وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس – مستغانم

كلية الحقوق و العلوم السياسية

قسم القانون العام .

المرجع : .....

مذكرة التخرج لنيل شهادة الماستر في الحقوق.

المسؤولية الجنائية عن جريمة الإبتزاز الالكتروني وفق التشريع الجزائري .

-الشعبة : حقوق.

-التخصص :قانون جنائي و علوم جنائية.

-من إعداد الطالب (ة) :

غزالي نور الهدى .

- تحت اشراف الاستاذ (ة) :

وافي الحاجة .

اعضاء لجنة المناقشة :

-الأستاذ(ة).....بن قطاط خديجة ..... رئيسا.

-الأستاذ(ة).....وافي حاجة..... مشرفا مقررا.

-الأستاذ(ة).....لطروش أمينة..... مناقشا.

السنة الجامعية :2025/2024.

نوقشت في :2025/06/11 .

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية
في إنجاز البحث

أنا الممضي أدناه،

السيد: خزالي نور الهدى الصفة: طالبة

الحامل لبطاقة التعريف الوطنية رقم: 412710470 والصادرة بتاريخ: 2024.09.12

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون العام

والمكلف بإنجاز مذكرة ماستر بعنوان:

المسؤولية الجنائية عن جريمة الابتزاز الالكتروني وفق التشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025.06.15

نظرا لشرعية امضاء
السيد(ة): خزالي نور الهدى
بطاقة الهوية رقم: 412710470
الصادرة بتاريخ: 2024.09.12
القضاء المعني
المعلومة بيوم 15 جوان 2025

من رئيس المجلس الشعبي البلدي
و بتفويض منه
ملحق الإدارة الإقليمية
محمد الأمين قوعلش

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

"ومن آياته أن خلق لكم من أنفسكم أزواجًا لتسكنوا إليها وجعل بينكم مودة ورحمة" (الروم– 21)

الإهداء

الى قرة العين إلى من جعلت الجنة تحت قدميها الى التي حرمت على نفسها واعطتني من نبع حنانها

فسقتني الى من وهبتني الحياة ومنحتني الحب والحنان الى تلك المرأة العظيمة امي الحنونة الى أعظم الرجال

صبرا ورمز الحب والعطاء إلى الذي تعب كثيرا من أجل راحتي وافنى بحياته من أجل تعليمي ،وتوسم في

درجات العلى والسمو إلى ذلك الرجل العظيم ابي العزيز الى من كانو معي دوما ووقفوا بجانبي طيلة

مشواري الدراسي إلى من يعيش في ظل وجودهم املي اخوتي إلى كل الأهل والاقارب وإلى كل من تربطني

مودة بهم الى من جمعني بهم القدر صديقاتي إلى كل من وسعتهم ذاكرتي ولم تسعهم مذكرتي...

غزالي نور الهدى

كلمة شكر :

أحمد الله عز وجل أن يسر إتمام هذا البحث وأشكره أن سهل إخراجه فهو أهل للحمد والشكر وأصلي وأسلم على رسول الله الرحمة المهداة والنعمة المسداة والسراج المنير وعلى اله وصحبه ومن تبعه بإحسان

إلى يوم الدين ثم اتقدم بخالص الشكر والتقدير للأستاذة المشرفة وافي حاجة التي تكرمت بقبول الاشراف على هذا

العمل وعلى كل ما قدمته من ملاحظات وتوجيهات القيمة فجزاك الله عني خير جزاء كما أود أن أشكر اعضاء لجنة

الموقرين لتفضلهم مناقشة مذكرتي فلهم كل التقدير على الملاحظات التي سيسدونها والتي ستثري بلا شك هذه

الدراسة كما لايفوتنا في هدا المقام أن نشكر اساتذة كلية الحقوق والعلوم السياسيه وإلى كل من ساعدني

وشجعني الى كل من قاسمني معاناة هدا البحث فجزاكم الله كل خير

غزالي نور الهدى

قائمة المختصرات :

- ق.ع : قانون العقوبات .
- ق.إ.ج : قانون الإجراءات الجزائية .
- ج.ر.ج.ج: الجريدة الرسمية.
- ص : الصفحة.
- ط : الطبعة .
- د.ط : دون طبعة.

المقدمة :

في ظل التطور السريع والمتسارع لتكنولوجيا المعلومات والاتصال، أضحى العالم يعيش ثورة رقمية غيرت ملامح الحياة اليومية وأثرت في مختلف المجالات، خاصة ما تعلق بالتواصل الاجتماعي والمعاملات الإلكترونية ،غير أن هذا التطور لم يكن خاليا من التحديات، إذ ساهم في ظهور أنماط جديدة من السلوك الإجرامي، من بينها جريمة الابتزاز الإلكتروني، التي تمثل تهديدًا حقيقيًا للفرد والمجتمع على حد سواء، بالنظر إلى خطورتها وطبيعتها المعقدة التي تستغل الفضاء الرقمي لتحقيق أغراض إجرامية. فالابتزاز الإلكتروني يعد من أخطر الجرائم المستحدثة التي تمس كرامة الأشخاص وخصوصيتهم، بل قد تصل آثارها إلى المساس بحياتهم الاجتماعية والنفسية وحتى الجسدية، خاصة مع تزايد حالات الانتحار المرتبطة بهذه الجريمة، ويعرف الابتزاز الإلكتروني على أنه استخدام التهديد عبر الوسائل الرقمية لإجبار الضحية على القيام بفعل أو الامتناع عنه، عادة مقابل مال أو خدمة أو حتى صور ومعلومات شخصية، مستغلًا بذلك الخوف والحرج والعجز عن المواجهة، لاسيما بين الفئات الهشة كالأطفال والنساء.

وقد أصبحت هذه الجريمة أكثر تعقيدا بفضل التقنيات الحديثة، كإخفاء الهوية، استخدام الشبكة المظلمة(Dark Web) ، وتشفير الرسائل، مما يصعّب من عملية تعقب الجناة وإثبات التهمة. لذلك، لم يعد ممكناً التعامل مع هذه الجرائم بالأدوات القانونية التقليدية، بل بات من الضروري تكييف المنظومة التشريعية لمواجهة الجريمة في بعدها الرقمي، وذلك بإرساء قواعد جنائية حديثة تضمن حماية فعّالة لضحايا الابتزاز الإلكتروني وتردع مرتكبيها ،وفي هذا الإطار، حاول المشرع الجزائري مجاراة هذه التغيرات من خلال إدراج مواد قانونية تجرّم هذا النوع من السلوك، سواء عبر قانون العقوبات المعدل أو من خلال النصوص الخاصة كقانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أن الإشكال لا يزال قائما حول مدى فعالية هذه النصوص وكفايتها، سواء من حيث تحديد عناصر الجريمة أو ضبط المسؤولية الجنائية المترتبة عليها.

وانطلاقا من هذه المعطيات، تتبلور أهمية هذا البحث في محاولة الوقوف على مدى استجابة التشريع الجزائري للتحديات التي تفرضها جريمة الابتزاز الإلكتروني، من خلال دراسة طبيعتها القانونية، أركانها، صورها، وأسس المسؤولية الجنائية الناشئة عنها، سواء بالنسبة للشخص الطبيعي أو المعنوي، بالإضافة إلى تقييم السياسات العقابية المقررة لها والآليات المعتمدة في مكافحتها، كما يسعى هذا البحث إلى الكشف عن أوجه القصور أو الثغرات القانونية، واقتراح حلول تشريعية ومؤسساتية تواكب حجم وخطورة هذه الظاهرة المتنامية بما يحقق التوازن بين حماية الحقوق الرقمية وضمان الحريات الفردية من جهة ،وتحقيق الردع العام والخاص من جهة أخرى ، وفي هذا السياق أصبح من الضروري أن يتدخل المشرع الجزائري لمواكبة هذا التطور التكنولوجي والتصدي لآثاره السلبية من خلال تأطير قانوني محكم وفعال، يحدد المسؤولية الجنائية المرتبطة بهذا الفعل ويضع آليات قانونية رادعة لمكافحته. وعليه يطرح هذا الموضوع إشكالية محورية تتعلق بكيفية تنظيم التشريع الجزائري لجريمة الابتزاز الإلكتروني، وتحديد أركانها وأسس المسؤولية الجنائية عنها سواء تعلق الأمر بالأشخاص الطبيعيين أو المعنويين، ومدى فعالية النصوص الحالية في ردع هذا النوع من الإجرام الرقمي. ومن هنا تنبع أهمية هذا البحث، الذي يسعى إلى تسليط الضوء على الإطار القانوني لجريمة الابتزاز الإلكتروني في الجزائر، وتحليل عناصرها وخصائصها، ومناقشة أوجه القصور التي قد تعتري المنظومة التشريعية في هذا المجال، من أجل تقديم مقترحات من شأنها تعزيز الحماية الجزائية للفرد والمجتمع في ظل تحديات العصر الرقمي، وقد لا تكمن خطورة جريمة الابتزاز الإلكتروني فقط في الأضرار الفعلية التي تلحق بالضحية، بل تتعدى ذلك إلى الآثار النفسية والاجتماعية بعيدة المدى، حيث تؤدي في كثير من الأحيان إلى اضطرابات سلوكية، حالات من الانطواء والاكتئاب، بل والانتحار أحيانًا، خصوصا لدى فئات ضعيفة مثل القصر والمراهقين الذين يجدون أنفسهم عاجزين عن مواجهة هذا النوع من الجرائم، إما بسبب الخوف من الفضيحة، أو غياب الوعي القانوني، أو صعوبة الحصول على الدعم، كما أن طبيعة الجريمة ذات الطابع العابر للحدود، وتعدد الفاعلين والضحايا وتنوّع الوسائط الرقمية المستخدمة، يجعل من الابتزاز

الإلكتروني تحديًا حقيقيا ليس فقط للضحايا بل للمنظومة القانونية والقضائية ككل ذلك أن هذه الجريمة تقع في فضاء افتراضي بلا حدود، غالبا ما يمارس فيها الجاني نشاطه من خارج إقليم الدولة، مما يطرح إشكاليات جدية على مستوى الاختصاص القضائي، الإثبات، والتعاون القضائي الدولي ،وعلى الصعيد التشريعي ورغم الجهود التي بذلها المشرع الجزائري، خاصة من خلال تعديل قانون العقوبات وتضمين جرائم تكنولوجية جديدة، إلا أن النصوص الحالية قد لا ترقى دائمًا لمستوى التحديات المفروضة سواء من حيث دقة التكييف، أو شمولية العقوبات، أو مواكبة تطور الأساليب الإجرامية الإلكترونية. فغياب تعريف دقيق لبعض المصطلحات التقنية، والتداخل بين مفاهيم قانونية تقليدية وأخرى مستحدثة، قد يخلق فجوات قانونية يستغلها المجرمون في الإفلات من العقاب، ومن هنا تبرز الحاجة الملحة لإعادة النظر في الإطار القانوني الجزائري الخاص بالجرائم السيبرانية، خاصة ما تعلق بجريمة الابتزاز الإلكتروني، بغرض تقويته وتحسين أدوات إنفاذه، بما يضمن تحقيق الردع العام، وفعالية الحماية الخاصة، واستقرار المنظومة العدلية في مواجهة هذا النوع من الجرائم المستجدة.

كما لم تعد تكنولوجيا الاتصال والمعلومات مجرد أدوات ترفيه أو تواصل، بل أصبحت ركيزة أساسية في حياة الأفراد والمؤسسات، حيث أثرت بشكل عميق في الأنماط الاقتصادية والاجتماعية والثقافية،غير أن هذه الثورة التكنولوجية، وإن حملت في طياتها الكثير من الإيجابيات، إلا أنها أفرزت في المقابل أشكالاً جديدة من الانحرافات السلوكية والإجرامية التي لم تكن مألوفة في السابق، وأبرزها ما يُعرف بالجرائم السيبرانية أو الجرائم الإلكترونية، والتي تنامت بشكل خطير خلال السنوات الأخيرة.

ومن بين أخطر هذه الجرائم، تبرز جريمة الابتزاز الإلكتروني، التي أصبحت تهدد أمن الأفراد وخصوصياتهم، وتزرع الخوف والقلق في نفوسهم، نظرا لما تنطوي عليه من استغلال غير مشروع للمعلومات الشخصية أو الصور أو التسجيلات الخاصة، للحصول على منافع مالية أو جنسية أو تنفيذ أوامر معينة تحت طائلة التهديد بالفضح أو الإضرار بالسمعة، وتكمن

خطورة الابتزاز الإلكتروني في طبيعته المركبة، فهو من جهة يعتمد على الوسائل التكنولوجية الحديثة التي تتيح للجاني إخفاء هويته والتحرك بحرية عبر الفضاء الرقمي دون قيود زمانية أو مكانية، ومن جهة أخرى يوجه ضد ضحايا غالبًا ما يكونون في موضع ضعف نفسي أو اجتماعي، ما يجعلهم عرضة للاستسلام والرضوخ للتهديدات، كما أن هذه الجريمة لا تقتصر على الأفراد فحسب، بل قد تستهدف حتى المؤسسات حيث يقوم الجناة بابتزاز شركات أو إدارات مقابل عدم نشر بيانات حساسة أو تعطيل نظمها الإلكترونية ،ولأن هذه الأفعال تتخذ صورا مستحدثة وتتطور بشكل متسارع، فإن مواجهتها تتطلب بدورها تطورا تشريعيا وقضائيا وأمنيا يوازي حجم التحدي.

وفي هذا السياق حاول المشرع الجزائري الاستجابة لتلك التحديات، من خلال تعديل قانون العقوبات لاسيما في المواد المتعلقة بالمساس بحرمة الحياة الخاصة ووسائل التهديد والابتزاز عبر الوسائط الإلكترونية، ومن خلال إدراج نصوص قانونية في قوانين خاصة: مثل قانون مكافحة الجريمة المعلوماتية ومع ذلك، فإن تطبيق هذه النصوص على أرض الواقع ما يزال يطرح العديد من الإشكاليات سواء من حيث التكييف القانوني الدقيق لجريمة الابتزاز الإلكتروني، أو من حيث التمييز بينها وبين الجرائم المتشابهة كالتشهير، التهديد، أو نشر الصور دون إذن، فضلا عن صعوبة تحديد المسؤولية الجنائية في بيئة رقمية تسمح بإخفاء الهوية واستعمال تقنيات متقدمة لطمس الأدلة وإرباك التحقيق.

كما أن المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في الجزائر تثير جدلا قانونيا، لاسيما عندما يتعلق الأمر بالأشخاص المعنويين كالشركات والمؤسسات التي قد تُستعمل منصاتها في ارتكاب الفعل الإجرامي، أو التي قد تقصر في حماية بيانات مستخدميها، ويزداد هذا الجدل تعقيدًا في ظل نقص الوعي الرقمي القانوني لدى العديد من الأفراد، مما يدفعهم في الغالب إلى الامتناع عن التبليغ خوفا من الفضيحة أو من تعقيد الإجراءات، الأمر الذي يؤثر سلبا على فعالية المتابعة القضائية ويضعف الردع الجنائي.

وبناءا على ما سبق فإن دراسة المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في التشريع الجزائري تكتسي أهمية بالغة، لأنها لا تلامس فقط الجانب القانوني المحض بل تنفتح أيضا على أبعاد اجتماعية وأمنية ونفسية، وتطرح أسئلة عميقة حول مدى قدرة المنظومة القانونية الوطنية على التأقلم مع طبيعة الجريمة الإلكترونية، ومن هنا تنبع إشكالية هذا البحث في التساؤل حول مدى فعالية الإطار القانوني الجزائري في مواجهة جريمة الابتزاز الإلكتروني وتحديد أسس المسؤولية الجنائية المترتبة عنها، وكذا مدى كفاية الآليات القانونية والمؤسساتية المعتمدة في مكافحتها، وسيسعى هذا البحث إلى تفكيك هذه الإشكالية من خلال تحليل العناصر المكونة للجريمة، واستعراض أوجه القصور في النصوص الحالية، واقتراح سبل تطويرها بما يحقق حماية فعالة لضحايا هذا النوع الخطير من الإجرام المستحدث ،فمنه نطرح الإشكالية : **إلى أي حد توفّق المشرع الجزائري في التكييف القانوني لجريمة الابتزاز الإلكتروني، وتحديد المسؤولية الجنائية عنها، في ظل الطبيعة المعقدة لهذه الجريمة وصعوبة تتبع مرتكبيها ؟**

و قد تمحورت تساؤلات الدراسة حول ما يأتي:

-ماهية جريمة الابتزاز الالكتروني ؟

-ماهي دوافع الابتزاز الالكتروني ؟

-على من تقع المسؤولية الجنائية في حال وقوع الجريمة؟

-ماهي العقوبات الملائمة للجاني ؟

تنبع أهمية هذا الموضوع من الواقع العملي والظرفية الراهنة التي تشهد تناميًا مطّردًا في وتيرة الجرائم الإلكترونية، وعلى وجه الخصوص جريمة الابتزاز الإلكتروني، التي أصبحت تمثل تهديدا حقيقيا لأمن الأفراد وخصوصيتهم وسلامتهم النفسية والاجتماعية فهذه الجريمة، التي تستغل التكنولوجيا الحديثة والفضاء الرقمي، لم تعد مقتصرة على الفئات الهشة فقط، بل

أصبحت تطال جميع شرائح المجتمع، أفرادا ومؤسسات، ما يجعلها من أبرز التحديات القانونية التي تواجه الدول في العصر الحديث،وتكتسي أهمية هذه الدراسة بعدا مزدوجا نظريا وعمليا، فهي من جهة تهدف إلى تحليل الإطار القانوني الوطني الذي ينظم جريمة الابتزاز الإلكتروني، والكشف عن مدى فعاليته في تحديد المسؤولية الجنائية المترتبة عنها، ومن جهة أخرى تسعى إلى إبراز أوجه النقص أو القصور التي تعتري هذا الإطار، اقتراح حلول تشريعية وقضائية تواكب طبيعة هذا النوع المستحدث من الجرائم.

كما تتجلى أهمية البحث كذلك في محدودية الدراسات الوطنية المتخصصة التي تناولت جريمة الابتزاز الإلكتروني بشكل معمّق، ما يمنح هذا العمل بعدا إضافيًا كونه يسهم في إثراء المكتبة القانونية الجزائرية بمجال لا يزال في طور التبلور التشريعي والقضائي ، من أجل مقاربة موضوع "المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في التشريع الجزائري" بشكل علمي دقيق وشامل، تم الاعتماد على المنهج التحليلي، وذلك من خلال تحليل النصوص القانونية ذات الصلة، وعلى رأسها قانون العقوبات، القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى بعض النصوص ذات العلاقة مثل القانون المدني وقانون الإجراءات الجزائية، بهدف الوقوف على الكيفية التي تم بها تنظيم هذه الجريمة من حيث الأركان والعقوبة والمسؤولية، كما تم توظيف المنهج المقارن في بعض المواضع، من خلال استعراض مواقف بعض التشريعات المقارنة (مثل القانون الفرنسي أو المصري)، وذلك لتسليط الضوء على التجارب التشريعية المختلفة ومحاولة الاستفادة منها في تقييم الوضع القانوني الجزائري ،ولم يغفل البحث أيضا استخدام المنهج الوصفي في بداية الدراسة من خلال عرض الظاهرة وتطورها وأسباب انتشارها، وذلك لوضع القارئ في الإطار العام للمشكل محل الدراسة،ويتوج هذا المنهج بتقديم قراءة نقدية تحليلية تسعى إلى اقتراح حلول واقعية قابلة للتنفيذ بهدف تعزيز فعالية السياسة الجنائية في مكافحة الابتزاز الإلكتروني.

أهداف البحث:

-تحليل الإطار القانوني لجريمة الابتزاز الإلكتروني في التشريع الجزائري وتحديد أوجه القوة والقصور فيه.

-دراسة أركان الجريمة وشروط تحققها على ضوء النصوص القانونية والاجتهاد القضائي.

-تسليط الضوء على المسؤولية الجنائية عن هذه الجريمة، سواء بالنسبة للأشخاص الطبيعيين أو المعنويين.

-مناقشة مدى كفاية العقوبات والآليات القانونية المعتمدة في الردع والمكافحة.

-تقديم توصيات عملية وتشريعية تساهم في تعزيز حماية الأفراد من هذه الجريمة الرقمية الحديثة.

وللإجابة على الإشكالية المطروحة أعلاه، ستتم معاجلة الموضوع من خلال تقسيمه إلى فصلين و لكل مبحث مطلبين، يخصص أولهما للتعرض إلى الاطار المفاهيمي لجريمة الابتزاز الالكتروني ، وخصصنا الفصل الثاني لبيان العقوبات المقررة لجريمة الابتزاز الالكتروني .

الفصل الاول :

الإطار المفاهيمي لجريمة الابتزاز الالكتروني في التشريع الجزائري.

إن التطورات والتغيرات التي عرفها العالم في شتى المجالات اقترن بظهور أنماط جديدة من الجرائم المستحدثة اتخذت من الفضاء الافتراضي بيئة خصبة لممارسة هذه النشاطات الإجرامية، ومن أكثر الجرائم استفحالا في وقتنا الحالي، تلك الجرائم نتاج الاستخدام السلبي للأنترنت بصفة التي ترتكب بواسطة وسائل التواصل الاجتماعي كجريمة الابتزاز الالكتروني تعد الجريمة الإلكترونية من أبرز الظواهر الإجرامية المعاصرة التي فرضها التطور التكنولوجي المتسارع، وتُمثل تحديًا قانونيًا وأمنيًا متزايدا على الصعيدين الوطني والدولي،ويقصد بها كل فعل غير مشروع يتم باستخدام الحاسوب أو الشبكات المعلوماتية أو أي وسيلة إلكترونية، ويهدف إلى الاعتداء على الأشخاص أو الممتلكات أو المصالح العامة أو الخاصة، سواء تعلق الأمر بسرقة البيانات أو انتهاك الخصوصية أو الاحتيال المالي أو نشر محتوى غير مشروع. وتمتاز الجريمة الإلكترونية بعدة خصائص تجعلها مختلفة عن الجرائم التقليدية، أبرزها الطابع التقني الذي يميز وسائل ارتكابها، والطابع العابر للحدود الذي يعقد سبل تتبع مرتكبيها، إضافة إلى صعوبة جمع الأدلة الرقمية وإثبات الجريمة، فضلًا عن سرعة تطورها وتنوع أشكالها. وتنقسم هذه الجرائم إلى عدة أنواع، منها ما يستهدف نظم المعلومات كاختراق الشبكات وتعطيل المواقع، ومنها ما يطال الأموال كمثل جرائم الاحتيال وسرقة البطاقات المصرفية،[1] وأخرى تمس بالخصوصية الشخصية من خلال التجسس أو الابتزاز أو تسريب الصور والمعلومات. وتتطلب الجريمة الإلكترونية توافر أركان قانونية كأي جريمة، حيث يتمثل ركنها المادي في السلوك الإجرامي المتمثل في الاستخدام غير المشروع للتكنولوجيا، ويقتضي ركنها المعنوي وجود القصد الجنائي والعلم بطبيعة الفعل المحظور، إلى جانب الركن الشرعي المتمثل في النص القانوني الذي يجرّم ذلك الفعل، وقد أسهمت عوامل عديدة في انتشار هذا النوع من الجرائم، من بينها زيادة الاعتماد على الوسائل الرقمية، وضعف الثقافة الأمنية الإلكترونية لدى المستخدمين، وسهولة إخفاء هوية الجناة على الشبكة، بالإضافة إلى عدم مواكبة بعض التشريعات الوطنية للتطورات التقنية المتسارعة، ومن أبرز التحديات التي تواجه مكافحة الجريمة الإلكترونية عدم

[1] حسني عبد الكرمي يونس، خليل يوسف جندي، الابتزاز الالكتروني والجرائم الإلكترونية المفهوم و الأسباب، الطبعة الأولى، دار الكفاءة المعرفة، عمان، الأردن، سنة 2021،ص 30.

وجود تعريف دولي موحد لها، وصعوبة التعاون الدولي في هذا المجال، فضلا عن الحاجة إلى كفاءات بشرية متخصصة قادرة على التعامل مع الأدلة الرقمية والتقنيات الحديثة. ويستوجب التصدي لهذه الظاهرة تبني إستراتيجية قانونية وأمنية متكاملة، تشمل التوعية المجتمعية، وتحديث التشريعات، وتعزيز التعاون الدولي، وتطوير قدرات الأجهزة القضائية والأمنية في مجال الجرائم السيبرانية.

ومن الجرائم الإلكترونية التي انتشرت في الآونة الأخيرة جريمة الابتزاز الإلكتروني، التي تعد أنينة، لأنها تلقي الروع في نفس اعتداء على حق الإنسان في الأمن للمجني عليه، وذلك عن طريق استدراجه والحصول على معلومات خاصة به ،ومن ثم تهديده بنشرها بهدف إرغامه على تلبية رغبات الجاني، وإلا عليه أن يواجه الفضيحة إذ إن العلاقة الجنسية ينفذ المطلوب منه، وهذا المطلوب قد يتمثل في دفع المبالغ المالية أو القيام بعمل من الأعمال أو الامتناع عنه، كما أنه قد يكون مشروعا لا يجرمه القانون، وقد يكون عملا غير مشروع يعد جريمة قانونا والمجني عليه في هذه الجرائم قد يكون شخصا طبيعيا من الرجال والنساء، قاصرين كانوا أم بالغين كما يكون شخصا اعتباريا مثل البنوك والمؤسسات والهيئات الدولية والمحلية، والحكومات بمختلف أجهزتها، كما أن وسيلة ارتكابها قد يكون الحاسوب، أو الهاتف، أو عبر البريد الإلكتروني أو مواقع التواصل الاجتماعي مثل الفيس بوك أو التيك توك، أو غيرها من الوسائل أو الواتساب أو السناب شات متاحة وسائلها في يد جميع الفئات هذه الجريمة في سهولة ارتكابها تكمن خطورة العمرية، وسهولة العبث بأدلة الإثبات بالمحو والتغيير[1]، كما أنها ترتكب في فضاء سيبراني، مكن تتبع أدلة الإثبات، حيث لم يعد مسرح الجريمة مسرحا ماديا كالجرائم التقليدية حتى ي وإنما مسرحها ومضات كهربائية ومغناطيسية ورموز وشفرات، مما يثير صعوبات في التحقيق والإثبات، فجريمة الابتزاز الإلكتروني جريمة العصر، والتي تزعزع أمن وطمأنينة الأفراد والأسر.

[1] خالد حسن أحمد لطفي ،جرائم الأنترنت بين القرصنة الإلكترونية كجرائم الابتزاز الالكتروني، دراسة مقارنة، الطبعة الأولى،سنة 2008 ،ص106.

المبحث الأول : ماهية جريمة الإبتزاز الإلكتروني .

يعد الابتزاز الإلكتروني ظاهرة متنامية في عالم الجريمة الرقمية، حيث يستغلّ المجرمون التقدم التكنولوجي الواسع، وانتشار وسائل التواصل الاجتماعي، وسهولة الحصول على البيانات الشخصية في ارتكاب هذا النوع من الجرائم. وغالبا ما يقع ضحايا الابتزاز الإلكتروني من مختلف الأعمار والفئات، خاصة النساء والفتيات والمراهقين، نظرًا لاستخدامهم المكثف للتطبيقات والمنصات الرقمية من دون إدراك كاف للمخاطر الأمنية المرتبطة بها ،وتتنوع أساليبه في الوصول إلى المعلومات المستغلة في الابتزاز، فقد يستخدمون الحيل النفسية للإيقاع بالضحية كالتقرب الوهمي عبر حسابات مزيفة، أو يلجؤون إلى وسائل تقنية متقدمة كاختراق الحسابات أو الأجهزة، أو استغلال الثغرات الأمنية في التطبيقات ،ولا يقتصر الابتزاز الإلكتروني على الجانب المالي، بل قد يكون ذا طابع أخلاقي، جنسي، اجتماعي، أو حتى سياسي، خصوصًا إذا تعلّق الأمر بشخصيات معروفة أو مؤثرة. كما أنه قد يمارس من طرف أفراد أو عصابات منظمة تعمل على نطاق محلي أو دولي، وتوظف أدوات متطورة لإخفاء الهوية، مما يصعّب من ملاحقتهم قضائيا،وقد تسبب هذه الجريمة أضرارا جسيمة على الضحية، تبدأ من الأذى النفسي كالخوف والقلق والاكتئاب، وقد تصل إلى التهديد بالقتل أو إيذاء الأسرة، أو التسبب في انهيار العلاقات الأسرية أو فقدان الوظيفة، بالإضافة إلى الانعزال الاجتماعي أو الانتحار في بعض الحالات القصوى[1].

وفي ظل هذه التهديدات المتزايدة، تحرص العديد من الدول على تطوير أطرها القانونية لمكافحة الابتزاز الإلكتروني، سواء من خلال سن تشريعات جديدة تواكب طبيعة هذه الجريمة، أو من خلال تخصيص وحدات شرطة متخصصة في مكافحة الجرائم السيبرانية، وتدريب القضاة والأمنيين على كيفية التعامل مع الأدلة الرقمية،ومع ذلك تبقى الوقاية هي خط الدفاع الأول، حيث ينبغي تعزيز الوعي الرقمي لدى الأفراد، وتثقيف المستخدمين حول أساليب

[1] أحمد بسيوني أبو الروس ،التحقيق الجنائي و التصرف فيه و الادلة الجنائية ،الطبعة 01،الاسكندرية ،2015،ص 26.

الحماية، مثل تفعيل المصادقة الثنائية، وتجنب مشاركة المعلومات الحساسة، وعدم الثقة بالغرباء عبر الإنترنت،كما يُنصح باللجوء السريع إلى الجهات الأمنية المختصة في حال التعرض لأي تهديد، وعدم الرضوخ لمطالب المبتز، لأن الخضوع له يشجعه على الاستمرار ويعرض الضحية للمزيد من الأذى،فإن مواجهة الابتزاز الإلكتروني تتطلب تضافر الجهود القانونية والتقنية والاجتماعية، من أجل بناء بيئة رقمية أكثر أمانا وعدالة،و لمعرفة تعريف دقيق للإبتزاز الاكتروني سوف نقدم من خلال المطلب الموالي و فروعه.

المطلب الأول : تعريف الإبتزاز الإلكتروني .

أكد رجال دين واختصاصيون نفسيون ومحامون ان الابتزاز الإلكتروني سلوك غير سوي يعود بأثر سلبي على الفرد والأسرة والمجتمع، حيث يعتبر مؤشرا خطيرا على تغير القيم وانحدارها، وله انعكاسات على نفسية الضحية واستقرار أسرتها، ما يؤدي إليه من تفكك أسري وشيوع الخيانة والاستغلال، ما يفضي الى نشر الجريمة وهدم شخصيات الضحايا، ونشر الأمراض النفسية والجنسية، وإشاعة الفوضى والخوف والرعب في المجتمع،[1] فالابتزاز يعد جريمة أخلاقية، وسلوكا معوجا، وخسة نفس، قبل أن تكون محرمة شرعا، أما بخصوص نظرة الاسلام حول موضوع الابتزاز الالكتروني، فقد أوضح أن الابتزاز بشكل عام يشكل قيدا على حرية الشخص وإرادته، ومعلوم أن الشخص في الشرع محترم في نفسه وماله وعرضه وعقله ودينه، وهذه الخمس هي ما يطلق عليها مقاصد الشريعة الإسلامية، والابتزاز حقيقة وواقعا يشكل مصادرة لحرية الإنسان في إحدى تلك المقاصد الخمسة، ويشكل خطرا يهدد أمن الإنسان في سمعته وعرضه أو ذاته وبدنه، وكل ذلك منهي عنه شرعا، مشيرا إلى أن الابتزاز تطفل على خصوصية الناس واطلاع على عوراتهم ومصادرة لحرياتهم، والشرع الحنيف حرص كل الحرص على ستر عورات المسلمين وحفظ خصوصياتهم الشخصية بعيدا عن أعين الناس، وشرع لذلك تشريعات عديدة، منها: أحكام الاستئذان، والسلام، والنظر وغض البصر، واللباس،

[1] جاسم حممد جندل، الجرائم الإلكترونية، الطبعة الأولى، دار معتز للنشر والتوزيع، عمان، الأردن، سنة 2022،ص 46.

والدخول والخروج، ونحو ذلك، وفي المقابل نهى عن التجسس والاطلاع على العورات والدخول من غير استئذان اذ أن كل هذه الأحكام الشرعية عبارة عن سياج يحمي الإنسان ويحيطه بمزيد من الحماية والأمن والخصوصية والستر، خاصة مع توسع الناس في الاشتراك في شبكات التواصل الاجتماعي وانتشار تكنولوجيا الاتصال، ولا شك أن أي سلوك أو عمل يكسر هذه الحواجز أو يحاول اختراق هذا السياج فهو مدان في الشرع، بل ويطبق عليه أحيانا مع تماديه حد الحرابة لإفساده في الأرض بهذا السلوك المشين.

أولا-التعريف الفقهي للابتزاز الإلكتروني :يقوم على أساس ربط هذا الفعل بمفاهيم أصول الفقه الإسلامي ومقاصد الشريعة، باعتباره نوعا من الاعتداء والظلم الذي يُمارَس باستخدام وسائل التكنولوجيا الحديثة.[1]

ويمكن تعريف الابتزاز الإلكتروني فقهيا بأنه: كل تهديد يصدر من شخص تجاه غيره، باستخدام وسائل إلكترونية، من أجل حمله على القيام بفعل أو الامتناع عنه، بغير حق، مع استغلال معلومات أو صور أو بيانات خاصة تم الحصول عليها بوسيلة مشروعة أو غير مشروعة،وينظر إليه في الفقه على أنه من باب أكل أموال الناس بالباطل أو التهديد المحرم أو العدوان على العرض والكرامة، بحسب نوعية الابتزاز،وقد أشار العلماء إلى أن التهديد والوعيد من غير حق يعد حراما شرعا، سواء كان لغرض مادي أو معنوي، لأن فيه إكراهًا وظلمًا، والله تعالى يقول: "ولا تعتدوا إن الله لا يحب المعتدين" (البقرة: 190).[2]

-كما أن الرسول صلى الله عليه وسلم قال: كل المسلم على المسلم حرام دمه وماله وعِرضه. (رواه مسلم).

ومن هذا المنطلق، فإن الابتزاز الإلكتروني يعد في ميزان الشريعة اعتداء مركبا، يجمع بين انتهاك للخصوصية، والتهديد بالإكراه، وقد يصل إلى هتك العرض أو الغصب، مما يجعله من

[1] حسني عبد الكرمي يونس، خليل يوسف جندي، المرجع السابق ،ص 40.
[2] سورة البقرة الآية 190.

الكبائر التي تستوجب التعزير، أو حتى العقوبة الأشد إذا اقترنت بجرائم أخرى كالقذف أو نشر الفاحشة أو التشهير.

يتضح أن كل وسيلة تؤدي إلى الإضرار بالناس أو إذلالهم أو ابتزازهم تمنع شرعا، سواء كانت تقليدية أو رقمية، ولا يُبيح استخدامها إلا في حالات الضرورة القصوى ووفقًا لضوابط شرعية صارمة، لا تنطبق على أفعال المبتزين ،وبالتالي فإن الفقه الإسلامي لا يقرّ هذا السلوك بأي حال، ويوجب على السلطات الشرعية والقضائية وضع العقوبات المناسبة لردع مرتكبيه، وحماية الأفراد من الاستغلال والابتزاز بكافة أشكاله ، يعد الابتزاز الإلكتروني من الأفعال المحرّمة شرعًا والمجرّمة فقهيًا، إذ يتنافى مع القيم الإسلامية والمقاصد الشرعية التي جاءت لحفظ الضروريات الخمس: الدين، النفس، العقل، المال، والعِرض. ويُنظر إليه فقهيًا بوصفه نوعًا من الإكراه والظلم والعدوان على حقوق الآخرين، حيث يستغل الجاني وسيلة إلكترونية، كالهاتف أو البريد الإلكتروني أو مواقع التواصل الاجتماعي، للضغط على الضحية وإجبارها على القيام بفعل معين أو الامتناع عنه دون وجه حق، تحت التهديد بنشر معلومات أو صور أو محتويات خاصة تم الوصول إليها بوسائل شرعية أو غير شرعية.[1] وقد أجمعت المذاهب الفقهية على تحريم كل سلوك يقوم على استغلال الناس وإذلالهم أو الإضرار بسمعتهم أو أعراضهم أو أموالهم، سواء تم ذلك عن طريق القوة أو الحيلة أو التهديد، لأن في ذلك تعديا صارخا على الكرامة الإنسانية، ومساسا بحرمة الإنسان التي كفلها الإسلام، وهو العقاب الذي يقدّره ولي الأمر لكل جريمة لا حد فيها ولا كفارة، ويُراعى فيه حجم الجريمة وأثرها على الفرد والمجتمع، إذ أن الابتزاز عبر الوسائل الحديثة لا يختلف في جوهره عن الابتزاز التقليدي، بل قد يكون أشد خطرا وأوسع تأثيرًا، لسرعة انتشار المعلومات وسهولة التشهير عبر المنصات الرقمية. ويُفهم من القواعد الفقهية، كقاعدة لا ضرر ولا ضرار، وقاعدة الوسائل لها أحكام المقاصد، أن استخدام الوسائل التقنية بقصد الإضرار بالناس أو ابتزازهم يُعد محرّمًا شرعًا،

[1] بن طالب ليندة، الدليل الالكتروني ودوره في الإثبات الجنائي ،دراسة مقارنة، أطروحة دكتوراه ، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، نوقشت في 2019/01/23 ،ص 22.

وتُطبق عليه أحكام التعزير بما يتناسب مع الجريمة وظروفها. ويُعدّ هذا الفعل من مظاهر الفساد في الأرض إذا تكرر وارتبط بعصابات أو نظم ممنهجة، ويستوجب تشديد العقوبة فيه بما يحقق الردع والزجر، حمايةً للأعراض، وصيانةً للمجتمع، وتحقيقا للعدل الذي هو من أعظم مقاصد الشريعة الإسلامية.

ثانيا –التعريف اللغوي:

الابتزاز في اللغة مأخوذ من الفعل "ابتز"، ويُقال :ابتزّ الشيء أي انتزعه قهرا وظلما أو أخذه غصبًا دون وجه حق، ويقال أيضا :ابتز المال أي استولى عليه بالقوة أو الحيلة، وابتزه الكلام أي ألزمه به وأخذه منه على غير رضى،وقد ورد في المعاجم اللغوية أن "الابتزاز" يدل على معنى الاستلاب والانتزاع بالإكراه أو بالإغراء المقرون بالتهديد أو الضغط النفسي والمعنوي. ووفقا لما جاء في "لسان العرب" لابن منظور، فإن الابتزاز يحمل دلالات متعددة، كلها تدور حول أخذ الشيء من الغير دون رضاه وباستعمال نوع من القهر أو الخداع أو الحيلة.[1]

كما نجد في "المعجم الوسيط" أن الفعل "ابتز" يعني "انتزع الشيء منه عنوة أو مكرا"، وهو فعل يفيد الغلبة أو الاستيلاء على ما لا يستحق، وغالبا ما يرتبط بمعاني الإكراه والإجبار، وهو ما يُعبّر عن ظلم بين وعدوان على حقوق الآخرين.

ومن خلال هذا البعد اللغوي، يتضح أن الابتزاز في أصله فعل يتضمن اعتداءً على الإرادة الحرة للإنسان، ويقوم على إرغامه على القيام بأمر أو تركه مقابل الخوف من عاقبة معينة يُلوّح بها الطرف الآخر.

من حيث الدلالة اللغوية لا يشترط أن يكون ماديا فقط، بل قد يكون معنويا أيضا، فيأخذ شكل تهديد يتعلق بالسمعة أو الشرف أو العلاقات الشخصية، وهو ما ينسجم مع صور الابتزاز المعاصرة، خاصة الابتزاز الإلكتروني، الذي وإن اختلفت وسائله وأدواته، إلا أنه لا يخرج عن

[1] مروة صالح الدين محمد، الدليل الالكتروني ومدى حجيته في الإثبات الجنائي، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية ، القاهرة، مصر، سنة 2021،ص 31.

المعنى اللغوي الأصلي: أي انتزاع حق أو تحصيل منفعة بطريقة غير مشروعة، تعتمد على التهديد والضغط، وهكذا يتضح أن المفهوم اللغوي للابتزاز يتسم بالشمول ويشكل أساسا مهما لفهم المفهوم الاصطلاحي والفقهي والقانوني لهذه الظاهرة.

بالنظر إلى الابتزاز من الناحية اللغوية، يتبين أن الكلمة تحمل جذورًا دلالية غنية ومتشعبة تُساعد على فهم عمق هذا المفهوم ومظاهره المختلفة فكلمة ابتزاز مأخوذة من الجذر الثلاثي (ب ز ز)، وهو جذر يدل في أصله على السلب والانفصال والانتزاع ،ويقال في اللغة: "بَزَ فلان فلانًا متاعه" أي أخذه منه عنوة أو غلبة، ومنه جاء الفعل "ابتز" بصيغة المزيد للدلالة على المبالغة في الفعل أو الاستمرار فيه ،وعليه فإن الابتزاز لا يقتصر على المال فحسب، بل يشمل كل ما يمكن انتزاعه قسرا، سواء كان ماديا كالأموال أو معنويًا كالمعلومات أو الأفعال أو السكوت على أمر معين.[1]

ويتميز الابتزاز لغويا :بأنه سلوك عدواني ينطوي على عدم تكافئ في العلاقة بين الطرفين، حيث يقوم المبتز بالضغط على الضحية من موقع قوة أو تهديد سواء كان حقيقيًا أو موهومًا مستغلا نقطة ضعف عند الضحية لتحقيق مصلحة ذاتية. كما أن من خصائص الابتزاز اللغوية أنه يمارس خفية أو بشكل غير مباشر أحيانا، وقد يتم بالتدريج أو الإلحاح أو المراوغة، وهو ما يتناسب تماما مع أنماط الابتزاز الحديثة كالابتزاز العاطفي" أو "الابتزاز الإلكتروني".

كما أن كلمة "ابتزاز" من حيث استعمالها في اللغة العربية الحديثة اكتسبت دلالة سلبية خالصة، فهي لا تُستخدم إلا للدلالة على فعل مُشين وغير مشروع، سواء في السياسة أو الإعلام أو العلاقات الاجتماعية أو حتى في الفقه والقانون، فحين يقال "ابتزاز إعلامي" أو "ابتزاز سياسي"، يقصد به استغلال ظرف أو موقف معين لتحقيق مصلحة خاصة عن طريق التهديد أو التشهير ،ولعل من أهم ما يميز المعنى اللغوي لكلمة الابتزاز هو تلازمه مع القهر والإكراه وغياب الرضا، وهو ما يعد عنصرا جوهريا في تكييف هذا السلوك ضمن الجرائم المعنوية والأخلاقية

[1] مروة صلاح الدين محمد ، المرجع السابق،ص 33.

سواء في الفقه أو القانون، مما يظهر أهمية العودة إلى الأصل اللغوي في فهم الجريمة وبيان خطرها على الفرد والمجتمع.

الفرع الأول :أسباب جريمة الإبتزاز الإلكتروني .

يعد الابتزاز الإلكتروني من الجرائم الحديثة التي باتت تثير قلقا متزايدا في المجتمع الجزائري، نتيجة التطور التكنولوجي المتسارع، والانتشار الواسع لاستخدام الإنترنت ووسائل التواصل الاجتماعي بين مختلف فئات المجتمع، وخاصة فئة الشباب. وقد عرفت المنظومة القانونية الجزائرية هذه الجريمة من خلال القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذلك من خلال تعديل قانون العقوبات، حيث سعت السلطات إلى مواكبة هذا التحول الرقمي بتحديث النصوص القانونية، لكن بالرغم من ذلك، تبقى هناك عدة أسباب قانونية واجتماعية وتقنية ساهمت في تنامي ظاهرة الابتزاز الإلكتروني في الجزائر.[1]

من الأسباب الرئيسية لانتشار الابتزاز الإلكتروني في الجزائر، ضعف الوعي القانوني لدى المواطنين، حيث أن الكثير من الأفراد، وخصوصًا الفئات الشابة والمراهقين، لا يملكون إدراكًا كافيًا بخطورة مشاركة بياناتهم الشخصية وصورهم ومقاطعهم عبر الإنترنت، ولا يعرفون الحقوق القانونية التي تكفل لهم الحماية، ولا كيفية التصرف في حال التعرض للابتزاز، كما يعزى تفشي هذه الظاهرة إلى الفراغ التشريعي الجزئي أو قصور بعض النصوص القانونية عن تغطية كافة أشكال الابتزاز الإلكتروني المستحدثة، لا سيما تلك التي تتم عبر تطبيقات جديدة يصعب تتبعها أو التحكم فيها، مما يمنح الجناة هامشا واسعًا للمناورة والتهرب من العقاب.

1القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009.

بالإضافة إلى ذلك، فإن صعوبة تتبع هوية مرتكبي الجرائم الإلكترونية بسبب استخدامهم وسائل إخفاء الهوية مثل الشبكات الخاصة الافتراضية (VPN)، والحسابات المزيفة، يحد من فعالية المتابعة القانونية، ويُضعف من عنصر الردع، وهو ما يشجع بعض الأشخاص على ارتكاب هذه الأفعال الإجرامية وهم مطمئنون إلى الإفلات من العقاب، كما تعد قلة التكوين المتخصص لدى الضبطية القضائية وأعوان إنفاذ القانون في مجال الأدلة الرقمية والتحقيقات السيبرانية من العوامل التي تقلل من فاعلية النظام القضائي في الرد على هذا النوع من الجرائم ،ومن جهة أخرى فإن التحولات الاجتماعية والثقافية التي يعرفها المجتمع الجزائري، والتي ترافقت مع الانفتاح الإعلامي والثقافي، ساهمت في توسع مساحات التعبير والنشر عبر الإنترنت دون ضوابط أخلاقية أو قانونية واضحة، مما زاد من فرص وقوع الأفراد في شرك الابتزاز الإلكتروني، ويضاف إلى ذلك غياب الرقابة الأسرية والتربوية على استخدام الإنترنت من طرف القصر، و ضعف البنية التحية الإلكترونية لمؤسسات الحماية الاجتماعية، ما يجعل من فئة الأطفال والفتيات والنساء هدفًا سهلا للمبتزين، وعليه فإن معالجة ظاهرة الابتزاز الإلكتروني في القانون الجزائري لا تقتصر فقط على إصدار تشريعات جديدة، بل تتطلب رؤية شاملة تقوم على تحديث النصوص القانونية، وتعزيز قدرات الضبطية القضائية، وتطوير التعاون الدولي، إضافة إلى برامج توعوية وتربوية تستهدف مختلف فئات المجتمع، لبناء ثقافة رقمية قانونية تحمي الأفراد وتحد من هذه الظاهرة المتصاعدة.[1]

بالإضافة إلى ما سبق، يمكن تحليل أسباب الابتزاز الإلكتروني في الجزائر من زوايا متعددة تشمل الجوانب القانونية والتقنية والاجتماعية والنفسية، مما يُبرز تعقيد هذه الظاهرة ويؤكد الحاجة إلى مقاربة متعددة الأبعاد في معالجتها.

[1] لعور، سمية، التحقيق الجنائي في الجرائم المعلوماتية، دار المعرفة، الجزائر، 2020،ص 75.

1-ضعف الحماية القانونية التقنية والرقمية:

رغم وجود قوانين جزائرية تُجرّم الأفعال المرتبطة بالابتزاز الإلكتروني، مثل القانون 18-04 المتعلق بتحديد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ، إلا أن الوسائل التقنية المتاحة لجهات إنفاذ القانون لا تزال محدودة من حيث التتبع، والتحليل الجنائي الرقمي، ومراقبة الشبكات. كما أن بعض النصوص التشريعية لا تغطي بوضوح كل صور الابتزاز المستحدثة، مثل الابتزاز باستخدام الذكاء الاصطناعي(Deepfake) ، أو التطبيقات التي تُخفي هوية المستخدم[1].

2-الفراغ التشريعي في حماية ضحايا الابتزاز:

من أبرز الإشكالات القانونية أن التشريع الجزائري يركز على تجريم الفعل دون توفير آليات واضحة لحماية الضحية، سواء من حيث سرية الشكاوى، أو توفير مرافقة نفسية واجتماعية، أو حتى توفير حماية قانونية مؤقتة ضد التهديد المستمر من الجاني، وهذا يثني كثيرا من الضحايا، وخاصة النساء، عن التبليغ خوفا من الفضيحة أو من انتقام المبتز[2].

3-الجهل الرقمي والانفتاح غير الآمن على الإنترنت:

يعد ضعف الثقافة الرقمية في أوساط المجتمع الجزائري من أبرز الأسباب المؤدية للابتزاز الإلكتروني، إذ ينشر الكثير من المستخدمين معلوماتهم الشخصية وصورهم الحساسة دون إدراك للمخاطر. كما يُقبل الشباب على استخدام التطبيقات الجديدة ،والمواقع دون الاطلاع على شروط الخصوصية والأمان، مما يجعلهم عرضة لسرقة بياناتهم أو خداعهم.

[1]القانون رقم 18-04 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، سنة 2018.

[2]لعور، سمية، المرجع السابق،ص 78.

4-البطالة والفراغ والانحراف السلوكي:

يلاحظ أن كثيرا من مرتكبي جرائم الابتزاز الإلكتروني في الجزائر من فئة الشباب العاطل عن العمل، الذين يجدون في هذه الأفعال وسيلة سهلة للحصول على المال أو لتحقيق نوع من السيطرة والإثبات الذاتي، كما أن بعض الحالات مرتبطة بـ الانحراف الأخلاقي أو الاضطرابات النفسية، خاصة عندما يكون الابتزاز بدوافع انتقامية أو جنسية.

5-تضاؤل الردع الاجتماعي:

في بعض الحالات، يساهم التطبيع المجتمعي مع السلوكيات الرقمية غير الأخلاقية كالمحادثات الحميمة، أو تبادل الصور الخاصة أو استخدام الألفاظ الفاحشة، في تقليل الحساسية تجاه الأذى الذي يسببه الابتزاز، مما يُضعف الرقابة الذاتية ويسهل ارتكاب الجريمة. ويلاحظ أيضا أن بعض المجتمعات لا تتعامل بجدية مع هذا النوع من التهديدات، مما يجعل الضحايا يخشون من عدم تصديقهم أو لومهم بدلًا من حمايتهم.

6-ضعف التعاون الدولي في المجال السيبراني:

نظرا لأن العديد من جرائم الابتزاز الإلكتروني ترتكب من خارج الحدود، أو باستخدام حسابات مُسجّلة في بلدان أجنبية، فإن ضعف الاتفاقيات الثنائية أو الإقليمية في المجال القضائي الرقمي يعيق الوصول إلى الجناة وتقديمهم للعدالة، خاصة في ظل البيروقراطية الإدارية وقلة الخبراء في التحقيقات السيبرانية[1].

7- قصور البرامج التعليمية والتربوية:

يغيب في كثير من المناهج الدراسية الجزائرية برامج توعية سيبرانية تعلّم التلاميذ الاستخدام الآمن للإنترنت، وكيفية التعامل مع التحرش الرقمي أو الابتزاز، كما لا يتم إشراك الأسرة

[1] بن عمارة، فوزية، حماية الحياة الخاصة في البيئة الرقمية، مجلة الباحث، العدد 9، جامعة قالمة، 2022،ص 36.

والمدرسة بشكل فعال في التوجيه الوقائي والتربوي الذي يقلل من فرص السقوط في الفخاخ الرقمية.

الفرع الثاني : انواع الابتزاز الالكتروني في التشريع الجزائري .

مع التطور المتسارع في مجال تكنولوجيات الإعلام والاتصال، برزت إلى السطح أنماط جديدة من الجرائم، لعل أبرزها الابتزاز الإلكتروني، الذي يعد من أخطر الجرائم التي تستهدف الأفراد في حياتهم الخاصة، وتمارس غالبا عبر وسائل رقمية يصعب ضبطها بالوسائل التقليدية. وقد أولى المشرّع الجزائري اهتمامًا ملحوظا بهذا النوع من الجريمة، حيث سعى من خلال القانون رقم 09-04 المؤرخ في 5 أوت 2009 إلى وضع إطار قانوني يواكب التحولات الرقمية، وينظم الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1].

يقصد بالابتزاز الإلكتروني ذلك الفعل الذي يقوم فيه الجاني بتهديد الضحية، باستخدام معلومات أو صور أو تسجيلات أو معطيات تم الحصول عليها أو إنشاؤها عن طريق الوسائط الإلكترونية، بقصد إرغامها على القيام بفعل أو الامتناع عنه، وغالبًا ما يكون الهدف الحصول على أموال، خدمات، أو حتى خضوع جنسي. وبالنظر إلى الطبيعة المركبة لهذا الفعل، وتعدد صوره وأساليبه، فقد تنوعت كذلك أنواعه من الناحية القانونية.

1-الابتزاز المالي الإلكتروني:

يعد من أكثر أشكال الابتزاز الإلكتروني شيوعا، ويقوم على تهديد الضحية بنشر صور أو معلومات خاصة ما لم تدفع مبلغا ماليا وغالبا ما يستخدم الجناة تطبيقات المحادثة أو البريد الإلكتروني أو مواقع التواصل الاجتماعي للوصول إلى الضحايا، ويكيف هذا النوع في التشريع الجزائري ضمن جريمة التهديد للحصول على منفعة مادية، المنصوص عليها في المادة 371

[1] القانون 09-04 ،المرجع السابق.

من قانون العقوبات، [1]ويعززه القانون 09-04 من خلال تجريم استخدام الوسائط التكنولوجية لهذا الغرض، خاصة في المادة 13 التي تنص على معاقبة كل من يستخدم تكنولوجيا الإعلام والاتصال لارتكاب أفعال التهديد أو الابتزاز.[2]

2-الابتزاز الجنسي الإلكتروني:

يتمثل في تهديد الضحية بنشر صور أو فيديوهات ذات طابع جنسي أو حميمي، عادة بعد الحصول عليها خلال علاقات افتراضية، أو عبر تصوير الضحية دون علمها. ويمثل هذا النوع خرقًا صارخا لحرمة الحياة الخاصة واعتداءً على الكرامة الإنسانية. وقد عالجه المشرّع الجزائري من خلال نصوص متعددة، منها المادة 303 مكرر من قانون العقوبات، التي تجرّم الاعتداء على الحياة الخاصة بتسجيل أو تصوير أو نشر صور دون رضا الشخص المعني، والمادة 333 مكرر 1 المتعلقة بالتحرش الجنسي، فضلا عن أحكام قانون 09-04 التي تجرّم هذا النوع من الممارسات الرقمية[3].

3- الابتزاز المعنوي أو العاطفي:

يأخذ هذا النوع طابعا نفسيا أكثر منه ماديا، حيث يستغل الجاني معلومات أو أسرارا شخصية أو عائلية للضغط على الضحية عاطفيًا، سواء بدافع الانتقام أو التهديد بتشويه السمعة. وتتعامل القوانين الجزائرية مع هذا النوع من خلال تجريم التهديد المعنوي المادة 284 من قانون العقوبات، وكذلك من خلال تكييفه في بعض الحالات ضمن القذف أو التشهير الإلكتروني، خاصة إذا تم نشر تلك المعلومات في الفضاء الرقمي.

[1]المادة 371 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية للجمهورية الجزائرية، العدد 49، سنة 1966.
[2]المادة 13 من قانون 09-04،المرجع السابق .
[3]المادة 333 من قانون 09-04 ،المرجع السابق.

4-الابتزاز المهني أو السياسي:

يرتبط هذا الشكل من الابتزاز غالبًا بالشخصيات العامة، أو الإعلاميين، أو المسؤولين، حيث يتم تهديدهم بنشر معلومات أو وثائق تمس حياتهم المهنية أو سمعتهم السياسية، وتكيف مثل هذه الأفعال في القانون الجزائري ضمن المساس بالحياة الخاصة أو التشهير، وفي بعض الحالات، قد تشكل خرقا لسرية المراسلات أو الوثائق الرسمية، وهو ما قد يشكل جناية إذا تضمن تسريبا لمعلومات حساسة، خصوصًا في حال تعلق الأمر بمؤسسات الدولة أو الشأن العام.

5- الابتزاز باستخدام محتوى مزيف ،الفبركة الرقمية:

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

6- الابتزاز ضد القصر:

يعد من أخطر أشكال الابتزاز الإلكتروني، حيث يستهدف فئة هشة من المجتمع، إما عن طريق استدراجهم عبر الإنترنت والحصول على صورهم، أو بتهديدهم بهدف استغلالهم جنسيًا أو تجاريًا. ويندرج هذا النوع ضمن الجرائم الخطيرة التي تتقاطع مع الاتجار بالبشر، ويعاقب عليها القانون بشدة، خاصة إذا ترافقت مع تحريض على الفساد أو نشر محتوى فاضح، إضافة إلى القوانين الخاصة بحماية الطفل[1].

[1] خليف عبد القادر، الابتزاز الإلكتروني في القانون الجزائري، مجلة الدراسات القانونية والسياسية، العدد 15، جامعة باتنة، 2021،ص 44.

المطلب الثاني : آثار الابتزاز الالكتروني .

يعد الابتزاز الإلكتروني من الجرائم المستحدثة التي خلفت آثارا بالغة الخطورة على مختلف الأصعدة، سواء النفسية أو الاجتماعية أو القانونية، حيث لا تقتصر تبعاته على الضحية فقط، بل تمتد لتطال الأسرة والمجتمع بشكل عام. فعلى الصعيد النفسي، يعاني ضحايا الابتزاز الإلكتروني من القلق المستمر، والتوتر، والخوف من الفضيحة أو التشهير، مما يؤدي في كثير من الحالات إلى الانطواء والعزلة، بل قد يصل الأمر إلى الاكتئاب أو الانتحار، خاصة لدى القصر والفئات الهشة، أما على الصعيد الاجتماعي، فإن هذه الجريمة تُهدد التماسك الأسري، وتُعرض الضحية للوصم والنبذ الاجتماعي، خاصة في المجتمعات المحافظة، حيث يستخدم الابتزاز كسلاح لهدم السمعة والكرامة، من جهة أخرى فإن الابتزاز الإلكتروني يُخلخل الثقة في وسائل الاتصال الحديثة ويزرع الشك في العلاقات الرقمية، مما يخلق حاجزًا نفسيًا بين الأفراد والتكنولوجيا. وعلى الصعيد القانوني، يشكل الابتزاز تحديًا كبيرًا للمنظومة القضائية، من حيث تعقب الجناة الذين غالبًا ما يتخفون خلف هويات مزيفة، واستخدام أدوات رقمية متطورة، الأمر الذي يتطلب تحديثا دائمًا للتشريعات وتعزيز قدرات أجهزة إنفاذ القانون في المجال الرقمي ومن ثم فإن آثار الابتزاز الإلكتروني تتجاوز الفعل الجرمي في حد ذاته، لتشكل تهديدًا حقيقيا للأمن النفسي والاجتماعي والرقمي للمجتمع ، فقد خلف الابتزاز الإلكتروني آثارا عميقة ومتداخلة تمتد لتشمل الفرد والمجتمع والدولة، مما يجعله من أخطر الجرائم السيبرانية التي لا تقتصر أضرارها على الجانب المادي فقط، بل تتجاوز ذلك لتطال الصحة النفسية، العلاقات الاجتماعية، وحتى الثقة العامة في الفضاء الرقمي. [1]

و منه سوف نتعرف على هذه الآثار من خلال الفروع الموالية للبحث .

[1] زروقي، نصيرة، الجريمة الإلكترونية في ضوء التشريع الجزائري والمقارن، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2021/2020 ،ص 50.

الفرع الاول : الاثار الاجتماعية و النفسية .

أولا- **المستوى النفسي:** يعاني الضحايا خصوصا القصر والنساء من مشاعر الخوف، القلق، الذنب، والإحراج، وقد يتحول الضغط النفسي الناتج عن التهديد المستمر إلى اضطرابات عقلية مثل الاكتئاب الحاد، الأرق، والعزلة الاجتماعية، وقد تؤدي في بعض الحالات القصوى إلى الانتحار، لا سيما عندما يكون الابتزاز متعلقا بصور أو محتوى حميمي موجه للفضيحة أو التشهير.

ثانيا- من الناحية الاجتماعية: فإن الضحية قد تفقد مكانتها في الوسط الأسري أو المهني، خصوصًا في المجتمعات التي لا تفرق بين الجاني والمجني عليه، وهو ما يخلق تبعات اجتماعية ثقيلة كقطع العلاقات الأسرية، الطلاق، أو فقدان الوظيفة. كما أن الأسرة قد تدخل في دوامة من التوتر والصراعات بسبب تداعيات القضية، ما يُضعف بنيتها ويهدد استقرارها.

ثالثا- التربوي والتعليمي: قد يتأثر أداء الضحايا لا سيما الطلبة حيث يعجزون عن مواصلة الدراسة بسبب الشعور بالخزي أو التعرض للتنمر الإلكتروني من قبل الزملاء، وهو ما يُفقد المجتمع عناصر شابة قد تكون فاعلة في التنمية. أما الأثر الاقتصادي، فيظهر في الخسائر المالية المباشرة الناتجة عن دفع الأموال للمبتز، وكذلك في تكلفة التحقيقات الإلكترونية، والملاحقة القضائية، وتأمين البيانات والحسابات، كما أن الابتزاز الإلكتروني يؤثر في مناخ الاستثمار الرقمي، إذ يخشى الأفراد والشركات من الاختراقات والابتزاز، مما قد يؤدي إلى تراجع الثقة في التجارة الإلكترونية والتعاملات الرقمية[1].

الفرع الثاني : الاثار الامنية .

إن الجرائم المرتبطة بالابتزاز الإلكتروني تمثل عبئا على أجهزة الأمن والعدالة، نظرا لتعقيد أساليب الجناة واعتمادهم على أدوات إخفاء الهوية، وشبكات الإنترنت المظلم واستعمال

[1] زروقي نصيرة ، المرجع السابق،ص 55.

تطبيقات يصعب تتبعها، مما يتطلب تكوينا متخصصًا للكوادر الأمنية والقضائية في مجال التحريات الرقمية، كما أن هذا النوع من الجرائم يفرض تحديات تشريعية وتنظيمية، منها ضرورة مواءمة القوانين مع التطورات التقنية، وضمان سرعة الاستجابة لحماية الضحايا، وتفعيل آليات الإنابة القضائية الدولية في حال كان الجاني خارج حدود الدولة ،وفي المحصلة فإن الابتزاز الإلكتروني لا يمثل فقط جريمة فردية، بل هو تهديد مركب لأمن المجتمع الرقمي، ويستلزم مواجهته مقاربة متعددة الأبعاد، تشمل التوعية المجتمعية، التأهيل النفسي للضحايا، التحديث التشريعي، والتعاون الدولي في المجال السيبراني، بهدف الحد من آثاره المتشعبة وحماية الضحايا من الانهيار النفسي والاجتماعي والقانوني[1].

يشكل الابتزاز الإلكتروني تهديدا أمنيا متناميا يتجاوز البعد الفردي ليمس الأمن العام والمجتمعي والمؤسساتي، حيث إن هذه الجريمة، التي تمارس عادة عبر منصات رقمية يصعب تعقبها، تضعف من قدرة الدولة على حماية مواطنيها، وتفتح الباب أمام أشكال جديدة من الإجرام المنظم والعابر للحدود، فعلى الصعيد الفردي يؤدي الابتزاز إلى زرع الخوف المستمر في نفوس الضحايا، ويضعهم تحت ضغط نفسي يجعلهم أحيانا يخضعون لمطالب المبتز، وهو ما قد يزج بهم في مواقف تمس بكرامتهم وأمنهم الشخصي، كما يعمّق من شعورهم بفقدان الحماية من طرف المؤسسات الأمنية المختصة.

أما على الصعيد الأمني العام، فإن انتشار الابتزاز الإلكتروني يعد مؤشرا على ثغرات أمنية في البنية الرقمية للدولة، ويخلق بيئة خصبة لتنامي الجرائم الإلكترونية الأخرى، مثل الاتجار بالبيانات، التهديد الممنهج، والهجمات السيبرانية. وتزداد خطورة الأمر عندما يتعلق الأمر بابتزاز موظفين في مؤسسات حكومية أو حساسة، حيث قد يُستغل الابتزاز للحصول على معلومات أو تسريبات تمس الأمن الوطني، وهو ما يفتح الباب أمام الاستغلال السياسي أو الاقتصادي أو حتى الاستخباراتي من قبل جهات أجنبية. كما أن الابتزاز الرقمي أصبح يُستخدم

[1] حماني، عبد العزيز،التحرش والابتزاز عبر الإنترنت: دراسة قانونية، مجلة العلوم القانونية، العدد 12، جامعة وهران،2021، ص 45.

ضمن أدوات الحروب السيبرانية الحديثة التي تعتمد على التشويش، نشر الفوضى، وزعزعة استقرار المجتمعات عبر استهداف البنية المعلوماتية.

وتعقد طبيعة الابتزاز الإلكتروني مهمة أجهزة الأمن الوطني، نظرًا لاستخدام الجناة لتقنيات التخفي والتشفير، وتطبيقات تواصل مشفرة، وتكنولوجيا الذكاء الاصطناعي لإنشاء محتوى زائف، بالإضافة إلى استغلالهم الفضاء السيبراني غير الخاضع لحدود جغرافية، ما يجعل التعاون الدولي بين الدول في مجال الجرائم المعلوماتية ضرورة ملحّة لضمان تعقب الجناة وملاحقتهم قضائيا، وقد أكد القانون الجزائري، خاصة من خلال القانون 09-04، على ضرورة تحديث الآليات القانونية لمواكبة هذه التحديات، إلا أن الواقع الأمني يفرض تطويرا مستمرا للقدرات التكنولوجية والبشرية لضمان الأمن السيبراني الوطني[1].

[1] أبو الخير، كمال ،تحديات الأمن السيبراني في ظل الابتزاز الإلكتروني، مجلة الدراسات القانونية المعاصرة، العدد 11، جامعة قسنطينة، 2022 ،ص 23.

المبحث الثاني : الطبيعة القانونية لجريمة الابتزاز الالكتروني.

إن الطبيعة القانونية لجريمة الابتزاز الإلكتروني في القانون الجزائري هي طبيعة مركبة، تجمع بين خصائص الجريمة التقليدية :الابتزاز أو التهديد، وخصائص الجريمة الإلكترونية، فالوسيلة المستعملة هي الأنترنت ووسائل التواصل الاجتماعي، البريد الإلكتروني...إلخ)،وقد أخذ المشرع الجزائري بهذا التوجه عبر إدماج هذه الأفعال ضمن المنظومة العقابية الرقمية، ما يعكس وعيا تشريعيا بمخاطر الجرائم المعلوماتية وضرورة مكافحتها بفعالية.

في عصر الرقمنة والتكنولوجيا أصبحت المعاملات اليومية تعتمد بشكل كبير على الوسائط الإلكترونية، مما أدى إلى بروز أنماط جديدة من الجرائم، أبرزها جريمة الابتزاز الإلكتروني، التي تمثل اعتداءً خطيراً على الحياة الخاصة وسلامة الأفراد النفسية والمادية. ويقصد بالابتزاز الإلكتروني التهديد بنشر أو إفشاء معلومات أو صور أو بيانات ذات طابع خاص عبر الوسائط الرقمية، مقابل الحصول على منفعة أو مكسب غير مشروع.

وفي القانون الجزائري لم يكن التشريع في بدايته يتضمن نصوصا خاصة تعالج هذا النوع من الجرائم، مما استدعى تدخل المشرع من خلال القانون 18-04 المؤرخ في 10 ماي 2018 المتعلق بالقواعد العامة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وقد تم بموجب هذا القانون تعديل بعض أحكام قانون العقوبات الجزائري، لاسيما من خلال إدراج نص المادة 303 مكرر 1، التي تجرم التعدي على الحياة الخاصة عن طريق تسجيل أو نقل أو نشر صور أو أقوال أو معلومات شخصية دون رضا صاحبها باستخدام أي وسيلة بما فيها الوسائل الإلكترونية[1].

[1] المادة 303 مكرر 1 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، لا سيما بموجب القانون رقم 18-04 المؤرخ في 10 ماي 2018، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، الصادرة في 13 ماي 2018.

كما يمكن تكييف جريمة الابتزاز الإلكتروني على ضوء المادة 371 من قانون العقوبات خاصة بالتهديد، إذا اقترن الابتزاز بوعيد أو بإنذار يمس شخص الضحية أو ممتلكاته ،وفي حال تم الابتزاز للحصول على مبالغ مالية فقد تتدرج الجريمة أيضا ضمن أحكام الاحتيال المنصوص عليها في المادة 372 وما يليها، إذا توافرت أركانه.

المطلب الاول : اركان جريمة الابتزاز الالكتروني .

يعد الابتزاز الإلكتروني من الجرائم المستحدثة التي فرضتها الثورة الرقمية وانتشار وسائل التواصل الحديثة، وقد سارعت العديد من التشريعات الوطنية والدولية إلى تقنين هذا الفعل الإجرامي لما ينطوي عليه من تهديد خطير لأمن الأفراد واستقرار المجتمع، ويعرف قانونيا بأنه كل سلوك يُمارس من قبل شخص أو جهة باستخدام وسائل إلكترونية بقصد تهديد شخص آخر أو الضغط عليه للحصول على منفعة غير مشروعة، سواء مادية أو معنوية مقابل عدم الكشف عن معلومات سرية أو صور أو مقاطع فيديو أو بيانات شخصية، تم الحصول عليها عبر وسائل مشروعة أو غير مشروعة، ويقوم الابتزاز الإلكتروني على فكرة الاستغلال التقني للمعلومات الخاصة بهدف الإكراه أو التحكم في إرادة المجني عليه، وغالبا ما يتم من خلال وسائل الاتصال الحديثة كالهاتف المحمول، البريد الإلكتروني، الرسائل النصية، أو شبكات التواصل الاجتماعي[1]،إذ يبنى التكييف القانوني لهذه الجريمة على ثلاثة أركان رئيسية: الركن القانوني (النص القانوني)، الركن المادي (السلوك الإجرامي)، الركن المعنوي (القصد الجنائي).

-الفرع الاول :الركن المادي و الشرعي .

إن الحديث عن جريمة الابتزاز الإلكتروني لا يكتمل إلا من خلال الوقوف على أركانها القانونية الأساسية، التي تشكل البنية الهيكلية لهذا الفعل الإجرامي وتميزها عن غيرها من الجرائم التقليدية أو الإلكترونية الأخرى، فكما هو الحال في مختلف الجرائم المنصوص عليها

[1]فتوش، سعاد، الجرائم المستحدثة في التشريع الجزائري: دراسة في الابتزاز والاحتيال عبر الإنترنت، رسالة ماجستير، جامعة الجزائر 1، كلية الحقوق، 2021/2020 ،ص 63.

في قانون العقوبات، فإن قيام المسؤولية الجزائية يتطلب توافر ثلاثة أركان رئيسية :الركن القانوني، الركن المادي، والركن المعنوي.

أولا–الركن القانوني:

يعد الركن القانوني شرطا أساسيا لقيام المسؤولية الجنائية، عملا بمبدأ الشرعية الجنائية المنصوص عليه في المادة الأولى من قانون العقوبات الجزائري، والتي تنص على أنه "لا جريمة ولا عقوبة أو تدبير أمني إلا بنص".[1] وقد كفل المشرع هذا الركن فيما يتعلق بالابتزاز الإلكتروني من خلال إدراج نصوص قانونية مستحدثة، على رأسها المادة 303مكرر 1 التي تجرم المساس بالحياة الخاصة عن طريق التقاط أو تسجيل أو نشر أو نقل صور أو معلومات شخصية دون إذن صاحبها، متى تم ذلك باستعمال تكنولوجيات الإعلام والاتصال، كما قد تُطبّق في بعض الحالات نصوص أخرى مثل المادة 371 من قانون العقوبات، التي تجرم التهديد، **و**المواد 372 إلى 379 إذا كانت الأفعال تنطوي على احتيال أو استغلال غير مشروع. وبهذا، فإن وجود نصوص صريحة توفر الإطار القانوني الذي يقوم عليه التكييف الجنائي لجريمة الابتزاز الإلكتروني.

كما ينص الدستور الجزائري في مادته 58 على أن" :الحياة الخاصة، بشتى صورها، محترمة ومحمية من قبل القانون" ما يعكس توجه الدولة إلى تعزيز الحماية القانونية للحرمة الشخصية في مواجهة الاعتداءات بما فيها تلك الواقعة في البيئة الرقمية [2]،وقد أدرك المشرع الجزائري خطورة الأفعال الإجرامية التي تتم عبر الوسائط الإلكترونية، خاصة تلك التي تنتهك الحياة الخاصة، لذلك بادر **إلى** تعديل قانون العقوبات بموجب القانون رقم 18–04 المؤرخ في 10 ماي 2018، حيث أُدرجت المادة 303مكرر 1، التي تُجرّم أي مساس بحرمة الحياة

[1] المادة 01 من قانون العقوبات الجزائري .

[2] المادة 58 من دستور الجمهورية الجزائرية الديمقراطية الشعبية، المراجَع بموجب التعديل الدستوري لسنة 2020، الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية، العدد 83، الصادرة في 30 ديسمبر 2020.

الخاصة للأشخاص، متى تم بواسطة تسجيل أو تصوير أو نقل أو نشر معلومات أو صور دون إذن صاحبها، باستخدام أي وسيلة، بما في ذلك الوسائل الرقمية.

ولم يقتصر المشرّع على تجريم مجرد الاعتداء، بل ضاعف العقوبة متى اقترن الفعل بغرض الابتزاز أو تحقيق مصلحة مادية أو معنوية أو الإساءة إلى شرف واعتبار الشخص، ما يُظهر إدراج المشرّع لجريمة الابتزاز الإلكتروني ضمن فئة الجرائم ذات الطبيعة المشددة في حال اقترنت بأهداف خبيثة ،إضافة إلى المادة 303 مكرر 1، نجد أن بعض حالات الابتزاز الإلكتروني قد تُكيّف أيضاً وفقًا لأحكام أخرى من قانون العقوبات، مثل:

-المادة 371 التي تجرم التهديد بالكتابة أو القول، متى كان مصحوبًا بأمر أو شرط.

-المادتين 372 و 374 المتعلقتين بجريمة الاحتيال متى تم خداع الضحية باستعمال شبكة إلكترونية وهمية أو حساب مزيف.

-المادة 394 مكرر التي تجرم الاستخدام غير المشروع لأنظمة الإعلام الآلي متى أدى ذلك إلى ضرر بالغير.

من خلال هذا الإطار التشريعي، يتبين أن الركن القانوني في جريمة الابتزاز الإلكتروني في الجزائر لا يستند إلى مادة واحدة فقط، بل يقوم على منظومة قانونية متكاملة تشمل قانون العقوبات العام، والنصوص الخاصة الواردة في قانون الجرائم المعلوماتية،و هذا التعدد في الأساس القانوني يبرز الطبيعة المركبة للجريمة، ويمنح القاضي الجنائي مرونة في التكييف حسب طبيعة الوقائع والوسيلة المستعملة[1].

[1] عبد الكريم بن عربية، شرح قانون العقوبات ،القسم العام نظرية الجريمة والمسؤولية الجزائية، ديوان المطبوعات الجامعية، الجزائر، طبعة 2019، ص115.

ثانيا-الركن المادي :

إن الركن المادي لجريمة الابتزاز الإلكتروني في القانون الجزائري لا يقوم على مجرد التهديد اللفظي أو الكتابي، بل يتجسّد في سلوك مدروس، يتم غالبا بوسائل تقنية متطورة تهدف إلى زعزعة إرادة الضحية لتحقيق منافع غير مشروعة، وتبرز هذه الجريمة مدى تداخل الوسائل الرقمية بالمسؤولية الجنائية، ما يفرض على المشرع والقضاء مواكبة التحولات التقنية عبر تحديث النصوص وتكييف المفاهيم القانونية بما ينسجم مع الواقع الإلكتروني المعاصر.

يعد الركن المادي من الأركان الجوهرية التي تميز الفعل الجرمي عن غيره من التصرفات المشروعة، حيث لا يمكن مساءلة شخص جنائيا على مجرد النية أو التفكير، ما لم يتجسد ذلك في سلوك خارجي محسوس ،وبالرجوع إلى جريمة الابتزاز الإلكتروني فإن هذا الركن يمثل الإطار العملي للجريمة، ويتجلى في السلوك الإجرامي المتمثل في التهديد أو الضغط باستخدام الوسائل التكنولوجية بقصد حمل المجني عليه على القيام بفعل أو الامتناع عنه لتحقيق مصلحة غير مشروعة للجاني،[1]ويتكون الركن المادي في جريمة الابتزاز الإلكتروني من عدة عناصر مترابطة، وهي :السلوك الإجرامي ذاته، الوسيلة المستعملة، محل الجريمة، والعلاقة السببية بين الفعل والنتيجة.

1-السلوك الإجرامي:

يتمثل في ارتكاب الجاني لفعل مادي يرهب أو يضغط به على الضحية، مثل إرسال تهديد بنشر صور أو تسجيلات خاصة، أو التهديد بإفشاء معلومات حساسة ما لم يتم تنفيذ مطالب معينة. هذا التهديد قد يكون صريحا أو ضمنيا، لفظيا أو كتابيا، وغالبا ما يتم عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني أو الرسائل النصية، وقد يأخذ التهديد طابعا جنسيا أو ماليا أو أخلاقيا،حسب طبيعة الغرض الذي يسعى الجاني لتحقيقه، وفي القانون الجزائري نجد

[1]فتحي بودفلة، الإثبات في الجرائم الإلكترونية أمام القضاء الجزائي الجزائري، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 7، 2021، ص144.

أن هذا النوع من السلوك الإجرامي يجرم من خلال المادة 303مكرر 1 من قانون العقوبات، التي تجرّم تسجيل أو نشر صور أو أقوال أو معلومات دون رضا صاحبها، إذا تم ذلك بقصد الإضرار به أو ابتزازه، مما يُخرج الفعل من إطار المباح إلى دائرة المحظور.

2- الوسيلة المستعملة:

تعد الوسيلة من العناصر التي تمنح الجريمة وصفها "الإلكتروني، إذ تختلف عن الابتزاز التقليدي بكونها تتم باستعمال وسائل الاتصال الحديثة كالحواسيب، الهواتف الذكية، التطبيقات الرقمية، والبريد الإلكتروني، وغيرها من الوسائل الرقمية، ويشترط أن تتم هذه الأفعال في الفضاء الرقمي حتى تدرج ضمن فئة الجرائم السيبرانية ما يتطلب توافر الكفاءة التقنية في التحقيق وجمع الأدلة الرقمية، وهذا ما أكدته التعديلات التشريعية الأخيرة التي وسعت من نطاق التجريم ليشمل الجرائم المرتكبة عبر الوسائط التكنولوجية[1].

3- محل الجريمة:

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

4-العلاقة السببية:

وهي الرابط بين التهديد أو السلوك الإجرامي الذي قام به الجاني والنتيجة التي تحققت أو كانت متوقعة، كخضوع الضحية لرغبات الجاني أو تضررها نفسيا أو اجتماعيا، فالعبرة ليست

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

فقط بقيام الجاني بإرسال تهديد، بل بأن يكون ذلك التهديد قد شكل ضغطا فعليا على إرادة الضحية، وتقدر العلاقة السببية من خلال ظروف الواقعة وسياقها الاجتماعي والتقني ،وبذلك فإن الركن المادي في جريمة الابتزاز الإلكتروني يظهر الطابع المركب والمعقد لهذه الجريمة، لكونها ترتكز على عناصر مادية متعددة تمتزج فيها الوسائل التقنية مع الأفعال الجرمية التقليدية،وهو ما يتطلب من الجهات القضائية والأمنية تدريبا خاصا وتقنيات دقيقة لرصد السلوك الإجرامي الرقمي، وجمع الأدلة التقنية بطريقة قانونية[1].

الفرع الثاني : الركن المعنوي .

الركن المعنوي في جريمة الابتزاز الإلكتروني يعتبر أساس المسؤولية الجنائية، ولا يمكن إدانة الجاني ما لم يثبت أن فعله قد صدر عن إرادة حرة وعن نية تهدف إلى الإضرار بالغير أو ابتزازه، وتكمن خطورته في أنه غالبا ما يمارس عن بعد وفي بيئة رقمية تخفي شخصية الجاني، مما يفرض على القضاء والخبراء التقنيين بذل جهود مضاعفة للكشف عن نية الإجرام الرقمي وتقديم الدليل القاطع على توفر القصد الجنائي[2].

يمثل الركن المعنوي القصد الجنائي البعد الذهني أو النفسي للجريمة، ويعبر عن الإرادة الحرة الواعية التي تصدر عن الجاني لارتكاب فعل غير مشروع يجرمه القانون ،ويختلف هذا الركن عن الركن المادي الذي يتجسّد في فعل خارجي ملموس، إذ يركز على النية الداخلية أو الدافع الذهني الذي حرّك الجاني نحو ارتكاب السلوك الإجرامي،وفي جريمة الابتزاز الإلكتروني يعد القصد الجنائي أحد أهم أركان التجريم، لأنه يميز الفعل الجرمي عن الأفعال المباحة التي قد تشابهها في الشكل مثل نشر معلومة على شبكة رقمية، لكنه يختلف عنها في الغاية والمقصد.

[1] نور الدين زروقي، الجريمة الإلكترونية في التشريع الجزائري: الطبيعة والأركان والجزاءات، دار العلوم للنشر والتوزيع، الجزائر، 2022، ص212.

[2] ربيعة خريس، الجرائم الإلكترونية في التشريع الجزائري ، دراسة تحليلية مقارنة، دار هومة، الجزائر، 2020، ص137.

أولا–مفهوم القصد الجنائي في الابتزاز الإلكتروني:

وفقا للنظرية العامة للقانون الجزائي يتكون القصد الجنائي من عنصرين أساسيين:

أ–العنصر الإدراكي (العلم): أي علم الجاني بطبيعة فعله ونتائجه المحرمة.

ب–العنصر الإرادي (الإرادة): أي توجّه إرادته نحو ارتكاب الفعل مع قبوله للنتائج الجرمية.

في الابتزاز الإلكتروني، يتحقق هذا القصد عندما يعلم الجاني:

–بأنه يقوم بتهديد الضحية أو الضغط عليها عبر وسائل رقمية.

–وبأن الفعل الذي يرتكبه مخالف للقانون ومساس بحرمة الحياة الخاصة.

–ثم يتجه قصده الإرادي نحو استخدام ذلك السلوك للحصول على فائدة أو منفعة مادية، جنسية، معنوية ،بالتالي فالقصد هنا ليس مجرد تهديد عبثي، بل تهديد هادف إلى الإضرار بالضحية أو إجبارها على القيام بفعل معين، وهو ما يضفي على الركن المعنوي طابعا خاصا يميزه عن مجرد النية السيئة أو الغضب العابر[1].

ثانيا–طبيعة القصد الجنائي في القانون الجزائري:

يندرج الابتزاز الإلكتروني ضمن طائفة الجرائم العمدية، التي لا يمكن تحققها إلا بقصد جنائي، ولا يكفي فيها الخطأ أو الإهمال أو الرعونة. فالمادة 303مكرر 1 من قانون العقوبات تشترط صراحة أن يكون الهدف من تسجيل أو نشر أو إرسال المحتوى هو: الإضرار بالضحية، أوحملها على القيام بفعل أو الامتناع عنه أي ابتزازها، أوالمساس بكرامتها أو خصوصيتها.

ومن هنا، فإن القصد المطلوب في هذه الجريمة هو قصد خاص ، أي أن يكون لدى الجاني نية محددة لتحقيق غرض معين لا يكفي فيها مجرد القصد العام إرادة الفعل وعلمه فقط

[1] لمياء رحماني، الجرائم المستحدثة في ظل تطور تكنولوجيا الإعلام والاتصال: الابتزاز الإلكتروني نموذجا، مجلة العدالة والقانون، جامعة سعيدة، العدد 14، جوان 2022، ص112.

ويعد هذا النوع من القصد أكثر دقة وتحديدا، ويستلزم من القاضي التأكد من نية الإضرار أو التهديد أو تحقيق غرض ابتزازي، لا مجرد تنفيذ الفعل التقني بحد ذاته[1].

ثالثا–وسائل إثبات الركن المعنوي:

نظرا لكون الركن المعنوي عنصرا داخليا نفسيا لا يلمس بالحواس، فإنه يستدل عليه بالقرائن والظروف المحيطة بالفعل، مثل:

–طبيعة الرسائل التي أرسلها الجاني كلهجة التهديد، الطلبات، الأسلوب.

–تكرار الاتصالات أو متابعة الضحية على منصات مختلفة.

–وجود مقابل مشروط طلب مال، صور إضافية، علاقة غير شرعية، سكوت عن فضيحة.

–سوابق العداء أو المعرفة السابقة بين الطرفين.

وقد يلجأ القاضي أيضا إلى التحليل الفني للأدلة الرقمية لاستخلاص النية الإجرامية، مثل تتبع مصدر الرسائل، وتوقيت إرسالها، وربطها بتصرفات الضحية كالتبليغ أو التحويل المالي.

رابعا–القصد الاحتمالي والقصد الاحتيالي:

في بعض الحالات، يكون القصد الجنائي احتماليا، أي أن الجاني لا يسعى بالضرورة لتحقيق النتيجة (كالنشر الفعلي)، لكنه يقبل باحتمال وقوعها، كأن يقول للضحية: ربما أنشر صورك إذا لم ترضي طلبي، وهذا يكفي لتكوين القصد الجنائي في الابتزاز خاصة إذا أظهر تكرار التهديد وجود نية مستمرة للإخضاع.

وفي حالات أخرى يتخذ القصد الجنائي طابعًا احتياليا، عندما يستخدم الجاني هوية وهمية أو حسابا مزيفا لاستدراج الضحية وجمع معلومات ثم تهديدها بها، وهو ما يبرر في بعض الأحيان الجمع بين جريمة الابتزاز وجرائم أخرى كالنصب أو انتحال الهوية.

[1] فتحي بودفلة، الإثبات في الجرائم الإلكترونية أمام القضاء الجزائي الجزائري، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 7، 2021، ص 144.

المطلب الثاني : ضبطية جريمة الابتزاز الالكتروني .

تشكل ضبطية جريمة الابتزاز الإلكتروني إحدى أهم الإشكالات الإجرائية التي تواجه الجهات القضائية والأمنية في الجزائر، نظراً للطبيعة التقنية لهذه الجريمة وارتباطها بالفضاء السيبراني، الذي غالبا ما يتجاوز النطاق الجغرافي للدولة، ويدار عبر أدوات وتطبيقات يصعب تتبعها بسهولة.

فالابتزاز الإلكتروني يُرتكب عادة من خلال وسائل التواصل الاجتماعي أو البريد الإلكتروني أو التطبيقات المشفرة، ما يستوجب تدخلًا تقنيا متخصصا من قبل وحدات الشرطة القضائية المكلفة بمكافحة الجرائم المعلوماتية التي تتولى مهمة تعقب الآثار الرقمية كعناوين الـ IPومصدر الرسائل وسجلات الاتصالات الإلكترونية، وتخضع إجراءات ضبط هذه الجريمة لأحكام قانون الإجراءات الجزائية، لاسيما المواد من 65 مكرر إلى 65 مكرر 18، التي تسمح بالتفتيش الإلكتروني وحجز الوسائط الرقمية بإذن من وكيل الجمهورية أو قاضي التحقيق مع ضمان احترام الحياة الخاصة وحقوق الأفراد في إطار الشرعية الإجرائية ،[1]كما تعد الخبرة التقنية أداة لا غنى عنها في كشف هوية الجاني خاصة إذا استخدمت تقنيات الإخفاء أو الحسابات الوهمية، مما يدفع الجهات القضائية للاستعانة بمخابر التحليل الرقمي والخبراء المختصين،[2] وقد عرفت الجزائر تطورا في البنية المؤسساتية لمواجهة هذه الجرائم، من خلال استحداث فرق مختصة ضمن جهاز الأمن الوطني والدرك الوطني، فضلا عن الدور الذي تلعبه الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، التي تقدم دعما فنيا وتحليليا للقضايا ذات الصلة،ورغم هذا التقدم ما تزال هناك جملة من العراقيل التي تعيق الضبط الفعّال لهذه الجريمة، من أبرزها ضعف التبليغ من قبل الضحايا خاصة في حالات الابتزاز الجنسي، ونقص التكوين التقني المتخصص لدى بعض الأعوان، وصعوبة

[1]قانون الإجراءات الجزائية الجزائري، المواد 65 مكرر إلى 65 مكرر 18، الأمر رقم 66-155 المؤرخ في 8 جوان 1966، المعدل والمتمم.

[2]سامي بوعزيز، التحقيق في الجرائم الإلكترونية: بين النص القانوني والواقع العملي، مجلة دفاتر القانون، جامعة وهران، العدد 15، 2022، ص93.

الحصول على تعاون دولي في حال ارتُكبت الجريمة من الخارج، ولعل من أبرز التوصيات لتجاوز هذه العراقيل، تحديث الإمكانات التقنية للشرطة القضائية، وتكثيف التكوين المتخصص للقضاة والمحققين، فضلا عن ضرورة إدراج ثقافة الأمن الرقمي في المجتمع، وتوفير آليات فعالة لحماية ضحايا هذه الجرائم وتيسير التبليغ عنها. [1]

أولا- مفهوم الضبطية القضائية في الجرائم الإلكترونية:

يقصد بالضبطية القضائية في الجرائم الإلكترونية الإجراءات التي تتخذها الضبطية القضائية الشرطة القضائية تحت إشراف النيابة العامة لضبط الفعل الجرمي وجمع الأدلة، والقبض على المشتبه فيه، وفقا لما تقرره قواعد الإجراءات الجزائية مع مراعاة الخصوصية التقنية للجرائم التي ترتكب باستعمال الوسائل التكنولوجية الحديثة.

ثانيا-خصوصيات ضبط الابتزاز الإلكتروني:

أ-الطبيعة الخفية للجريمة الابتزاز الإلكتروني غالباً ما يتم عبر تطبيقات التواصل الاجتماعي، أو البريد الإلكتروني، أو برامج مشفرة، ويستعمل فيها الجاني حسابات وهمية أو أدوات إخفاء الهوية(VPN – Tor) ، مما يصعب من مهمة كشفه، وهنا تكتسي الخبرة التقنية أهمية كبيرة في تحديد مصدر الرسائل، وتتبع أثرها الرقمي[2].

ب- سرعة التبليغ والاستجابة الأمنية كلما تم التبليغ عن الابتزاز مبكرا زادت فرص الحصول على الأدلة قبل حذفها من قبل الجاني أو قبل أن يتفاقم الضرر بالضحية، لذلك شددت النيابات العامة في الجزائر على أهمية التبليغ الإلكتروني الفوري لدى فرق مكافحة الجرائم السيبرانية.

ج-إجراءات التفتيش والحجز الإلكتروني تتم عمليات التفتيش الرقمي طبقا للمادة 65 مكرر من قانون الإجراءات الجزائية، التي تسمح لوكيل الجمهورية أو قاضي التحقيق بتفتيش الأجهزة

[1] عبد القادر بن يوسف، الضبطية القضائية في مكافحة الجريمة المعلوماتية، دار الخلدونية، الجزائر، 2020، ص65.
2بوحنية قوي، الجرائم الإلكترونية وآليات التصدي لها في الجزائر، مجلة القانون والمجتمع، جامعة تلمسان، العدد 10، 2021، ص104.

الرقمية، والحصول على محتويات الحسابات الإلكترونية بعد ترخيص قانوني، شرط احترام خصوصية الأفراد.

ح-الاستعانة بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهي هيئة تابعة لوزارة الداخلية، تملك صلاحيات في التحقيق والتحليل الرقمي الجنائي، ومساعدة الجهات القضائية في تتبع وحماية الضحايا.

الفرع الاول : المسؤولية الجنائية للشخص الطبيعي.

إن المشرع الجزائري راعى أن الشخص الطبيعي يمكن أن يتقمص أدوارا متعددة في تنفيذ جريمة الابتزاز الإلكتروني، فقد يكون الفاعل الأصلي، أو المحرّض، أو حتى مجرد مساهم في تسهيل تنفيذ الفعل، مما يستدعي تطبيق القواعد العامة للمساهمة الجنائية المنصوص عليها في المواد 41 و42 من قانون العقوبات، وتتسع دائرة المسؤولية الجنائية في هذا السياق لتشمل أيضًا الأفعال التي تُرتكب خارج النطاق الزمني أو المكاني المباشر للجريمة، مثل التحريض على إرسال صور خاصة أو تسريب معلومات شخصية، طالما ثبتت العلاقة السببية بين تلك الأفعال وتحقيق النتيجة الإجرامية، كما أن نية الجاني والتي تُشكّل العنصر الجوهري في الركن المعنوي لا يشترط إثباتها من خلال اعتراف صريح، بل يكفي أن تستخلص من مجمل ظروف القضية كطريقة التهديد والمطالب الموجهة للضحية، وطبيعة المحتوى المستخدم في الابتزاز، وهو ما تؤكده الاجتهادات القضائية التي اعتمدت على قرائن تقنية مثل تحليل مضمون الرسائل الرقمية وتوقيت إرسالها وسجلات الدخول إلى الحسابات الإلكترونية.[1]

وعلى المستوى العملي لوحظ أن أغلب الجناة في قضايا الابتزاز الإلكتروني من فئة الشباب، ممن لديهم إلمام تقني متوسط أو متقدّم، ويستغلون الثغرات القانونية أو ضعف الوعي لدى الضحايا، ما يجعل من الضروري، إلى جانب تجريم الفعل، التأكيد على الطابع الشخصي للمسؤولية الجنائية، بحيث لا يمكن للمسؤولية أن تُنقل إلى شخص آخر، سواء بالنيابة أو

[1] عبد الكريم بن عربية، شرح قانون العقوبات القسم العام، ديوان المطبوعات الجامعية، الجزائر، 2019، ص121.

التمثيل، كما تلزم المادة 51 من قانون العقوبات القاضي عند النطق بالحكم بتحديد شخصية الجاني وصفته بدقة، وبيان الأسباب التي حملته على ارتكاب الجريمة، وخاصة في القضايا التي يحتمل فيها وجود دافع انتقامي أو استغلالي ،وتزداد حدة المسؤولية الجنائية متى ارتبط الفعل الابتزازي بانتهاك الخصوصية المعلوماتية، وهو ما يُعد ظرفًا مشددا في بعض القضايا، وفق ما أقرته بعض المحاكم التي رأت أن تسريب صور الضحية أو التهديد بنشرها يعد مساسا مباشرًا بالحق الدستوري في حماية الحياة الخاصة، والمكرّس في المادة 58 من دستور 2020.

ومن ثم فإن المسؤولية الجنائية للشخص الطبيعي في جريمة الابتزاز الإلكتروني لا تقتصر على مجرد الفعل المادي للتهديد، بل تمتد لتشمل كل شكل من أشكال التدخل العمدي الواعي الذي يفضي إلى المساس بحقوق الآخرين الرقمية أو النفسية، وتقتضي أحكامًا عقابية تتناسب مع جسامة السلوك الإجرامي، بما يحقق الردع ويكرس مبدأ المسؤولية الفردية في ظل المجتمع الرقمي المتحوّل[1].

وتتحقق المسؤولية الجنائية للشخص الطبيعي في هذا الإطار إذا ثبت أنه تعمد استعمال وسيلة إلكترونية بقصد الحصول على منافع مادية أو معنوية من الغير، مقابل الامتناع عن نشر محتوى معين يخص الضحية، وهو ما يدخل ضمن مفهوم الابتزاز، ويشترط في الفاعل أن يكون متمتعًا بالإدراك والتمييز وقت ارتكاب الفعل، أي أنه لا يعاني من عذر مانع للمسؤولية كالجنون أو الإكراه الملجئ، وتشدد العقوبة إذا كانت الوسيلة المستعملة فيها تهديد بالمساس بالحياة الخاصة أو بنشر صور حميمية، أو إذا كانت الضحية قاصرا أو في حالة ضعف.

كما أن المسؤولية لا تنتفي في حال ارتكبت الجريمة عبر حساب مزيف أو باستخدام أجهزة الغير، طالما ثبت أن الشخص الطبيعي هو من قام بالفعل الجرمي بنفسه أو شارك فيه بتحريض أو اتفاق، وقد وسّع الاجتهاد القضائي في الجزائر من مفهوم المساهمة الجنائية في

[1] كبابسة فاطمة الزهراء،التكييف القانوني للجريمة المعلوماتية في ضوء قانون العقوبات الجزائري،أطروحة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2020/2019 ،ص 53.

هذا النوع من الجرائم، فاعتبر أن مجرد تواطؤ شخص في تسهيل الفعل الإلكتروني مثل تزويد الجاني بمحتوى خاص أو المساعدة في إنشاء حساب مزيف يمكن أن يرتب مسؤوليته كشريك.

وبالرجوع إلى أحكام المادة 42 من قانون العقوبات فإن الشخص الطبيعي يسأل جنائيا بصفته فاعلاً أصليًا أو شريكا، وتُطبق عليه العقوبات المقررة حسب جسامة الجريمة. ويشمل ذلك الحبس والغرامة فضلا عن العقوبات التكميلية كحظر الاتصال بالضحية أو مراقبة إلكترونية، حسب ما تراه المحكمة مناسبا لتحقيق الردع العام والخاص، ولضمان فعالية المسؤولية الجنائية في هذا المجال، يجب أن تواكبها حماية قانونية متوازنة للضحايا، واستراتيجية وطنية للتوعية بمخاطر الابتزاز الرقمي بما يضمن شمولية المنظومة الجنائية في مواجهة هذه الجريمة المعاصرة[1].

الفرع الثاني : المسؤولية الجنائية للشخص المعنوي.

الجرائم الإلكترونية أصبحت تشكل تهديدا حقيقيا للأفراد والمجتمعات والدول على حد سواء ومن بين هذه الجرائم، برزت جريمة الابتزاز الإلكتروني كأحد أخطر أشكال التعدي على حرية الأفراد وسريتهم وكرامتهم، حيث يستغل الجاني الوسائط التقنية لابتزاز الضحية ماديا أو معنويا، من خلال تهديده بنشر بيانات أو صور أو معلومات خاصة.

وإذا كانت هذه الجريمة ترتكب غالبا من طرف أشخاص طبيعيين، فإن الممارسة أثبتت إمكانية تورط أشخاص معنويين كالشركات أو الهيئات في تسهيل أو تنظيم هذا النوع من الجرائم، سواء بصورة مباشرة أو غير مباشرة، مما يثير التساؤل حول مدى إمكانية مساءلة الشخص المعنوي جزائيا عن هذه الجريمة في ظل التشريع الجزائري.

[1] عكوش سيهام، الحماية القانونية لحق الخصوصية من جريمة التهديد عرب مواقع التواصل الاجتماعي وفقا للقانون الجزائري، مجلة السياسة العالمية، الصادرة عن مخبر الدراسات السياسية والدولية بجامعة احمد بوقرة بومرداس، المجلد 06،العدد1،الجزائر، سنة2022،ص 25.

أصبحت مسألة المسؤولية الجنائية للشخص المعنوي من بين الإشكاليات القانونية التي فرضت نفسها على الساحة الفقهية والتشريعية، خاصة في ظل التطورات التكنولوجية المتسارعة التي أنتجت أنماطا جديدة من الجرائم، وفي مقدمتها الجرائم الإلكترونية، وقد فرضت هذه التطورات مراجعة العديد من المفاهيم الكلاسيكية في القانون الجنائي، ومنها ارتباط المسؤولية الجزائية بالفعل الإجرامي الصادر عن الإرادة الذاتية لشخص طبيعي، ذلك أن النشاط الإجرامي لم يعد حكرًا على الأفراد الطبيعيين فقط، بل أصبح من الممكن أن يتخذ طابعا منظما يتم عبر كيانات قانونية منظمة، مثل الشركات والمؤسسات، التي قد تستغل أو توظف في ارتكاب جرائم باستخدام الوسائل الإلكترونية، ومن بينها جريمة الابتزاز الإلكتروني.

في هذا الإطار، أقرّ المشرع الجزائري بموجب التعديلات التي أدخلها على قانون العقوبات لاسيما من خلال المادة 51 مكرر وما يليها بإمكانية مساءلة الشخص المعنوي جنائيا، عندما ترتكب جريمة باسمه أو لحسابه أو لفائدته من قبل أحد ممثليه أو أحد أعضائه أو حتى من خلال أحد موظفيه، وذلك شريطة أن يكون الفعل قد تم في إطار ممارسة نشاطه وتحت إشرافه أو بتقصير منه في الرقابةن وتأسيسا على ذلك، يمكن القول إن الشخص المعنوي لا يسأل عن الفعل الإجرامي بصفة آلية، بل يشترط لقيام مسؤوليته توافر علاقة سببية بين الجريمة المرتكبة ومصلحة الشخص المعنوي، أو ثبوت تقصير في منظومة الرقابة الداخلية لديه[1].

وتتجلى خطورة هذا النوع من المسؤولية في جريمة الابتزاز الإلكتروني تحديدًا، عندما تكون البنية التحتية الرقمية للشخص المعنوي كالمواقع الإلكترونية، أو قواعد البيانات، أو وسائل الاتصال الداخلية هي الوسيلة التي استغلت لارتكاب الجريمة، أو عندما يتم ذلك بعلم القائمين على الإدارة أو بسبب تغاضيهم. بل إن بعض الكيانات القانونية قد تنخرط بصورة غير مباشرة في مثل هذه الجرائم، عبر توفير خدمات تُستخدم لاحقا في الابتزاز، مثل استضافة مواقع غير آمنة أو تجاهل بلاغات الضحايا بشأن محتوى مضر منشور ضمن نطاق نشاطهم في هذه الحالات، لا يمكن القول إن الشخص المعنوي مجرد أداة محايدة، بل يصبح طرفا مسؤولًا عن

[1] عكوش سيهام،المرجع السابق،ص 66.

النتائج المترتبة على هذا الفعل، وقد تطاله العقوبات المنصوص عليها قانونا، والتي تشمل الغرامات، المنع من النشاط وحتى الحل النهائي في بعض الحالات الجسيمة.

ويعد إقرار المسؤولية الجنائية للشخص المعنوي عن مثل هذه الجرائم خطوة مهمة في مواكبة التطور التقني، وتأكيدا على أن الكيانات القانونية مطالبة، ليس فقط بعدم الانخراط في أفعال إجرامية، بل أيضا باتخاذ كافة التدابير التقنية والإدارية لمنع استخدام بنيتها في ارتكابها.[1] فالمطلوب من الشخص المعنوي اليوم أن يظهر حسن النية الإجرائية من خلال اعتماد سياسات حماية إلكترونية فعالة، وتدريب الموظفين وتطبيق آليات الرقابة الداخلية، وتقديم التعاون مع السلطات المختصة، وإذا ما أخل بهذه الالتزامات أو سكت عن أفعال تشكل جريمة ابتزاز إلكتروني، فإنه لا يمكن التذرع بغياب الإرادة الجزائية الذاتية خاصة في ظل التأكيد التشريعي الواضح على أن الشخصية القانونية لا تعفي من الجزاء الجنائي.

[1] التواتي نوال، الابتزاز الإلكتروني ووسائل مكافحته في ظل التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة بسكرة، 2022/2021 ، ص66.

الفصل الثاني :

الاليات القانونية لمكافحة جريمة الابتزاز الالكتروني.

إلى جانب البنية القانونية الصلبة التي وضعها المشرع الجزائري تلعب الآليات الوقائية دورا أساسيًا في التصدي لجريمة الابتزاز الإلكتروني، وتتمثل هذه الآليات في مجموعة من التدابير الإدارية والتقنية التي تهدف إلى تجفيف منابع هذه الجريمة، من خلال مراقبة الفضاء السيبراني، وإطلاق حملات التوعية الرقمية، وإنشاء منصات للإبلاغ الفوري عن الجرائم الإلكترونية، وقد قامت مصالح الأمن الوطني والدرك الوطني بإطلاق مواقع إلكترونية وتطبيقات مخصصة لتلقي الشكاوى المتعلقة بالجرائم الإلكترونية، بما فيها الابتزاز وهو ما يشجع الضحايا على التبليغ ويسهل من مهام التحري والمتابعة.

وتبرز الآليات الإجرائية كركيزة محورية في مكافحة الابتزاز الإلكتروني، حيث أجاز القانون لقاضي التحقيق والضبطية القضائية، في إطار الجرائم المرتكبة باستعمال تكنولوجيا المعلومات، استخدام وسائل خاصة كاعتراض الاتصالات الإلكترونية، ومراقبة الحسابات الرقمية، والاطلاع على المراسلات، وذلك شريطة احترام الضمانات القانونية والإذن القضائي المسبق، كما نص عليه القانون رقم 07-17 المعدل لقانون الإجراءات الجزائية، وهذا التمكين الإجرائي يُعتبر تحولاً نوعيًا في تحقيق التوازن بين مقتضيات الأمن الرقمي والحريات الفردية[1].

أما على مستوى الآليات الجزائية فقد تم تكريس نظام عقابي صارم لمواجهة هذا النوع من الجرائم فنظرا لخطورة الابتزاز الإلكتروني، الذي قد يمس بالحياة الخاصة أو يؤدي إلى أضرار نفسية جسيمة للضحايا، خصوصا النساء والقصر، فقد شدد المشرع العقوبات المنصوص عليها في هذا الإطار، واعتبرها من الجرائم الماسة بحرمة الحياة الخاصة، والتي لا تسقط بالتقادم في بعض الحالات، وهو ما يظهر من خلال تكييف الجريمة على ضوء المادة 303 مكرر وما يليها من قانون العقوبات.

---

[1] بن شيخ، سليم، حماية ضحايا الابتزاز الإلكتروني في القانون الجزائري، مجلة القضاء والسياسة، جامعة تلمسان، العدد 14، 2022، ص89.

وتعتبر الحماية القضائية للضحايا من بين الآليات المهمة كذلك حيث يمكن للضحية بموجب القانون طلب إجراءات حمائية مستعجلة، مثل حجب المحتوى المبتز، أو إصدار أوامر قضائية لحذف الصور أو التسجيلات المستخدمة في الابتزاز، كما أن للنيابة العامة سلطة التحرك تلقائيًا إذا تعلق الأمر بمصلحة قاصر أو بمساس بالنظام العام، كما يمكن للضحية المطالبة بتعويض عن الضرر المادي والمعنوي وفق قواعد المسؤولية المدنية أمام القضاء الجزائي.

ولا يمكن الحديث عن مكافحة فعالة لجريمة الابتزاز الإلكتروني دون التطرق إلى الآليات الدولية للتعاون القضائي، نظرًا للطبيعة العبر–وطنية لهذه الجريمة، وقد انضمت الجزائر إلى عدد من الاتفاقيات الدولية ذات الصلة، أبرزها اتفاقية بودابست لسنة 2001 المتعلقة بالجريمة الإلكترونية، وهي الاتفاقية المرجعية عالميا في هذا المجال، والتي تنص على ضرورة تبادل المعلومات وتنسيق التحقيقات، وتنفيذ الإنابات القضائية الدولية بسرعة وفعالية[1].

وبالتالي فإن مجمل هذه الآليات القانونية التشريعية، الإجرائية، الوقائية، والعقابية تعكس سعي المشرّع الجزائري إلى وضع منظومة قانونية شاملة تتماشى مع طبيعة الجريمة الإلكترونية وخطورتها، وعلى رأسها جريمة الابتزاز، لكنها تظل بحاجة دائمة إلى تحديث وتطوير مستمرين لمواكبة تطور الوسائل التقنية المستعملة في ارتكاب هذه الأفعال.

[1] فاطمة الزهراء رياحي،التحقيق في الجرائم المعلوماتية بين مقتضيات الواقع ونص القانون، مجلة الدراسات القانونية والسياسية، جامعة تبسة، العدد 8، 2021،ص 86.

المبحث الاول : اجراءات التحقيق الخاصة بجريمة الابتزاز الالكتروني .

أدى التطور السريع في وسائل التكنولوجيا الرقمية إلى ظهور أنماط إجرامية مستحدثة، من أبرزها جريمة الابتزاز الإلكتروني، التي تتميز بكونها خفية، عابرة للحدود، وصعبة الإثبات وللحد من خطورتها، أصبح من الضروري تطوير آليات التحقيق بما يتلاءم مع طبيعة هذه الجريمة، التي تختلف عن الجرائم التقليدية من حيث وسيلة ارتكابها وأثرها، وقد استجابت المنظومة القانونية الجزائرية لهذا التحدي من خلال تكريس إجراءات خاصة في مجال التحقيق، تراعي الطبيعة التقنية للجرائم المعلوماتية، وتمنح جهات التحري صلاحيات أوسع، كاعتراض الاتصالات الإلكترونية، ومراقبة المواقع والحسابات، مع إخضاع هذه الإجراءات لشروط قانونية تضمن حماية الحقوق والحريات الأساسية،[1] ويهدف هذا المبحث إلى إبراز الإطار القانوني لهذه الإجراءات، وبيان مدى فعاليتها في التصدي لجريمة الابتزاز الإلكتروني،و منه سوف نتعرف على هذه الإجراءات من خلال المطلب الموالي .

المطلب الاول : اجراءات التحقيق في جريمة الابتزاز الالكتروني .

تعد جريمة الابتزاز الإلكتروني من الجرائم المعقدة التي تتطلب تعاملا دقيقا من حيث إجراءات التحري والتحقيق، نظرا لطبيعتها التقنية واعتمادها على وسائل الاتصال الرقمية التي قد تنفذ من خارج الحدود الجغرافية التقليدية، وقد استوجب هذا الواقع من المشرّع تكييف القواعد الإجرائية الكلاسيكية مع خصوصيات الجريمة الإلكترونية، من خلال اعتماد إجراءات تحقيق خاصة تتيح للجهات القضائية والضبطية وسائل فعالة لملاحقة مرتكبي هذا النوع من الجرائم، دون الإخلال بالضمانات القانونية الممنوحة للأفراد، وتشمل هذه الإجراءات وسائل حديثة مثل اعتراض المراسلات الإلكترونية، ومراقبة نظم المعلومات، والتتبع الرقمي، وغيرها من الآليات

[1] فاطمة الزهراء رياحي،المرجع السابق،ص 66.

التي تم تكريسها صراحة في قانون الإجراءات الجزائية الجزائري، لاسيما بعد التعديلات التي أقرها القانون 07-17[1].

أولا-صور إجراءات التحقيق الخاصة في جريمة الابتزاز الإلكتروني:

أ-اعتراض المراسلات والاتصالات الرقمية:

1-المقصود باعتراض المراسلات.

2-شروطه وضوابطه القانونية.

3-تطبيقه في قضايا الابتزاز عبر البريد الإلكتروني ووسائل التواصل.

ب- المراقبة الإلكترونية للأشخاص والأنظمة المعلوماتية:

1-تقنيات التتبع الرقمي.

2-مراقبة الحسابات والبريد والمكالمات عبر التطبيقات.

3-مراقبة المواقع المشبوهة أو المغلقة.

ج-التفتيش الإلكتروني وضبط الأدلة الرقمية:

1-مفهوم التفتيش المعلوماتي.

2-ضوابط حجز الأجهزة والوسائط.

3-إثبات الجريمة من خلال البيانات المحجوزة.

[1]القانون رقم 07-17 المؤرخ في 27 مارس 2017، المتضمن تعديل وإتمام قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 21 لسنة 2017.

تعد إجراءات التحقيق الخاصة أداة فعالة لمكافحة جريمة الابتزاز الإلكتروني، لكنها تبقى ذات طابع استثنائي يتطلب التزامًا صارما بالشروط القانونية، حتى لا تتحول من وسيلة لحماية المجتمع إلى تهديد للحقوق والحريات الدستورية،ومن هنا تظهر أهمية التكوين المستمر للقضاة وضباط الشرطة القضائية في مجال التقنيات الحديثة والتحقيق الرقمي، بما يضمن حسن تطبيق النصوص القانونية وتحقيق العدالة الرقمية المنشودة.

الفرع الاول : الاجهزة المكلفة بالبحث و التحري .

نظرا لطبيعة جريمة الابتزاز الإلكتروني التي تتسم بالغموض والتعقيد، نظراً لاعتمادها على أدوات التكنولوجيا الحديثة، برزت الحاجة الملحة إلى تكليف جهات مختصة تتمتع بالخبرة الفنية والسلطة القانونية للقيام بأعمال البحث والتحري في هذا النوع من الجرائم، وقد استجاب المشرّع الجزائري لهذه الضرورة من خلال إسناد هذه المهام إلى جهات أمنية وقضائية معينة، تتمتع بالصلاحيات القانونية والتقنية التي تؤهلها للتعامل مع الجريمة المعلوماتية بوجه عام، وجريمة الابتزاز الإلكتروني بوجه خاص، وتتوزع هذه الجهات ما بين هيئات شرطية متخصصة، وأجهزة قضائية، وهيئات تنسيق وطنية تعمل مجتمعة ضمن إطار قانوني محدد يهدف إلى ضمان الفعالية من جهة، وحماية الحقوق من جهة أخرى.

أولا-الأجهزة المكلفة بالبحث والتحري في جريمة الابتزاز الإلكتروني:

يُناط بالبحث في جريمة الابتزاز الإلكتروني عدة جهات رسمية، تتكامل أدوارها وتنسق فيما بينها وفقًا لما ينص عليه قانون الإجراءات الجزائية، والقوانين ذات الصلة بمكافحة الجريمة الإلكترونية. وتأتي في مقدمة هذه الأجهزة[1]:

أ-الشرطة القضائية المختصة في الجرائم السيبرانية: وهي مصالح تابعة للأمن الوطني والدرك الوطني، تضم وحدات تقنية متخصصة في ميدان مكافحة الجرائم المعلوماتية، وقد تم

[1] عصام المكي، الإثبات الجنائي بالوسائل العلمية الحديثة في التشريع الجزائري، لنيل مذكرة الماستر، قسم العلوم السياسية، جامعة عبد الحميد ابن باديس/ مستغانم، سنة2017/2016 ،ص 49.

إنشاء فرق خاصة بمكافحة الجريمة السيبرانية على مستوى المديريات الولائية للأمن الوطني، وتزويدها بوسائل رقمية حديثة، وخبرات بشرية مؤهلة في مجال تحليل الأدلة الرقمية، تتولى مهام التحري في الجرائم المرتكبة عبر وسائل الاتصال التكنولوجي، بما فيها الابتزاز الإلكتروني[1].

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

ج-النيابة العامة: باعتبارها صاحبة السلطة في تحريك الدعوى العمومية، تشرف مباشرة على أعمال البحث والتحري، وتصدر أوامرها للضبطية القضائية في إطار المادة 36 من قانون الإجراءات الجزائية، كما أن لها صلاحية إصدار الأذون الخاصة باعتراض الاتصالات وتفتيش الأجهزة، وتحرير الإنابات القضائية على المستويين الوطني والدولي.

د-قاضي التحقيق: الذي يلعب دورا محوريا في حالة ما إذا تم فتح تحقيق قضائي، حيث يتولى الإشراف على الإجراءات الخاصة المنصوص عليها في المواد المستحدثة بموجب القانون 07-17، كاعتراض المراسلات الإلكترونية، ومراقبة المواقع، والاطلاع على محتوى الحسابات الرقمية، شريطة توافر مبررات قانونية جادة.

هـ-الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي: وإن لم تكن جهازا تحقيقيا بالمعنى التقليدي، إلا أن لها دورًا وقائيا واستشاريا، خصوصا في مراقبة مدى احترام قواعد حماية الحياة الخاصة في سياق الجرائم المعلوماتية، وقد تساهم في الإبلاغ أو تقديم تقارير في حال وقوع ابتزاز إلكتروني يتضمن انتهاكا للخصوصية.

[1] سليماني علاء الدين، دور الشرطة في اثبات الجريمة، لنيل مذكرة الماستر، حقوق تخصص والعلوم السياسية، جامعة خيضر، سنة 2014/2013 ،ص 78.

و-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: المنشأة بموجب القانون رقم 18-04، والتي تسعى إلى تنسيق الجهود بين الأجهزة المختلفة، وتقديم الدعم الفني والمعلوماتي للجهات القضائية والأمنية.

ويعزز دور هذه الأجهزة من خلال التعاون الدولي مع هيئات إنفاذ القانون الأجنبية، ولا سيما عبر INTERPOL و Europolوالمنظمات الإقليمية، في الحالات التي يرتكب فيها الابتزاز من خارج التراب الوطني أو عبر منصات أجنبية، مما يتطلب آليات قانونية خاصة كطلب المساعدة القضائية أو الإنابة الدولية.

وهكذا فإن تعدد الأجهزة المكلفة بالتحري والبحث في جريمة الابتزاز الإلكتروني يعكس وعي الدولة بخطورة هذه الجريمة وتطورها المستمر، كما يدل على محورية التنسيق المؤسساتي والتكوين التكنولوجي المستمر كشرطين أساسيين لفعالية المكافحة[1].

إلى جانب الأدوار القانونية التي تضطلع بها الأجهزة الأمنية والقضائية، تكتسي المهارات التقنية والتجهيزات الرقمية أهمية بالغة في فعالية تدخل هذه الجهات، لاسيما في ظل الطبيعة المعقدة التي تتسم بها جريمة الابتزاز الإلكتروني، والتي تعتمد على تقنيات مثل إخفاء الهوية (VPN) استخدام الخوادم الوهمية(Proxies) ، أو التشفير الطرفي للمحادثات .

لذلك سعت مصالح الأمن الوطني إلى إنشاء خلايا خاصة على مستوى المديرية العامة، تضم مهندسين ومحللين في أمن المعلومات، ومختصين في الأدلة الجنائية الرقمية يتكفلون بتحليل أجهزة الحاسوب، الهواتف، وسجلات السيرفرات، لاستخراج الأدلة الرقمية الصالحة للاستغلال القضائي، كما يتم تكوين ضباط الشرطة القضائية بشكل مستمر في مجال تقنيات التتبع الإلكتروني واسترجاع البيانات.

[1] سليماني علاء الدين،المرجع السابق،ص 99.

في المقابل، يعمل الدرك الوطني على تعزيز فعالية وحداته التقنية من خلال استخدام برامج وتقنيات متطورة لرصد الحسابات المشبوهة وتتبع عناوين الـ IPالمستخدمة في ارتكاب الابتزاز، خاصة في المناطق الريفية وشبه الحضرية، كما تنسق هذه الفرق بشكل دائم مع الهيئات القضائية، خصوصا النيابات المتخصصة في الجريمة السيبرانية.

أما على الصعيد القضائي فقد تم إحداث أقسام قضائية متخصصة في الجريمة المعلوماتية على مستوى بعض المحاكم، تتولى النظر في قضايا الابتزاز الإلكتروني، وهو ما يسهم في ضمان معالجة نوعية لهذه القضايا، من خلال قضاة متمكنين من أبعاد الجريمة التقنية، ومدركين لخصوصية وسائل الإثبات الرقمية.

الفرع الثاني : خصائص التحقيق في جريمة الابتزاز الالكتروني.

يمتاز التحقيق في جريمة الابتزاز الإلكتروني بعدة خصائص تميزه عن التحقيقات التقليدية في الجرائم العادية، وذلك بسبب طبيعة الجريمة الرقمية المعقدة التي تعتمد على وسائل تكنولوجية متطورة ومحيط إلكتروني خاص. وتتمثل أبرز هذه الخصائص فيما يلي[1]:

أولا-الطابع التقني والتخصصي: التحقيق في جريمة الابتزاز الإلكتروني يتطلب معرفة تقنية متعمقة بأنظمة الحاسوب، الشبكات، البرمجيات، وأدوات التشفير، إذ لا يمكن الاستناد إلى الطرق التقليدية للتحري دون وجود خبرة في المجال الرقمي، ولذلك يشارك في التحقيق خبراء فنيون متخصصون في الأدلة الرقمية لتحليل الأجهزة والبيانات الرقمية.

ثانيا-سرعة انتقال الأدلة وحفظها: الأدلة في الجرائم الإلكترونية قد تكون مؤقتة وسريعة الزوال، مثل الرسائل المحذوفة، سجلات التصفح، أو ملفات التشفير التي قد تحذف تلقائيا. لذلك يجب على المحققين التدخل السريع لاستصدار أوامر الحجز والتجميد، وضبط الأدلة الرقمية قبل فقدانها أو العبث بها.

[1]قداري صارة، أساليب التحري الخاصة في القانون إجراءات الجزائية، لنيل مذكرة الماستر، في العلوم الجنائية، سنة 2011/2010 ،ص 55.

ثالثا-**عبور الحدود الجغرافية:** غالبا ما يتم ارتكاب جريمة الابتزاز الإلكتروني من خلال منصات تقع خارج الحدود الوطنية، مما يستوجب تعاونا دوليا متينا عبر طلبات المساعدة القضائية، والتنسيق مع هيئات دولية مثل الإنتربول، لتحديد هوية الجاني وملاحقته.

رابعا-السرية والحذر في طرق التحقيق: نظرا لطبيعة الجريمة وخطورتها على الضحية، فإن التحقيق يتطلب إجراءات سرية للغاية لمنع تسريب معلومات قد تؤدي إلى إفساد الأدلة أو زيادة الضغط على الضحية، إضافة إلى حماية مصادر التحقيق والأدلة الرقمية.

خامسا-الاعتماد على إجراءات قانونية خاصة: نص القانون الجزائري خاصة بعد تعديل قانون الإجراءات الجزائية بالقانون رقم 07-17 على إجراءات تحقيق خاصة مثل اعتراض المراسلات الإلكترونية، مراقبة الحسابات، والتفتيش الرقمي، والتي تخضع لإذن قضائي مسبق لضمان التوازن بين مصلحة التحقيق وحقوق الأفراد.

سادسا-التطور المستمر والتجدد: يجب على جهات التحقيق مواكبة التطورات التقنية المستمرة في مجال الجرائم الإلكترونية، حيث تظهر أدوات وأساليب جديدة يستخدمها المجرمون، مما يتطلب تحديث المعرفة والتقنيات المستخدمة في التحري والتحقيق باستمرار[1].

سابعا-تعدد الجهات المشاركة: يتطلب التحقيق في الابتزاز الإلكتروني تنسيقا بين عدة جهات أمنية، قضائية وتقنية، بالإضافة إلى التعاون مع مزودي خدمات الإنترنت والشركات المختصة في الأمن السيبراني، لضمان جمع الأدلة كاملة وموثقة.

هذه الخصائص تجعل من التحقيق في جريمة الابتزاز الإلكتروني عملية معقدة ومتخصصة، تستوجب تجهيزات قانونية وتقنية متقدمة.

[1] خربوش خالد، الدليل العلمي وأثره في اثبات الجنائي، لنيل مذكرة الماجستير، جامعة أم البواقي، سنة 2009/2008،ص 77.

المطلب الثاني : صعوبات الاثبات في جريمة الابتزاز الالكتروني.

يعد الإثبات حجر الزاوية في العملية الجزائية إذ لا يمكن إقامة الدعوى الجنائية ومعاقبة الجاني دون توفر أدلة قانونية تقطع بوقوع الجريمة ونسبتها إلى فاعلها، غير أن جريمة الابتزاز الإلكتروني باعتبارها من الجرائم المستحدثة والمعقدة تقنيا، تطرح إشكاليات عميقة في مجال الإثبات تختلف عن تلك المطروحة في الجرائم التقليدية،و ذلك أن هذه الجريمة ترتكب في فضاء افتراضي يفتقر إلى الحدود المكانية الواضحة، وتتم غالبا من خلال وسائل إلكترونية يصعب تعقبها أو تتعرض للتلاشي السريع بفعل طبيعة البيانات الرقمية القابلة للتعديل أو الإخفاء، كما أنهم يستخدمون تقنيات متطورة كالتشفير وتزوير الهويات الرقمية والبرمجيات الخبيثة، ما يصعب على جهات التحقيق الوصول إلى أدلة مادية ملموسة يمكن البناء عليها في إسناد الاتهام.

تزداد صعوبة الإثبات حينما يتردد الضحايا في الإبلاغ عن الجريمة، إما بسبب الخوف من الفضيحة أو لجهلهم بالإجراءات القانونية، ما يؤدي إلى ضياع العديد من الأدلة الرقمية بمرور الزمن. كما أن الإثبات في هذا النوع من الجرائم يتطلب مهارات تقنية عالية وكفاءات متخصصة في تحليل البيانات الرقمية وتتبع آثار الجريمة عبر الشبكة العنكبوتية، مما يطرح تحديًا على السلطات القضائية والأمنية التقليدية التي لم تواكب بعد التطورات التكنولوجية بالقدر الكافي، وبالتالي فإن صعوبة الإثبات في جريمة الابتزاز الإلكتروني لا تتعلق فقط بجمع الأدلة، بل تمتد إلى مسألة قانونية الدليل الرقمي، وحجيته أمام القضاء ومدى توافقه مع القواعد الإجرائية المعمول بها في القانون الجزائري خاصة في ظل الحاجة إلى مواءمة الإجراءات التقليدية مع خصوصيات الفضاء السيبراني[1].

[1] أبو الخير كمال ،إثبات الجريمة الإلكترونية في ضوء القانون المقارن، مجلة العلوم القانونية والسياسية، العدد 16، جامعة قسنطينة، 2021،ص 83.

أولا- الصعوبات التقنية للإثبات:

تشكل الطبيعة التقنية للابتزاز الإلكتروني تحديا كبيرا أمام الأجهزة القضائية والأمنية، إذ يعتمدون على وسائل رقمية معقدة لتنفيذ الجريمة مثل استخدام تطبيقات المراسلة المشفرة ،وإخفاء الهوية عبر الشبكات الخاصة الافتراضية أو حتى ارتكاب الجريمة عبر خوادم موجودة في دول أجنبية ،كما أن طبيعة الأدلة الرقمية نفسها تطرح إشكالية فهي أدلة غير مادية قابلة للحذف أو التعديل أو التشفير، ما يجعل عملية جمعها وتوثيقها وتحليلها تتطلب خبرة تقنية عالية وأدوات متقدمة في مجال الجرائم المعلوماتية، وأي تقصير في التعامل معها تقنيا قد يؤدي إلى ضياعها أو فقدان قيمتها القضائية[1].

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

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

[1]أبو الخير كمال،المرجع السابق،ص 93.

علاوة على ذلك، فإن صعوبة إثبات زمن ومكان إرسال الرسالة الابتزازية بدقة تعد من العراقيل التقنية، حيث يمكن تغيير الطابع الزمني للرسائل أو التلاعب بها باستخدام برامج تعديل متقدمة، ما يُفقد الدليل الإلكتروني مصداقيته أمام القضاء أضف إلى ذلك أنهم قد يستخدمون حسابات بريد إلكتروني مؤقتة ،أو هواتف افتراضية تلغى تلقائيا بعد تنفيذ الجريمة، مما يصعب عملية الربط بين الفعل وصاحبه الحقيقي.

كما يسجل ضعف في الإمكانيات التقنية لبعض وحدات الضبط القضائي في الجزائر، إذ لا تتوفر جميعها على مختبرات رقمية متخصصة، أو فرق ذات تكوين عالي في تحليل الأدلة الرقمية وتحقيق الهوية الرقمية للمجرمين ،و منه فإن هذا النقص في الإمكانيات قد يؤدي إلى ضياع بعض الأدلة أو إلى التشكيك في مصداقية الإجراءات التقنية، وهو ما يستغله دفاع الجاني للطعن في مشروعية الإثبات.

ثانيا-الصعوبات العملية والإجرائية:

إن الصعوبات العملية من أبرز العراقيل التي تواجه إثبات جريمة الابتزاز الإلكتروني، لاسيما في ظل امتناع بعض الضحايا عن التبليغ إما بدافع الخوف من الفضيحة أو بسبب الجهل بالإجراءات القانونية، مما يؤدي إلى ضياع أدلة حاسمة كما أن بطئ إجراءات التحقيق أحيان أو نقص التكوين لدى أعوان الضبطية القضائية في التعامل مع الملفات الإلكترونية، يؤدي إلى ضعف النتائج ،وقد يتعذر على الضحية أحيانا إثبات هوية الجاني في ظل استخدام حسابات وهمية أو أجهزة غير قابلة للتتبع.

كما أن تحديد الاختصاص الإقليمي يصبح إشكالا عند ارتكاب الجريمة عبر الإنترنت من خارج التراب الوطني، مما يعقد آليات الملاحقة القضائية، ويجعل الأمر مرهونا بالتعاون القضائي الدولي، الذي يعاني بدوره من عدم وجود اتفاقيات فعالة[1].

[1] القرافي سامي،الإثبات في الجرائم الإلكترونية بين التشريع والتطبيق، منشورات الحلبي الحقوقية، بيروت، 2020،ص 100.

الفرع الاول :الصعوبات الذاتية .

لا تقتصر صعوبات إثبات جريمة الابتزاز الإلكتروني على الجوانب التقنية أو القانونية فحسب، بل تمتد لتشمل صعوبات ذاتية متعلقة بالعنصر البشري، سواء من جهة الضحية أو من جهة القائمين على تطبيق القانون، وهي من أكثر العوامل التي تساهم في تعطيل سير العدالة وتعقيد إثبات الوقائع.

فمن جهة الضحية يلاحظ في كثير من الحالات امتناعها عن التبليغ بسبب الخوف من الفضيحة الاجتماعية أو العائلية خصوصا عندما يتعلق الابتزاز بمحتويات شخصية أو حساسة، مثل الصور أو مقاطع الفيديو الخاصة، كما أن بعض الضحايا خاصة من فئة المراهقين أو النساء يعانون من جهل قانوني وافتقار للوعي الرقمي، ما يجعلهم غير قادرين على حفظ الأدلة أو توثيق الوقائع بطريقة صحيحة، وبالتالي يُفقد ذلك الملف عناصر الإثبات المهمة[1] .

أما من جهة القائمين على التحقيق في الضبطية القضائية أو الجهات القضائية، فقد يظهر أحيانا قصور في التكوين أو ضعف في الكفاءة الشخصية، خاصة عندما لا يكون لديهم إلمام كاف بالتقنيات الرقمية أو آليات تتبع الأدلة الإلكترونية، كما أن بعض القضاة أو المحققين لا يزالون يفضلون الأدلة التقليدية المادية على الأدلة الرقمية، ما ينعكس سلبا على قناعتهم القضائية ويضعف حظوظ الإدانة في هذا النوع من القضايا و من ناحية أخرى قد تواجه بعض الجهات الفاعلة ترددا شخصيا أو تحفظا أخلاقيا في التعامل مع ملفات الابتزاز الإلكتروني التي تتضمن معطيات حساسة أو ذات طابع حميمي، مما يؤثر على جودة المعالجة القضائية، أو يجعل القضية تواجه نوعا من التباطؤ غير المعلن في المتابعة ،وفي حالات أخرى تلعب العوامل النفسية دورا في تضليل التحقيق، سواء بسبب اضطراب الضحية وارتباكها عند الإدلاء

[1] بوحنية قوي، الأمن السيبراني ومواجهة الجريمة الإلكترونية في الجزائر، المجلة الجزائرية للأمن والتنمية، العدد 6، جامعة ورقلة، 2022، ص88.

بشهادتها أو بسبب ما يسميه الفقهاء بالصدمة الإلكترونية التي قد تؤدي إلى تغير في إدراك الوقائع أو إغفال تفاصيل مهمة، وهو ما يصعب عملية تجميع الصورة الكاملة للجريمة

الفرع الثاني : الصعوبات القضائية .

رغم تطور الإطار التشريعي الجزائري خاصة مع صدور القانون 09-04 والقانون 18-04، إلا أن الواقع لا يزال يشهد قصورا في تنظيم الإثبات الرقمي، إذ تواجه الجهات القضائية صعوبات في تكييف الرسائل النصية أو الصور أو التسجيلات على أنها دليل جنائي معتمد بسبب غياب نصوص تفصيلية تنظم حجية الأدلة الإلكترونية، كما أن شرعية هذه الأدلة غالبا ما تكون محل جدل إذا ما تم الحصول عليها دون إذن قضائي ،ومن ناحية أخرى تواجه النيابة العامة صعوبة في إثبات الركن المعنوي للجريمة، أي القصد الجنائي خاصة في الحالات التي تكون فيها التهديدات غير مباشرة أو مشفرة بلغة رمزية، وهو ما قد يستغله الجاني للطعن في نية الابتزاز[1].

من أبرز الصعوبات القانونية أن قانون الإجراءات الجزائية الجزائري لم يفصل في قواعد الإثبات الرقمي، ولم ينظم بدقة كيفية جمع الأدلة الإلكترونية وتقديمها أمام القضاء، فمثلا لا توجد آلية قانونية واضحة تحدد متى يمكن تفتيش جهاز إلكتروني، أو ما هي الضمانات التي تحكم اعتراض الرسائل الإلكترونية أو المراسلات عبر التطبيقات، هذه الفجوة القانونية تجعل المحاكم تتردد أحيانًا في اعتماد الأدلة الرقمية كوسيلة إثبات رئيسية خاصة عند الطعن في مشروعيتها.

كما تطرح صعوبة قانونية تتعلق بتحديد المسؤولية الجنائية في بعض الحالات، إذ قد يكون الجاني مجهول الهوية، أو يستخدم حسابا مستعارا، أو حتى ينفذ الجريمة من خلال أجهزة غير مملوكة له، وفي هذه الحالة يبرز إشكال التكييف القانوني: هل يدان من يستخدم حسابه دون

[1] فتوش سعاد،المرجع السابق،ص 66.

علمه؟ هل يفترض علم صاحب الجهاز بما يتم عبره؟ وهل تكفي القرائن التقنية لتجريم شخص ما دون وجود دليل مباشر على الفعل الإجرامي؟

تضاف إلى ذلك مسألة التعاون القضائي الدولي إذ أن العديد من منصات التواصل ومزودي خدمة الإنترنت التي تستخدم في جرائم الابتزاز تخضع لقوانين دولية ولا تلزمها التشريعات الجزائرية، وبالتالي فإن الإجراءات القانونية الجزائية في الجزائر قد تصطدم بعقبات عند محاولة الحصول على بيانات رقمية محفوظة لدى شركات أجنبية، ما يعرقل سير الدعوى ويضعف ملف الإثبات ،أيضا لا يمكن إغفال أن القواعد التقليدية المتعلقة بسرية المراسلات والخصوصية قد تستخدم من قبل الدفاع كوسيلة للطعن في مشروعية الأدلة، خاصة إذا تم الحصول عليها من قبل الضحية دون إذن قضائي مثل تصوير محادثات، أو تسجيل مكالمات دون علم الطرف الآخر وهو ما يجعل القاضي أمام مفارقة بين ضرورة إثبات الجريمة واحترام الحريات الدستورية[1].

[1] بن خليفة مصطفى،المرجع السابق،ص102.

المبحث الثاني : العقوبات المقررة لجريمة الابتزاز الالكتروني.

يولي المشرع الجزائري أهمية بالغة لزجر جريمة الابتزاز الإلكتروني بالنظر لما تمثله من مساس خطير بحرية الأفراد وكرامتهم وخصوصيتهم، وقد سعى إلى تجريم مختلف صورها من خلال تكييفها ضمن أطر قانونية متعددة سواء في قانون العقوبات **أو** القانون رقم 18-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] وقد تم التنصيص في هذا السياق على عقوبات أصلية وأخرى تكميلية تختلف بحسب خطورة الفعل وظروف ارتكابه، و من هذا السياق سوف نتطرق الى العقوبات من خلال المطلب الأول و فروعه.

المطلب الاول : العقوبات الاصلية .

العقوبات الأصلية من أهم المفاهيم الجوهرية في قانون العقوبات، إذ تشكل جوهر الجزاء الجنائي المقرر للجريمة، وهي الأداة القانونية التي يُعبّر من خلالها المشرّع عن رد فعله تجاه الأفعال الإجرامية، وذلك بإيقاع جزاء يتناسب مع خطورة الجريمة المرتكبة.

أولا- تعريف العقوبات الأصلية:

العقوبة الأصلية هي الجزاء الأساسي الذي يقرره القانون لردع الجاني ومعاقبته على الفعل الإجرامي الذي ارتكبه، وهي تلك العقوبة التي تُحدَّد في النص القانوني مباشرة مقرونة بوصف الجريمة، وتُعد بمثابة العقوبة الرئيسية التي لا يُمكن الاستغناء عنها في الحكم، إلا في حالات معينة تسمح بها القوانين كظروف التخفيف.

وقد نصت المادة 5 من قانون العقوبات الجزائري على أنواع العقوبات الأصلية، مفرّقة بينها حسب ما إذا كانت الجريمة جناية، جنحة، أو مخالفة، ومن أبرزها:

[1] سليمان بن عبد الرزاق الغديان، يحيى بن مبارك خطاطبة، عزالدين بن عبد الله النعيمي، صور جرائم الابتزاز الإلكتروني ودوافعها وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد27 ،العدد69 ، يناير2018 ،ص166.

-الإعدام، السجن المؤبد، السجن المؤقت في الجنايات.

-الحبس، والغرامة في الجنح.

-الغرامة فقط في المخالفات.

ثانيا- خصائص العقوبات الأصلية:

تتميز العقوبات الأصلية بعدة خصائص تجعلها مختلفة عن غيرها من العقوبات التكميلية أو التدابير الأمنية، من بينها:

أ-الوجوب القانوني: لا يمكن للقاضي أن يحكم في الجريمة بدون أن يصدر حكما بالعقوبة الأصلية المحددة قانونًا، لأنها تمثل الحد الأدنى لمساءلة الجاني.

ب-الارتباط بالنص التجريمي:تقترن العقوبة الأصلية دوما بالنص المجرم للفعل، وتحدد من حيث النوع والمدة أو المقدار، مما يضمن الشرعية العقابية ،وعدم إمكان استبدالها إلا في الحالات التي يقرها القانون مثلا بظروف التخفيف أو وقف التنفيذ.[1]

ج-قابليتها للتشديد أو التخفيف: وذلك وفقا لظروف الجريمة أو شخصية الجاني، كما في حالات العود أو الشروع أو الظروف المشددة.

ثالثًا- الطبيعة القانونية للعقوبات الأصلية:

من حيث طبيعتها القانونية، تعد العقوبات الأصلية جزاءا جنائيا ذو طابع زجري وردعي، فهي ليست فقط وسيلة لمعاقبة الجاني، وإنما كذلك أداة لحماية المجتمع وتحقيق الردع العام والخاص. كما أنها تعبر عن سلطة الدولة في إنفاذ القانون وحماية المصالح العامة والفردية، ولهذا فهي تصدر باسم الشعب وتنفذها السلطات العامة.

[1] سليمان بن عبد الرزاق الغديان، يحيى بن مبارك خطاطبة، عزالدين بن عبد الله النعيمي،المرجع السابق،ص 103.

وفي السياق الحديث، تثير العقوبات الأصلية جدلًا فقهيًا حول مدى فعاليتها في تحقيق إصلاح الجاني وإعادة تأهيله، خاصة في الجرائم غير العنيفة مثل الابتزاز الإلكتروني، إذ يرى البعض ضرورة اعتماد بدائل عقابية ذات طبيعة إصلاحية بدلًا من العقوبات السالبة للحرية وحدها، خصوصًا مع التطور السريع لأساليب الجريمة في المجال الرقمي.

الفرع الاول : :العقوبات التكميلية.

تعد العقوبات التكميلية مكونا مهما من مكونات المنظومة العقابية في القانون الجنائي، حيث يلجأ إليها المشرّع لتعزيز فعالية الردع القانوني، لاسيما في الجرائم التي تستدعي اتخاذ تدابير إضافية إلى جانب العقوبة الأصلية، مثل الجرائم التي تمس النظام العام أو تنطوي على إساءة استغلال المركز أو التكنولوجيا، كما هو الحال في الجرائم الإلكترونية، وقد نظم المشرع الجزائري العقوبات التكميلية ضمن أحكام قانون العقوبات.

أولا- تعريف العقوبات التكميلية:

العقوبة التكميلية هي جزاء جنائي غير مستقل بذاته، يضاف إلى العقوبة الأصلية من أجل تعزيز الردع أو إزالة آثار الجريمة، وقد يفرضها القاضي وجوبا أو جوزا بحسب ما ينص عليه القانون، وهي لا تطبق بمفردها بل تأتي مرافقة لعقوبة أصلية كالحبس أو الغرامة، وتحدد صراحة في النصوص القانونية المجرمة للفعل[1].

مثال ذلك :مصادرة الأجهزة المستخدمة في الجريمة الإلكترونية، أو الحرمان من الحقوق المدنية بعد إدانة شخص في قضية تمس الأمن العام أو الحياة الخاصة.

[1]علي بوسعدية، مشاكل إثبات الجرائم الإلكترونية، مجلة الدراسات القانونية والسياسية، العدد 18، جامعة تبسة، 2021، ص66-67.

ثانيا- خصائص العقوبات التكميلية:

تتميز العقوبات التكميلية بجملة من الخصائص القانونية والوظيفية، منها:

-**التبعية للعقوبة الأصلية:** لا يمكن الحكم بها مستقلة، بل يجب أن تُضاف إلى عقوبة أصلية صادرة على الجاني.

-**الطابع الشخصي أو المهني:** ترتبط في كثير من الأحيان بصفة الجاني أو بنشاطه، كمنعه من مزاولة مهنة معينة أو شطبه من هيئة مهنية.

-**المرونة في التطبيق:** يجوز للقاضي أن يختار توقيعها أو لا، في حال لم يكن القانون قد جعلها وجوبية.

-**الأثر الطويل الأجل:** غالبا ما يكون أثرها مستمرا بعد تنفيذ العقوبة الأصلية، مثل الحرمان من الترشح أو التصويت، مما يضاعف من حدة العقوبة.

-**الغرض الوقائي:** تهدف في كثير من الأحيان إلى منع الجاني من تكرار الجريمة أو استغلال ظروف مشابهة للعودة إلى الفعل الإجرامي[1].

ثالثا- الطبيعة القانونية للعقوبات التكميلية:

من حيث طبيعتها القانونية، تعد العقوبات التكميلية إجراءا وقائيا زجريا ذو طابع خاص، حيث لا تهدف فقط إلى إيلام الجاني، وإنما إلى منع استمرار خطورته الإجرامية أو التأثير الضار للجريمة، وهي تجسد جانبا من العدالة الجنائية الوقائية، الذي يأخذ بعين الاعتبار ليس فقط الفعل المرتكب بل وظروف الجاني وإمكانية ارتكابه للجرائم مستقبلا.

[1] علي بوسعدية،المرجع السابق،ص 88.

وقد اعتمدها المشرع الجزائري كآلية ردعية فاعلة في الجرائم الخطيرة والمعقدة، مثل الجرائم الإرهابية، وجرائم الفساد، والجرائم الإلكترونية، التي قد لا تكفي فيها العقوبة الأصلية وحدها لتحقيق الردع المطلوب.

ومن أبرز صورها المنصوص عليها في التشريع الجزائري:

1-الحرمان من الحقوق الوطنية أو المدنية أو العائلية .

2-المنع من الإقامة.

3-نشر أو تعليق الحكم القضائي.

4-مصادرة الأموال أو الأدوات المستعملة في الجريمة.

5-المنع من مزاولة مهنة أو نشاط معين.

وقد نص القانون رقم 18-04 المتعلق بالجرائم السيبرانية في مادته 66 على المصادرة كعقوبة تكميلية وجوبية لكل الوسائل المستعملة في الجريمة، مثل الحواسيب، والهواتف الذكية، والحسابات الإلكترونية.

خلاصة:

العقوبات التكميلية ليست مجرد عقوبات إضافية، بل تعد أدوات قانونية ذات وظيفة ردعية ووقائية، تكمّل فعالية العقوبة الأصلية، وتسهم في منع تكرار السلوك الإجرامي من خلال تقليص قدرة الجاني على إعادة ارتكاب الجريمة، خصوصا في الجرائم المعاصرة كالابتزاز الإلكتروني، حيث تلعب المصادرة، والمنع من النشاط الإلكتروني، والحرمان من الحقوق، دورا جوهريا في حماية المجتمع الرقمي[1].

[1] حنان طواهرية ،المرجع السابق،ص 95.

الفرع الثاني : عقوبة الاشتراك و الشروع في جريمة الابتزاز الالكتروني .

يشكل كل من الاشتراك والشروع في جريمة الابتزاز الإلكتروني امتدادا قانونيا لمفهوم المسؤولية الجنائية، حيث يسأل جنائيا ليس فقط من ارتكب الفعل الإجرامي بصورة مباشرة، وإنما كذلك كل من ساعد أو سهّل أو حرّض على ارتكابه، حتى ولو لم يكن هو من باشر التهديد أو الابتزاز نفسه، وهو ما كرّسه المشرع الجزائري في إطار القواعد العامة لقانون العقوبات، لاسيما في المادتين 41 و42 تنصان صراحة على أن الشريك في الجريمة يعاقب بنفس العقوبة المقررة للفاعل الأصلي ما لم ينص القانون على خلاف ذلك، وتكتسب هذه الأحكام أهمية خاصة في الجرائم الإلكترونية، مثل الابتزاز الإلكتروني، نظرا لطبيعتها المعقدة والمتشابكة من حيث تعدد الفاعلين وتوزعهم عبر الفضاء الافتراضي، حيث قد يلعب أحدهم دور المبتز المباشر، بينما يكتفي الآخرون بتوفير الوسائل أو التخطيط أو الدعم التقني. وعلى هذا الأساس، فإن الشخص الذي يوفر برمجيات الاختراق، أو يساعد في إنشاء حساب وهمي يستخدم في تهديد الضحية، أو يحرّض على تنفيذ الفعل، يقع تحت طائلة المسؤولية الجنائية كشريك في الجريمة، وتطبق عليه نفس العقوبات المنصوص عليها في القانون، والتي قد تصل إلى السجن والغرامات، بحسب طبيعة الابتزاز الإلكتروني وخطورته[1] .

أما بالنسبة للشروع في جريمة الابتزاز الإلكتروني فقد أولاه المشرّع عناية خاصة أيضا، حيث نصت المادة 30 من قانون العقوبات على أن كل من شرع في ارتكاب جناية وُقفت أو خابت لأسباب خارجة عن إرادته، يعاقب بالعقوبة المقررة للجريمة التامة، وفي السياق ذاته إذا كانت جريمة الابتزاز الإلكتروني جنحة، فإن الشروع فيها قد يعاقب عليه كذلك متى نص القانون صراحة على ذلك، ويمكن تصور الشروع في الابتزاز الإلكتروني في حالات متعددة، من قبيل محاولة إرسال رسائل تهديد إلكتروني دون أن تصل، أو تحضير المواد التي يراد استخدامها للضغط على الضحية دون استخدامها فعليا، أو حتى البدء في التفاوض مع

[1] حنان طواهرية، جرائم الابتزاز الإلكتروني في التشريع الجزائري، مجلة العلوم القانونية والسياسية، العدد 15، جامعة سطيف 2، 2020، ص92.

الضحية ومطالبته بالأموال دون إنهاء العملية بسبب تدخل أمني أو تقني، وتكمن أهمية العقاب على الشروع هنا في الردع الاستباقي، إذ إن الجريمة الإلكترونية تنفذ بسرعة ودون إنذار ما يجعل من الضروري التعامل بصرامة مع المراحل الأولية لها قبل تحقق الضرر، ويلاحظ أن القضاء الجزائري بات يكيف العديد من الوقائع الإلكترونية في هذا السياق تحت وصف الشروع، خاصة عندما تضبط وسائل الجريمة (صور، برامج، رسائل مسودة) قبل تنفيذ الفعل، وهو ما يبرر قانونا معاقبة الجاني وإن لم يكمل جريمته.

أولا- عقوبة الاشتراك في جريمة الابتزاز الإلكتروني:

وفقا للمواد 41إلى 44 من قانون العقوبات الجزائري، يعد مشتركا في الجريمة كل من ساهم في ارتكابها دون أن يكون هو الفاعل الأصلي، ويشمل ذلك:

أ-من حرض على ارتكاب الجريمة.

ب-من قدّم الوسائل أو التعليمات أو المساعدة.

ج-من سهل ارتكاب الجريمة أو التستر عليها[1].

ويعاقب المشترك بنفس عقوبة الفاعل الأصلي، ما لم يقرر القانون خلاف ذلك ،وبالتالي إذا كانت جريمة الابتزاز الإلكتروني تعاقب مثلا بالحبس من سنة إلى خمس سنوات، فإن الشخص الذي ساهم في تنفيذها عبر تزويد الجاني ببرنامج اختراق، أو قام بابتزاز الضحية بناءا على معلومات قدمها غيره، يعاقب بنفس العقوبة على اعتبار أن المشاركة العقلية أو المادية لها نفس الأثر القانوني في تكوين الجريمة ،وتجدر الإشارة إلى أن الاشتراك في الجريمة الإلكترونية قد يتخذ طابعا تقنيا معقدا، مثل:

[1] فتحي عبد العال، الجرائم الإلكترونية ،دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2020، ص157.

1-تهيئة بيئة إلكترونية للابتزاز (منصات مزيفة، حسابات وهمية).

2-تقديم دعم فني لتأمين هوية الجاني.

3-مشاركة الأرباح أو توزيع الأدوار في تنفيذ الجريمة.

ثانيا- عقوبة الشروع في جريمة الابتزاز الإلكتروني:

ينظم المشرع الشروع في الجرائم بموجب المادتين 30 و31 من قانون العقوبات الجزائري، ويعرف الشروع بأنه البدء في تنفيذ الجريمة بنية واضحة دون أن تكتمل بسبب ظروف خارجة عن إرادة الجاني ،وفيما يخص جريمة الابتزاز الإلكتروني، فإن محاولة إرسال رسائل التهديد، أو إعداد الصور والمقاطع بغرض التهديد دون الوصول إلى التنفيذ الفعلي للابتزاز، قد تُكيف على أنها شروع في الجريمة .[1]

-يخضع الشروع في الجناية أو الجنحة لعقوبة، بشرط أن يكون الفعل قد بدأ تنفيذه فعليا ولم يكن مجرد نية أو تحضير فقط.

-يعاقب الشروع في جريمة الابتزاز الإلكتروني بنفس العقوبة المقررة للجريمة التامة، وذلك وفقا لما تقرره المادة 30 من قانون العقوبات: كل شروع في ارتكاب جناية يطبق عليه نفس العقوبة المقررة للجناية ذاتها إذا تم إيقافه أو خاب أثره لأسباب خارجة عن إرادة الجاني.

وفي هذا الإطار، يمكن تصور حالات الشروع في الابتزاز الإلكتروني من خلال:

-إرسال رسالة تهديد دون أن تصل إلى الضحية.

-فشل الجاني في استكمال تحميل المحتوى الذي يهدد بنشره.

-تدخل السلطات الأمنية قبل تنفيذ التهديد.

[1] فتحي عبد العال،المرجع السابق،ص 159.

المطلب الثاني :الوقاية من جريمة الابتزاز الالكتروني .

في ظل التوسع المتسارع لتكنولوجيا المعلومات وتغلغلها في جميع مجالات الحياة، أصبحت الجريمة الإلكترونية، وعلى رأسها جريمة الابتزاز الإلكتروني تشكل تهديدا متزايدا للأفراد والمؤسسات والدول على حد سواء، وقد انتقلت السياسة الجنائية الحديثة من التركيز على القمع والزجر إلى اعتماد مقاربة شمولية تدمج بين المكافحة الوقائية والردعية من خلال استباق وقوع الجريمة والعمل على الحد من مسبباتها. ويفهم من الوقاية في المجال الجنائي عموما، والإلكتروني خصوصا مجموعة التدابير والإجراءات التشريعية والتقنية والاجتماعية والتربوية التي تهدف إلى منع ارتكاب الأفعال الإجرامية، أو الحد من آثارها، أو تقليل فرص تكرارها. وتكتسي الوقاية من جريمة الابتزاز الإلكتروني أهمية قصوى، نظرا للطابع الخفي لهذه الجريمة وسرعة ارتكابها، وسهولة وقوع الضحية، وصعوبة كشف الجاني أو تعقبه، فضلا عن الآثار النفسية والاجتماعية الجسيمة التي قد تخلفها على المجني عليهم، خصوصا القصر والنساء[1].

أولا-الوقاية التشريعية والقانونية:

تعد التدابير القانونية من أهم وسائل الوقاية من الجريمة الإلكترونية حيث تمثل الأداة النظامية التي تؤطر السلوك الاجتماعي وتضع الضوابط اللازمة لاستخدام التكنولوجيا الحديثة في حدود مشروعة، وفي الجزائر جاء القانون رقم 18-04 المؤرخ في 10 ماي 2018، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، استجابة لتطور الجرائم السيبرانية، ونص صراحة على ضرورة تطوير البنية التشريعية لمواكبة مخاطر الجرائم الإلكترونية، ومن بينها جريمة الابتزاز الإلكتروني، ويعد هذا القانون خطوة تشريعية مهمة، كونه لا يقتصر على الجانب الزجري فقط، بل يُعنى كذلك بالتدابير الوقائية، إذ نص في مادته 3 على إلزام الهيئات المكلفة بالبريد والاتصالات الإلكترونية بتأمين نظمها المعلوماتية،

[1] جلال ثامر، الجريمة الإلكترونية بين الوقاية والمكافحة، مجلة الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، العدد 14، 2016، ص103.

وحماية بيانات المستخدمين، وضمان سرية المراسلات الرقمية، كما شجع القانون على تطوير التعاون بين القطاعين العام والخاص في مجال أمن المعلومات، وتبادل الخبرات، وتحديث البرامج والتجهيزات لمواجهة الهجمات الإلكترونية.

تكمن أهمية الوقاية القانونية كذلك في التوعية القانونية بحقوق الضحايا، وتحفيزهم على الإبلاغ عن الابتزاز، وتوفير آليات حماية قانونية لهم، مثل إخفاء الهوية خلال الشكوى، وضمان سرية البيانات الرقمية أثناء التحقيق، الأمر الذي يُسهم في تقليل إحجام الضحايا عن التبليغ خوفًا من الفضيحة أو من الانتقام، كما أن تجريم أفعال التحريض على الجريمة الإلكترونية، أو تسهيل ارتكابها أو التستر عليها، يشكل عنصر ردع وقائي فعال، يعاقب على التصرفات الممهّدة للجريمة قبل وقوعها[1].

ثانيا– الوقاية التقنية والتكنولوجية:

تحتل الوسائل التقنية والتكنولوجية صدارة أدوات الوقاية من جريمة الابتزاز الإلكتروني، باعتبار أن الجريمة في حد ذاتها تحدث من خلال وسائط رقمية، وبالتالي فإن حماية هذه الوسائط تشكل الخط الدفاعي الأول للوقاية، وتتجسد هذه الوقاية في ضرورة اعتماد برامج مضادة للفيروسات والاختراقات، وتحديث أنظمة التشغيل، واستخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، والامتناع عن فتح الروابط المشبوهة أو تحميل التطبيقات من مصادر غير موثوقة. كما تلعب تقنيات التشفير دورا أساسيا في حماية المعطيات الشخصية، خاصة عند تبادل الصور أو المستندات الحساسة عبر البريد الإلكتروني أو تطبيقات المراسلة.

وتتحمل الشركات التكنولوجية ومزودو خدمات الإنترنت مسؤولية كبيرة في هذا المجال، إذ يتعين عليهم تطوير بنية تحتية رقمية آمنة، وتقديم خدمات تستجيب لمعايير الحماية العالمية، وتفعيل نظم إنذار مبكر عن الأنشطة المشبوهة. كما يجب على السلطات المختصة إنشاء وحدات خاصة لرصد الفضاء السيبراني، وتوظيف الذكاء الاصطناعي في اكتشاف المحتوى

[1] جلال ثامر ،المرجع السابق،ص 104.

غير المشروع، وتحليل أنماط السلوك الرقمي التي قد تنذر بوقوع جريمة ابتزاز، وتجدر الإشارة إلى أن الوقاية التقنية لا تقتصر على الأدوات، بل تشمل أيضا التدريب المستمر لموظفي الدولة، وأفراد الشرطة، وحتى عموم المستخدمين، حول سبل الوقاية الرقمية، وكيفية التصرف عند التعرض لمحاولات ابتزاز.

ثالثا- الوقاية الاجتماعية والتربوية:

تعد الوقاية الاجتماعية والتربوية من الركائز الجوهرية في التصدي لجريمة الابتزاز الإلكتروني، حيث إن التربية السليمة والتنشئة الرقمية الواعية تمثلان خط الدفاع الأول في مواجهة الاستغلال الإلكتروني والانحراف الرقمي، وتبدأ هذه الوقاية من الأسرة باعتبارها الحاضنة الأولى للقيم، إذ يجب أن تسهر على مراقبة استعمال أبنائها للإنترنت، وتوجيههم لاستخدام آمن ومسؤول، ومرافقتهم في فهم مخاطر النشر المفرط للصور والمعلومات الشخصية، ومساعدتهم على بناء وعي قانوني وأخلاقي عند التفاعل مع الآخرين عبر الإنترنت. كما تضطلع المدرسة بدور مهم في إدماج الثقافة الرقمية في المناهج الدراسية، وتعليم الطلبة أسس السلامة المعلوماتية، وسبل حماية الخصوصية الرقمية، وأساليب الإبلاغ عن التحرش أو الابتزاز الإلكتروني[1].

ولا يقل دور المجتمع المدني أهمية، حيث يمكن للجمعيات والهيئات الحقوقية تنظيم حملات توعوية، وورشات تدريبية، ولقاءات مفتوحة حول خطورة الجرائم الإلكترونية، وطرق التعامل مع محاولات الابتزاز دون الوقوع في فخ الخوف أو التستر، وتتمثل أحد التحديات الكبرى في تنامي شعور الضحية بالخجل والذنب، خصوصًا عندما يتعلق الأمر بصور أو رسائل خاصة، وهو ما يستوجب مقاربة وقائية تقوم على الدعم النفسي، والاحتواء، وتكريس ثقافة الإبلاغ المبكر.

---

[1] رضوان بوحملة، الدور الوقائي لتكنولوجيا المعلومات في مواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن والعدالة، جامعة الجزائر 1، العدد 12، 2020، ص92.

رابعا- الوقاية من خلال التعاون الأمني والمؤسساتي:

تفرض الطبيعة العابرة للحدود لجريمة الابتزاز الإلكتروني مقاربة وقائية دولية تقوم على تعزيز التعاون الأمني والقضائي بين الدول، وتبادل المعلومات الجنائية ذات الصلة بالجريمة السيبرانية، وإنشاء آليات إنذار مبكر، وتوحيد التشريعات الوطنية بما يتوافق مع المعايير الدولية، مثل اتفاقية بودابست لسنة 2001، كما يتعين على الأجهزة الأمنية الجزائرية تطوير وحدات خاصة بالجرائم الإلكترونية، وتزويدها بالكفاءات البشرية المؤهلة والتجهيزات التقنية الحديثة، وتكثيف دورات التكوين والتدريب[1].

أما على المستوى المؤسساتي الداخلي، فينبغي تحقيق التكامل بين مختلف القطاعات (التربية، الإعلام، الداخلية، العدالة، تكنولوجيات الاتصال...إلخ) من أجل بناء استراتيجية وطنية موحدة للوقاية من الجريمة الإلكترونية، تتسم بالاستمرارية والمرونة، وتشمل كل الفئات المستهدفة، مع إشراك المجتمع في رسم الخطط وتنفيذها، وفي هذا السياق، يمكن استحداث منصات رقمية تفاعلية تمكن المواطنين من التبليغ الآني عن أي ابتزاز أو تهديد إلكتروني، مع ضمان السرية والحماية القانونية للمبلغ.

الفرع الاول : دور هيئات الضبط الإلكتروني والشرطة القضائية المتخصصة.

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

[1] رضوان بوحملة،المرجع السابق،ص 94.

البيانات، وتأمين البنى التحتية الرقمية، ومراقبة خدمات الإنترنت ومزوديها، بما يُحد من استغلال الثغرات في الأنظمة الإلكترونية لتنفيذ عمليات الابتزاز أو التهديد أو الاختراق.

وتسند إلى هذه الهيئات جملة من المهام ذات طابع وقائي وتنظيمي، أبرزها ضبط سوق الاتصالات الإلكترونية، ومنح التراخيص للمتعاملين مع الالتزام بالشروط الأمنية، وإلزامهم بوضع وسائل حماية للبيانات الشخصية للمستخدمين، مثل التشفير، وسجلات التتبع، والتخزين الآمن، كما تقوم هذه الهيئات بالتنسيق مع السلطات القضائية والأمنية لتقديم المعلومات الفنية عند الضرورة، وتتدخل كذلك في متابعة الشكاوى المتعلقة بالممارسات غير المشروعة التي تتم عبر الشبكات، وهو ما يعد أداة فعالة في كشف ومعالجة محاولات الابتزاز قبل تفاقمها.[1]

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

وفي هذا الإطار يتعين على هيئات الضبط الإلكتروني مواكبة التطور التكنولوجي السريع من خلال تحديث أدوات الرقابة، وتوظيف الذكاء الاصطناعي في رصد الأنماط الشاذة للسلوك الرقمي، والاستفادة من قواعد البيانات الإقليمية والدولية لتبادل المعلومات حول المواقع الخطرة وأساليب الجريمة السيبرانية المتجددة، كما ينتظر منها اقتراح تعديلات تشريعية دورية لملائمة النصوص القانونية مع الواقع التقني المتغير، بما يضمن فعالية الردع والوقاية.

---

[1] خالد عبد الحميد، مكافحة الجرائم الإلكترونية ، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2018، ص232.

وبالتالي فإن دور هيئات الضبط الإلكتروني لا يقتصر على المراقبة الإدارية أو منح التراخيص، بل يتجاوز ذلك إلى المساهمة في صياغة منظومة وطنية متكاملة للأمن السيبراني ،تكون فيها الوقاية من جريمة الابتزاز الإلكتروني هدفا محوريا، من خلال العمل المشترك مع جميع الفاعلين من سلطات عامة، قطاع خاص، وجمعيات مدنية، في سبيل حماية الفضاء الرقمي من كل التهديدات والمخاطر.[1]

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

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

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

[1] خالد عبد الحميد ،المرجع السابق،ص 233.

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

علاوة على ذلك تساهم سلطة الضبط في الجانب الوقائي التوعوي حيث تشرف على حملات تحسيسية تستهدف مختلف فئات المجتمع، وتعمل على نشر ثقافة الاستخدام الآمن للإنترنت، والتحذير من مخاطر مشاركة البيانات الحساسة أو الصور الخاصة على الفضاء الرقمي. كما تعزز التعاون مع الهيئات الأمنية والقضائية، خاصة في توفير الأدلة الفنية عند الضرورة، أو تسهيل الوصول إلى المشتبه بهم عبر تتبع عناوين IP أو سجلات الاتصالات، بما يسرع من كشف المبتزين وتقديمهم للعدالة.[2]

ولأداء دورها بفعالية تحتاج هذه الهيئة إلى دعم لوجيستي وتقني متطور، وتكوين مستمر لمواردها البشرية في مجالات الأمن الرقمي وتحليل البيانات السيبرانية، فضلا عن توسيع صلاحياتها في مجال التعاون الدولي، خاصة أن جريمة الابتزاز الإلكتروني كثيرا ما تتم عبر وسائط خارج النطاق الوطني، وبالنظر إلى التحديات المستجدة التي تطرحها التطورات الرقمية، فإنه من الضروري تمكين هذه الهيئة من تحديث أدواتها القانونية والرقمية، وتعزيز التنسيق بينها وبين وزارات الداخلية، العدل، والدفاع، ضمن رؤية وطنية شاملة للأمن المعلوماتي.

- دور الشرطة القضائية المتخصصة:

إن دور الشرطة القضائية المتخصصة لا يقتصر على الجانب التنفيذي، بل يمتد إلى المشاركة في صياغة السياسات العمومية الخاصة بالأمن السيبراني، واقتراح تعديلات تشريعية، والمساهمة في إعداد بروتوكولات وطنية ودولية للتعاون القضائي والأمني في مجال الجريمة

[1] عبد العزيز صالحي،المرجع السابق،ص 80.
[2] خالد عبد الحميد،المرجع السابق،ص 235.

الإلكترونية، مما يعزز البنية المؤسساتية الوطنية في مواجهة الابتزاز الإلكتروني وغيره من الأفعال الإجرامية الرقمية.

وقد أولى المشرع الجزائري أهمية خاصة لهذه الجهة من خلال تخصيص وحدات متخصصة داخل أجهزة الأمن الوطني والدرك الوطني، وهو ما تكرّس بوضوح ضمن أحكام القانون رقم 18-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتضطلع هذه الفرق بمهام دقيقة تشمل التحري، والتحقيق، وجمع الأدلة الرقمية، وتحليل المحتوى الإلكتروني، وتتبع مصدر الرسائل التهديدية، وكشف هوية مرتكبي جرائم الابتزاز، الذين غالبًا ما يتخفّون خلف هويات وهمية أو يستخدمون تقنيات متطورة لإخفاء أثرهم.

وفي إطار الوقاية، تعمل هذه الوحدات المتخصصة على رصد الأنشطة الإلكترونية المشبوهة عبر منصات التواصل الاجتماعي، وغرف الدردشة، والمواقع التي تستخدم كوسائط لارتكاب جرائم الابتزاز، حيث تقوم بعمليات مراقبة إلكترونية متقدمة باستخدام تقنيات تحليل البيانات الضخمة والذكاء الاصطناعي، بهدف الكشف المبكر عن الجرائم ومنع وقوعها، كما تنخرط في حملات توعية وتحسيس بالتنسيق مع وزارتي التربية الوطنية والتعليم العالي، من أجل نشر ثقافة الوقاية الرقمية، وتعليم المواطنين لاسيما فئة الشباب والمراهقين كيفية حماية بياناتهم والتمييز بين السلوكيات الإلكترونية المشروعة وتلك الإجرامية. [1]

تساهم الشرطة القضائية المتخصصة أيضا في تهيئة بيئة قانونية وفنية تسهّل إثبات الجريمة الإلكترونية، لاسيما من خلال إعداد تقارير الخبرة الرقمية، والحفاظ على سلاسل الأدلة، وتمثيل النيابة العامة في تقديم المعطيات التقنية الضرورية لملاحقة المتورطين،وبالنظر للطابع العابر للحدود الذي تتسم به الكثير من جرائم الابتزاز الإلكتروني، فقد أصبح لهذه الوحدات دور متزايد في التعاون الأمني الدولي، خصوصا من خلال تبادل المعلومات مع

[1]ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، مقال منشور على الشبكة الإلكترونية، المجلة العربية للدراسات ألمنية، المجلد33 ،العدد70 ،الرياض2017 ،ص199.

أجهزة الشرطة الدولية (مثل الإنتربول) والوحدات الأجنبية المناظرة، وهو ما يسمح بتعقب الجناة الموجودين خارج الإقليم الوطني وتقديمهم إلى العدالة[1].

وتجدر الإشارة إلى أن نجاح هذه الشرطة القضائية المتخصصة يتطلب موارد بشرية مؤهلة، وتكوينًا تقنيًا وقانونيا مستمرا، إضافة إلى إطار تشريعي مرن يسمح بالتدخل السريع، ومواكبة التطورات التكنولوجية، ومن هذا المنطلق فإن تطوير هذه الهيئة وتعزيز إمكانياتها يعتبر ركيزة أساسية لأي سياسة فعالة للوقاية من جريمة الابتزاز الإلكتروني في الجزائر.

ومن أبرز المهام التي تضطلع بها الشرطة القضائية المتخصصة:

1-رصد المحتوى المجرم مسبقا مثل الصور أو المقاطع الشخصية التي تستخدم في التهديد.

2-التحقيق المفتوح والمقنع تقنيا من خلال جمع البيانات من الحواسيب والهواتف الذكية وأقراص التخزين.

3-إعداد تقارير الخبرة التقنية التي تحال إلى وكيل الجمهورية أو قاضي التحقيق ضمن ملف القضية.

4-المساعدة في توقيف المشتبه بهم داخل وخارج الوطن بالتنسيق مع الهيئات الدولية.

من الناحية المؤسسية، تحتاج هذه الفرق إلى دعم مالي وتقني كبير، خصوصا من حيث تجهيز مخابر التحليل الجنائي الرقمي، وتوفير برامج متقدمة في استرجاع البيانات والتشفير، بالإضافة إلى تكوين دوري في المستجدات الرقمية، حيث أن أدوات الجريمة تتطور بوتيرة متسارعة. ولهذا، تتعاون المصالح الأمنية مع وزارات العدل والداخلية والرقمنة، بهدف بناء منظومة وطنية متكاملة للأمن السيبراني.

[1] ممدوح رشيد مشرف الرشيد العنزي،المرجع السابق،ص 201.

من جهة أخرى، تلعب الشرطة القضائية المتخصصة أيضًا دورًا في نشر الثقة الرقمية داخل المجتمع .فهي تشجع على التبليغ من خلال توفير قنوات سرية وآمنة، وتضمن السرية التامة لهوية المشتكين، وهو عامل مهم في الجرائم التي تتعلق بالابتزاز الجنسي أو بالصور الخاصة. كما تُصدر نشرات توعوية دورية، وتشارك في الإعلام العمومي والجامعات لتثقيف المستخدمين حول كيفية الوقاية من الابتزاز، سواء عبر تأمين حساباتهم أو تجنب التفاعل مع جهات مجهولة[1].

الفرع الثاني : التعاون الدولي في مكافحة الابتزاز الإلكتروني.

إن التطورات التقنية المتسارعة في مجال تكنولوجيا المعلومات والاتصالات قد خلقت فضاءً رقميا واسعا يتجاوز الحدود الجغرافية التقليدية، مما أسهم في نقل العديد من النشاطات الإجرامية إلى العالم الافتراضي، وعلى رأسها جريمة الابتزاز الإلكتروني، التي أصبحت من أبرز التحديات التي تواجه الدول والمجتمعات على السواء، فهذه الجريمة لا تتقيد بمكان ارتكابها، ولا بهوية مرتكبها أو جنسية ضحيتها، بل تمارس أحيانا من قارات أخرى عبر أدوات تخفي الهوية الرقمية، مما يجعل مواجهتها على الصعيد الوطني قاصرة ومحدودة في فعاليتها.

في هذا السياق لم يعد من الممكن الحديث عن مكافحة فعالة لهذه الجريمة بمعزل عن إطار تعاون دولي واسع ومنظم، يضمن تبادل المعلومات بسرعة، وتوحيد إجراءات البحث والتوقيف، والاستجابة الفورية للتهديدات التي تستهدف الأفراد والمؤسسات داخل وخارج الوطن. فالتحدي لم يعد فقط في إثبات الجريمة، بل في الوصول إلى مرتكبيها الذين يتحصنون خلف تقنيات التشفير، ويستغلون ضعف البنية التشريعية أو القضائية في بعض الدول.

ومن هذا المنطلق تزايدت الدعوات إلى تعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية، سواء من خلال الاتفاقيات الدولية مثل اتفاقية بودابست، أو عبر الشراكات الثنائية والإقليمية، أو ضمن شبكات العمل الأمنية والقضائية متعددة الأطراف. وقد أولت الجزائر

[1] سامية بعزيزي،المرجع السابق،ص 162.

اهتمامًا متزايدًا بهذا الجانب، وبدأت بتعزيز حضورها في المنظمات الدولية ذات الصلة، إلى جانب إدخال تعديلات على قوانينها الوطنية بما يسمح لها بالاستجابة لمتطلبات التعاون العابر للحدود، خاصة فيما يخص جرائم الابتزاز الإلكتروني التي باتت تمس أمنها السيبراني ومصالح مواطنيها.

أولا-تعريف التعاون الدولي :

يعد التعاون الدولي من المفاهيم الجوهرية في العلاقات بين الدول، ويعكس التوجه الجماعي نحو معالجة القضايا ذات البعد العالمي أو المشترك، التي تتجاوز حدود الدولة الواحدة. ويقصد به الجهود المنسقة التي تبذلها دولتان أو أكثر، أو المنظمات الدولية، بهدف تحقيق مصالح مشتركة، سواء كانت سياسية، اقتصادية، أمنية، بيئية أو إنسانية، ويستند التعاون الدولي إلى مبادئ القانون الدولي العام، ولاسيما مبادئ الاحترام المتبادل، وعدم التدخل في الشؤون الداخلية، والمساواة في السيادة. [1]

يمثل التعاون الدولي أحد المبادئ الأساسية لمواجهة الجرائم الإلكترونية، ويشمل جملة من التدابير القانونية والإدارية والتقنية التي تُتخذ بشكل مشترك بين الدول، سواء بشكل ثنائي أو ضمن أطر إقليمية ودولية، من أجل تبادل المعلومات، تنفيذ الإنابات القضائية، أو المساعدة في التتبع الإلكتروني للأدلة الرقمية،وتعتبر اتفاقية بودابست بشأن الجريمة الإلكترونية أول إطار دولي شامل يُنظم هذا التعاون، وقد انضمت الجزائر إليها بصفة غير مباشرة من خلال مواءمة تشريعاتها، لاسيما عبر القانون رقم 18-04.

وفي السياق ذاته، تنص المادة 35 من اتفاقية بودابست على ضرورة إنشاء نقاط اتصال دائمة على مدار الساعة، تكون مكلفة بالتواصل السريع بين الدول في حالات الطوارئ الرقمية،

[1] التوجي محمد، المرجع السابق،ص 103.

وهي الممارسة التي تبنّتها الجزائر من خلال إنشاء خلية "CERT" التابعة للهيئة الوطنية للأمن السيبراني، وفرق الشرطة القضائية المتخصصة في الجرائم المعلوماتية[1].

ثانيا- أوجه التعاون الأمني بين الجزائر والمنظمات الإقليمية والدولية:

تتجلى مظاهر التعاون الأمني الجزائري في مكافحة الابتزاز الإلكتروني من خلال مشاركتها في عدد من الأطر والمؤسسات الإقليمية والدولية، مثل:

1-الإنتربول :(INTERPOL) حيث تستفيد الجزائر من شبكة I-24/7 الخاصة بالإنتربول لتبادل المعلومات المتعلقة بالجرائم الرقمية، والبحث عن الجناة دوليًا. كما تشارك عبر مركزها الوطني في إعداد نشرات حمراء لتوقيف المشتبه بهم في قضايا ابتزاز إلكتروني عبر الحدود.

2-المنظمة العربية لتقنيات الاتصال والمعلومات :(AICTO) وهي منظمة عربية تساهم الجزائر في أنشطتها المتعلقة بالتكامل السيبراني العربي ومكافحة الجريمة الرقمية.

3-الشراكة مع الاتحاد الأوروبي والهيئات الإفريقية :تشارك الجزائر في مشاريع لبناء القدرات مع الاتحاد الأوروبي، من خلال برامج مثل GLACY+ التي تهدف إلى دعم الدول في تطوير تشريعاتها السيبرانية وتعزيز التعاون الدولي.

4-برنامج :AFRIPOL الذي يضم أجهزة الشرطة الإفريقية، ويُعد أداة للتنسيق الأمني في مواجهة الشبكات الإجرامية العابرة للحدود، والتي تنشط في الابتزاز الإلكتروني، لاسيما عبر الاستهداف المنظم لمواطنين ومؤسسات في دول متعددة.

ثالثًا- آليات التعاون القضائي في قضايا الابتزاز الإلكتروني:

إلى جانب الجانب الأمني يعد التعاون القضائي الدولي ركنا جوهريا في مكافحة الابتزاز الإلكتروني، ويشمل هذا التعاون: تبادل الإنابات القضائية، تنفيذ طلبات التسليم، والاعتراف

[1] رضوان بوحملة،المرجع السابق،ص 113.

بالأحكام الأجنبية المتعلقة بالجرائم الإلكترونية. وقد سمح تعديل قانون الإجراءات الجزائية الجزائري بإدراج قواعد تخص التعاون في الجرائم التي تُرتكب عبر الإنترنت، مما مهّد الطريق أمام الجزائر لإبرام اتفاقيات ثنائية مع عدة دول مثل فرنسا، إيطاليا، وتونس.

وتبرز أهمية هذا التعاون عند محاولة استرجاع بيانات الضحية الموجودة على خوادم خارج الجزائر، أو تتبع المبتز الذي يستخدم بريدًا إلكترونيًا مسجلا في دولة أجنبية، كما يسمح هذا التعاون بتنسيق الجهود لإجراء تحقيقات موازية في أكثر من دولة ضد نفس الجاني أو الشبكة الإجرامية[1].

رابعا- التحديات التي تواجه التعاون الدولي في مجال مكافحة الابتزاز الإلكتروني:

رغم الجهود المبذولة لا تزال هناك صعوبات تعيق فعالية التعاون الدولي، من أبرزها:

-الاختلاف في الأنظمة القانونية، حيث لا تعتبر جميع الدول الابتزاز الإلكتروني جريمة بذات التعريف أو العقوبة، مما يعقد آليات التسليم.

-ضعف التنسيق بين الهيئات المختصة، وغياب آليات اتصال فورية في بعض الدول.

-حماية المعطيات الشخصية، حيث تفرض بعض الدول قيدًا على مشاركة البيانات بسبب قوانينها الداخلية لحماية الخصوصية.

-البطئ في الاستجابة لطلبات التعاون، ما يجعل توقيف الجناة أو حماية الضحايا أكثر تعقيدا.

[1] خالد عبد الحميد،المرجع السابق،ص 242.

خامسا- سبل تعزيز فعالية التعاون الدولي في مكافحة الابتزاز الإلكتروني:

لضمان استجابة فعالة وسريعة في قضايا الابتزاز الإلكتروني، يقتضي الأمر من الجزائر ومن غيرها من الدول[1]:

1-الانضمام الرسمي لاتفاقية بودابست، لتسهيل التنسيق مع الدول الموقعة.

2-تعزيز القدرات التقنية والبشرية للشرطة القضائية والقضاة المكلفين بالجرائم الرقمية.

3-تطوير قواعد بيانات مشتركة للمجرمين الرقميين.

4-التكوين المشترك للقضاة والضباط من خلال برامج تدريب دولية.

5-عقد اتفاقيات ثنائية جديدة مع دول يلاحظ منها ارتفاع في أنشطة الابتزاز الإلكتروني ضد المواطنين الجزائريين.

[1] عبد العزيز صالحي،المرجع السابق،ص 83.

الخاتمة :

جريمة الابتزاز الإلكتروني من الجرائم المستحدثة التي أفرزتها الطفرة التكنولوجية وانتشار الوسائل الرقمية، وقد أصبحت تمثل تهديداً خطيراً على الأفراد والمجتمعات لما لها من تأثير نفسي، اجتماعي، واقتصادي على الضحايا. وتتمثل هذه الجريمة في قيام الجاني بتهديد الضحية بنشر أو كشف معلومات خاصة أو صور أو مقاطع فيديو تم الحصول عليها بطريقة مشروعة أو غير مشروعة، بهدف حمل الضحية على القيام بفعل معين أو الامتناع عنه، وغالبا ما يكون هذا الفعل ذا طابع مالي أو جنسي.

من الناحية القانونية ترتب جريمة الابتزاز الإلكتروني مسؤولية جنائية كاملة على مرتكبها، حيث تتوفر فيها أركان الجريمة الجنائية التقليدية، وهي الركن القانوني نص التجريم،و الركن المادي الفعل المادي المتمثل في التهديد باستخدام وسيلة إلكترونية، والركن المعنوي القصد الجنائي المتمثل في إرادة التهديد وابتغاء تحقيق غرض غير مشروع.

وتكمن المسؤولية الجنائية في هذه الجريمة في تحميل الفاعل نتائج أفعاله الإجرامية وفقاً لما يقرره القانون الجزائي، وقد تصدت عدة تشريعات حديثة ومنها التشريع الجزائري لهذه الظاهرة بنصوص خاصة في قوانين مكافحة الجرائم الإلكترونية، أو من خلال تكييفها في إطار الجرائم التقليدية كجريمة التهديد، أو الابتزاز، أو انتهاك الحياة الخاصة، مع تشديد العقوبات في حال استعمال الوسائل المعلوماتية، ويلاحظ أن هذه المسؤولية لا تتوقف عند مرتكب الفعل الأصلي، بل قد تمتد إلى المساهمين والشركاء، خاصة إذا ثبتت نيتهم الإجرامية ومساهمتهم الفعالة في تنفيذ الجريمة، سواء من خلال توفير الوسائل التقنية، أو المساعدة في النشر، أو التحريض.

كما تبرز أهمية المسؤولية الجنائية في تحقيق الردع العام والخاص، وضمان حماية المجتمع من خطر هذه الجريمة المتنامية، خصوصاً وأنها غالباً ما تستهدف الفئات الهشة كالقصر والنساء. ولهذا السبب، تسعى الدول إلى تعزيز الأطر القانونية، وتحديث أدوات التحقيق الرقمي، وتفعيل آليات التعاون الدولي لملاحقة الجناة الذين قد ينشطون عبر الحدود ،وعليه فإن المسؤولية الجنائية في جريمة الابتزاز الإلكتروني تمثل حجر الزاوية في مواجهة هذه الجريمة،

وتتطلب جهداً تشريعيا، قضائيا، وأمنيا متكاملا لضمان تحقيق الردع والعدالة، وحماية الأفراد من الاستغلال الرقمي.

أولا- النتائج:

-تطور الجريمة الإلكترونية، ومن بينها الابتزاز، أصبح يسبق في كثير من الأحيان تطور النصوص القانونية، ما يخلق فراغًا تشريعيًا يَصعُب معه التجريم والمتابعة.

-الركن المادي والمعنوي لجريمة الابتزاز الإلكتروني يثبتان توافر النية الإجرامية واستغلال الوسائل التقنية لإلحاق الأذى بالضحية ماديًا أو نفسيا.

-ضعف الوعي القانوني والتقني لدى فئات المجتمع، خاصة فئة الشباب، يزيد من احتمالات الوقوع ضحية لهذا النوع من الجرائم.

-الطابع العابر للحدود لهذه الجريمة يجعل من التعاون الدولي عنصرًا أساسيًا في تعقب الجناة، خاصة عندما يتم تنفيذ الجريمة من خارج الإقليم الوطني.

-التوصيات:

-ضرورة مراجعة وتحديث التشريعات الوطنية، وبخاصة قانون العقوبات وقانون الوقاية من الجرائم الإلكترونية، بما يسمح بتجريم أشكال الابتزاز الرقمي الحديثة وتحديد العقوبات المناسبة.

-تعزيز قدرات الشرطة القضائية في المجال التقني، من خلال تكوين متخصصين في الأدلة الرقمية والتحقيقات الإلكترونية.

-إطلاق حملات توعية وطنية موجهة نحو فئات مستهدفة (الشباب، النساء، الأطفال)، تهدف إلى التحذير من أخطار الابتزاز الإلكتروني وأساليب الوقاية منه.

-تفعيل الاتفاقيات الدولية والإقليمية الخاصة بمكافحة الجريمة الإلكترونية، وتوسيع مجالات التعاون القضائي والأمني بين الدول.

-إنشاء منصات إلكترونية وطنية آمنة ومخصصة للإبلاغ عن الجرائم الإلكترونية، تضمن خصوصية الضحية وسرعة التفاعل مع الشكاوى.

قائمة المراجع :

-المراجع باللغة العربية :

أولا- النصوص القانونية:

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية، المراجَع بموجب التعديل الدستوري لسنة 2020، الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية، العدد 83، الصادرة في 30 ديسمبر 2020.

2- القانون رقم 07-17 المؤرخ في 27 مارس 2017، المتضمن تعديل وإتمام قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 21 لسنة 2017.

3- قانون الإجراءات الجزائية الجزائري، المواد 65 مكرر إلى 65 مكرر 18، الأمر رقم 66-155 المؤرخ في 8 جوان 1966، المعدل والمتمم.

4-القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، يتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009.

5-الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم، لا سيما بموجب القانون رقم 18-04 المؤرخ في 10 ماي 2018، الجريدة الرسمية للجمهورية الجزائرية، العدد 27، الصادرة في 13 ماي 2018.

ثانيا- الكتب باللغة العربية:

1-أحمد بسيوني أبو الروس، التحقيق الجنائي و التصرف فيه و الأدلة الجنائية، الطبعة الأولى، الإسكندرية، 2015.

2-جاسم محمد جندل، الجرائم الإلكترونية، الطبعة الأولى، دار معتز للنشر والتوزيع، عمان، الأردن، 2022.

3-حسني عبد الكرمي يونس، خليل يوسف جندي، الابتزاز الإلكتروني والجرائم الإلكترونية: المفهوم و الأسباب، الطبعة الأولى، دار الكفاءة المعرفة، عمان، الأردن، 2021.

4-خالد حسن أحمد لطفي، جرائم الإنترنت بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني: دراسة مقارنة، الطبعة الأولى، 2008.

5-خالد عبد الحميد، مكافحة الجرائم الإلكترونية: دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2018.

6-سامية بوشريط، الابتزاز الإلكتروني كجريمة مستحدثة في القانون الجزائري: دراسة تحليلية للمادة 303 مكرر *1*، مجلة العلوم القانونية والسياسية، جامعة قسنطينة، العدد 10، 2022.

7-سمية لعور، التحقيق الجنائي في الجرائم المعلوماتية، دار المعرفة، الجزائر، 2020.

8-عبد القادر بن يوسف، الضبطية القضائية في مكافحة الجريمة المعلوماتية، دار الخلدونية، الجزائر، 2020.

9-عبد الكريم بن عربية، شرح قانون العقوبات: القسم العام، ديوان المطبوعات الجامعية، الجزائر، 2019.

10-عبد الكريم بن عربية، شرح قانون العقوبات: القسم العام، نظرية الجريمة والمسؤولية الجزائية، ديوان المطبوعات الجامعية، الجزائر، 2019.

11-فتحي عبد العال، الجرائم الإلكترونية: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2020.

12-مروة صالح الدين محمد، الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي، الطبعة الأولى، المكتب العربي للمعارف، دار البحوث القانونية، القاهرة، مصر، 2021.

13-نور الدين زروقي، الجريمة الإلكترونية في التشريع الجزائري: الطبيعة والأركان والجزاءات، دار العلوم للنشر والتوزيع، الجزائر، 2022.

14-ربيعة خريس، الجرائم الإلكترونية في التشريع الجزائري: دراسة تحليلية مقارنة، دار هومة، الجزائر، 2020.

15-سامي القرافي، الإثبات في الجرائم الإلكترونية بين التشريع والتطبيق، منشورات الحلبي الحقوقية، بيروت، 2020.

ثالثا-المقالات العلمية :

1- أبو الخير، كمال ،تحديات الأمن السيبراني في ظل الابتزاز الإلكتروني، مجلة الدراسات القانونية المعاصرة، العدد 11، جامعة قسنطينة، 2022 .

2- أبو الخير كمال ،إثبات الجريمة الإلكترونية في ضوء القانون المقارن، مجلة العلوم القانونية والسياسية، العدد 16، جامعة قسنطينة، 2021.

3- بوحنية قوي، الأمن السيبراني ومواجهة الجريمة الإلكترونية في الجزائر، المجلة الجزائرية للأمن والتنمية، العدد 6، جامعة ورقلة، 2022.

4-بن شيخ، سليم، حماية ضحايا الابتزاز الإلكتروني في القانون الجزائري، مجلة القضاء والسياسة، جامعة تلمسان، العدد 14، 2022.

5- بن عمارة، فوزية، حماية الحياة الخاصة في البيئة الرقمية، مجلة الباحث، العدد 9، جامعة قالمة، 2022.

6- بوحنية قوي، الجرائم الإلكترونية وآليات التصدي لها في الجزائر، مجلة القانون والمجتمع، جامعة تلمسان، العدد 10، 2021.

7- جلال ثامر، الجريمة الإلكترونية بين الوقاية والمكافحة، مجلة الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، العدد 14، 2016.

8- حماني، عبد العزيز،التحرش والابتزاز عبر الإنترنت: دراسة قانونية، مجلة العلوم القانونية، العدد 12، جامعة وهران،2021.

9- فتحي بودفلة، الإثبات في الجرائم الإلكترونية أمام القضاء الجزائي الجزائري، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 7، 2021.

10- لمياء رحماني، الجرائم المستحدثة في ظل تطور تكنولوجيا الإعلام والاتصال: الابتزاز الإلكتروني نموذجا، مجلة العدالة والقانون، جامعة سعيدة، العدد 14، جوان 2022.

11- فتحي بودفلة، الإثبات في الجرائم الإلكترونية أمام القضاء الجزائي الجزائري، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 7، 2021.

12- سامي بوعزيز، التحقيق في الجرائم الإلكترونية: بين النص القانوني والواقع *العملي*، مجلة دفاتر القانون، جامعة وهران، العدد 15، 2022.

13- عكوش سيهام، الحماية القانونية لحق الخصوصية من جريمة التهديد عرب مواقع التواصل الاجتماعي وفقا للقانون الجزائري، مجلة السياسة العالمية، الصادرة عن مخبر الدراسات السياسية والدولية بجامعة احمد بوقرة بومرداس، المجلد 06،العدد1،الجزائر، سنة2022.

14- فاطمة الزهراء رياحي،التحقيق في الجرائم المعلوماتية بين مقتضيات الواقع ونص القانون، مجلة الدراسات القانونية والسياسية، جامعة تبسة، العدد 8، 2021.

15- سليمان بن عبد الرزاق الغديان، يحيى بن مبارك خطاطبة، عزالدين بن عبد الله النعيمي، صور جرائم الابتزاز الإلكتروني ودوافعها وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد27 ،العدد69 ، يناير2018 .

16- علي بوسعدية، مشاكل إثبات الجرائم الإلكترونية، مجلة الدراسات القانونية والسياسية، العدد 18، جامعة تبسة، 2021.

17- حنان طواهرية، جرائم الابتزاز الإلكتروني في التشريع الجزائري، مجلة العلوم القانونية والسياسية، العدد 15، جامعة سطيف 2، 2020.

18- رضوان بوحملة، الدور الوقائي لتكنولوجيا المعلومات في مواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن والعدالة، جامعة الجزائر 1، العدد 12، 2020.

19- ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الابتزاز، مقال منشور على الشبكة الإلكترونية، المجلة العربية للدراسات ألأمنية، المجلد33 ،العدد70 ،الرياض2017 .

رابعا-الرسائل الجامعية :

أ-مذكرات الماستر :

1- خربوش خالد، الدليل العلمي وأثره في اثبات الجنائي، لنيل مذكرة الماجستير، جامعة أم البواقي، سنة 2009/2008.

2-قداري صارة، أساليب التحري الخاصة في القانون إجراءات الجزائية، لنيل مذكرة الماستر، في العلوم الجنائية، سنة 2011/2010 .

3- سليماني علاء الدين، دور الشرطة في اثبات الجريمة، لنيل مذكرة الماستر، حقوق تخصص والعلوم السياسية، جامعة خيضر، سنة 2014/2013 .

4-عصام المكي، الإثبات الجنائي بالوسائل العلمية الحديثة في التشريع الجزائري، لنيل مذكرة الماستر، قسم العلوم السياسية، جامعة عبد الحميد ابن باديس/ مستغانم، سنة2016 /2017 .

5- التواتي نوال، الابتزاز الإلكتروني ووسائل مكافحته في ظل التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة بسكرة، 2021.

ب-رسائل الدكتوراه:

1- بن طالب ليندة، الدليل الالكتروني ودوره في الإثبات الجنائي ،دراسة مقارنة، أطروحة دكتوراه ، جامعة مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، نوقشت في 2019/01/23.

- كبابسة، فاطمة الزهراء،التكييف القانوني للجريمة المعلوماتية في ضوء قانون العقوبات الجزائري،أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر 1، 2020/2019.

الفهرس:

قائمة المحتويات **الصفحة**

الملخص :

الابتزاز الإلكتروني هو سلوك إجرامي يتم عبر الوسائط الرقمية يقوم فيه الجاني بتهديد الضحية بهدف تحقيق مكاسب غير مشروعة، وتقوم المسؤولية الجنائية على توافر أركان الجريمة التقليدية، مع تكييف الوسيلة الإلكترونية كظرف مشدد، ويعاقب الفاعل وفقا للتشريعات الوطنية، في القانون الجزائري الذي يولي اهتماما متزايدا لمكافحة هذه الجريمة نظرا لتأثيرها الخطير على الأفراد والمجتمع،و تهدف المسؤولية الجنائية إلى حماية الحقوق الرقمية وتحقيق الردع الفعال.

الكلمات المفتاحية : 1/ابتزاز إلكتروني 2/ مسؤولية جنائية 3/ تهديد رقمي 4/ قانون جزائي.

Summary:

Digital extortion is a criminal behavior conducted through digital media, where the perpetrator threatens the victim in order to achieve unlawful gains. Criminal liability is based on the presence of the elements of traditional crime, with the digital means being treated as an aggravating circumstance. The offender is punished according to national legislation, particularly in Algerian law, which is increasingly focusing on combating this crime due to its severe impact on individuals and society. The aim of criminal liability is to protect digital rights and achieve effective deterrence.

Keywords: 1) Digital Extortion 2) Criminal Liability 3) Digital Threat 4) Penal Law.