجمة، وتطالب بفدية مالية مقابل "مفتاح فك التشفير". غالباً ما يستخدم الجاني في هذه المرحلة أسلوب **"الابتزاز المزدوج"**؛ أي التهديد بعدم فك

التشفير (خسارة البيانات) والتهديد بنشر البيانات (فضيحة تجارية)، لإجبار الإدارة على الدفع السريع وتجنب ابلاغ السلطات[1].

صور الابتزاز المتطورة (Leakware & Doxware)

لم يعد المبتز الإلكتروني في عام 2026 يكتفي بالنمط التقليدي القائم على تشفير البيانات والمساومة على مفتاح الفك، بل طوّر "استراتيجيات ضغط" تجعل الشخصية المعنوية أمام خيارات مستحيلة. وتتمثل أبرز هذه الصور المتطورة فيما يلي:

1. استراتيجية الابتزاز المزدوج (Double Extortion - Leakware)

تعد هذه الصورة هي الأكثر شيوعاً وتدميراً للمؤسسات حالياً. لا يقوم المبتز هنا بتشفير البيانات فحسب، بل يقوم أولاً بـ "سرقة نسخة منها" ونقلها إلى خوادمه الخاصة. إذا رفضت المؤسسة دفع الفدية اعتماداً على وجود "نسخ احتياطية" لديها، يقوم المبتز بتهديدها بـ نشر البيانات الحساسة (أسرار تجارية، بيانات زبائن، سجلات ضريبية) على "مواقع التسريب" في الإنترنت المظلم (Dark Web) هنا يتحول محل الجريمة من "حجب المعطيات" إلى "إفشاء الأسرار"، وهو ما يضع المؤسسة أمام ملاحقات قضائية من الزبائن وغرامات من هيئات الرقابة.

2. الابتزاز المتعدد الطبقات (Quadruple Extortion & Triple)

في تطور مرعب، بدأ المبتزون باستخدام "الابتزاز الثلاثي والرباعي". فبعد تشفير بيانات الشركة وتهديدها بتسريبها، يقوم المبتز بـ:

- استهداف أطراف خارجية: التواصل مع "زبائن" الشركة أو "مورديها" وإبلاغهم بأن بياناتهم المسجلة لدى الشركة قد سُرقت، ومطالبتهم بالضغط على الشركة للدفع، أو حتى مطابتهم هم أنفسهم بفدية.
- الهجمات المتزامنة (DDoS) شن هجمات حجب خدمة لتعطيل موقع الشركة تماماً أثناء مفاوضات الفدية لزيادة الضغط النفسي والمادي على الإدارة.[2]

3. الابتزاز كخدمة (Ransomware as a Service – RaaS)

هذه الصورة تمثل "الجانب المؤسساتي للجريمة". حيث تقوم عصابات محترفة (مثل RansomHub أو Qilin المذكورة في تقرير فورتينت) بتطوير برمجيات تشفير وبيعها أو تأجيرها لمجرمين أقل خبرة (Affiliates) مقابل نسبة من الفدية. هذا النموذج أدى إلى "ديمقراطية الجريمة"، حيث أصبح بإمكان أي شخص لديه نية إجرامية أن يبتز كبرى الشركات دون الحاجة لمهارات برمجية عالية، مما ضاعف عدد القضايا أمام المحاكم بشكل هائل.[3]

4. التشفير المتقطع (Intermittent Encryption):

[1] تقرير شركة فرورنيت (fortinet)،مشهد التهديدات العالمية2026، متاح على الرابط [https://www.fortinet.com/resources/reports/threat-landscape-report]، تاريخ زيارة الموقع2026/5/22على الساعة21:17.

[2] مقال احصائي متاح على مدونةA10/امن الشبكات، اشهر هجمات حجب الخدمة الموزعة(ddos) في التاريخ، تاريخ النشر2026/5/12، الرابط [https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=Traditional%20DDoS%20attacks%20are%20now,point%20in%20DDoS%20attack%20methodology.] تاريخ زيارة الموقع2026/5/22الساعة22:10.

[3] تقرير شركة فورتنيت، المرجع السابق.

وهي تقنية "ذكية" تستخدم لتجاوز أنظمة الدفاع بدلاً من تشفير الملف بالكامل (وهو ما قد يكتشفه نظام الحماية ويوقفه)، تقوم البرمجية بتشفير "أجزاء" فقط من الملف (مثلاً تشفير 16 بايت وترك 16 بايت). هذه الطريقة تجعل الملف غير قابل للقراءة تماماً، ولكنها تتم بسرعة فائقة وتخفي نشاط البرمجية الخبيثة عن أعين برامج الحماية، مما يجعل "الركن المادي" للجريمة يتم في صمت تام.

5. ابتزاز "التعدين الخفي" (Cryptojacking Extortion):

كما أشار تقرير 2026، يتم أحياناً اختراق خوادم الشركات لا لتشفير ملفاتها، بل لاستغلال "قوة المعالجة" لديها لتعدين العملات الرقمية. الابتزاز هنا يكمن في تهديد الشركة إما بدفع مبلغا معيناً أو الاستمرار في استهلاك مواردها الطاقوية والتقنية وتدمير خوادمها بالاحتراق أو التعطيل نتيجة الضغط العالي، وهو ما يمس بسلامة الأجهزة المادية للشخصية المعنوية.

الآثار القانونية والاقتصادية المترتبة على الابتزاز

تتجاوز آثار الابتزاز الجانب المالي الصرف لتشمل أبعاداً قانونية معقدة؛ فالشخصية المعنوية الضحية قد تجد نفسها تحت طائلة المسؤولية القانونية نتيجة فشلها في حماية بيانات زبائنها (المسؤولية المدنية والتقصيرية)، بالإضافة إلى الغرامات الإدارية التي قد تفرضها هيئات الضبط نتيجة خرق معايير الأمن الرقمي. أما اقتصادياً، فإن "وقت التوقف (Downtime) "يمثل الخسارة الأكبر، إذ أثبتت إحصائيات عام 2024 و2025 أن قطاعات حيوية مثل الصحة والبرمجيات سجلت مطالب فدية تجاوزت في متوسطها 5.2 مليون دولار، مما يعكس جسامة الضرر المادي الذي يلحق بالكيان المعنوي.[1]

ثانيا: هجمات حجب الخدمة الموزعة (DDoS Attacks)

تتميز جريمة حجب الخدمة الإلكترونية بطبيعة إجرامية خاصة تختلف عن باقي الجرائم السيبرانية؛ إذ لا يعمد المبتز في هذه الحالة إلى البحث عن ثغرات أمنية لاختراق الأنظمة وسرقة محتوياتها، بل يقوم الركن المادي للجريمة على استغلال الأنظمة القانونية العادية والشرعية للاتصال بالإنترنت من أجل إحداث شلل تشغيلي للضحية، ثم مساومتها مالياً.[2]

1_ مفهوم الهجوم وآليته التشغيلية

تعتمد هذه الجريمة بشكل أساسي على قيام المهاجم بإرسال كميات هائلة ومكثفة من طلبات الاتصال الوهمية نحو الموقع الإلكتروني أو التطبيق المستهدف (مثل منصات الدفع الإلكتروني أو مواقع الشركات).

ومن المعلوم أن خوادم الويب والبنية التحتية لشبكات المؤسسات تمتلك بطبيعتها قدرة استيعابية محدودة لمعالجة الاتصالات في الوقت ذاته. وعندما يتم إغراق هذه الخوادم بطلبات وهمية تفوق طاقتها، فإنها تستهلك كامل القدرة التشغيلية للشبكة، مما يؤدي تلقائياً إلى بطء النظام أو انهياره تماماً، وبالتالي منع المستخدمين والزبائن الحقيقيين من الوصول إلى الخدمات، وهو ما يُعرف بـ "حجب الخدمة.

2_ المراحل التنفيذية للجريمة

يمر تنفيذ هذه الجريمة بمرحلتين أساسيتين تعكسان التخطيط المسبق للجاني:

---

[1] نفس المرجع.

[2] الآليات التقنية لحجب الخدمة: دليل مفاهيم الأمن السيبراني، **التقرير الدولي حول الهجمات الموزعة لحجب الخدمة (DDoS)**، مؤسسة (IBM) للحلول الرقمية، منشور في 2025/2024، متاح على الرابط الإلكتروني للمؤسسة،[https://www.ibm.com/qa-ar/think/topics/ddos] تاريخ الاطلاع: 22 ماي 2026، الساعة21:13.

- **المرحلة الأولى: حشد وتجهيز شبكات الأجهزة المخترقة:**

يعتمد المبتز في هجومه على استخدام شبكة موسعة من الأجهزة المتصلة بالإنترنت (مثل الحواسيب والهواتف الذكية أو الأجهزة المنزلية الذكية) التي جرى اختراقها مسبقاً بفيروسات أو برمجيات خبيثة تتيح للمجرم التحكم فيها وتوجيهها جماعياً عن بُعد دون علم أصحابها الأصليين.

وفي بيئة الجريمة المنظمة عبر الإنترنت، أصبح بإمكان المبتز الكسول استئجار هذه الشبكات الجاهزة من قراصنة آخرين عبر أسواق الإنترنت المخفي مقابل مبالغ مالية، وهو نمط إجرامي حديث يسهّل ارتكاب الجريمة دون الحاجة لخبرة تقنية عالية.[1]

- **المرحلة الثانية: توجيه الهجوم وعملية الإغراق الوهمي:**

في هذه المرحلة، يصدر الجاني أمراً موحداً لآلاف الأجهزة المخترقة التي يسيطر عليها، لتقوم في لحظة واحدة بإرسال سيل جارف من طلبات الاتصال نحو العنوان الرقمي للمؤسسة المستهدفة.

هذا التدفق الضخم يؤدي إلى اختناق الشبكة. ولإخفاء هويته ومنع السلطات الأمنية من تتبعه، يلجأ المبتز إلى تقنيات "تزوير الهوية الرقمية للاتصال"، حيث تظهر الطلبات الخبيثة وكأنها صادرة من عناوين وهمية أو حتى من عنوان الضحية نفسه. وفي كثير من الأحيان، يُستغل هذا الهجوم كأداة تمويه لشل حركة الطاقم الأمني للمؤسسة وصرف انتباهه، بينما يقوم المبتز في الخفاء بجريمة أخرى مثل زرع برمجيات فدية أو سرقة ملفات سرية.[2]

3_القطاعات المستهدفة وخلفيات الابتزاز

يتحرك المجرمون لشن هذه الهجمات بدافع الحصول على فدية مالية ضخمة مقابل وقف الهجوم وإعادة الخدمة لطبيعتها، وتشمل الأهداف الأكثر عرضة لهذه الجريمة:

- **المؤسسات المالية والبنوك:** حيث يؤدي تعطيل منصاتها الرقمية إلى شل حركة المعاملات المصرفية وضرر بليغ بالاقتصاد الوطني.
- **شركات التجارة الإلكترونية والتجزئة:** يتسبب حجب مواقعها في خسائر مالية فورية ناتجة عن توقف عمليات البيع والشراء.
- **الشركات المستضيفة للبيانات والخدمات السحابية:** يمثل استهدافها خطورة كبرى لأن تعطيل خادم سحابي واحد يترتب عليه شلل عشرات الشركات والمؤسسات المرتبطة به.
- **المرافق العامة والوكالات الحكومية:** وتُستهدف غالباً لدوافع سياسية أو تخريبية لتعطيل مصالح المواطنين.

4_الأساليب التقنية المبسطة لتعطيل الأنظمة

تتخذ عملية حجب الخدمة عِدة صور وأساليب تشغيلية يمكن تلخيصها في ثلاثة أنواع رئيسية:

1. **التعطيل على مستوى واجهة التطبيق:** وفيه يتم تكرار طلب تصفح صفحة الويب بشكل مستمر ومتزامن من آلاف الأجهزة، مما يشبه قيام آلاف الأشخاص بالضغط على زر "تحديث الصفحة" في ثانية واحدة، فينهار الموقع.

[1] الآليات التقنية لحجب الخدمة: دليل مفاهيم الأمن السيبراني، المرجع السابق.
[2] نفس المرجع.

2. **التعطيل عبر الاتصالات المعلقة (الوهمية):** يستغل المبتز طريقة بناء الاتصال بين الأجهزة؛ حيث يرسل طلباً لفتح خط اتصال مع الخادم، وعندما يفتح الخادم الباب وينتظر التأكيد، يتجاهله المبتز ويترك الاتصال معلقاً، ويكرر هذا السلوك بآلاف الطلبات حتى تمتلئ قدرة الخادم باتصالات وهمية معلقة، فلا يجد المستخدم الحقيقي مكاناً للدخول.[1]

3. **التعطيل بالحجم الضخم (الإغراق التضخيمي):** يعتمد المهاجم هنا على إرسال حزم بيانات ذات أحجام ضخمة جداً تسد ممرات شبكة الإنترنت الخاصة بالمؤسسة بالكامل، مما يمنع مرور أي بيانات أخرى مشروعة.

5_آليات الحماية وتخفيف الأضرار

لحماية كيانها الاقتصادي واستمرار مرفقها الرقمي، تلجأ الشخصيات المعنوية إلى تبني تدابير وقائية ودفاعية، من أبرزها:

- **جدران الحماية الرقمية المستحدثة:** وهي برمجيات ذكية توضع كحارس عند مدخل الشبكة، تدقق في هوية الطلبات الواردة وتفرزها، فتسمح بمرور الزبائن الحقيقيين وتلقي بالطلبات الوهمية خارجاً
- **توزيع الحمولات الشبكية:** تشتيت خوادم المؤسسة على مواقع جغرافية متعددة، بحيث إذا تعرض أحد الخوادم لضغط كبير، يتم تحويل حركة الزبائن تلقائياً وبسلاسة إلى خادم آخر احتياطي لضمان استمرار الخدمة.
- **تقنية الحفرة المغلقة (التوجيه الصامت):** عند اكتشاف الهجوم، يتم عزل و"تحويل" سيل البيانات الضارة إلى مسار وهمي مغلق يتم فيه إتلاف هذه البيانات دون معالجتها ودون أن تؤثر على سير الخادم الأصلي.[2]

ثالثا: الابتزاز عبر البريد الالكتروني

يُشكل البريد الإلكتروني البيئة الرقمية الأكثر استهدافاً من قِبل شبكات الابتزاز الإلكتروني، خاصة عندما يتعلق الأمر باستهداف الشخصيات المعنوية كالمؤسسات الاقتصادية والشركات التجارية. ونظراً لاعتماد هذه الكيانات على البريد الإلكتروني كوسيلة رسمية أساسية لتبادل المراسلات، وتوقيع العقود، وإرسال الفواتير، فقد أضحى هذا القناة المدخل المفضّل للجناة لتنفيذ جرائمهم ومساومة الإدارة ماليا[3].

أولاً: الأساليب المادية للابتزاز عبر البريد الإلكتروني

يتخذ الابتزاز عبر البريد الإلكتروني عِدة صور سلوكية تنبئ عن خطورة إجرامية بالغة، ويمكن حصر الأساليب الأكثر شيوعاً في النقاط التالية:

1. **الرسائل الاحتيالية الموجهة (الصيد الإلكتروني المستهدف):** في هذه الصورة، يقوم الجاني بجمع معلومات دقيقة حول الشركة المستهدفة، ثم يرسل بريداً إلكترونياً مزيفاً ومصمماً بدقة عالية يبدو وكأنه صادر من جهة رسمية موثوقة (مثل البنك المتعامل معه، أو مصلحة الضرائب، أو حتى من إدارة الشركة نفسها). تتضمن هذه الرسالة عادةً رابطاً خبيثاً أو ملفاً مرفقاً، وبمجرد قيام الموظف بفتحه، يتم اختراق نظام الشركة وسحب معلوماتها الحساسة، لتبدأ مرحلة الابتزاز والمساومة على إعادتها مقابل فدية ماليّة.

---

[1] الآليات التقنية لحجب الخدمة: دليل مفاهيم الأمن السيبراني، المرجع السابق,

[2] الآليات التقنية لحجب الخدمة: دليل مفاهيم الأمن السيبراني، المرجع السابق

[3] شركة فورتنيت،المرجع السابق،[https://www.fortinet.com/resources/cyberglossary/cyber-extortion].

2. **انتحال صفة المدير أو الشريك التجاري**: يعمد المبتز في هذا السلوك إلى تزوير بريد إلكتروني يطابق تماماً بريد المدير التنفيذي للشركة أو أحد الموردين الأساسيين. يرسل الجاني رسالة مستعجلة إلى قسم المحاسبة يطلب فيها تحويل مبالغ مالية فورية إلى حساب بنكي معين تحت طائلة التهديد بفسخ عقود مهمة أو إحداث أضرار بمصالح الشركة، مستغلاً في ذلك عامل الخوف وسلطة الوظيفة لدى الموظف المستقبِل.

3. **التهديد بكشف المراسلات السرية (الابتزاز بالفضائح التجارية):** تحدث هذه الجريمة عندما يتمكن المخترق من الدخول فعلياً إلى علبة البريد الإلكتروني الرسمية للمؤسسة، والاطلاع على أرشيف الرسائل والاتفاقيات، والخطط المستقبلية، أو حتى العيوب التقنية في منتجات الشركة. هنا، يقوم المبتز ببعث رسالة تهديد إلى مجلس الإدارة، مفادها أنه سيقوم بنشر هذه الأسرار والمراسلات إلى العلن أو إرسالها إلى الشركات المنافسة، مما يؤدي إلى تدمير السمعة التجارية للشركة واهتزاز قيمتها في السوق، ما لم تدفع المبالغ المطلوبة.[1]

ثانياً: الآثار القانونية والاقتصادية المترتبة على الجريمة

يترتب على الابتزاز عبر البريد الإلكتروني أضرار جسيمة تمس بالكيان القانوني والاقتصادي للشخص المعنوي، وتتجلى هذه الآثار في:

- **الخسائر المادية الفورية**: وتتمثل في المبالغ التي قد تضطر بعض الشركات لدفعها تحت وطأة الضغط والتهديد، أو تكاليف الاستعانة بالخبراء لإعادة تأمين الأنظمة المخترقة.
- **المسؤولية القانونية والمدنية للشركة:** إذا تسربت عبر البريد الإلكتروني بيانات ذات طابع شخصي تخص الزبائن أو المتعاملين، فإن الشركة قد تواجه ملاحقات قضائية وتلتزم بدفع تعويضات مالية للمتضررين بسبب إهمالها في حماية معطياتهم، وذلك وفقاً للتشريعات الحديثة لحماية البيانات.
- **فقدان الثقة الائتمانية**: إن مجرد انتشار خبر تعرض بريد الشركة للاختراق والابتزاز يؤدي فوراً إلى تراجع ثقة المستثمرين والعملاء، مما قد يسبب إفلاس المؤسسة أو تراجع نشاطها التجاري بشكل حاد.

ثالثاً: سبل الوقاية الإدارية والتقنية المبسطة

لمواجهة هذه المعضلة وتجنب الوقوع في شباك المبتزين، يتعين على المؤسسات تفعيل جملة من التدابير الحمائية، أبرزها:

- **تفعيل أنظمة التحقق الثنائي:** وهي آلية بسيطة تمنع الدخول إلى البريد الإلكتروني بمجرد كتابة كلمة المرور، بل تشترط إدخال رمز مؤقت يرسل إلى هاتف الموظف المسؤول، مما يصعّب مهمة المخترق حتى لو عرف كلمة السر.
- **التدريب الدوري للموظفين:** رفع مستوى وعي العاملين بالشركة حول كيفية التمييز بين الرسائل الرسمية الحقيقية والرسائل الاحتيالية المزيفة، وعدم فتح أي روابط مجهولة.

[1] كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية: كيف تحمي شركتك من رسائل البريد الإلكتروني الاحتيالية، مقال منشور على منصة" axsos " عبر الرابط [https://axsos.de/ar/phishing-mails-erkennen-so-schutzen-sie-ihr-unternehmen-vor-betrugs-e-mails/]، تاريخ الدخول للموقع2026/5/24 على الساعة21:54.

- **اعتماد أنظمة الفرز الذكي (التصفية):** تنصيب برمجيات تقوم تلقائياً بفحص الرسائل الواردة وعزل المشبوهة منها قبل وصولها إلى صندوق البريد الرئيسي للموظف.[1]

المطلب الثاني: دراسة ميدانية حول وعي المجتمع بجريمة الابتزاز الإلكتروني (تحليل الاستبيان)

من أجل ربط الجانب النظري للمذكرة بالواقع المعاش، ومعرفة مدى انتشار جريمة الابتزاز الرقمي، قمنا بإعداد دراسة ميدانية تتمثل في "استبيان "وزعناه على عينة تتكون من (خمسين فرداً) تشمل طلبة وأساتذة جامعيين ومواطنين. وسنخصص هذا المطلب لعرض وتفريغ نتائج هذا الاستبيان في جداول إحصائية، ثم القيام بتحليلها لمعرفة مستوى وعي الأفراد بهذه الجريمة، والوصول إلى حلول وتوصيات عملية للوقاية منها.

الفرع الأول: البيانات الشخصية (الديموغرافية) لعينة الدراسة

يهدف هذا الفرع إلى تحديد الخصائص العامة للأفراد الذين شاركوا في الاستبيان من حيث (الصفة، الجنس، والفئة العمرية)

أولاً: توزيع عينة الدراسة حسب "الصفة":

يظهر الجدول التالي التوزيع المهني والأكاديمي للخمسين فرداً المشاركين في الدراسة

الصفة (المهنة)	*التكرار (العدد)*	*النسبة المئوية (%)*
طالب	**22**	**%44**
موظف	**13**	**%26**
استاذ	**7**	**%14**
فئات اخرى	**8**	**%16**
المجموع	**50**	**%100**

التحليل والتعليق :

نلاحظ من خلال الجدول أن فئة "الطلبة" هي الأكثر مشاركة في الاستبيان بنسبة "44%"، تليها فئة "الموظفين" بنسبة "26%"، ثم "الأساتذة" بنسبة "14%". وهذا التوزيع يخدم موضوع المذكرة بشكل كبير؛ لأن الطلبة والموظفين هم الفئات الأكثر استخداماً للتكنولوجيا والوسائل الرقمية في الجامعة والإدارة، مما يجعل آرائهم تعكس الواقع الفعلي للتعامل مع الفضاء الرقمي.

ثانياً: توزيع عينة الدراسة حسب "الجنس":

يبيّن الجدول التالي توزيع أفراد العينة بين الذكور والإناث:

الجنس	*التكرار (العدد)*	*النسبة المئوية (%)*
انثى	**27**	**%54**
ذكر	**23**	**%46**
المجموع	**50**	**%100**

[1] كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية: كيف تحمي شركتك من رسائل البريد الإلكتروني الاحتيالية، المرجع السابق.

التحليل والتعليق:

يتضح من الجدول أن نسبة "الإناث" في العينة بلغت "54%"، بينما بلغت نسبة "الذكور" "46%". هذا التقارب الكبير في النسب يمنح الدراسة مصداقية عالية، حيث يتيح لنا معرفة وجهات نظر الغير اخلاقين وتجنب الانحياز، خاصة وأن ظاهرة الابتزاز الإلكتروني تمس كلا الغير اخلاقين في الواقع وإن كانت حدتها تختلف من فئة لأخرى.

ثالثاً: توزيع عينة الدراسة حسب "الفئة العمرية":

يوضح الجدول أدناه الفئات السنية للمشاركين في الاستبيان :

الفئة العمرية(السن)	التكرار (العدد)	النسبة المئوية (%)
من 18 إلى 22 سنة	**14**	**%28**
من 23 إلى 30 سنة	**20**	**%40**
من 31 إلى 45 سنة	**7**	**%14**
أكثر من 45 سنة	**9**	**%18**
المجموع	**50**	**%100**

التحليل والتعليق :

تشير النتائج الإحصائية إلى أن الفئة العمرية المحصورة بين "23 و 30 سنة" هي الغالبة في هذه الدراسة بنسبة "40%"، تليها الفئة من "18 إلى 22 سنة" بنسبة "28%". هذا يعني أن "68%" من عينة الدراسة هم من فئة الشباب (أقل من 30 سنة)، وهي الفئة الحيوية والأكثر نشاطاً على منصات التواصل الاجتماعي والتطبيقات الحديثة، مما يجعلهم الأكثر احتكاكاً بتهديدات الابتزاز الرقمي ومظاهره المستحدثة.

الفرع الثاني: عرض وتحليل المحور الأول (مظاهر وأبعاد جريمة الابتزاز الرقمي ـ خيارات متعددة)

نظراً لأن المشاركين في الاستبيان كانت لهم الحرية الكاملة في اختيار أكثر من إجابة واحدة للسؤال الواحد، فإن النسب المئوية أدناه تم حسابها بقسمة تكرار كل خيار على العدد الإجمالي للعينة (50 فرداً)، ولذلك فإن مجموع النسب يتجاوز100%.

أولاً: الفئة الأكثر عرضة للابتزاز الرقمي (حسب تكرار الاختيارات):

يظهر الجدول التالي التكرارات الحقيقية لكل فئة اختارها المشاركون:

الفئة المستهدفة	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
الإناث	33	66%
الأطفال	17	34%
كلاهما بالتساوي (الذكور والإناث)	16	32%
شركات ومؤسسات	7	14%
الذكور بصفة خاصة	1	2%

التحليل والتعليق

يتضح بعد تفكيك الخيارات المشتركة أن **الإناث** يتربعن على رأس الفئات الأكثر استهدافاً؛ حيث اختارهن **33فرداً من أصل 50** بنسبة **66%** ، وتأتي فئة **الأطفال** في المرتبة الثانية بنسبة **34%** ، مما يثبت واقعياً أن المبتزين يركزون بشكل أساسي على الفئات المستضعفة اجتماعيّاً ونفسيّاً في المجتمع (النساء والأطفال) لسهولة الضغط عليهم وسرعة رضوخهم مقارنة بالشركات أو الذكور.

ثانياً: المنصات الرقمية الأكثر استعمالاً في ارتكاب الجريمة:

يبيّن الجدول التالي حجم انتشار الجريمة عبر مختلف التطبيقات

المنصات الرقمية	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
فيسبوك (Facebook)	44	88%
إنستغرام (Instagram)	24	48%
تطبيقات التعارف	12	24%
واتساب (WhatsApp)	10	20%
البريد الإلكتروني	3	6%
منصات أخرى (تيليغرام، إلخ)	2	4%

التحليل والتعليق

تظهر النتائج الدقيقة هيمنة شبه مطلقة لـ **منصة فيسبوك**؛ حيث اختارها **44 مشاركاً من أصل 50** بنسبة **88%**، يليه **إنستغرام** بنسبة**48%** ، هذه الأرقام تؤكد أن وسائل التواصل الاجتماعي التابعة لشركة (Meta)هي المسرح الأساسي لجرائم الابتزاز بالجزائر، نظراً لسهولة اختراق الحسابات فيها أو تزوير الهويات واستدراج الضحايا .

ثالثاً: الوسيلة التقنية المستخدمة في التهديد والابتزاز:

يوضح الجدول أدناه طبيعة المواد الحساسة المستغلة من قِبل الجناة:

الوسيلة المستخدمة في الابتزاز	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
الصور ومقاطع الفيديو الخاصة	44	88%
المحادثات النصية المكتوبة	15	30%
الوصول إلى ملفات الهاتف وصور الضحية	10	20%
بيانات ومعلومات مهنية (خاصة بالشركات)	7	14%
وسائل أخرى (بضائع، فضائح)	2	4%

التحليل والتعليق

تؤكد الإحصائيات الحقيقية المفرزة أن **الصور ومقاطع الفيديو الخاصة** هي السلاح الفتاك للمبتز؛ حيث حظيت بنسبة**88%** اختيرت 44 مرة ،وتكشف هذه النتيجة عن خطورة "المحتوى البصري" في قضايا الابتزاز، حيث يتكامل هذا الخيار مع خيار "الوصول لملفات الهاتف" بنسبة**20%** ، مما يدل على أن الجناة يعتمدون على سرقة المحتويات الشخصية الحساسة كأداة ضغط لا تترك للضحية مجالاً للمناورة.

رابعاً: الهدف الأساسي الذي يسعى إليه المبتز:

يظهر الجدول الخيارات المتعددة التي تعكس نوايا ودوافع المجرمين:

الهدف الأساسي للمبتز	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
الحصول على مبالغ مالية	37	74%
استدراج الضحية لأفعال غير أخلاقية	28	56%
الانتقام وتشويه السمعة	18	36%
التسلية وفرض السيطرة	12	24%

التحليل والتعليق

يبين التحليل الشامل للخيارات المتداخلة أن **الدافع المالي الكسب غير المشروع** يتحرك في عقول المبتزين بنسبة **74%** اختير 37 مرة ، تليها مباشرة الرغبة في **الاستدراج لأفعال غير أخلاقية بنسبة 56 %** هذه النسبة المرتفعة المزدوجة توضح أن الابتزاز الرقمي في الجزائر لا يقف عند حد الجشع المالي، بل يتعداه بشكل خطير إلى استغلال الضحايا أخلاقياً وجسدياً، مما يضاعف من الأضرار الاجتماعية والجسيمة للجريمة.

خامساً: مدى التعرض الفعلي للابتزاز الإلكتروني داخل عينة الدراسة:

يُظهر الجدول التالي عدد الحالات الحقيقية التي وقعت ضحية لهذه الجريمة من بين المشاركين:

هل تعرضت للابتزاز الإلكتروني سابقاً؟	التكرار (عدد)	النسبة المئوية
لا	39	%78
نعم	11	%22
المجموع	50	%100

التحليل والتعليق:

تكشف المؤشرات الإحصائية عن حقيقة صادمة؛ فبالرغم من أن عينة الدراسة محصورة في مجتمع جامعي واعي، إلا أن"22%"منهم (أي 11 شخصاً من أصل 50) قد وقعوا بالفعل ضحايا مباشرين لجريمة الابتزاز الإلكتروني. هذه النسبة المرتفعة نسبياً تؤكد أن الظاهرة لم تعد مجرد تهديد افتراضي بعيد، بل هي خطر واقعي يداهم الفضاء الجامعي الجزائري، مما يستدعي دراسة الوسائل والتقنيات التي يتسلل بها الجناة.

سادساً: مدى وعي ومعرفة العينة بالتقنيات المتطورة للابتزاز (مثل التزييف العميقDeepfake)

يُبين الجدول مستوى إدراك المستجوبين للأساليب التكنولوجية الحديثة التي أفرزها التحول الرقمي:

هل سمعت بالتقنيات المتطورة للابتزاز (كالديب فيك)؟	التكرار (عدد)	النسبة المئوية
لا (لم أسمع بها تماماً)	23	%46
سمعت عنها ولكن لا أعرف تفاصيلها	18	%36
نعم (أعرفها وأعرف تفاصيلها)	9	%18
المجموع	50	%100

التحليل والتعليق:

تشير البيانات إلى فجوة معرفية وتقنية خطيرة جداً لدى مجتمع الدراسة؛ حيث أن "46%"لم يسمعوا مطلقاً بهذه التقنيات المتطورة، و"36%" سمعوا بها سماعاً سطحياً دون معرفة آلياتها. هذا يعني أن "82%" من العينة يفتقرون للوعي بالأساليب التكنولوجية الحديثة للابتزاز الرقمي كالتزييف العميق (Deepfake)، وتفسر هذه النتيجة علمياً سبب وقوع الضحايا بسهولة؛ فالمستخدم الذي يجهل وجود تقنيات قادرة على تزوير صوته أو وجهه بدقة مرعبة، يسهل ترويعه وابتزازه بمواد مفبركة لعدم قدرته على التمييز التقني بين الحقيقي والمزيف.

سابعاً: النوع الأكثر انتشاراً للابتزاز الرقمي من وجهة نظر العينة (خيارات متعددة):

بناءً على تداخل وتعدد الاختيارات للمشاركين، تم تفريغ وتفكيك الإجابات للوقوف على النمط الإجرامي السائد:

نوع الابتزاز الأكثر انتشاراً	***التكرار (عدد المرات المختارة)***	***النسبة المئوية من العينة (N=50)***
الابتزاز العاطفي والغير اخلاقي	37	74%
الابتزاز المالي	24	%48
ابتزاز الشركات والمؤسسات	4	%8

التحليل والتعليق:

يتضح بعد تفكيك الخيارات المشتركة أن "الابتزاز العاطفي والغير اخلاقي" يأتي في طليعة الأنماط الإجرامية الأكثر انتشاراً بنسبة "74%" (اختير 37 مرة)، يليه "الابتزاز المالي" بنسبة "48%". هذه النتيجة تترجم بدقة التحليل السابق؛ فالجناة يستغلون العاطفة والجنس كأقوى وسيلة للضغط النفسي والاجتماعي على الضحية، ثم يربطونها غالباً بالابتزاز المالي كوسيلة لجني الأرباح، مما يثبت تلازم البُعدين العاطفي والاقتصادي في مسار هذه الجريمة الرقمية بالجزائر.

الفرع الثالث: عرض وتحليل المحور الثاني (الوعي القانوني والحلول الوقائية لظاهرة الابتزاز)

ملاحظة: تم حساب نسب هذا الفرع أيضاً على أساس خيارات متعددة مفرّغة بشكل مستقل لـ 50 مبحوثاً

أولاً: مدى علم أفراد العينة بالإجراءات القانونية المتبعة:

هذا السؤال اختار فيه كل مشارك جواباً واحداً حاسماً، لذا مجموع النسب 100%

الإجابة	***التكرار (العدد)***	***النسبة المئوية***
لا (ليس لدي علم)	19	38%
إلى حد ما	16	32%
نعم (لدي علم)	15	30%
المجموع	**50**	**100%**

التحليل والتعليق:

يظهر استقرار واضح في ضعف الثقافة القانونية الإجرائية؛ حيث أن **38%** يجهلون تماماً الإجراءات، و **32%**يعلمونها "إلى حد ما، هذا يؤكد أن الأجهزة الأمنية والقوانين الردعية رغم وجودها، إلا أن المواطن والجامعي بالجزائر لا يزال يحتاج إلى حملات إرشادية مكثفة لتبسيط طرق الوصول إلى قنوات التبليغ والعدالة.

ثانياً: العائق الأكبر الذي يمنع ضحايا الابتزاز من التبليغ عن الجريمة:

يبيّن الجدول التالي العوامل النفسية والاجتماعية التي تمنع الضحايا من اللجوء للقانون:

العوائق الأساسية المفترضة	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
الخوف من نظرة المجتمع والفضيحة	33	66%
عدم الوعي بالإجراءات القانونية وقنوات التبليغ	19	38%
الخوف من عدم سرية التحقيقات	16	32%
عوائق شخصية (كالخوف من العائلة أو عدم نيل العدالة)	4	8%

التحليل والتعليق المعدل:

قفزت نسبة **الخوف من نظرة المجتمع والفضيحة** بعد التفكيك الدقيق لتصل إلى **66%** كأكبر عائق على الإطلاق يكبّل الضحايا ويدعم هذا العائق عائقان آخران هما :**عدم الوعي بالإجراءات (38%)** و**الخوف من غياب السرية(32%)** هذا التداخل يثبت أن حسم معركة مكافحة الابتزاز يتطلب طمأنة المجتمع سوسيو-قانونياً؛ أي عبر تعزيز ثقة الضحية في سرية تحقيقات الضبطية القضائية لتجاوز حاجز الخوف المجتمعي.

ثالثاً: التصرف الأول الذي يُنصح به عند الوقوع ضحية للابتزاز:

يوضح الجدول السلوكيات التي يراها المستجوبون كخط دفاع أول:

التصرف المنصوح به	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
إبلاغ السلطات الأمنية فوراً	39	78%
استشارة مختص تقني (لتأمين الحساب)	10	20%
تجاهل المبتز وحظره كلياً ($Block$)	5	10%
سلوكيات أخرى (الرضوخ المؤقت، العنف، حل وسط)	6	12%

التحليل والتعليق المعدل:

يظهر من الإحصائيات ثبات وعي العينة بالجهة الشرعية الوحيدة المخولة بحل الأزمة؛ حيث يرى **78%** أن **إبلاغ السلطات الأمنية** هو التصرف السليم ورغم لجوء البعض للحلول التقنية الفردية (كاستشارة مختص تقني بنسبة 20%)، إلا أن الوعي العام يتجه دائماً نحو الدولة وأجهزتها كحل جذري وقانوني لإنهاء المساومة.

رابعاً: أنجح الحلول الوقائية للحد من الظاهرة من وجهة نظر العينة:

يبيّن الجدول التالي التصورات والحلول المقترحة من قِبل مجتمع الدراسة

الحلول الوقائية المقترحة	التكرار (عدد المرات المختارة)	النسبة المئوية من العينة (N=50)
عدم مشاركة الصور والبيانات الحساسة عبر الإنترنت	38	76%
سن قوانين ردعية أكثر صرامة ضد المبتزين	24	48%

تكثيف الندوات التوعوية والحملات داخل الجامعة	9	18%
حلول أخرى فردية	2	4%

التحليل والتعليق:

تؤكد البيانات الحقيقية المعدلة أن الحل الأمثل يبدأ من "الوعي السلوكي الفردي"؛ حيث اختار **76%** من المشاركين **عدم مشاركة الصور والبيانات الحساسة** كأفضل وسيلة وقائية وبالموازاة مع ذلك، يرى **48%** أن تفعيل **القوانين الردعية الصارمة** أمر حتمي لردع المجرمين هذه النتيجة تمنح مذكرتكِ توصية رائعة مفادها أن مواجهة الابتزاز الإلكتروني قائمة على جناحين متكاملين :**الوعي الرقمي للمواطن من جهة، والردع الجزائي الصارم من طرف المشرع من جهة أخرى**.

نتائج عامة للدراسة الميدانية (خلاصة الاستبيان)

بناءً على الدراسة الميدانية الإحصائية التي قمنا بها، ومن خلال تفريغ وتحليل إجابات عينة الدراسة المكونة من (50 فرداً) عبر الاستبيان الموزع، توصلنا إلى مجموعة من النتائج والمؤشرات العلمية الهامة التي تفسر واقع ومظاهر جريمة الابتزاز الإلكتروني في ظل التحول الرقمي. ويمكن استخلاص واستعراض هذه النتائج وفق المحاور الأساسية التالية:

أولاً: المؤشرات الشخصية (الديموغرافية) وعلاقتها بالبيئة الرقمية

تعد دراسة الخصائص والسمات الديموغرافية لعينة البحث منطلقاً أساسياً لتفكيك وفهم أبعاد السلوك الرقمي للأفراد، ورسم خريطة واضحة لمدى تأثرهم بالظواهر المستحدثة في البيئة الافتراضية. ومن بين أبرز هذه المتغيرات الشخصية التي تشكل محوراً محورياً في قراءة معطيات الاستبيان هي "الفئة الجامعية"؛ إذ يمثل مجتمع الطلبة الشريحة الأكثر تفاعلاً وانغماساً في ثقافة التحول الرقمي، مما يرفع من وتيرة استخدامهم اليومي للوسائط المتعددة والشبكات الاجتماعية، ويجعل من استقراء مدى ارتباطهم وثيق الصلة بتحديد وتفسير مؤشرات التعرض لمخاطر هذه البيئة وتداعياتها الأمنية، وهو ما نوضحه ونحلله إحصائياً من خلال الآتي

1. **ارتباط الفئة الجامعية بالشبكة الرقمية:** أظهرت النتائج أن فئة الشباب (الأقل من 30 سنة) تمثل النسبة الأكبر من مجتمع الدراسة بـ **68%**، مدعومة بمشاركة حيوية من النخبة الجامعية (طلبة وأساتذة وموظفين). هذا المؤشر يثبت منطقياً أن مجتمع الجامعة هو البيئة الأكثر استخداماً وتفاعلاً مع أدوات التحول الرقمي، مما يجعله في الوقت ذاته الفئة الأكثر احتكاكاً بالمظاهر المستحدثة للجريمة الإلكترونية وأكثر عرضة لتهديداتها.
2. **توازن عينة الدراسة:** حقق الاستبيان تقارباً وتوازناً ممتازاً بين الغير اخلاقين (الإناث بنسبة **54%** والذكور بنسبة **46%**)، مما يعطي النتائج مصداقية وموضوعية عالية بعيدة عن الانحياز، ويعكس بدقة تامة كيف ينظر كلا الغير اخلاقين إلى ظاهرة الابتزاز في الجزائر.

ثانياً: استخلاص أبعاد المظاهر المستحدثة للجريمة (الجناة والضحايا)

1. **استهداف الفئات المستضعفة اجتماعياً ونفسياً:** أكدت الدراسة الميدانية بشكل قاطع أن **الإناث** (بنسبة **66%**) يليهن **الأطفال** (بنسبة **34%**) هن الفئات الأكثر عرضة واستهدافاً من قِبل شبكات المبتزين. وتفسر هذه النتيجة علمياً بأن الجناة والهاكرز يركزون على الضحايا الذين يسهل الضغط عليهم نفسياً واجتماعياً، مستغلين حساسية مركزهن وخوفهن الزائد من تشويه السمعة في البيئة المحافظة.
2. **هيمنة وتغلغل منصات شركة ميتا (Meta):** كشفت النتائج أن **منصة فيسبوك** تحتل صدارة المسارح الرقمية التي تُرتكب عبرها الجريمة بنسبة ساحقة بلغت **88%**، يليه **إنستغرام** بنسبة

48%. هذا يوضح بشكل جلي أن سهولة تزوير الحسابات وإنشاء الهويات الوهمية على هذه المواقع بالجزائر، حولها إلى أدوات أساسية يستغلها المجرمون للإيقاع بالضحايا واستدراجهم.

3. **خطورة السلاح البصري للمبتز:** أجمعت عينة الدراسة بنسبة **88%** على أن **الصور ومقاطع الفيديو الخاصة** هي الوسيلة الأساسية والأكثر فتكاً للتهديد. هذه النتيجة تؤكد أن المحتوى المرئي الحساس يمثل أداة ضغط فوري تشل إرادة الضحية، وتتكامل بشكل خطير مع عمليات "اختراق ملفات الهاتف" (بنسبة **20%**)، مما يمنع الضحية من المناورة ويجبره على الاستسلام لنفوذ الجاني.
4. **طغيان الدافع المالي والاستغلال الأخلاقي:** تبيّن أن الرغبة في **الحصول على مبالغ مالية** تأتي في مقدمة أهداف المبتز بنسبة **74%**، تليها رغبته في **استدراج الضحية لأفعال غير أخلاقية بنسبة 56%**. هذا يثبت تحول الابتزاز الرقمي من سلوك عشوائي إلى "تجارة طفيلية منظمّة" تهدف إلى تحقيق كسب مالي سريع غير مشروع، أو ممارسة نفوذ وسيطرة غير أخلاقية على الأفراد.
5. **واقعية التهديد داخل البيئة الجامعية :**أثبتت الدراسة الميدانية أن الابتزاز الرقمي خطر داهم ومعيش، حيث أكد **22%**من المشاركين (11 ضحية) تعرضهم الفعلي للجريمة، مما ينفي عنها صفة الجرائم النادرة أو البعيدة عن الفضاء الأكاديمي .
6. **الأمية التقنية بالأساليب المستحدثة :**كشفت النتائج عن ضعف تقني حاد؛ حيث أن **82%**من العينة يجهلون الآليات الدقيقة للتقنيات المستحدثة كالتزييف العميق(Deepfake) ، مما يجعلهم أهدافاً سهلة للمجرمين الرقميين ويضاعف من نجاح خطط الابتزاز .

ثالثاً: واقع الوعي القانوني والتوجهات الوقائية في المجتمع

1. **فجوة حادة في الثقافة القانونية الإجرائية:** كشفت النتائج عن مؤشر مقلق جداً، وهو أن **70%** من أفراد العينة (بين من أجاب بـ "لا" و"إلى حد ما") يفتقرون إلى المعرفة الكافية بالقوانين والآليات الإجرائية المتبعة بالجزائر في حالات الابتزاز. هذه الفجوة القانونية تشكل خطراً حقيقياً؛ لأن جهل المواطن أو الطالب بقنوات التبليغ الرسمية يجعله يستمر مكبلاً تحت رحمة المبتز خوفاً وتخبطاً.
2. **الضغط الاجتماعي كحامٍ للمجرمين:** توصلت الدراسة إلى أن **الخوف من نظرة المجتمع والفضيحة** هو العائق الأكبر والأساسي الذي يمنع الضحايا من اللجوء إلى القانون بنسبة **66%**، يليه **الخوف من عدم سرية التحقيقات بنسبة 32%**. هذه النتيجة تؤكد أن الموروث الاجتماعي والضغط الأسري يلعبان دوراً سلبياً غير مباشر يخدم مصالح المبتز، ويستدعي بالضرورة توفير ضمانات قانونية وأمنية صارمة ومُعلنة لحماية سرية هوية الضحايا أثناء التحقيق.
3. **الإجماع على دور الأجهزة الأمنية للدولة:** رغم نقص المعرفة بالإجراءات، أظهرت العينة وعياً سلوكياً ممتازاً بتقديم النصيحة، حيث أكد **78%** منهم أن التصرف الفوري والأسلم هو **إبلاغ السلطات الأمنية فوراً** (كالشرطة والدرك الوطني). هذا يعكس ثقة مجتمعية كبيرة في أن الدولة ومصالحها الأمنية المختصة هي الملاذ الحقيقي والوحيد القادر على ردع الجناة وضمان الحماية.
4. **ثنائية الحل (الوعي الفردي والردع الجزائي):** خلصت الدراسة في نهايتها إلى صياغة رؤية متكاملة للمواجهة؛ حيث يرى **76%** أن الحل يبدأ من سلوك المستخدم عبر **عدم مشاركة الصور والبيانات الحساسة**، بينما يرى **48%** أن المواجهة تتطلب **سن قوانين ردعية وتشديد العقوبات**. وبناءً على ذلك، فإن نجاح التحول الرقمي الآمن في الجزائر يقوم على جناحين لا ينفصلان: **الوعي والحرص الرقمي الذاتي للأشخاص، والردع الجزائي الصارم والقوي من قِبل المشرع**.

المبحث الثاني: التحديات و الجزاءات القانونية للابتزاز الالكتروني

ان الطبيعة الافتراضية لجريمة الابتزاز الالكتروني لم تكثف بفرض نمط اجرامي مستحدث فحسب، بل افرزت تعقيدات بالغة طالت منظومة العدالة الجنائية في شقيها الاجرائي و الموضوعي، فمن ناحية، يواجه المحققون و اجهزة انفاد القانون ترسانة من التحديات الاجرائية التي تفرضها البيئة الرقمية، بدأ من المعضلة التقنية في تحديد الهوية الحقيقية للجاني الدي يختفي خلف جدران التشفير و الاسماء المستعارة، وصولا الى صعوبة استنباط و توثيق الدليل الرقمي الدي يتميز بالهشاشة و سهولة المحو و الاندثار، مما يجعل مهمة الأثبات الجاني عبئا تقنيا و قانونيا ثقيلا. وعلى الجانب الاخر واستجابة لهده المخاطر المتزايدة، كان لزاما على المشرع الجزائري التدخل لرسم الحدود الردعية لهده الجريمة، حيث افرد لها منظومة جزائية تجمع بين العقوبات الاصلية و التبعية، ساعيا من خلالها الى موائمة السياسية العقابية التقليدية مع جسامة الاعتداءات المعلوماتية، و انطلاقا من هده الاشكالية، يسعى هدا المبحث الى تسليط الضوء على المعوقات التي تواجه جهات التحقيق في ملاحقة مرتكبي هده الجرائم، مع تحليل دقيق لطبيعة العقوبات و التدابير التي اقرها قانون العقوبات الجزائري و القوانين المكملة له، و دلك لضمان فعالية الملاحقة و تحقيق الردع العام و الخاص في الفضاء السيبيراني، وهو ما سنفصله عبر المطالب التالية.

المطلب الاول:تحديات التحقيق الرقمي(المعوقات):

"يعتبر التحقيق في جرائم الابتزاز الالكتروني أمر ليس بالهين بسبب الصعوبات التي تواجه المحقق أمام جريمة ما زالت غامضة، حتى انعدم التمكن من السيطرة على مجريات التحقيق قد يؤدي إلى فقدان الثقة في المجتمع وزيادة نسبة الجريمة."[1]

الفرع الاول: الصعوبات التي تواجه جهات التحقيق:

تتميز الجرائم التي ترتكب عبر الانترنت بكون محلها معلومات أو برامج معالجة آلية عبر الحواسيب، أو جرائم تتعلق بالأشخاص عبر عالم افتراضي غير متناهي وغير محدود مما يعطيها طابع خاص ليس فقط في طريقة ارتكابها بل كذلك في الوسيلة التي ترتكب بها، أمر الذي ينجم عنه صعوبات اكتشاف الجريمة والتحقيق فيها، فهي تتنوع بين صعوبات متعلقة بالجريمة و الجهات المتضررة، و صعوبات متعلقة بالجانب القضائي[2].

اولا: صعوبة اكتشاف الجريمة الابتزاز الالكتروني:

تواجِه جهود الكشف عن الجرائم المعلوماتية جملة من العقبات الجوهرية؛ إذ تتنازعها اعتبارات قانونية تتمثل في **الخصوصية الرقمية** وضمانات الحرمة الشخصية، وعوائق تقنية تكمن في **الطبيعة اللامادية** للجريمة التي تؤدي إلى سرعة تلاشي آثارها. كما تبرز تحديات سيكولوجية تتعلق بـ **إحجام الضحايا** عن التبليغ، فضلاً عن العائق المؤسساتي المتمثل في **الفجوة التقنية** ونقص التأهيل التخصصي لدى بعض أجهزة التحقيق في مواكبة الأساليب الإجرامية المتطورة.[3]

أ. حق الانسان في خصوصية:

قد أجمعت التشريعات المقارنة على تجريم الانتهاكات التي تطال حرمة الحياة الخاصة عبر الفضاء الرقمي، مستمدةً مشروعيتها من المبادئ الراسخة في المواثيق الدولية، وعلى رأسها **الإعلان العالمي لحقوق الإنسان لعام 1948** .حيث نصت المادة 15 منه كما ورد في بعض السياقات— على عدم جواز التدخل التعسفي في خصوصيات الفرد أو أسرته أو مراسلاته، أو المساس بشرفه وسمعته، مع كفالة الحق لكل

[1] المادة 15 ميثاق الامم المتحدة سنة 1948.

[2] بن سليمان محمد الطاهر، واخرون، جريمة الابتزاز الالكتروني، مدكرة لنيل شهادة ماستر اكاديمي، تخصص قانون جنائي و علوم جنائية، كلية حقوق و العلوم السياسية، جامعة قاصدي مرباح ورقلة، 2023، ص52.

[3] بن سليمان محمد طاهر[واخرون]، المرجع السابق، ص52.

شخص في التماس الحماية القانونية ضد هذه الاعتداءات، وهو ما يشكل اليوم حجر الزاوية في تجريم أفعال الابتزاز والتشهير الإلكتروني.[1]

ب. فقدان الاثار المادية الجريمة :

تظل الجريمة المعلوماتية مجهولة مالم يتم تبليغ عنها، فهي تتميز عن الجرائم التقليدية بطبيعة تنفيذها التي تعتمد على نبضات إلكترونية غير مرئية تتدفق عبر الأنظمة والشبكات. وتكمن الإشكالية الجوهرية في سهولة محو الآثار الرقمية؛ إذ يكفي ضغط زر واحدة لإتلاف قواعد بيانات كاملة، مما يجعل عملية ضبط المعطيات وتحديد هويتها أمراً بالغ التعقيد، فغالباً ما تصطدم مصالح الضبطية القضائية عند معاينة مسرح الجريمة الافتراضي ببيانات تفتقر إلى البصمات التقليدية التي تسمح بالاستدلال المباشر على الجاني[2].

تتوافر جملة من العقبات التي تحول دون الوصول إلى الفاعل الحقيقي في الجرائم المعلوماتية؛ فاعتماد الجناة على الهويات المستعارة والولوج إلى الشبكة عبر وسائط عمومية (كمقاهي الإنترنت) يؤدي إلى تضليل سلطات التحقيق وتشتيت جهود تحديد موقع الاتصال. وتتضاعف هذه الإشكالية ببروز 'تنازع الاختصاص المكاني حيث يثير ارتكاب الجريمة في الخارج تساؤلات قانونية معقدة حول القانون الواجب التطبيق فضلاً عن غياب الأدلة المادية الملموسة[3]، وعجز الوسائل التقليدية عن رصد الأثر الرقمي الزائل[4].

ت. فرض الجناة لتدابير أمنية:

يعتمد الجناة في الجرائم المعلوماتية على أساليب تقنية متطورة لإزالة أثار الجريمة، مستغلين الطبيعة اللامادية للتخزين الإلكتروني ولغة البيانات الرقمية التي تستعصي على الفهم المباشر لغير المتخصصين. وتكمن الصعوبة في كون هذه الفئة من المجرمين تتمتع بقدر عالي من الذكاء التقني، مما يمكنهم من إحاطة أفعالهم بسياج أمني وقائي يحول دون استخلاص الدليل الجنائي، كما يعمد هؤلاء إلى توظيف برمجيات إخفاء الهوية وانتحال الشخصية، لا سيما عبر البريد الإلكتروني، لخلق فجوة بين الفعل المادي وشخص الفاعل، مما يعيق جهود التعرف عليهم عند اكتشاف الجريمة[5].

ث. نقص خبرة السلطات الاستدلال:

"مازالت جهات التحقيق تعاني من قلة الخبرة الفنية وقلة التدريب على التعامل مع الادلة الرقمية، وكيفية البحث عنها، وكيفية الحصول على هذا الدليل، كما أن خبرة التحقيق مع مجرم ذكي له طبيعة خاصة، سيما وان هذا المجرم يراوغ ويحاول التهرب من جرمه، ربما بإغراق المحقق في تفاصيل لا يعلمها جيدا، حيث ان المحقق الجنائي في جرائم الابتزاز الالكتروني يجب أن يكون له تكوين تقني ، فيجب ان يجمع بين مهارة استخدام التقنية الحديثة وكذلك مهارة تقييم الجريمة الإلكترونية ومدى الخطورة الاجرامية لمرتكبها، وكذا مهارة التعرف على المكونات المادية الاجهزة وعلى ملحقاتها من طابعات وماسحات ضوئية وكاميرات، وذلك للتأكد من ارتباطها بالجهاز الاصلي من عدمه، وتقييم الوسائط الخاصة بتخزين الادلة الرقمية لتحديد مدى ارتباطها بالأنترنت وما إذا كانت جزء من أدوات الجريمة من عدمه."[6]

فقد تكون شخصية المحقق تميل الى التهيب من استخدام الكمبيوتر و التهيب من استخدام الانترنت ، و عدم الخبرة الكافية و عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية ، وهي كلها صعوبات تتعلق

[1] عماد جواد موسى، التحقيق والصعوبات التي تواجه جريمة الابتزاز الالكتروني، مجلة كلية المعارف الجامعة، كلية التربية للعلوم الانسانية، جامعة الانبار، الرمادي، العراق، ص 244.

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنت، شهادة الماجيستير كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه " القانون الاساسي والعلوم السياسية " جامعة مولود معمري تيزي وزو2013.

[3] جبلي سعيدة، حداد شيماء، المرجع السابق، ص47.

[4] المرجع نفسه، ص 47.

[5] خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنت، ط1 ،دار الثقافة للنشر و التوزيع ، دبي ،2011 ،ص224.

[6] عماد جواد موسى ، المرجع السابق ، ص 245.

بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم ، كذلك عدم توفر المعرفة بأساليب ارتكاب الجريمة الالكترونية و كذا قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية.[1]

إن عدم التوازي بين الثورة المعلوماتية المتسارعة وبين وتيرة التحديث التشريعي والأمني يُعد من أبرز معوقات مكافحة الجريمة الإلكترونية، حيث يستغرق بناء الكوادر القضائية والأمنية وقتاً طويلاً مقارنةً بالانتشار اللحظي للتقنية، هذا الخلل في التوازن يؤدي إلى قصور في إجراءات البحث والتحري، مما يستوجب تبني سياسة جنائية استباقية ترتكز على التكوين المستمر والشامل لجهات التحقيق والحكم، لردم الفجوة المعرفية وتمكينهم من أدوات السيطرة على الجرائم المرتبطة بالتقنية الحديثة[2].

ج. التكتم عليها من قبل الجاني:

يعد تكتم عن التبليغ من أبرز المعوقات التي تواجه اكتشاف الجرائم الإلكترونية؛ إذ غالباً ما يفضل المجني عليهم التكتم على الواقعة لدوافع احترازية، تهدف إلى منع انتشار الأساليب الجرمية والحيلولة دون محاكاتها من قبل جناة آخرين. وتتضاعف هذه الظاهرة لدى المؤسسات المالية كالبنوك وشركات التأمين، التي تخشى من أن يؤدي الإفصاح عن اختراق أنظمتها إلى زعزعة الثقة في مركزها المالي أو كشف ثغرات أمنية قد تستغلها أطراف أخرى، مما يجعلها تفضل المعالجة السرية للأزمة بعيداً عن أروقة القضاء[3].

الفرع الثاني:صعوبات الاثبات في جريمة الابتزاز الالكتروني:

الرغم من الترسانة القانونية والجهود الأمنية المبذولة، إلا أن مكافحة الابتزاز الإلكتروني تصطدم بعقبات موضوعية ناتجة عن طبيعة الجريمة ذاتها؛ فهي جريمة 'خفية' تُرتكب في فضاء افتراضي يمنح الجاني ميزة التخفي وراء هويات رقمية مزيفة. إن اتصاف مرتكبي هذه الجرائم بالذكاء التقني الحاد يفرز صعوبات بالغة في مرحلة الإثبات الجنائي، حيث يواجه المحققون تحدي التعامل مع الدليل الرقمي الذي يتميز بالهشاشة وسهولة المحو أو التعديل، مما يجعل من عملية استخلاصه وتقديمه كحجة قاطعة أمام القضاء أمراً محفوفاً بالتعقيدات الفنية والإجرائية[4].

اولا:الصعوبات المتعلقة بالدليل:

1. سهولة محو الدليل:

تتمثل أولى معوقات الإثبات في الابتزاز الإلكتروني في سهولة محو الأثر الجرمي، فالبناء الرقمي للدليل يسمح للجاني بإعدام وجوده المادي في لحظات معدودة. وغالباً ما يحرص المبتز على تطهير الأجهزة والوسائط المستخدمة من أي بيانات قد تدينه، مستفيداً من مرونة التعامل مع الملفات الإلكترونية. إن هذا المحو المتعمد يحول دون قدرة أجهزة البحث والتحري على إعادة بناء مسرح الجريمة الافتراضي، ويجعل من عملية الوصول إلى الدليل الأصلي عقبة تقنية قد تنتهي بضياع الحقيقة القضائية نتيجة اختفاء المادة الجرمية بصفة نهائية[5].

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

تنفرد جريمة الابتزاز الإلكتروني بخصائص تميزها عن الجريمة التقليدية، كونها تقع في 'فضاء غير مادي' تحكمه الخوارزميات والبيانات الرقمية، وتفتقر إلى العنف المادي الملموس. فبينما يعتمد التحقيق في الجرائم التقليدية على الآثار البيولوجية والفيزيائية كبصمات الأصابع أو الدماء ، يواجه المحقق في عالم الابتزاز الرقمي 'أدلةً رمزية' غير مرئية للعين المجردة. هذا الانفصال عن الواقع

[1] خالد عياد الحلبي. إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. ط1 ،دار الثقافة للنشر والتوزيع، دبي، 2011.
[2] بن سليمان محمد طاهر، و اخرون، المرجع السابق، ص 54.
[3] المرجع نفسه، ص53.
[4] بن سليمان محمد طاهر، واخرون، المرجع السابق، ص 67
[5] المرجع نفسه.

المادي يجعل من عملية تتبع الجاني واختراق جدار السرية الذي تفرضه الرموز الرقمية عقبةً إجرائية تتطلب أدوات استدلالية وتقنية فائقة الحداثة[1].

3. عرقلة الوصول للدليل:

تتمثل إحدى أعقد صور عرقلة الوصول للدليل الرقمي في قيام الجاني بتبني 'استراتيجية التحصين الرقمي التي تتبعها المواقع العالمية، إذ يستخدم تقنيات التشفير وكلمات السر كحواجز فنية لحجب المعلومات ومنع اكتشاف مصدر التهديد أو التلاعب بالبيانات. إن هذا السياج الأمني، الذي صُمم في الأصل لمنع التسلل والتدمير، يتحول في يد المجرم إلى وسيلة لإخفاء أدلة الإدانة وضمان الإفلات من الملاحقة. وبذلك، يصبح الدليل الرقمي رهينة تقنية خلف شيفرات معقدة، مما يفرض على المشرع ضرورة وضع آليات قانونية تُلزم المتهم أو ذوي الصلة بالإفصاح عن مفاتيح التشفير لتسهيل مأمورية العدالة[2].

كما يؤكد المختصون في الجريمة التقنية أن 'النمط التقليدي' للبحث والتحري، المستند إلى قانون العقوبات بصورته الكلاسيكية، يقف عاجزاً أمام الطبيعة الافتراضية لجريمة الابتزاز المعلوماتي. فالمحقق غير المتخصص، الذي اعتاد معاينة مسارح الجريمة المادية، يجد نفسه أمام وسائط تخزين وبرمجيات معقدة تتطلب آليات ضبط وتفتيش خاصة. إن هذا النقص في التخصص لا يعيق عملية الوصول إلى الجاني فحسب، بل قد يؤدي إلى إهدار الأدلة الرقمية نتيجة الجهل بطرق التعامل معها، مما يجعل من تأهيل 'الشرطة التقنية' ضرورة حتمية لا ترفاً إدارياً.[3]

4. صعوبات المتعلقة بنقص الخبرة :

تتطلب ملاحقة جريمة الابتزاز الرقمي محققاً يجمع بين المهارة القانونية والخبرة المعلوماتية، لذا فإن غياب التخصص التقني يضعف من فاعلية الاستجواب الجنائي. فالمحقق الذي يفتقر لمهارات استخدام الحاسب الآلي يجد صعوبة في محاصرة المتهم تقنياً أو فهم المصطلحات والوسائل التي استخدمها في تنفيذ الابتزاز. علاوة على ذلك، فإن نقص الدراية بكيفية التحريز السليم لأوعية المعلومات والذاكرات الومضية والممغنطة يعرضها للتلف المادي أو المنطقي، مما يجعل الدليل الرقمي غير قابل للاستخدام أمام المحكمة نتيجة سوء التداول الإجرائي الناتج عن نقص الخبرة[4]. . :

5. امتناع المجني عليه عن الابلاغ :

يعد إحجام المجني عليه عن التبليغ من أبرز الصعوبات التي تعرقل ملاحقة جريمة الابتزاز الرقمي، فالتلازم بين التهديد بنشر الأسرار وخوف الضحية على سمعتها يخلق حالة من الشلل الإجرائي. ويلاحظ الباحث أن ضحايا الابتزاز ولاسيما الإناث يميلون إلى التسوية الذاتية مع الجاني عبر الخضوع لإكراهه، مما يؤدي إلى ضياع فرصة ضبط الأدلة في حينها. إن هذا السلوك لا يعكس ضعفاً في القوانين بقدر ما يعكس حاجةً ملحة لتوفير ضمانات قصوى للسرية والحماية للمجني عليهم، لتشجيعهم على كسر حاجز الصمت ومواجهة التغول الرقمي للجناة[5].

---

[1] غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر و التوزيع، ط1، الجزائر، 2016، ص45.

[2] معتوق عبد اللطيف، الاطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجيستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر باتنة2011_2012.

[3] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، ط1 ،دار الفكر الجامعي مصر، ص89.

[4] برحال أمال، جريمة الابتزاز عبر الوسائط الالكترونية، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2020.

[5] بن سليمان محمد طاهر [و اخرون،] المرجع السابق، ص

لا تقتصر آثار الابتزاز الإلكتروني على الأفراد فحسب، بل تمتد لتطال الكيانات الاقتصادية والمؤسسات التي تجد نفسها أهدافاً لهجمات رقمية تستهدف بياناتها الحساسة، وفي هذا السياق، يبرز الخوف على الائتمان التجاري كعائق يحول دون إبلاغ هذه المؤسسات عن الجرائم التي تتعرض لها؛ إذ تخشى الشركات من أن يؤدي إشهار واقعة الاختراق أو الابتزاز إلى اهتزاز ثقة المتعاملين والمساهمين، مما يترتب عليه أضرار اقتصادية جسيمة قد تتجاوز قيمتها الفدية المطلوبة من قِبل المبتز، وهو ما يجعل المؤسسة تُفضل 'التسوية الصامتة' على المواجهة القانونية.[1]

و بالتالي يترتب على التأخر في الإبلاغ عن جريمة الابتزاز الرقمي تداعيات إجرائية خطيرة، إذ يمنح عامل الزمن للجاني فرصة مثالية لاستغلال الطبيعة الديناميكية للدليل الرقمي، فالدليل في هذا النوع من الجرائم ليس قاراً بطبعه، بل هو عُرضة للحذف السلس أو التلاعب السريع بمحتواه، مما يؤدي حتماً إلى إهدار قيمته القانونية. إن مضي الوقت دون تحرك إجرائي فوري يحول دون قدرة خبراء الأدلة الجنائية على استعادة البيانات أو التحقق من موثوقيتها، مما يترتب عليه في نهاية المطاف سقوط الحجية القضائية للدليل وإفلات الجناة من قبضة العقاب[2].

ثانيا: معالجة الاشكالات التي يثيرها الدليل الرقمي في جريمة الابتزاز الالكتروني:

على الرغم من جسامة التحديات الإجرائية والتقنية سالفة الذكر، إلا أن التطور المتسارع في تكنولوجيات الإعلام والاتصال أفرز بالتوازي 'منظومة دفاعية رقمية' قادرة على مجابهة الابتزاز الإلكتروني. وتعتمد هذه المنظومة على تقنيات حديثة تتلاءم والخصائص الفريدة للدليل الرقمي، حيث تتيح أدوات **التحقيق الجنائي الرقمي** استعادة البيانات المحذوفة، وتتبع المسارات المشفرة، وتحديد الهويات الرقمية بدقة عالية. إن تبادل الخبرات الأمنية والتقنية بين الدول أسهم في عولمة الحلول التقنية، مما جعل من ملاحقة الجناة أمراً ممكناً رغم التعقيدات الفضاء الافتراضي[3].

1) الاستعانة بالخبرة التقنية و الفنية :

يمثل الاستعانة بالخبير الرقمي ضرورة إجرائية لفك 'طلاسم الجريمة المعلوماتية'؛ ففي ظل سهولة محو الأدلة وصعوبة استخلاصها، يبرز دور المتخصص في التحليل الرقمي لإعادة تجميع مكونات الدليل المبدد واقتفاء أثره عبر برامج التتبع المتخصصة. إن مهام الخبير تتشعب لتشمل فحص مدى سلامة الدليل من الناحية الفنية وتفنيد أي تلاعب قد يطرأ على الخوارزميات الرقمية. لذا، فإن الاعتماد على كفاءات بشرية تحوز ناصية التكنولوجيا هو الحل الأمثل لمواجهة التحول الرقمي للجريمة، وتحويل التقنية من وسيلة للإفلات من العقاب إلى أداة قاطعة للإدانة[4].

2) تسخير التكنولوجيا الحديثة في استخلاص الادلة الرقمية :

يرتكز نجاح التحقيقات الجنائية في جرائم الابتزاز الإلكتروني على قدرة السلطات المختصة على استباق تكتيكات الجناة من خلال أدوات فنية مستحدثة. ويتمثل هذا المنهج المبتكر في استخدام برامج المعالجة المتطورة التي تتيح استقصاء الأدلة من الخوادم والوسائط المشفرة بدقة وسرعة فائقة. إن تطوير حلول تقنية مضادة' لا يساعد فقط في الوصول إلى الهوية الحقيقية للمبتز، بل يضمن أيضاً حماية المحتوى الرقمي من التلف أو الضياع أثناء عملية التحليل، وهو ما يعزز من كفاءة منظومة الإثبات الجنائي في

[1] عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والاجرائية، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، الاردن، سنة 2022.
[2] ديب اكرم، بوعبد الله نورة، المرجع السابق، ص 413.
[3] المرجع نفسه، ص 414.
[4] المرجع نفسه.

مواجهة الجريمة المعلوماتية العابرة للحدود[1].و استخلاص الادلة من برمجيات الالكترونية متطورة تخضع للتحديث الدائم حسب التغيرات و التحولات التي تشهدها البيئة الرقمية، و إدراج الذكاء الاصطناعي في هذه العملية والذي يتيح إمكانية الكشف عن الوجه و التعرف التلقائي على الصوت.[2]

ثانيا: صعوبات المتعلقة بالجانب قضائي و التعاون الدولي:

تستدعي الطبيعة الجريمة الإلكترونية استجابة دولية موحدة، حيث أن الواقع يشير إلى وجود فارق شاسع بين سرعة تطور الجريمة وبين بطء آليات التعاون الأمني والقضائي بين الدول. هذا القصور الإجرائي يمثل ثغرة جوهرية يستغلها الجناة للإفلات من العقاب، حيث تصطدم ضرورة الملاحقة الفورية بعقبات تنازع الاختصاص وبطء تنفيذ الاتفاقيات الدولية، مما يكرس الفجوة بين واقع إجرامي متطور وجهاز عدالة دولي مثقل بإجراءات تقليدية رتيب

"وقد نجم عن هذه الاشكالية أيضا صعوبات تتمثل في القانون الواجب التطبيق، و المحكمة المختصة تنازع الاختصاص"[3].

اختصاص القضائي في الجريمة الالكترونية:

يصطدم التقدم في إجراءات الملاحقة الجنائية لجرائم الإنترنت بإشكالية تعدد جهات الاختصاص وتنازع اختصاص القضائي على المستويين المحلي والدولي. فبسبب الطبيعة الافتراضية للجريمة، قد يقع السلوك الإجرامي في دولة، وتتحقق النتيجة في ثانية، ويوجد المجني عليه في ثالثة؛ مما يفتح الباب واسعاً أمام تنازع إيجابي أو سلبي بين المنظومات القضائية، هذا التشتت الإجرائي يلقي بظلاله على تماسك الأدلة الجنائية وصحة الإجراءات المتبعة، مما يجعل من تحديد القاضي الطبيعي للجريمة الإلكترونية تحدياً قانونياً قائماً[4].

تجسدت استجابة المشرع الجزائري للتحديات الإجرائية في وضع إطار قانوني خاص القانون 09-04 يهدف إلى تذليل عقبات الاختصاص القضائي بنوعيه الوطني والدولي. فمن جهة، تم تكييف قواعد الاختصاص المحلي لتستوعب الجرائم المرتكبة عبر الوسائط التقنية، ومن جهة أخرى، تم تبني معايير إسناد دولية موسعة تسمح للقضاء الجزائري بالنظر في الجرائم التي تمس مصالح الدولة أو رعاياها حتى وإن ارتكبت خارج الإقليم الوطني. وتعد هذه القواعد المستحدثة الركيزة التي استند إليها المشرع لتمكين سلطات التحقيق من تجاوز عائق اللامكانية في الفضاء السيبراني[5].

أ. الاختصاص القضائي داخلي:

بموجب المادة 37 من قانون الإجراءات الجزائية، يتحدد النطاق الإقليمي للقضاء المختص عبر ثلاثة ضوابط تشريعية: مكان وقوع الجريمة، محل إقامة أحد المتهمين، أو مكان إلقاء القبض على أحدهم. ويشكل هذا النص المرجعية القانونية التي تحكم توزيع الاختصاص المحلي بين المحاكم الجزائرية؛ حيث سعى المشرع من خلاله إلى تمديد ولاية وكيل الجمهورية بما يكفل استيعاب كافة صور المساهمة الجنائية، وضمان عدم وجود نزاع قضائي يحول دون المباشرة الفورية لإجراءات البحث والتحري في الجرائم المستحدثة والتقليدية على حد سواء[6].

كما نجد ان في نفس المادة في فقرتها الثانية تنص على: "يجوز تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم والجريمة المنظمة عبر الحدود

[1] عبد الله ذيب محمود، أسامة إسماعيل دراج، المرجع السابق، ص232.
[2] ديب اكرم، بوعبد الله نورة، المرجع السابق، ص414.
[3] المرجع نفسه، ص54
[4] مولاي ملياني دلال، إشكالية الاثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017، ص79.
[5] بوديسة بجاد عبد رؤوف، المرجع السابق، ص 80.
[6] المرجع نفسه.

الوطنية والجرائم الماسة المعالجة الالية بالمعطيات وجرائم تبييض الاموال و إرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".[1]

نظراً للطبيعة العابرة للحدود التي تتميز بها الجرائم المعلوماتية، وتجاوزها للمفاهيم المادية التقليدية لمسرح الجريمة، فقد أقر المشرع الجزائري امتداداً نوعياً للاختصاص القضائي ليشمل كافة إقليم الدولة. ويتجلى هذا التوجه بوضوح في الجرائم الماسة بنظم المعالجة الآلية للمعطيات؛ حيث تقتضي الضرورة الإجرائية منح ولاية قضائية مرنة تسمح بملاحقة هذه الأفعال أينما تحقق أثرها أو وسيلتها داخل الإقليم الوطني، استجابةً للخصائص الفنية التي سبق تفصيلها في الفصل الأول، وضماناً لعدم إفلات الجناة من العقاب بذريعة عدم تحديد نقطة جغرافية ثابتة للجريمة[2].

أرسى المشرع الجزائري منظومة متكاملة لتمديد الاختصاص المحلي تشمل كافة أجهزة العدالة الجنائية، فبموجب المواد (37، 40، 47، 80، 329) من قانون الإجراءات الجزائية، لم يعد الاختصاص محصوراً في نطاق ضيق بل امتد ليشمل صلاحيات وكيل الجمهورية وقاضي التحقيق، وصولاً إلى اختصاص المحاكم ذاتها. وقد تعزز هذا التمديد بمنح ضباط الشرطة القضائية صلاحيات أوسع وفق المادة 40 مكرر 1، مع إجازة تمديد الاختصاص إلى دوائر محاكم أخرى بموجب التنظيم (المرسوم التنفيذي 06-348)[3]، مما يضمن مرونة إجرائية تسمح بملاحقة الجرائم المستحدثة التي تتجاوز آثارها الحدود الإقليمية للمحاكم التقليدية فان الاختصاص القضائي في الجرائم يتحدد حسب:

❖ **ضرورة التحقيق:**

يخضع تمديد اختصاص قاضي التحقيق في الجرائم المعلوماتية لضوابط إجرائية صارمة توازن بينه مقتضيات التحقيق وحرمة الاختصاص المحلي. وتتمثل هذه الشروط في ضرورة توافر أدلة قوية وقرائن كافية على ارتكاب الجريمة، مع قيام حالة الضرورة القصوى التي تستدعي الانتقال خارج النطاق المكاني المعتاد. كما أوجب القانون مراعاة شكليات الإخطار المسبق لكل من وكيل الجمهورية التابع له القاضي، ووكيل الجمهورية في الدائرة المراد الانتقال إليها، مع تسبيب قرار التمديد بوضوح. وباعتبار أن قواعد الاختصاص هي من **النظام العام**، فإنها تشكل القيد القانوني الذي يحدد الأهلية الإجرائية لجهة القضاء، وأي إخلال بها يمس جوهر حسن سير العدالة[4].

❖ **التمديد لا يتم الا في جرائم معينة:**

تُعد المادة5 من القانون 09-04 سنداً إجرائياً جوهرياً لتعزيز كفاءة البحث والتحري في الجرائم المعلوماتية، إذ أقرت ما يمكن تسميته بـ 'التفتيش الرقمي الممتد'. فالمشرع أجاز تمديد إجراءات التفتيش بسرعة فائقة لتشمل منظومات معلوماتية أخرى أو أجزاء منها، بشرط وجود ترابط تقني يسمح بالوصول إليها من المنظومة محل التفتيش الأصلي، ومع وجوب إعلام السلطة القضائية مسبقاً. هذه الآلية تدمج بين المسرح التقليدي والافتراضي، وتسمح بتتبع الأثر الرقمي عبر الشبكات، مما يُعد استجابة فعالة لخصائص الجريمة الإلكترونية التي غالباً ما تتوزع أدلتها بين أنظمة متعددة ومتباعدة[5].

ب. الاختصاص القضائي الدولي:

تثير مسألة تمديد الاختصاص في الفضاء الرقمي إشكالية قانونية بالغة التعقيد حين يتسع مسرح الجريمة ليشمل أقاليم دول متعددة، فإذا كان تمديد الاختصاص داخلياً أمراً ميسوراً باعتبار الدولة وحدة سيادية واحدة،

[1] المادة 37 القانون رقم 04-14 المؤرخ - 10 نوفمبر سنة 2004، جريدة رسمية، للجمهورية الشعبية ديمقراطية، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الاجراءات الجزائية، العدد71، ص 4.

[2] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص80.

[3] مولاي ملياني دلال، المرجع السابق، ص250.

[4] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص 81.

[5] المادة 5 من القانون 09-04 ،المرجع السابق.

فإنه يصطدم دولياً بمبدأ **'إقليمية القوانين الجنائية '** فإن الطبيعة العابرة للحدود للجريمة المعلوماتية تفرض واقعاً تقنياً يجعل من أقاليم دول شتى مسرحاً لواقعة إجرامية واحدة، مما يضع سلطات التحقيق في مواجهة مأزق الحفاظ على سيادة الدول الأخرى أثناء محاولة تحصيل الدليل الإلكتروني، ويستوجب التوفيق بين مقتضيات الملاحقة الجنائية والمبادئ الاحترازية المكرسة دولياً[1].

- **مبدأ الاقليمية في جرائم الانترنت:**

يُعد اختصاص المحاكم الجزائرية بالنظر في الجرائم المعلوماتية تجسيداً صريحاً لمبدأ **'إقليمية القوانين الجنائية '**المكرس في المادة 3 من قانون العقوبات. وبموجب هذا المبدأ، تنعقد الولاية القضائية الأصيلة للقضاء الجزائري بمجرد تحقق السلوك الإجرامي سواء كلياً أو جزئياً فوق الإقليم الوطني، دون الاعتداد بغير اخلاقية الجاني أو صفته. إن هذا التوجه التشريعي لا يعد مجرد قاعدة لتوزيع الاختصاص فحسب، بل هو مظهر سيادي يعكس بسط الدولة لسلطتها القانونية على كافة الأفعال المرتكبة ضمن حدودها، بما في ذلك تلك التي تتخذ من الوسائط الرقمية مسرحاً لها[2].

ويُقصد بمبدأ إقليمية القوانين سريان النص الجزائي الوطني على جميع الجرائم المرتكبة داخل إقليم الدولة، بقطع النظر عن غير اخلاقية أطرافها. وبموجب هذا المبدأ المستقر دولياً، تنعقد الصلاحية الإجرائية لسلطات التحقيق والحكم في مكان وقوع الجريمة. وفي سياق الجرائم الحديثة، يكفي لتحريك الدعوى العمومية وقوع جزء من العناصر المادية المكونة للجريمة داخل الإقليم، مما يجعل من مكان التنفيذ أو مكان النتيجة ضابطاً حاسماً في تحديد الجهة القضائية المختصة بالنظر في الخصومة[3].

وعلى خلاف الجرائم التقليدية التي تتقيد عناصر ركنها المادي سلوكاً ونتيجة بنطاق جغرافي موحد، تفرض الجرائم المعلوماتية واقعاً يتسم بـ التجزئة المكانية للنشاط الإجرامي. فقد يُرتكب السلوك المادي (كالتلاعب بالبيانات أو قرصنتها) انطلاقاً من منظومة معلوماتية في دولة ما، بينما لا تتحقق الآثار التخريبية أو النتائج الجرمية إلا في إقليم دولة أخرى. هذا التباعد بين وحدة الجريمة وتعدد الأقاليم يضعنا أمام معضلة تنازع القوانين، وهو ما أدى إلى تباين الرؤى الفقهية عبر ثلاثة اتجاهات رئيسية سعت لضبط معايير الاختصاص في هذا الفضاء العابر للحدود:[4]

- **مذهب السلوك أو النشاط الاجرامي بوصفه معيارا لتحديد مكان وقوع الجريمة**

وفقاً لهذا المعيار، ينعقد الاختصاص القضائي للمحكمة التي شهدت دائرتُها مباشرة النشاط الإجرامي، وينطلق هذا التوجه من اعتبارات واقعية قوامها تيسير عملية الإثبات الجنائي وجمع الأدلة. فالسلطات القضائية في دولة السلوك هي الأقرب جغرافياً وتقنياً من مسرح الجريمة، مما يتيح لها ضبط الوسائل المستخدمة في الجريمة (كالحواسيب والوسائط الرقمية) ومعاينتها فوراً، وهو ما يضمن سرعة التحفظ على الأدلة الرقمية قبل تعرضها للمحو أو التعديل.[5]

- **مذهب النتيجة الاجرامية كمعيار لتحديد مكان وقوع الجريمة**

ينطلق هذا الاتجاه من رؤية قانونية ترتكز على مبدأ وحدة الجريمة، رافضاً الفصل التعسفي بين عناصرها المكونة. ويرى أنصار هذا المعيار أنه الأكثر واقعية في التطبيق؛ نظراً لأن النتيجة الإجرامية تُمثل المظهر الخارجي الملموس للضرر، على خلاف السلوك الذي قد يتخذ صوراً خفية أو سلبية وبناءً عليه، ينعقد

[1] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص82.
[2] نفس المرجع، ص 83.
[3] مريم عراب، المرجع السابق ، ص 277.
[4] دلال مولاي ملياني، المرجع السابق، ص252.
[5] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص 84.

الاختصاص للمحكمة التي تحقق في دائرتها الأثر الجرمي، وهو التوجه الذي تبنته تشريعات رصينة كالقانون الألماني، سعياً لضمان حماية المجني عليه في المكان الذي تضرر فيه فعلياً[1].

- **المذهب المختلط**

تجاوزاً للقصور الذي شاب المعيارين السابقين، تبلور اتجاه ثالث يتبنى المقاربة الشمولية في تحديد الاختصاص؛ ومفاده أن الجريمة تعتبر واقعة في كل مكان شهد تحقق عنصر من عناصر ركنها المادي. وينطلق هذا التوجه من حقيقة قانونية مفادها أن الجريمة وحدة لا تتجزأ، تشمل النشاط التنفيذي، والنتيجة الإجرامية، ورابطة السببية بينهما. وبناءً عليه، ينعقد الاختصاص للقضاء سواء في مكان صدور السلوك أو في مكان تحقق الأثر (أو حتى مكان توقعه)، وهو ما يمنح المنظومة الجنائية حماية مزدوجة تستوعب تشتت العناصر المادية للجريمة الإلكترونية عبر الأقاليم المختلفة[2].

➢ المبادئ الاخرى في مسألة الاختصاص في الجريمة المعلوماتية:

"تعمد الدولة الى حماية مصالحها على إقليمها الوطني وهذا الاصل ولكن حين تشكل الاعتداءات تهديدا لمصالحها وخارج حدود إقليمها لابد من أعمال مبادئ استثنائية حماية لمصالحها ومواطنيها وبالمقابل دون الاعتداء على سيادة الدولة الاخرى."[3]

- **مبدأ العينية:**

" يقصد به تطبيق القانون الجزائي على الجرائم التي تمس المصالح الاساسية للدولة والمرتكبة خارج إقليمها أيا كانت غير اخلاقية مرتكبها وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الاساسية".[4]

نظراً لقصور مبدأ الإقليمية التقليدي عن بسط حماية شاملة للمصالح الوطنية في الفضاء السيبراني، استوجبت الضرورة الملحة تفعيل مبدأ العينية كآلية دفاعية استباقية. ففي ظل الجرائم الإلكترونية التي تتجاوز الحدود المادية لتستقر في مسارح افتراضية عابرة للقارات، لا يمكن للدولة أن تقف مكتوفة الأيدي تجاه اعتداءات تنطلق من الخارج وتستهدف أنظمتها السيادية. لذا فإن مبدأ العينية يجد مبرره في كونه الأداة القانونية الكفيلة بحماية 'المصلحة الوطنية العليا من التهديدات الرقمية الخارجية، معتبراً أن أمن المعطيات الوطنية جزء لا يتجزأ من حرمة الدولة، حتى وإن نُفذ الاعتداء انطلاقاً من إقليم أجنبي[5]، "وهو ما جعل المشرع الجزائري إضافة الى المادة 588 من قانون إ. ج العمل بمبدأ العينية يضيف المادة 15 من القانون 09-04 والتي تنص على أن المحاكم الجزائرية وحدها تختص بالنظر في جرائم تكنولوجيا الإعلام والاتصال ولكن بشروط"[6] :

___أن يتعلق الأمر بجرائم تكنولوجيا الإعلام والاتصال.

_أن ترتكب الجريمة خارج الإقليم الوطني.

_ أن يكون مرتكب الجريمة أجنبيا.

_ أن يستهدف مؤسسات الدولة الجزائرية الدفاع الوطني المصالح الاستراتيجية للاقتصاد الوطني.

---

[1] دلال مولاي ملياني، المرجع السابق، ص 277.
[2] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص 84.
[3] نفس المرجع، ص85.
[4] مريم عراب، المرجع السابق، ص ص 278-279.
[5] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص85.
[6] المادة 15 من القانون 09-04 ،المرجع السابق.

- **مبدأ الشخصية :**

تقوم مبدأ شخصية القوانين على مد الولاية العقابية للدولة لتشمل رعاياها أينما وجدوا، وهو ما يضمن عدم إفلات المجرمين من العقاب بدعوى ارتكاب الفعل خارج الحدود. ويتفرع هذا المبدأ إلى صورتين؛ الأولى إيجابية، وتتمثل في خضوع المواطن الجزائري لقانون بلده عن الجرائم المعلوماتية التي يقترفها في الخارج، صوناً لسمعة الدولة ومنعاً لاتخاذ الأقاليم الأجنبية ملاذاً آمناً. والثانية سلبية، وتتجلى في بسط حماية القانون الوطني على الرعايا الجزائريين بصفتهم مجنياً عليهم، بحيث يختص القضاء الوطني بملاحقة أي جاني (مهما كانت غير اخلاقيته) اعتدي رقمياً على مواطن جزائري، ضماناً لحقوق المواطنين وحمايةً لهم من الجرائم العابرة للحدود[1].

1) التعاون الدولي في الجريمة الالكترونية:

نظراً للطبيعة العابرة للحدود التي تتسم بها الجريمة الإلكترونية، أضحت المواجهة الفردية من قِبل الدول قاصرة عن تحقيق الردع المطلوب. فالعقبة المكانية التي تواجه أجهزة الشرطة الوطنية عند اصطدامها بالحدود السيادية تحتم تفعيل آليات **'المساعدة القانونية المتبادلة '**والتحقيقات المشتركة. إن استئصال شأفة هذا الإجرام الرقمي يستوجب وجود كيان دولي جامع يعمل كمظلمة تنسيقية لتبادل المعلومات والبيانات الجنائية بمرونة وسرعة، بما يضمن تعقب الجناة في الفضاء الافتراضي وتجاوز العجز الإجرائي الذي تفرضه القيود الجغرافية التقليدية[2].

تعريف التعاون القضائي الدولي:

تعد المساعدة القضائية المتبادلة الأداة القانونية الأنسب لجمع الأدلة الجنائية في البيئة الافتراضية؛ حيث تتيح للدول التعاون في تنفيذ إجراءات التحقيق التي تتطلب ولوجاً إلى منظومات معلوماتية خارج إقليمها الوطني. ويشمل هذا التعاون الحصول على تسجيلات الاتصالات الإلكترونية، وفحص المعطيات المخزنة، وتبادل الخبرات الفنية بين الأجهزة الأمنية والقضائية. إن هذا التآزر الدولي يحول دون تشتت الدليل الرقمي، ويسمح للسلطات المختصة بالاستفادة من التسهيلات الإجرائية التي توفرها الاتفاقيات الثنائية والمتعددة الأطراف لمكافحة الإجرام المعلوماتي.[3]

ويعرف التعاون القضائي الدولي بأنه كل إجراء قضائي تقوم به دولة من شأنه تسهيل 3مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم.[4]

وعلى الرغم من أن الأصل في المساعدة القضائية الدولية هو سلوك القنوات الدبلوماسية التقليدية وفقاً للمادة 721 من قانون الإجراءات الجزائية، إلا أن المشرع الجزائري استجابةً لخصوصية الجريمة المعلوماتية أقر استثناءً جوهرياً يتيح التواصل عبر 'الوسائل السريعة'. ويأتي هذا التحول لمواكبة الطبيعة المتطايرة للأدلة الرقمية التي لا تحتمل بطء الإجراءات البيروقراطية، حيث أجاز المشرع تبادل طلبات التعاون عبر الفاكس والبريد الإلكتروني في حالات الاستعجال، شريطة الالتزام بضوابط معينة تضمن صحة الإجراء وتراعي مبادئ السيادة والمعاملة بالمثل[5].

[1] مريم عراب، المرجع السابق، ص 280.
[2] غانم مرضي الشمري، الجرائم المعلوماتية ماهيتها، خصائصها، كيفية التصدي لها قانونا، الدار العلمية الدولية للنشر والتوزيع، عمان، الاردن، 2016، ص 98.
[3] دلال مولاي ملياني، المرجع السابق، ص 270.
[4] غانم مرضي الشمري، المرجع السابق، ص 98.
[5] المادة 16 من القانون 09-04 ،المرجع السابق.

كما تتعدد صور التعاون قضائي في :[1]

- **تبادل المعلومات :**

يُعد تبادل المعلومات العصب الحيوي للتعاون القضائي الدولي في العصر الرقمي، حيث يتجاوز مجرد نقل البيانات التقليدية ليشمل تزويد السلطات بالوثائق، والمواد التقنية، والسوابق القضائية للجناة التي تُسهل من مأمورية المحاكمة[2]. وإن القناعة الراسخة بأن الجريمة المعلوماتية لا تُجابه إلا بتعاون دولي حقيقي، أدت إلى تعاظم دور منظمة الأنتربول في المشهد الجنائي الدولي. فمنذ إنشائها، أخذت المنظمة على عاتقها بناء جسور التواصل الفعال بين السلطات الشرطية في مختلف الدول، محولةً التعاون القضائي إلى واقع ملموس يتجلى في تبادل المعلومات والخبرات، وباعتبارها كياناً تنسيقياً جامعاً، تساهم الأنتربول في رفع كفاءة الملاحقة الجنائية الدولية، مما يضمن محاصرة الجريمة الإلكترونية في كافة مراحلها، من التحري والاستدلال وصولاً إلى تقديم الجناة للعدالة[3].

- **نقل الاجراءات :**

يمثل نقل الإجراءات تحولاً في قواعد الاختصاص التقليدية، حيث تباشر الدولة ملاحقة جنائية عن أفعال وقعت في إقليم دولة أخرى استناداً إلى اتفاقيات التعاون المتبادل. ويشترط لصحة هذا النقل أن يكون الفعل مجرماً قانوناً في كلتا الدولتين (التجريم المزدوج)، وأن تكون الإجراءات المطلوب اتخاذها مقررة ومعترفاً بها في قانون الدولة التي نُقلت إليها الملاحقة. وبموجب هذا المبدأ، تتحقق العدالة الجنائية من خلال تجاوز العقبات الجغرافية، مما يضمن استمرارية الملاحقة الجنائية للجاني أينما وجد، طالما أن فعله يصطدم بنصوص عقابية متطابقة في كلا النظامين القانونيين[4].

- **الانابة القضائية :**

تعد الإنابة القضائية الدولية وسيلة استثنائية يلجأ إليها القضاء عند اصطدامه بعائق مكاني يحول دون استكمال عناصر الدعوى الجنائية المعروضة أمامه. وتجد هذه الإنابة تبريرها في **'الضرورة الإجرائية'**؛ حيث تُطلب من الدولة الأجنبية مباشرة مهام قضائية محددة لفائدة الدولة الطالبة. ومن الناحية الفقهية، يذهب الاتجاه الغالب إلى أن تنفيذ طلبات الإنابة يستند أساساً إلى التعاون الاختياري واعتبارات المجاملة بين الدول، ما لم تكن هناك معاهدات ثنائية أو جماعية تنقل هذا الالتزام من حيز الاختيار إلى حيز الإلزام القانوني المتبادل[5]. والغاية الأسمى من الإنابة القضائية الدولية في ضمان انسيابية الإجراءات الجنائية عبر الأقاليم، بما يكفل استكمال التحقيقات وتقديم الجناة للعدالة. وتعمل هذه الآلية كجسر قانوني لتجاوز عقبة السيادة الإقليمية التي تمنع السلطات الوطنية من ممارسة أي صلاحيات قضائية خارج حدودها، كالتفتيش أو سماع الشهود. ومع ذلك، يظل التنسيق عبر القنوات الدبلوماسية يمثل تحدياً إجرائياً؛ نظراً لما يتسم به هذا المسار من بطء وروتين إداري قد يتعارض مع طبيعة الأدلة الجنائية، لاسيما المتطايرة منها في الجرائم الإلكترونية[6].

كما تجلى القصور التشريعي في الجزائر بشأن الإنابة القضائية الدولية في الاعتماد المفرط على اتفاقيات ثنائية وإقليمية قديمة (كاتفاقية 1964 مع مصر و1953 لجامعة الدول العربية)، والتي صِيغت قبل ظهور التحديات السيبرانية المعاصرة. ويكمن العيب الجوهري في هذه الآليات في تبنيها للمسلك الدبلوماسي الذي

[1] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص87.
[2] غانم مرضي الشمري، المرجع السابق، ص 99.
[3] محمد لموسخ، تنازع الاختصاص في الجرائم الإلكترونية، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 2 ،ديسمبر 2009 ،ص 153.
[4] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص88.
[5] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص 88.
[6] غانم مرضي الشمري، المرجع السابق، ص ص 99-100.

يتسم بالتعقيد البروتوكولي، وهو مسلك يتناقض جذرياً مع سرعة الإجرام المعلوماتي. فبينما تحرص الدول على استثناء الجرائم العسكرية والسياسية صوناً لنظامها العام، فإنها تغفل عن أن 'بطء الإجراءات الدبلوماسية' يخدم المجرم المعلوماتي؛ إذ يسمح له بمحو الآثار الرقمية وإخفاء بيانات الإدانة في وقت قياسي، مما يجعل من الإنابة القضائية التقليدية أداة غير مجدية في ملاحقة مبتزي الفضاء الافتراضي[1].

ثانيا :جهود المنظمة الدولية للشرطة الجنائية (الانتربول):

تعد المنظمة الدولية للشرطة الجنائية(الانتربول) التي كانت تُعرف سابقاً باللجنة الدولية للشرطة الجنائية الكيان الأمني الأضخم عالمياً، حيث تضم في عضويتها اليوم أكثر من 190 دولة. وتهدف المنظمة إلى مأسسة وتفعيل التعاون الشرطي العابر للحدود من خلال تبادل البيانات والمعلومات الجنائية الجوهرية عبر شبكة المكاتب المركزية الوطنية ، ولا يقتصر دورها على رصد وتحليل الأنماط الإجرامية، بل يمتد إلى توفير الدعم الميداني لضبط المجرمين الفارين، مما يجعلها منصة استخباراتية وأمنية لا غنى عنها في مواجهة الإجرام المعلوماتي المستحدث[2].و قد شهدت جهود منظمة الأنتربول تطوراً بنيوياً تمثل في تبني استراتيجية 'اللامركزية' عبر إنشاء مراكز اتصال إقليمية موزعة جغرافياً في (طوكيو، نيوزيلندا، نيروبي، أذربيجان، وبيونس أيرس)، فضلاً عن المكتب الفرعي في بانكوك، وذلك لضمان سرعة تدفق الرسائل الجنائية وتجاوز العوائق الزمنية والجغرافية. وبالتوازي مع هذا الجهد العالمي، برز الدور العربي من خلال 'المكتب العربي للشرطة الجنائية' التابع لمجلس وزراء الداخلية العرب، والذي أضحى ركيزة أساسية لتأمين التعاون الأمني بين الدول الأعضاء، وتطوير كفاءة الملاحقة القضائية للمجرمين، بما ينسجم مع الأنظمة القانونية الوطنية لكل دولة[3].

المطلب الثاني: الجزاءات المقررة لجريمة الابتزاز الالكتروني:

تعتبر العقوبة الأداة القانونية الأسمى التي يُفعل من خلالها المشرع نصوص التجريم، فلولا الجزاء لظلت القواعد الموضوعية مجرد توجيهات أخلاقية تفتقد للقوة الملزمة، وقد سعى المشرع من خلال رصد جزاء جنائي لكل سلوك مخالف سواء تمثل في فعل إيجابي أو امتناع إلى إرساء منظومة زجرية متكاملة توازن بين الردع الخاص المعني بتقويم الانحراف الإجرامي لدى الجاني، و الردع العام الهادف إلى تحصين المجتمع وحمايته. ومن منطلق هذه الوظيفة الحمائية ببعديها الوقائي والزجري، تبنى المشرع إستراتيجية 'تعدد الجزاءات لضمان تناسبها مع طبيعة الجرائم المستحدثة وجسامتها وهو ما أدى إلى ظهور هيكل عقابي مزدوج يجمع بين العقوبات الأصلية كجزاء جوهري، والعقوبات التكميلية كإجراءات متممة وضرورية لتحقيق العدالة الجنائية[4].

_الفرع الاول: العقوبات الاصلية و العقوبات التكميلية:

اولا العقوبات الاصلية :

" لقد حدد المشرع الجزائري في المواد 303 مكرر و303 مكرر 1 ،303 مكرر 2 .العقوبات الخاصة بهذه الجنحة وهي كالاتي[5]:

"ان المشرع الجزائري خصص موادا بهذا الصدد نشير إلى المادة 303 مكرر من قانون العقوبات إلى أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت، سواء للصور الشخصية أو المحادثات،

[1] محمد لموسخ، المرجع السابق، ص 155.
[2] بوديسة بجاد عبد الرؤوف، المرجع السابق، ص ص 89 90.
[3] غانم مرضي الشمري، المرجع السابق، ص 90.
[4] بن سليمان محمد طاهر [واخرون]، المرجع السابق، ص 38.
[5] المرجع نفسه.

سواء الارتكاب الفعلي أو الشروع فيه، بالعقوبات ذاتها المقررة للجريمة التامة، يرغم الضحية في الغالب الجاني للتخلي عن فكرة إفشاء مسائل تمسّ بسمعته."[1]

وعلاوة على ذلك، يتجلى الإطار القانوني المنظم للعقوبات المتعلقة بجنح التهديد بالابتزاز والتشهير العمدي، كدرع حامٍ للحياة الخاصة للأفراد من الأفعال الماسة بها والمكتملة الأركان. ففي جريمة الابتزاز، يمارس الجاني ضغطاً نفسياً وإكراهاً معنوياً يهدف من خلاله إلى إرغام الضحية على الانصياع لرغباته، خوفاً من تنفيذ الوعيد بإفشاء أمور شائنة أو أسرار قد تنال من سمعته واعتباره الاجتماعي، وهو ما يجعل من فعل التهديد في حد ذاته سلوكاً إجرامياً مستوجباً للعقاب بغض النظر عن تحقق النتيجة المرجوة منه[2].

ويتجسد القصد الجنائي في هذه الجريمة من خلال انصراف نية الجاني إلى توريط الضحية في وقائع ذات صبغة لا أخلاقية، أو التهديد بكشف أمور من شأنها المساس بشرفها واعتبارها أمام الرأي العام، وذلك بغرض تحقيق ربح مادي أو نفع معنوي غير مشروع. وقد أقر المشرع الجزائري تدرجاً عقابياً لفعل التهديد تماشياً مع وسيلة تنفيذه وجسامته؛ فبالرجوع إلى نص المادة 287 من قانون العقوبات، نجدها تعالج صور التهديد المصحوب بأمر أو شرط، حيث قررت عقوبة الحبس من ثلاثة أشهر إلى سنة، وغرامة مالية تتراوح بين 20.000 دج و100.000 دج إذا كان التهديد بالعنف أو القتل مكتوباً. أما إذا كان التهديد شفاهياً ومصحوباً بأمر أو شرط، فقد شدد المشرع العقوبة لتصل إلى الحبس من ستة أشهر إلى سنتين، مما يعكس رغبة المشرع في بسط حماية جزائية متكاملة ضد كل أشكال الضغط التي قد تمارس على إرادة الأفراد[3].

لم يكتفِ المشرع الجزائري بتجريم فعل الاعتداء الأولي على الخصوصية، بل مدّ الحماية الجزائية لتشمل مرحلة تداول المحتوى الرقمي المعتدى عليه؛ حيث نصت المادة 303مكرر 1 من قانون العقوبات على معاقبة كل من قام بنشر أو توزيع أو حتى مجرد الاحتفاظ بالصور أو التسجيلات التي تم الحصول عليها خفية. وتكتسي هذه المادة أهمية بالغة في ظل التحول الرقمي، كونها تجرم فعل "النشر الإلكتروني عبر منصات التواصل الاجتماعي، معتبرة أن إتاحة المحتوى الخاص للجمهور أو وضعه في متناول الغير يشكل جريمة قائمة بذاتها، تهدف إلى تشديد الحصار القانوني على المبتز ومنع استغلاله للمواد الرقمية في تهديد ضحاياه أو النيل من اعتبارهم الاجتماعي[4].

ثانيا العقوبات التكميلية :

تتميز العقوبة التكميلية عن العقوبة التبعية في طريقة تقريرها؛ فالأولى (التكميلية) لا تقع تلقائياً بل يشترط لتطبيقها أن ينص عليها القاضي صراحة في منطوق حكمه إلى جانب العقوبة الأصلية. في المقابل، تُطبق العقوبة الثانية (التبعية) بقوة القانون وبشكل آلي بمجرد صدور الحكم بالعقوبة الأصلية، نظراً لارتباطها العضوي والوثيق بها، دون حاجة لذكرها في حكم مستقل أو الإشارة إليها في منطوق الحكم[5].

وتطبيقاً للقواعد العامة في العقوبات التكميلية، أورد المشرع في المادة الثالثة عشرة من نظام مكافحة جرائم المعلوماتية جملة من التدابير الجوازية التي يملك القاضي سلطة تقديرها؛ حيث أجاز النظام للمحكمة الحكم بمصادرة كافة الأجهزة، البرمجيات، والوسائل المستخدمة في تنفيذ الجريمة، فضلاً عن مصادرة الأموال

---

[1] **الابتزاز والتشهير الإلكتروني وعقوبته في القانون الجزائري،متاحعلى الموقع العالم الجزائري، رابط (elidara.dz/?p=46150)https://www.elalem-، بتاريخ 14ماي 2026، بتوقيت 16:15.**

[2] نفس المرجع.

[3] نفس المرجع .

[4] المادة 303 مكرر 1 من الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم، لاسيما بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، الصادرة بتاريخ 24 ديسمبر 2006

[5] بن سليمان محمد طاهر [واخرون]، المرجع السابق، ص 39.

المتحصلة منها. كما امتدت هذه العقوبات لتشمل إغلاق الموقع الإلكتروني أو محل تقديم الخدمة بصفة مؤقتة أو نهائية شريطة أن يكون مكاناً لتسهيل ارتكاب الجريمة وثبوت علم مالكه بذلك[1].

وتُعرف المصادرة بأنها نقل ملكية المال أو الأشياء المحكوم بها إلى الدولة نهائياً وبلا مقابل، وتختلف المصادرة جوهرياً عن الغرامة، إذ إن الغرامة عقوبة مالية نقدية تقع كعقوبة أصلية وتستهدف ذمة الجاني المالية، في حين أن المصادرة عقوبة عينية تكميلية تنصبّ على أشياء عينية محددة. وتتميز المصادرة في الأصل بأنها ترد على أشياء حيازتها مشروعة في حد ذاتها، إلا أن مبرر نزع ملكيتها وإصابتها بهذا الجزاء يكمن في وجود صلة وثيقة ومباشرة تربطها بالجريمة، كأن تكون قد استُخدمت في ارتكابها أو نتجت عنها[2].

"هذه الصلة قد حددتها المادة 13 نظام مكافحة الجرائم المعلوماتية السعودي بقولها الاجهزة والبرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام."[3]

وبناءً عليه، يمتنع على القاضي نظاماً الحكم بمصادرة أي أشياء لا يثبت اتصالها بجريمة الابتزاز الإلكتروني كوسيلة أو كعائد كما لا ينعقد اختصاصه بالقضاء بها ما لم تكن تلك الأشياء قد خضعت للضبط الفعلي وتم التحفظ عليها أثناء مسار الدعوى؛ إذ إن غياب الضبط المادي للأدلة وقت النطق بالحكم يحول دون إمكانية مصادرتها[4].

تستهدف المصادرة الجوازية أعياناً حيازتها مشروعة في حد ذاتها، لكنها اكتسبت وصفاً غير مشروع نتيجة الدور الوظيفي الذي لعبته في خدمة الجريمة؛ وتطبيقاً لذلك في جريمة الابتزاز الرقمي، فإن الأجهزة والبرمجيات المستخدمة وإن كانت في أصلها وسائل تقنية مباحة التداول تخضع للمصادرة نظراً لتوظيفها في نشاط إجرامي قوامه التهديد وسلب الأموال[5].

"وللقاضي سلطة تقديرية في توقيع المصادرة من عدمه شريطة أن ترتبط بالعقوبة الاصلية على المبتز وهي الحبس، أو الغرامة أو إحداهما"[6].

"واذا لم تكن الاشياء تم استخدامها في الجريمة ليست ملكا للجاني فالا يحكم القاضي بمصادرتها وذلك كما 1نصت عليه م 13 بقولها مع عدم الاخلال بحقوق الغير حسن النية.... "[7]

"اما في التشريع الجزائري فالحكم بالمصادرة وجوبي حسب المادة 303 مكرر وذلك في ما يخص الاشياء المستعملة في ارتكاب الجريمة كما أن المادة 303 مكرر 2 أحالت الى المادة 9 مكرر 1".[8]

تفعيلاً للجزاءات التكميلية الجوازية في التشريع الجزائري، تتيح المادة (18) من قانون العقوبات للمحكمة عند قضائها بالإدانة في الجرائم المعلوماتية الماسة بالحياة الخاصة (المادتين 303 مكرر و303 مكرر 1) أن تأمر بحرمان الجاني من ممارسة بعض الحقوق الواردة في المادة (9 مكرر 1) لمدة لا تفوق خمس سنوات.

---

[1] المرجع نفسه.
[2] سليمان محمد طاهر [واخرون]، المرجع السابق، ص39.
[3] المرجع نفسه,
[4] سليمان محمد طاهر [واخرون]، المرجع السابق، ص39.
[5] المرجع نفسه.
[6] محمد بن عبد المحسن بن شلهوب، جريمة الابتزاز الالكتروني دراسة مقارنة، بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الانظمة، جامعة الامام محمد بن سعود الإسلامية، 2011.
[7] المادة 13، نظام مكافحة الجرائم المعلوماتية.
[8] المادة 9 مكرر 1 ق ع ج " يتمثل الحرمان من ممارسة الحقوق الوطنية و المدنية و العائلية في :العزل أو الاقصاء من جميع الوظائف والمناصب العمومية التي لها عالقة بالجريم، الحرمان من حق الانتخاب أو الترشح أو حمل أي وسام، عدم الاهلية لان يكون مساعدا محلفا او خبيرا أو شاهدا على اي عقد او شاهدا أما القضاء الاعلى سبيل الاستدلال، الحرمان من الحق في حمل الاسلحة و في التدريس و في إدارة مدرسة أو الخدمة في مؤسسة التعليم بوصفه أستاذا أو مدرسا أو مراقب، عدم الاهلية ليكون وصيا أو فيما.

كما يجوز للمحكمة إيقاع عقوبة تشهيرية تتمثل في نشر حكم الإدانة أو مستخرج منه في الصحف، أو تعليقه في الأماكن العامة لمدة لا تزيد عن شهر، ويكون ذلك على نفقة المحكوم عليه وتحت سقف المصاريف التي يحددها الحكم ذاته[1].

الفرع الثاني: الظروف المشددة للعقاب و المعفية للعقاب الجريمة الابتزاز الالكتروني:

اولا: الظروف المشددة للعقاب لجريمة الابتزاز الالكتروني:

ستدعي الخطورة الإجرامية لبعض صور الابتزاز الرقمي تفعيل القواعد الخاصة بالتشديد العقابي متى استوفت الجريمة شروطها النظامية. والمقصود بهذا التشديد إجرائياً هو دفع المنظومة القضائية نحو تبني الخيار العقابي الأقسى؛ ويتمثل ذلك إما في ارتقاء القاضي بالعقوبة الجنائية لتلامس سقف حدها الأقصى المقر قانوناً، أو في تخليه عن مكنة التخيير بين العقوبات والجمع بدلاً من ذلك بين العقوبتين البدنية والمالية (الحبس والغرامة) معاً بحق الجاني[2].

ان علة التشديد التي استحدثها المشرع لمواجهة الابتزاز الإلكتروني تدور وجوداً وعدماً مع تزايد الخطورة الكامنة في الجريمة. فصورة الجريمة المنظمة تعكس استفحالاً تقنياً يعجز الفرد الأعزل عن مواجهته، وصورة 'الموظف العمومي تخدش ثقة المجتمع في مؤسسات الدولة وتكشف عن انحراف وظيفي خطير، في حين يمثل التغرير بالقصر انتهاكاً لالتزام الدولة الدستوري بحماية الطفولة، وأخيراً فإن الاعتداد بالأحكام السابقة الصادرة وطنياُ أو دولياً يجد تبريره الفقهي في فلسفة 'العود الجنائي، حيث يصبح التشديد هنا أداة ضرورية لتحجيم خطورة إجرامية كامنة لدى جانٍ اعتاد اتخاذ الفضاء الافتراضي ساحة لتهديد حريات الآخرين وأموالهم[3].

أما المادة 42 تنص على انه: تقضي المحكمة بإبعاد ألجنبي الذي حكم عليه بالادانة لارتكاب أي جريمة من الجرائم المنصوصة عليها في هذا المرسوم بقانون وذلك بعد تنفيذ العقوبة المحكوم بها فيتم إبعاد الاجنبي بعد تنفيذه العقوبة الاصلية[4]

ثانيا: الظروف المعفية من العقاب لجريمة الابتزاز عبر وسائل الالكترونية:

"إن الاعفاء من العقوبة ليس له علاقة بالسياسة الجنائية أو علاقة بالقواعد العامة للمسؤولية الجزائية المرتكب الجريمة"[5].

1. عقوبة الشروع في الجريمة الالكترونية :

يُقصد بالشروع باعتباره مرحلة من مراحل السلوك الإجرامي البدء في تنفيذ مادي لجريمة عقد الجاني العزم على اقترافها، غير أن أثرها يتوقف أو يخيب لسبب أجنبي لا دخل لإرادته فيه، لتظل بذلك جريمة ناقصة لعدم اكتمال نتيجتها الإجرامية المستهدفة، وتطبيقاً للسياسة العقابية في التشريع الجزائري وعلى الرغم من أن الأصل العام يقضي بعدم العقاب على الشروع في الجنح إلا بنص صريح، فقد خرج المشرع عن هذا الأصل في المادة (303 مكرر) من قانون العقوبات، حيث قرر صراحة معاقبة الجاني على الشروع في الجنح الماسة بحرمة الحياة الخاصة بذات العقوبة المقررة للجريمة التامة، نظراً لخطورة السلوك ولو لم تتحقق النتيجة[6].

---

[1] المادة 18 من قانون العقوبات الجزائري.
[2] سليمان محمد طاهر[واخرون]، المرجع السابق، ص41
[3] المرجع نفسه.
[4] امال برحال، المرجع السابق.
[5] سليمان محمد طاهر، المرجع السابق ، ص42.
[6] سليمان محمد طاهر، المرجع السابق ، ص42..

بناءً عليه، يتبلور الشروع في الابتزاز الرقمي بمجرد إطلاق التهديد بنشر الأسرار أو البيانات الخاصة، وهي اللحظة التي يتحقق فيها الأثر النفسي المستهدف بإلقاء الرعب في نفس المجني عليه. ولا ينفي الشروع تراجع الجاني اللاحق إذا كان مدفوعاً بعامل خارجي (كخوفه من الملاحقة الأمنية أو افتضاح أمره)، إذ العبرة بوقوع فعل التهديد تحت تأثير الركن المعنوي (القصد الجنائي). وعليه، فإن الجريمة تظل قائمة بوصف الشروع المتكامل الأركان، طالما استجمع السلوك بدؤه التنفيذي المادي والمنع المعنوي، دون عبرة بعدم اكتمال النتيجة العينية للجريمة[1].

ثانيا: عقوبة الاشتراك في جريمة الابتزاز عبر الوسائل الالكترونية :

تحقق الاشتراك في الجريمة باعتباره مظهراً من مظاهر المساهمة الجنائية التبعية عبر اتخاذ الشريك سلوكاً إيجابياً يتمثل في الاتفاق مع الفاعل الأصلي، أو تقديم العون والمساعدة للمبتز بأي وسيلة كانت تسهل له بلوغ النتيجة الإجرامية المستهدفة. وتطبيقاً لذلك في بيئة التحول الرقمي، بسط نظام مكافحة جرائم المعلوماتية مظلة التجريم لتشمل كافة صور الاشتراك في جريمة الابتزاز متى نُفذت باستخدام الوسائط والوسائل التقنية؛ حيث أقر النظام قواعد مسؤوليّة متكافئة تقضي بمعاقبة الشريك بالتسبب بذات العقوبة المقررة للفاعل الأصلي، نظراً لخطورة الدور التبعي في تيسير الجرائم السيبيرانية[2].

ان إحالة المشرع الجزائري أحكام الاشتراك في جريمة الابتزاز الإلكتروني إلى القواعد العامة في المساهمة الجنائية (المواد 41، 42، 44، 45 من قانون العقوبات) تعكس كفاية النظرية العامة للجريمة في استيعاب المستجدات التكنولوجية. فالشريك الرقمي الذي لا يرتكب الركن المادي للجريمة بنفسه، بل يكتفي بتقديم الدعم المعنوي أو المادي (وفق المادتين 41 و42)، يظل خاضعاً لسلطة العقاب استناداً إلى مبدأ استعارة التجريم والعقاب المقررة في المادتين (44) و(45)؛ وبذلك، فإن العقاب على الجريمة التامة أو الشروع فيها يمتد بقوة القانون وبذات المقدار ليشمل كل من مهّد السبيل للمبتز أو ساعده على ولوج البيانات الشخصية للضحية.

[1] عبد الرحمن توفيق أحمد، شرح قانون العقوبات، القسم العام وفق أحدث التعديلات، طبعة 3، دار الثقافة والنشر والتوزيع، عمان، 2012، ص150.

[2] سليمان محمد طاهر، المرجع السابق، ص 42

الخاتمة

تعدّ جريمة الابتزاز الإلكتروني أحد أبرز تجليات الجرائم السيبرانية المستحدثة التي تخرج عن النمط التقليدي للجريمة. ويُصطلح عليها في الفقه الجنائي بـ "الجرائم الناعمة" لكونها تُقترف دون استخدام العنف المادي؛ إذ تنشأ وتتطور في بيئة افتراضية قوامها الرموز والشيفرات الرقمية. ويتعاظم التحدي القانوني والأمني أمام جهات التحقيق بسبب العقبات المعقدة التي تكتنف التعامل مع الدليل الرقمي وجمعه وتحريزه . ومع التسارع الهائل في منظومة التكنولوجيا الرقمية، تحول الاعتماد عليها إلى شغفٍ ومحرك أساسي للمجتمعات الحديثة. وأمام هذه الثورة التقنية، سعت الدول جاهدة إلى تحديث ترسانتها القانونية لمواكبة هذه الأنماط الإجرامية المستجدة، موفرةً نصوصاً وتشريعات خاصة تعاقب على الابتزاز الإلكتروني وتحدّ من مخاطره.

في ختام هذه الدراسة الموسومة بـ "جريمة الابتزاز في ظل التحول الرقمي"، والتي تتبعنا من خلالها الأبعاد الموضوعية والإجرائية والواقعية لهذه الظاهرة الخطيرة، نخلص إلى جملة من النتائج والتوصيات الاستراتيجية التي توجز ما تم التوصل إليه:

أولاً: النتائج

1. **مرونة النص الجنائي الجزائري :**أثبتت الدراسة أن المشرع الجزائري لم يفرد نصاً خاصاً مستقلاً بمسمى "الابتزاز الإلكتروني"، بل زاوج بذكاء بين القواعد العامة لجريمة التهديد المصحوب بأمر (المادة 371 ق.ع) والجرائم التقنية للمساس بأنظمة المعالجة الآلية للمعطيات (المواد 394 مكرر وما بعدها)، مما يمنع إفلات الجناة من العقاب.
2. **خصوصية الدليل الرقمي :**يعد الدليل الإلكتروني حجر الزاوية في إثبات الجريمة، وتتميز حجيته بالخضوع لسلطة القاضي التقديرية ومبدأ الاقتناع القضائي (المادة 212 إ.ج)، إلا أن قبوليتها تظل مشروطة بالمشروعية الإجرائية أثناء الضبط وحصانتها التقنية ضد التعديل أو الحذف.
3. **تطور الأنماط الإجرامية :**أدى التحول الرقمي إلى ديمقراطية الإجرام؛ حيث لم يعد الابتزاز حكراً على المحترفين (الهاكرز والكراكرز)، بل امتد إلى "المبتز الهاوي" الذي يستغل روابط الاصطياد البسيطة والهندسة الاجتماعية للإيقاع بالضحايا (خاصة النساء والأطفال في الألعاب الإلكترونية وتطبيقات بريدي موب).
4. **الاستثناءات الإجرائية :**منح المشرع الجزائري الضبطية القضائية صلاحيات استثنائية (كالمراقبة الإلكترونية واختراق السرية الرقمية والتحري عن بعد) بالنظر لسرعة محو الأدلة الرقمية وسيولتها في الفضاء الافتراضي.

ثانياً: التوصيات

1. استحداث نص خاص وهذا بإفراد نص قانوني جامع وعقابي خاص بـ "الجريمة المعلوماتية للابتزاز الإلكتروني" يحدد صورها الرقمية بدقة لتفادي القياس أو التوسع في التفسير.
2. تطوير التخصص القضائي بتكثيف الدورات التدريبية المتقدمة لرجال الضبطية القضائية والقضاة في مجالات "التحقيق الجنائي الرقمي (Digital Forensics) "لمجاراة الذكاء الاصطناعي والأساليب المستحدثة للتشفير.
3. تعزيز الوعي الرقمي بإطلاق حملات توعية وطنية مستمرة بالتنسيق بين المؤسسات الأمنية والتربوية لحماية الفئات الهشة (الأحداث والمراهقين)، وتفعيل السياسات التحذيرية للمؤسسات النقدية (مثل بريد الجزائر).
4. تفعيل الاتفاقيات الدولية لتعزيز التعاون القضائي الدولي، والانضمام إلى الاتفاقيات المتعلقة بمكافحة الجرائم الإلكترونية لضمان الملاحقة القضائية عبر الحدود

قائمة المصادر والمراجع

القرآن الكريم: سورة يوسف، الآية 32.

أولاً: المصادر الرسمية والنصوص القانونية

1. النصوص التشريعية (الأوامر والقوانين):

- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون الإجراءات الجزائية الجزائري، المعدل والمتمم (آخرها تعديل 14/25المؤرخ في 3اوت سنة 2025)، طبعة حمينة، دار بلقيس للنشر، الدار البيضاء، الجزائر، سنة 2020.
- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم (بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتعلق بالمساس بحرمة الحياة الخاصة، والقانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016)، دار بلقيس للنشر، الجزائر، سنة 2019.
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 25 شعبان عام 1430 الموافق 16 غشت سنة 2009.
- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34.
- ثانياً: المراجع الفقهية (الكتب باللغة العربية)

أ) الكتب المتخصصة (في الجريمة الإلكترونية، الابتزاز، والأدلة الرقمية):

- باطلي غنية، الجريمة الإلكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، ط1، الجزائر، 2016.
- بوحليط يزيد، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، د.ط، دار الجامعة الجديدة، الإسكندرية، 2019.
- جواد عائشة بن قارة، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، بدون طبعة، دار الجامعة الجديدة، الإسكندرية، سنة 2010.
- الحلبي خالد عياد، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، دبي، 2011.
- الخوري عمر، الحماية الجنائية للحياة الخاصة في ظل تكنولوجيا المعلومات والاتصال، دار الجامعة الجديدة، الإسكندرية، 2014.
- ذيب عبد الله محمود، ودراج أسامة إسماعيل، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة 2022.
- الشمراني غانم مرضي، الجرائم المعلوماتية ماهيتها، خصائصها، كيفية التصدي لها قانوناً، الدار العلمية الدولية للنشر والتوزيع، عمان، الأردن، 2016.
- صالح الدين مروة محمد، الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية، القاهرة، مصر، سنة 2021.
- عثمان ضياء مصطفى، السرقة الإلكترونية، دراسة فقهية، ط1، دار النفائس للنشر والتوزيع، 2011.
- عزت فتحي ،محمد أنور، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية للمجتمع المعلوماتي، بدون طبعة، دار النهضة العربية، القاهرة، 2010.

- العتيبي خالد، مرزوق سراج، الجوانب في الشروع في الجريمة السيبرانية، مكتبة القانون والاقتصاد، المملكة العربية السعودية، 2014.
- عمربن يونس، الدليل الرقمي، بدون دار نشر، الطبعة 1، مصر، 2008.

ب) الكتب العامة (القانون العام، العقوبات، والضبطية القضائية):

- أحمد عبد الرحمن توفيق، شرح قانون العقوبات، القسم العام وفق أحدث التعديلات، ط3، دار الثقافة والنشر والتوزيع، عمان، 2012.
- الحسون صالح عبد الزهرة، أحكام التفتيش وآثاره في القانون العراقي، دراسة مقارنة، الطبعة 1، بدون دار نشر، جامعة بغداد، 1989.
- العكالية عبد الله ماجد، الاختصاصات القانونية لمأمور الضبط القضائي في الأحوال العادية والاستثنائية، ط1، دار الثقافة، الأردن، 2010.
- قريشي حمزة، الوسائل الحديثة للبحث والتحري في ضوء القانون الجزائري، دراسة مقارنة، ط1، منشورات السائحي، الجزائر، 2017.

ثالثاً: المذكرات والرسائل العلمية

أ) أطروحات الدكتوراه:

- البشري محمد الأمين، التحقيق في الجرائم المستحدثة، أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة 1، 2002.
- بوحليط يزيد، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة دكتوراه، قسم القانون الخاص، كلية الحقوق، جامعة باجي مختار، عنابة، 2016.
- بن طالب ليندا، الدليل الإلكتروني ودوره في الإثبات الجنائي دراسة مقارنة، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، سنة 2019.
- حبيب سوزان نوري عمي محمد، الإثبات في مجال الإنترنت في القانون العراقي المقارن، رسالة دكتوراه في الحقوق، كلية الحقوق، جامعة المنصورة، مصر، 2015.
- مولاي ملياني دلال، إشكالية الإثبات في جرائم الإنترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2018/2017.

ب) رسائل الماجستير:

- أبو علي محمد علي أحمد، جريمة الابتزاز الإلكتروني في التشريع الفلسطيني، مذكرة استكمال متطلبات درجة الماجستير في تخصص العلوم الجنائية، كلية الدراسات العليا، الجامعة العربية الأمريكية، 2022.
- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة باتنة، 2013
- صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية"، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013 .

- شلهوب محمد بن عبد المحسن بن، جريمة الابتزاز الإلكتروني دراسة مقارنة، بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، قسم السياسة الشرعية، المعهد العالي للقضاء، جامعة الإمام محمد بن سعود الإسلامية، 2011.
- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة لخضر باتنة، 2011_2012.

جـ) مذكرات الماستر:

- امال برحال، جريمة الابتزاز عبر الوسائط الإلكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة.
- بوشعير الحسن، حداد شعيب، جريمة الابتزاز الإلكتروني دراسة مقارنة، مذكرة ماستر، تخصص قانون الإعلام الآلي والإنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2023 .
- بن عنطر سيهام، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر في القانون، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، سنة 2023.
- بنوخ حبيب، تحريك الدعوى العمومية، مذكرة ماستر، تخصص علم الإجرام والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، سنة 2019.
- بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة ماستر مهني، تخصص قانون الإعلام الآلي والإنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، السنة 2022.
- حداد شيماء، جبلي سعيدة، جريمة الابتزاز عبر الوسائل الإلكترونية في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، معهد الحقوق، جامعة عبد الحفيظ بوالصوف ميلة.
- دحية عبد اللطيف وآخرون، المواجهة الإجرائية لجرم المعلوماتية، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2019
- كروم فؤاد، إجراءات المعاينة التقنية لمسرح الجريمة، مذكرة ماستر في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، 2018.

رابعاً: المقالات والمجلات العلمية

- بمعابد عيدة، "الدليل الرقمي بين حتمية الإثبات الجنائي والحق في الخصوصية المعلوماتية"، مجلة آفاق علمية، المجلد 11، العدد 01، السنة 2019.
- بن فريحة رشيد، ميهوب يوسف، "التحري الجنائي في مسرح الجريمة الإلكترونية"، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد 42، 2017.
- بن عمر ياسين، "الابتزاز الإلكتروني للأطفال في التشريع الجزائري"، مجلة دفاتر السياسة والقانون، الجزائر، المجلد 16، العدد 02، جوان.
- بن ميسرة محمد الأمين، "الحماية الجنائية للطفل من الجرائم المعلوماتية في التشريع الجزائري"، مجلة البحوث والدراسات القانونية والسياسية، العدد 12، جامعة البليدة 2.

- ديب أكرم، بن عبد الله نورة، "دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني"، مجلة الحقوق والعلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، المجلد 16، العدد 01، سنة 2023.
- الزيوش سعيد، "ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها - قراءة سوسيولوجية وآراء نظرية -"، مجلة العلوم الاجتماعية، العدد 22، جانفي 2017.
- سليمان بن عبد الرزاق الغديان [وآخرون...]، "صور جرائم الابتزاز الإلكتروني ودوافعها وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين"، مجلة البحوث الأمنية، دار المنظومة، مجلد 27، العدد 69، يناير 2018.
- عراب مريم، "جريمة التهديد والابتزاز الإلكتروني"، مجلة الدراسات القانونية، الجزائر، المجلد 07، العدد 01، جوان 2021.
- العرفي فاطمة، "حجية الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري"، مجلة صوت القانون، المجلد 08، عدد خاص 2022.
- عثماني عز الدين، "إجراءات التفتيش والتحقيق في الجرائم الماسة بأنظمة الاتصال المعلوماتية"، مجلة دائرة البحوث والدراسات القانونية السياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة، العدد 04، جانفي 2018.
- عمي محمد بصائر، حسن مروى عبد الواحد، "الدليل الإلكتروني في مجال الإثبات الجنائي"، مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، العدد 27، سنة 2017.
- عز الدين ريطاب، نبيلة صدراتي، "الطبيعة القانونية لفعل التشهير الإلكتروني عبر أدوات الذكاء الاصطناعي"، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 09، العدد 01.
- كاهنة آيت حمودة، "آليات البحث والتحري الجنائي في مسرح الجريمة الإلكترونية"، مجلة الفكر القانوني السياسي، جامعة حسيبة بن بوعلي الشلف، المجلد السابع، العدد الأول، سنة 2023.
- لموسخ محمد، "تنازع الاختصاص في الجرائم الإلكترونية"، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، الجزائر، العدد 02، ديسمبر 2009.
- موسى عماد جواد، "التحقيق والصعوبات التي تواجه جريمة الابتزاز الإلكتروني"، مجلة كلية المعارف الجامعة، كلية التربية للعلوم الإنسانية، جامعة الأنبار، الرمادي، العراق.

خامساً: المؤتمرات العلمية والأيام الدراسية

أ) المؤتمرات والملتقيات العلمية:

- فرغلي عبد الناصر محمد محمود، والمسماري عبيد سيف، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، ورقة بحثية مقدمة لـ المؤتمر العربي الأول لعموم الأدلة الجنائية والطب الشرعي، المنعقد بالرياض، 12/ 14 نوفمبر 2008.

ب) الأيام الدراسية والندوات:

- اليوم الدراسي حول الجريمة السيبرانية المعنون بـ: (إجراءات التحقيق الخاصة بالجرائم السيبرانية)، بمشاركة بومحراث لينداء، المنعقد يوم 20 أفريل 2022، بجامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة.

سادساً: تقارير المنظمات والمواقع الإلكترونية الرسمية

- الإنتربول (منظمة الشرطة الجنائية الدولية): عملية (Strikeback)وتقرير "عملية ينسقها الإنتربول تستهدف شبكات الابتزاز الغير اخلاقي"، مقال منشور بتاريخ 02 ماي 2014، متاح على الموقع

الرسمي للإنتربول: www.interpol.int، (تاريخ الاطلاع: 07 ماي 2026 على الساعة 12:57 زوالاً).

- الإنتربول(Interpol) تقرير الإنتربول عن تقييم التهديدات السيبرية في أفريقيا، الإصدار الثالث، متاح على الرابط الإلكتروني الرسمي للمنظمة، (تاريخ زيارة الموقع: 11 ماي 2026 على الساعة 19:56 مساءً).
- بوقعدة، توفيق: "الجزائر: عصابات تستغل وسائل التواصل الاجتماعي للابتزاز"، مقال منشور بموقع (DW عربية)، بتاريخ 17 أبريل 2016، متاح على الرابط: https://www.dw.com/ar/a-19177395، (تاريخ الاطلاع: 06 ماي 2026، الساعة 21:28 ليلاً).
- مؤسسة بريد الجزائر والأمن الوطني: البيانات التحذيرية الصادرة عن مؤسسة بريد الجزائر عبر صفحاتها الرسمية حول حملات الاحتيال والابتزاز الإلكتروني بالتنسيق مع "خلية مكافحة الجريمة المعلوماتية"، منشور في (فيفري/مارس 2026).
- موقع الويب العالمي الجزائري (منصة إدارية قانونية): مقال حول "الابتزاز والتشهير الإلكتروني وعقوبته في القانون الجزائري"، متاح على الرابط الهيئاتي الإداري الرسمي للموقع، منشور بتاريخ 14 ماي 2026، (تاريخ الاطلاع والتوقيت: 14 ماي 2026 في حدود الساعة 16:15 زوالاً).
- مبادرة (No More Ransomلا لمزيد من الفدية): تقرير بالتعاون مع اليوروبول ((Europol، "برمجيات الفدية: التهديد المتزايد للمؤسسات"، متاح على الموقع الرسمي للمبادرة، الرابط: https://www.nomoreransom.org، (تاريخ الاطلاع: 09 ماي 2026، الساعة 11:35 صباحاً).
- شركة فورتينت (Fortinet)للأمن السيبراني: "دليل المفاهيم السيبرانية: ما هو الابتزاز الإلكتروني وأنواعه الشائعة؟"، وتقرير "مشهد التهديد العالمي 2026"، متاح على الموقع الرسمي للشركة، (تاريخ الاطلاع: 09 ماي 2026 و22 ماي 2026 على الساعة 21:17 ليلاً).
- مدونة A10 لأمن الشبكات: مقال إحصائي حول "أشهر هجمات حجب الخدمة الموزعة (DDoS)في التاريخ"، تاريخ النشر: 12 ماي 2026، الرابط الإلكتروني للمدونة، (تاريخ زيارة الموقع: 22 ماي 2026، الساعة 22:10 ليلاً).
- مؤسسة IBM للحلول الرقمية: التقرير الدولي حول الهجمات الموزعة لحجب الخدمة (DDoS)، "الآليات التقنية لحجب الخدمة: دليل مفاهيم الأمن السيبراني"، منشور في 2025/2024، متاح على الرابط الإلكتروني للمؤسسة، (تاريخ الاطلاع: 22 ماي 2026، الساعة 21:13 ليلاً).
- منصة AXSOS الرقمية: "كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية: كيف تحمي شركتك من رسائل البريد الإلكتروني الاحتيالية"، مقال منشور عبر الرابط الإلكتروني الرسمي للمنصة، (تاريخ الدخول للموقع: 24 ماي 2026 على الساعة 21:54 ليلاً).

الفهرس

الملخص

تناولت هذه الدراسة "جريمة الابتزاز في ظل التحول الرقمي" باعتبارها واحدة من أبرز الجرائم السيبرانية المستحدثة التي أفرزتها الثورة التكنولوجية المعاصرة. تهدف الدراسة إلى تبيان الإطار المفاهيمي والأركان القانونية (الشرعية، المادية، والمعنوية) لهذه الجريمة في التشريع الجزائري، مع التركيز على القواعد الإجرائية المنظمة لعمليات البحث والتحري الرقمي، وحجية الدليل الإلكتروني ومدى خضوعه للسلطة التقديرية للقاضي الجزائي. كما سلّطت الدراسة الضوء على الانعكاسات الواقعية للتحول الرقمي من خلال رصد الأنماط المستحدثة للجناة (الهاوي، المحترف، والمنظمات) والضحايا (الأفراد، النساء، والأطفال)، مع تقديم نماذج واقعية كابتزاز القصر عبر الألعاب الإلكترونية واصطياد مستخدمي تطبيق "بريدي موب". وقد خلصت الدراسة إلى كفاية النصوص العامة حالياً مع ضرورة إفراد نص خاص وتطوير الكفاءات التقنية لجهات التحقيق لمجابهة الطبيعة السائلة والعابرة للحدود لهذه الجريمة .**كلمات مفتاحية :**ابتزاز إلكتروني، تحول رقمي، دليل رقمي، ضبطية قضائي.

Résumé : Cette étude examine le « crime de chantage à l'ère de la transformation numérique » comme l'un des crimes cybernétiques les plus proéminents générés par la révolution technologique contemporaine. L'objectif est de clarifier le cadre conceptuel et les éléments légaux (légal, matériel et moral) de ce crime dans la législation algérienne, en mettant l'accent sur les règles de procédure régissant les opérations de recherche et d'enquête numérique, ainsi que sur l'admissibilité de la preuve électronique et son assujettissement au pouvoir discrétionnaire du juge pénal. L'étude met également en lumière les répercussions réelles de la transformation numérique en surveillant les nouveaux profils de criminels (amateurs, professionnels et organisations) et de victimes (individus, femmes et enfants), tout en présentant des cas réels tels que le chantage des mineurs via les jeux électroniques et le piratage des utilisateurs de l'application "BaridiMob". L'étude conclut que les textes généraux actuels sont suffisants, tout en soulignant la nécessité d'introduire un texte spécial et de développer les compétences techniques des autorités d'enquête pour faire face à la nature fluide et transfrontalière de ce crime. **Mots-clés:** Cyber-extorsion, Transformation digitale, Preuve numérique, Police judiciaire.

Abstract: This study addresses the "Crime of Blackmail in Light of Digital Transformation" as one of the most prominent modern cybercrimes generated by the contemporary technological revolution. The study aims to clarify the conceptual framework and legal elements (legal, material, and moral) of this crime under Algerian legislation, focusing on the procedural rules governing digital search and investigation operations, as well as the admissibility of electronic evidence and its subjection to the discretionary power of the criminal judge. The study also highlights the real-world repercussions of digital transformation by identifying new types of perpetrators (amateurs, professionals, and organized groups) and victims (individuals, women, and children), presenting practical examples such as the exploitation of minors through online games and the phishing of "BaridiMob" application users. The study concludes that while current general legal texts are temporarily sufficient, there is an urgent need for a specialized law and the enhancement of the technical capabilities of investigative authorities to confront the fluid and transboundary nature of this crime **Keywords:** Cyber-extortion, Digital transformation, Digital evidence, Judicial police.