

جامعة عبد الحميد بن باديس - مستغانم
كلية الحقوق والعلوم السياسية

المرجع:

قسم : القانون الخاص

مذكرة نهاية الدراسة لنيل شهادة الماستر

الآليات القانونية لمكافحة جريمة الابتزاز الالكتروني
في التشريع الجزائري

التخصص: قانون قضائي

الشعبة: حقوق

تحت إشراف الأستاذ:

من إعداد الطالبة:

بن عوالي علي

بلعيد نبيهة

أعضاء لجنة المناقشة

الأستاذ(ة).....	مجبر فاتحة.....	رئيسا
الأستاذ.....	بن عوالي علي.....	مشرفا مقرر
الأستاذ(ة).....	زواتين خالد.....	مناقشا

السنة الجامعية: 2025-2026

نوقشت يوم: 2026/06/17



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة عبد الحميد بن باديس مستقلم



كلية الحقوق و العلوم السياسية

مصلحة الترتيبات

تصريح شرقي خاص بالالتزام بقواعد النزاهة العلمية في إنجاز البحث

أنا الممضي أدناه , الطالب (ة) :

اللقب : الاسم : تاريخ : 2023/08/13

الحامل (ة) لبطاقة التعريف الوطنية رقم : 404677377 والصادرة بتاريخ : 2023/08/13

المسجل (ة) بكلية : القسم : قاضي الخليل

والمكلف (ة) بإنجاز مذكرة ماستر بعنوان :

الإبادة القاتونية كمكافحة جرمية الإلكترونية في التشريع

البحر :
البحر :
البحر :

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

التاريخ : 2023/06/17

امضاء المعني



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

قال الله تعالى:

{ فرحين بما آتاهم الله من فضله... }

الآية 170 من سورة آل عمران

الإهداء :

« وَمَا بِكُمْ مِنْ نِعْمَةٍ فَمِنَ اللَّهِ »

الحمد لله أولاً و أخيراً، حمداً كثيراً طيباً مباركاً فيه على فضله وكرمه وتوفيقه لي حتى وصلت إلى هذا اليوم.

إلى جدتي الحبيبة...

إلى قدوتي الأولى ومعنى الحب والحنان

إلى من كان دعاؤها سر نجاحي و حنائها بلسم جراحي،

إلى من أرشدتني ورافقتني في كل مشاوير حياتي ولا تزال تفعل إلى الآن،

اللهم احفظها وارزقها العفو والعافية.

إلى أبي الغالي...

إلى السند الذي لم يمل، والداعم الذي لم يتراجع يوماً،

إلى من زرع في الطموح وحصد اليوم الفخر.

هذا التخرج ثمرة تعبك قبل أن يكون إنجازي،

فلك مني كل الامتنان والحب، وأسأل الله أن يديمك تاجاً

فوق رأسي.

إلى والدتي الغالية...

التي احتضنتني بقلبها قبل يدها التي سهلت لي الطريق بدعائها

إلى الظل الخفي والقلب الحني إلى من تعبت وسهرت

وضحت لتصنع مني هذا النجاح.

تخرجي اليوم هو ثمرة صبرك اللهم احفظها وارزقها العفو والعافية.

إلى إخوتي وأخواتي...

إلى من أشاركهم الحب و الذكريات،

وإلى من أعتز بوجودهم في حياتي.

إلى عماتي العزيزات...
تقديرًا لمحبتهم ودعمهم وتشجيعهم المستمر .
كما أتقدم إليهن بخالص الشكر و الامتنان؛
داعية الله أن يحفظهن و يجزيهن خير الجزاء .
إلى رفيقاتي اللواتي كنّ بمثابة أخوات،
شارككني تفاصيل الطريق، فخففن عني العثرات وملأن أيامي بالأنس والمساندة.

الطالبة: بلعيد نيرة

شكر و تقدير

الشكرو الثناء لله عز وجل أولاً على نعمة الصبر والقدرة على إنجاز هذا العمل، فله الحمد على هذه النعم.

أتقدم بعظيم الشكر والإمتنان إلى مشرفي الفاضل الذي كان خير معلم لي، وقد نهلت من بحر علمه الواسع والذي لم يبخل علي بمعلومة من علمه الغزير.

فإنني أقف له إحتراماً على تفضله بالإشراف على هذه المذكرة، وأسأل الله أن يديم عليه صحته وأن يبقيه منارة لكل من أراد طريق العلم.

كما أتقدم بالشكر الجزيل إلى أستاذتي أعضاء المناقشة الأكارم الذين طوقوني بتكرمهم بالموافقة على مناقشة مذكرتي جزاهم الله جميعاً كل خير.

قائمة المختصرات:

ق.ع.ج	قانون العقوبات الجزائري
ق.إ.ج.ج.ج	قانون الإجراءات الجزائية الجديد
د.ط	دون طبعة
د.س	دون سنة
ص	صفحة
ص-ص	من صفحة إلى صفحة

مقدمة

تعتبر الجريمة الإلكترونية من الظواهر الإجرامية الحديثة التي برزت في عصرنا الحالي، المعروف بعصر السرعة. وقد عانت المجتمعات في الآونة الأخيرة من انتهاكات لحقوق الأفراد وخصوصياتهم الإلكترونية، وذلك في ظل انتشار هذه الجرائم وتفاقمها، وقد ارتبط تطور هذا النوع من الجرائم بالتطورات التكنولوجية التي سهلت سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات، مما ساهم في تسهيل حركة المعاملات. ومع ذلك، فإن هذا التقدم المذهل لا يخلو من عيوب، حيث أسفر عن مجموعة من الانعكاسات السلبية الخطيرة نتيجة سوء استخدام هذه التقنيات المتطورة و الانحراف عن الأغراض المرجوة منها. و بالتالي أدت هذه الظاهرة الإجرامية إلى ظهور فئة جديدة من المجرمين يعرفون بالمجرمين المعلوماتيين، الذين يستغلون تقنيات المعلومات لتعزيز قدراتهم الإجرامية مستخدمين الشبكة المعلوماتية كوسيلة سهلة لتنفيذ عملياتهم الإجرامية ، مما يلحق الضرر بالآخرين.

ومع ارتفاع معدلات الجريمة الإلكترونية و تطور أشكالها، أصبح هناك تهديد مباشر على الشعوب و الدول في جميع أنحاء العالم، مما يستدعي تنبيه مجتمعات العصر الحاضر إلى حجم المخاطر و الخسائر الجسيمة الناجمة عن هذا النوع من الجرائم، حيث تستهدف الاعتداء على المعطيات بمختلف دلالاتها التقنية الواسعة.

الأمر الذي دفع بالدول إلى البحث عن سبل الوقاية و الحد من هذه الظاهرة الخطيرة، من خلال تعزيز الوعي و تطبيق تدابير وقائية أمنية و غيرها من الوسائل.لذا، أصبح من الضروري أن يتزامن تطور الجريمة و أساليبها مع تطور في السياسة التشريعية بشكل عام و السياسة الجنائية بشكل خاص، فقد أصبح من الواضح أن استخدام الشبكة المعلوماتية يشكل تهديداً مباشراً للمنظومة الحقوقية. و من هذا المنطلق تكثفت الجهود الدولية و الوطنية لمواجهة الآثار السلبية الناجمة عن إساءة استخدام تقنيات الاتصالات و المعلومات.

و لقد أصبحت جريمة الابتزاز الإلكتروني واحدة من أكثر الجرائم قسوة و انتشاراً في العصر الحديث، خاصةً مع استخدام وسائل الاتصال الحديثة كأداة للاستغلال وانتهاك خصوصية الأفراد و تهديدهم بحيث يعرض هذا النوع من الجرائم الضحايا لمواقف حرجة داخل

المجتمع، حيث يتسلل الجاني إلى حياتهم الخاصة ليحولها إلى وسيلة للضغط عليهم أو ابتزازهم و عادةً ما يرتكب الجاني هذه الجرائم بعد حصوله على ما يمنحه القدرة على السيطرة على ضحيته و استغلالها لتحقيق مآربه.

ومن الجدير بالذكر أن الابتزاز الإلكتروني يعرف بأنه كل استخدام غير قانوني يقوم به شخص مبتدئ أو متخصص، مستخدماً وسائل الاتصال الحديثة، بهدف تهديد الضحية أو تخويفها من خلال نشر صور أو فيديوهات أو محادثات عبر منصات مثل واتساب أو فايسبوك و غيرها، يهدف هذا التهديد إلى تسريب معلومات سرية تخص الضحية عبر الوسائل الإلكترونية، و غالباً ما يكون الهدف منه الحصول على مبالغ مالية أو إجبار الضحية على القيام بأعمال غير مشروعة لصالح المبتزين.

و في ظل انتشار هذا النوع الجديد من الجرائم المعلوماتية الخطيرة، و مع زيادة مستخدمي المواقع الإلكترونية بطرق غير مشروعة، اتجهت العديد من الدول إلى معالجة هذه الجرائم الإلكترونية من خلال سن التشريعات القانونية اللازمة التي تجرم هذه الأفعال غير القانونية عبر الشبكات و المواقع الإلكترونية لمواجهة هذه التحديات.

و رغم أن الهدف الأساسي من جرائم الابتزاز الإلكتروني عبر الوسائل المختلفة غالباً ما يكون الحصول على المال، إلا أن ضحايا هذه الجرائم يعانون من ضغوط نفسية و بيئية قاسية خلال فترة تعرضهم للابتزاز، إن الخوف من الفضيحة أو التشهير يزيد الأمور سوءاً، مما يؤدي في كثير من الأحيان إلى تدهور حالتهم النفسية بشكل خطير و في بعض الحالات، قد تصل هذه المعاناة إلى أن يدفع اليأس ببعض الضحايا إلى إتخاذ قرار بانهاء حياتهم، إذا لم تتدخل الأجهزة الأمنية في الوقت المناسب لتقديم الدعم و إنهاء هذه المعاناة.

وتبرز أهمية الدراسة من خلال تسليط الضوء، على أحد الموضوعات الحديثة و المهمة بحيث تتمثل الأهمية العلمية لهذه الدراسة في اهتمامها بظاهرة إجرامية مستحدثة تتمثل في جريمة الابتزاز الإلكتروني، و التي برزت و تطورت في ظل التقدم المتسارع لتكنولوجيا المعلومات و الاتصال، و لاسيما مع الانتشار الواسع لاستخدام شبكة الإنترنت. وقد أفضى هذا

التطور إلى ظهور أنماط إجرامية تتميز بخصوصية تختلف عن الجرائم التقليدية، سواء من حيث الوسائل المستخدمة أو طبيعة الأفعال المرتكبة أو الآثار المترتبة عنها، الأمر الذي يقتضي ضرورة تبني معالجة قانونية تتلاءم مع طبيعتها الخاصة. و من هذا المنطلق، تبرز أهمية إعادة النظر في مدى كفاية النصوص القانونية المتعلقة بتجريم الابتزاز الإلكتروني، و تقييم فعاليتها في توفير الحماية القانونية اللازمة، و كذا مدى مساهمتها في مكافحة هذه الجريمة و الحد منها.

أما بالنسبة للأهمية العملية لهذه الدراسة، فتتمثل في إبراز خطورة جريمة الابتزاز الإلكتروني و توعية أفراد المجتمع بمخاطرها المتزايدة، خاصة في ظل التوسع المستمر في استخدام الوسائط و الأجهزة الإلكترونية. كما تسعى الدراسة إلى بيان الآثار السلبية الناجمة عن سوء استعمال التكنولوجيا الحديثة، حيث إن تزايد الاعتماد على شبكة الإنترنت يقابله بالضرورة ارتفاع في معدلات الجرائم الإلكترونية، و في مقدمتها جريمة الابتزاز الإلكتروني. و عليه، فإن مواجهة هذه الجريمة تقتضي الإحاطة الشاملة بمختلف أبعادها و آليات التصدي لها، سواء من الناحية التقنية، التي يضطلع بها المختصون في مجال تكنولوجيا المعلومات، أو من الناحية القانونية، التي تقع ضمن اختصاص رجال القانون و الجهات القضائية المختصة.

و لقد قمنا باختيار هذا الموضوع و جعلناه موضوع دراستنا في هذا البحث نظراً لأسباب ذاتية تتمثل في الرغبة في تسليط الضوء على جريمة تُعد من أخطر الجرائم المستحدثة التي تمس الحق في الخصوصية و حرمة الحياة الخاصة، لما تشكله من انتهاك صارخ لحقوق الأفراد و حرياتهم، و أسباب موضوعية تتمثل في الانتشار المتزايد لجريمة الابتزاز الإلكتروني داخل المجتمع، و ما صاحب ذلك من تنامي ملحوظ في عدد ضحاياها و أساليب ارتكابها، الأمر الذي يفرض ضرورة دراستها دراسة قانونية معمقة و التعرض لها باعتبار أن المجتمع الجزائري من المجتمعات العربية معروفة بالعادات و التقاليد و الأعراف الاجتماعية التي تحتفظ على كل ما يتعرض للسمعة و الشرف و هو ما حتم علينا تقييم النصوص القانونية التي لها صلة بجريمة الابتزاز الإلكتروني.

و علاوة على ذلك، فإن جريمة الابتزاز الإلكتروني فرضت نفسها كقضية حديثة تواجه المجتمع الجزائري و سائر المجتمعات الأخرى على اختلاف أعراقها. و على الرغم من الجهود التي بذلها المشرع الجزائري، شأنه شأن التشريعات المقارنة لمواكبة التطورات التقنية من خلال إصدار نصوص قانونية خاصة بمكافحة الجرائم الإلكترونية، إلا أن الطبيعة الخاصة لجريمة الابتزاز الإلكتروني، كونها جريمة مركبة و معقدة و عابرة للحدود، تثير العديد من التحديات القانونية فيما يتعلق بالتجريم و العقاب و عليه تتبلور الإشكالية الرئيسية لهذه الدراسة في التساؤل التالي:

إلى أي مدى نجح المشرع الجزائري في بناء منظومة قانونية متكاملة و فعالة لمجابهة جريمة الابتزاز الإلكتروني ؟

و عليه فإن المنهج المتبع في دراستنا هو المنهج الوصفي، والتحليلي من خلال إيراد النصوص القانونية ذات الصلة بموضوع البحث في التشريع الجزائري، و من ثم الاتجاه نحو السلوك الإجرامي لغرض الحد منه بفرض عقوبات مشددة على كل من يرتكب جريمة الابتزاز الإلكتروني و المنهج الوصفي من خلال وصف ظاهرة الابتزاز الإلكتروني، وكذا اعتمدنا على المنهج المقارن في المواضع التي تجب المقارنة من أجل معرفة أوجه الشبه و مواطن الاختلاف في ذلك.

وتتمثل أهداف الدراسة في تحقيق ما يأتي:

- تحديد ماهية جريمة الابتزاز الإلكتروني من خلال التعرف على مفهومها و مراحل ارتكابها وصورها.
- الآثار المترتبة عن جريمة الابتزاز الإلكتروني.
- بيان التكييف القانوني لظاهرة الابتزاز الإلكتروني في التشريع الجزائري.
- بيان العقوبات المترتبة على مرتكبي جريمة الابتزاز الإلكتروني.
- تحديد إجراءات التحقيق و أساليب الإثبات في جريمة الابتزاز الإلكتروني.
- دور المؤسسات الوطنية و الأمنية للحد من جريمة الابتزاز الإلكتروني.

و لغرض جمع شتات الموضوع و الإحاطة به، ومن أجل أن تكون دراستنا ملمة ومحيطة بالجوانب المتعلقة بموضوع بحثنا الموسوم ب "الآليات القانونية لمكافحة جريمة الابتزاز الإلكتروني في التشريع الجزائري" ، اقتضت ضرورة البحث العلمي تقسيم هذه الدراسة إلى فصلين، نتناول في الأول الإطار المفاهيمي لجريمة الابتزاز الإلكتروني، من حيث بيان ماهية جريمة الابتزاز الإلكتروني في بحث أول، و سنتناول التكييف القانوني لجريمة الابتزاز الإلكتروني في بحث ثان.

أما الفصل الثاني فسنخصصه لمناقشة الإطار الإجرائي للابتزاز الإلكتروني، و ذلك في بحثين، نبين في الأول التحقيق و الإثبات في جريمة الابتزاز الإلكتروني و نبحت في الثاني على مكافحة جريمة الابتزاز الإلكتروني على المستوى المؤسساتي و الأمني الوطني. و يعقب هذا الفصلين خاتمة تتضمن أهم النتائج التي سنتوصل إليها، و ما يمكن تقديمه من مقترحات في رد هذا الموضوع.

الفصل الأول:

الإطار المفاهيمي للابتزاز الإلكتروني

شهد العالم ثورة ملحوظة في مجالات التكنولوجيا و الاتصالات و تقنية المعلومات، حتى أن العبارة القائلة بأن العالم أصبح قرية صغيرة تقترب من الصواب في معظم جوانبها. و قد تجلت هذه الثورة التكنولوجية في التقدم اللافت في مجال الحواسيب الآلية وملحقاتها، بالإضافة إلى البرمجيات المرتبطة بها، كما أصبح الاعتماد على هذه التكنولوجيا واضحا في جميع المؤسسات الرسمية و غير الرسمية، مما أدى إلى تدمير العنصر البشري من استبدال الأجهزة الذكية بما في ذلك الحواسيب و البرامج للجهود البشرية، حتى بدأ الذكاء الاصطناعي يحل محل الذكاء البشري، و مع ذلك فإن هذه النعمة قد رافقتها نقمة ، تمثلت في الاستخدام غير المشروع لهذه التكنولوجيا، حيث أصبحت تستخدم كوسيلة للتدمير بدلا من البناء من قبل الأفراد الخارجين عن القانون و ضعفاء النفوس لتحقيق أهدافهم المشبوهة، بحيث ساهمت صعوبة تحديد مرتكبي هذا النوع من الجرائم للوصول إليهم، و من أبرز هذه الجرائم جرائم الابتزاز الإلكتروني التي ازدادت انتشاراً بشكل ملحوظ في العديد من دول العالم في الآونة الأخيرة.¹

استناداً إلى ما تم تقديمه، سيعنى هذا الفصل ببيان الإطار المفاهيمي لجريمة الابتزاز الإلكتروني من خلال مبحثين، في المبحث الأول سنستعرض ماهية جريمة الابتزاز الإلكتروني، بينما سنخصص المبحث الثاني لتناول التكييف القانوني لجريمة الابتزاز الإلكتروني في التشريع الجزائري.

¹ - أمير فرج يوسف ، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني - دراسة مقارنة، د.ط ، دار المطبوعات الجامعية ، الإسكندرية ، 2023 ، ص - ص 05 - 06 .

المبحث الأول : ماهية جريمة الإبتراز الإلكتروني

يعتبر الإبتراز الإلكتروني وفقاً لمعظم القوانين في دول العالم، أحد أشكال الجرائم الإلكترونية التي تثير قلق مستخدمي التكنولوجيا، و يعود ذلك إلى وجود العديد من الانتهاكات التي تمس خصوصياتهم وبياناتهم الشخصية، بالإضافة إلى صورهم و ما يتعلق بحياتهم الخاصة، مما يؤدي إلى تعريضهم للفضيحة أمام الجمهور وقد تطورت هذه الجرائم بشكل ملحوظ، حتى أصبحت تظهر انتشاراً أكبر مما هو مسجل على أرض الواقع¹، ولذا تعد جريمة الإبتراز الإلكتروني من الممارسات المرفوضة، حيث تؤثر سلباً على الأفراد الأمنيين، وتحول حياتهم من حالة من الهدوء إلى حالة من الخوف و الاكتئاب و الاضطراب، مما يجعل الضحية رهينة في يد المبتز، إذ يصبح مضطراً للامتثال لأوامره و تلبية رغباته بغض النظر عن مضمون التهديد، سواء كان يتعلق بالشرف و السمعة و الاعتبار أو بالنفس أو المال، وعليه يعتبر الإبتراز الإلكتروني من الجرائم الفظيعة، حيث قد يصل إلى درجة من الرق والعبودية إذ يتم تهديد الآخرين بوسائل متعددة لإشعارهم بالخطر المحدق بهم، مما يدفعهم للخضوع لرغبات الجناة (المبتزين) و يجعلهم تحت سيطرتهم.²

و بناءً على ذلك سنقسم هذا المبحث إلى مطلبين، نناقش في الأول مفهوم الإبتراز الإلكتروني و مراحل ارتكابه و صوره و نحدد في المطلب الثاني ذاتية الإبتراز الإلكتروني.

المطلب الأول: مفهوم الإبتراز الإلكتروني و مراحل ارتكابه و صوره

ظهرت العديد من الجرائم الإلكترونية التي تشكل تهديداً للأفراد و المجتمعات نتيجة للتقدم السريع في التكنولوجيا و انتشار وسائل الاتصال الرقمية، و من أبرز هذه الجرائم جريمة

¹ - أمير فرج يوسف، المرجع السابق، ص 7.

² - باقر غازي حنون الدراجي، المسؤولية الجنائية الناشئة عن الإبتراز الإلكتروني، د.ط، دروب المعرفة للنشر و التوزيع،

الإسكندرية -جمهورية مصر العربية ، 2024 ، ص 69 .

الإبتهاز الإلكتروني¹، مما يستدعي ضرورة منحها أهمية كبيرة نظراً لتأثيرها الواسع و غير المحدود ، بالإضافة إلى سهولة ارتكابها، حيث يمكن تنفيذها من خلال وسائل إلكترونية مما يتيح إمكانية انتشار الفعل بين عدد كبير من الأشخاص و في أماكن متعددة.²

و لذا ارتأينا أن نتطرق في هذا المطلب إلى مفهوم الإبتهاز الإلكتروني و مراحل ارتكابه وصوره عبر ثلاثة فروع الآتية :

الفرع الأول : تعريف الإبتهاز الإلكتروني لغة و اصطلاحاً

من أجل تعريف جريمة الإبتهاز الإلكتروني لا بد لنا من التطرق إلى التعريف اللغوي مروراً بالتعريف الإصطلاحي الذي يشمل التعريف الفقهي و التشريعي و هو ما سوف يتم تناوله في هذا الفرع .

أولاً : التعريف اللغوي للإبتهاز الإلكتروني

" وفقاً لما جاء في معجم لسان العرب للعلامة أبو الفضل جمال الدين محمد بن مكرم (ابن منظور) عد الإبتهاز لغة يأتي من البز و معناه السلب، و ابتزرت الشيء أي استلبته، وبز الشيء يبزُ بزا : انتزعه و أبتز المال من الناس، أي أخذه منهم بالقوة " .³

وبذلك يُعرف الإبتهاز بأنه: " الحصول على المال أو المنافع من شخص تحت التهديد بفضح بعض أسرارهِ أو غير ذلك " .⁴

" أما بالنسبة لـ(الإلكتروني) و مصدرها الإنكليزية المعربة (electronic) التي تعني طاقة النواة، و بالنتيجة فهو مصطلح أجنبي عن اللغة العربية و لا وجود له في معاجمها أو يقابلها

¹ - عبد القادر سعد حاتم الحبيب ، الإطار القانوني لمكافحة الإبتهاز الإلكتروني في العراق و لبنان : دراسة مقارنة ، مجلة العلوم الإنسانية و الطبيعية ، المجلد 06 ، العدد 01 ، 2025 ، ص784 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص20 .

³ - أماني هاشم لطيف ، الإبتهاز الإلكتروني و تداعياته على الواقع السياسي و الاجتماعي العراقي ، مجلة دراسات دولية ، العدد 98 ، 2024 ، ص563 .

⁴ - متاح على الموقع الإلكتروني www.almaany.com تاريخ الزيارة 2026/02/21 على الساعة 17:12 .

في الاصطلاح اليوم (التقنية الحديثة ذات الطبيعة الرقمية) ، و هو مشتق من ثقافة الشيء، وتصريفها أتعن، يتقن، إتقاناً¹.

ثانيا : التعريف الاصطلاحي للإبتراز الإلكتروني :

للإمام بالتعريف الاصطلاحي للإبتراز الإلكتروني يتعين علينا التطرق إلى التعريف الفقهي و التشريعي المرتبط به ، و ذلك على النحو التالي :

1- التعريف التشريعي للإبتراز الإلكتروني:

يميل المشرع إلى عدم وضع تعريفات دقيقة، مكتفياً بتحديد الأفعال المجرمة من خلال النصوص تاركاً مهمة صياغة التعريفات و تفسيرها للفقهاء القانوني لأن تعريف الجريمة في القانون لا يحمل قيمة فعلية، فالمشرع استناداً إلى مبدأ شرعية الجرائم و العقوبات، يقوم بتصنيف الأفعال المجرمة دون الحاجة إلى تحديد مفهوم الجريمة و يعود ذلك لعدة أسباب منها تنوع الجرائم و تغير النظرة إليها مع مرور الزمن²، لذا أوكلت هذه المهمة للفقهاء، حيث إن أي تعريف مهما كانت دقته و جهوده في صياغته، لن يكون شاملاً أو مانعاً لكل المعاني المطلوبة، و حتى إذا كان التعريف دقيقاً في فترة معينة، فقد لا يظل كذلك في أوقات لاحقة.³

واستكمالاً لما تم ذكره سنورد بعض التشريعات المقارنة التي تطرقت إلى الإبتراز الإلكتروني سواء بتشريع قوانين خاصة بالجرائم الإلكترونية بشكل عام، بالإضافة إلى بعض التشريعات التي نصت على الإبتراز في قانون العقوبات، بالإضافة إلى المشرع الجزائري.

" بالنسبة للمشرع العماني، فنجد أنه عرف الإبتراز الإلكتروني في قانون مكافحة جرائم تقنية المعلومات الصادر بالمرسوم السلطاني رقم 12 لسنة 2011، و ذلك في المادة (18) والتي نصت على..... كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 21 .

² - ياسر مهيب عبد العزيز المليكي ، جريمة الإبتراز الإلكتروني إشكالية الحماية الموضوعية و الإجرائية في التشريع اليمني ، مجلة العلوم التربوية و الدراسات الإنسانية ، العدد 36، د.س، ص 835 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص - ص 26 - 27 .

في تهديد شخص أو ابتزازه لحمله على القيام بفعل أو امتناع و لو كان هذا الفعل أو الامتناع عنه مشروعاً " ¹.

" أما المشرع الفلسطيني، فقد عرف الإبتراز الإلكتروني في المادة (15) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الالكترونية و تعديلاته (كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه و لو كان هذا الفعل أو الامتناع مشروعاً ، إذا كان التهديد بارتكاب جنائية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب) " ².

" أما بالنسبة للمشرع الفرنسي، فقد تم تعريف جريمة الإبتراز في قانون العقوبات الذي صدر عام 1992، حيث جاء في المادة 312 أن الفقرة الأولى منها تنص على أن (الإبتراز هو الحصول عن طريق التهديد بالعنف أو الإكراه، على توقيع التزام أو تنازل، أو كشف عن سر، أو تسليم أموال أو قيم أو على أي ممتلكات أخرى) كما ذهبت الفقرة العاشرة من المادة ذاتها في تعريفه إلى أن (الإبتراز هو الحصول ، عن طريق التهديد بكشف أو ادعاء وقائع من شأنها أن تضر بالشرف أو السمعة أو الاعتبار، على توقيع أو تعهد أو تنازل أو كشف عن سر أو تحويل أموال أو أوراق مالية أو أي سلعة أخرى) " ³.

" أما المشرع العراقي، فلم ترد كلمة إبتراز في متن قانون العقوبات رقم 111 لسنة 1969 و تعديلاته، و عند التدقيق في مشروع قانون جرائم المعلوماتية، فإننا نجد أن مسودة المشروع لم تعرف الإبتراز الإلكتروني بشكل صريح، إلا أنه يتضح من إستقراء نص المادة

¹ - باقر غازي حنون الدراجي ، ص - ص 27 - 28.

² - محمد علي أحمد أبو علي ، جريمة الإبتراز الإلكتروني في التشريع الفلسطيني ، ماجيستر ، العلوم الجنائية ، الجامعة العربية الأمريكية - كلية الدراسات العليا ، 2022/9 ، ص 12 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 27 .

(11 أولاً / أ.ب) أن جريمة الابتزاز تنطوي على التهديد و الترويع لحمل المجني عليه على القيام بالأفعال التي يطلبها الجاني¹.

و خلاصة القول، يتبين من خلال النصين العماني و الفلسطيني أنهما اعتمدا على مصطلح "ابتزاز" بشكل واضح في محتوياتهما، و قدما تعريفاً متشابهاً للإبتراز الإلكتروني .
بينما نجد أن المشرع الفرنسي و العراقي قد عرفا الابتزاز الإلكتروني في قانون العقوبات، إلا أن المشرع الفرنسي قد عاقب على جريمة الابتزاز بنص خاص و صريح، في حين اكتفى المشرع العراقي بالإشارة إلى الابتزاز كجزء من التهديد و الترويع الذي يستخدم لإجبار الضحية على القيام بالأفعال التي يطلبها الجاني.

وهنا يثار التساؤل هل قام المشرع الجزائري بمعاقبة جريمة الابتزاز الإلكتروني بشكل واضح من خلال نص قانوني خاص، أم أنه استمد على تكييف هذه الجريمة من خلال تطبيق القوانين الجنائية التقليدية ؟

وللإجابة على هذا السؤال، يتعين علينا استعراض الإطار القانوني الذي ينظم الجرائم الإلكترونية بشكل عام، مع التركيز على جريمة الابتزاز الإلكتروني كأحد صور هذه الجرائم بصفة خاصة، قام المشرع الجزائري على غرار العديد من التشريعات المقارنة، بتطوير مجموعة من القوانين لمواكبة التطورات التكنولوجية الحديثة و التصدي للجرائم الإلكترونية وذلك نتيجة الانتشار السريع لهذه الجرائم في المجتمع الجزائري، و قد أصدر القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها، و في عام 2018 تم إصدار قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .

ثم تلاه التعديل الأخير لقانون رقم 25-11 المعدل و المتمم للقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي .

¹ - باقر غازي حنون الدراجي، المرجع السابق ، ص 28 .

من خلال استقراءنا لنصوص القوانين المذكورة أعلاه لم يعرف المشرع الجزائري جريمة الابتزاز الإلكتروني إلا أنه يلاحظ بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها أن المشرع الجزائري اصطلح على الجرائم الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال فعرفها حسب المادة 02/أ على أنها " جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية ".¹ بناءً على ما تقدم، نرى أن المشرع قد نجح في تعريفه، حيث جمع بين الحالات التي تعتبر فيها نظم المعلومات و شبكات الاتصال إما موضوعاً للجريمة أو وسيلة أو دعامة للجرائم التقليدية، و لولا وجود هذه النظم المعلوماتية و شبكات الاتصالات إما اكتسبت هذه الجرائم الصفة المعلوماتية.²

و بالرجوع إلى أحكام قانون العقوبات الجزائري و تعديلاته، يتبين أن المشرع الجزائري لم يتناول جريمة الابتزاز الإلكتروني كنموذج إجرامي مستقل و صريح، بل عالجه من خلال النصوص العامة المتعلقة بجريمة التهديد ، و قد قام المشرع بتمييز نوعين من التهديد :

1- التهديد المجرد: حيث يقتصر الفعل الإجرامي على إحداث الرعب و الخوف في نفس الضحية و يعاقب عليه وفقاً للمادة 285 من ق.ع. ج .

¹ - راجع المادة 02/أ من القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادرة في 16 غشت 2009 .

² - إسمهان بوضياف ، الجريمة الإلكترونية و الاجراءات التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، العدد 11 ، 2018 ، ص 352 .

2- التهديد المصحوب بطلب أو تكليف بفعل معين أو الامتناع عن فعل: و هو نوع أكثر خطورة من التهديد المجرد، حيث يتضمن عناصر الابتزاز و يحقق نفعاً مادياً للمبتز، و يعاقب عليه وفقاً للمواد 284، 286، 371 من ق.ع.ج.¹

غير أن التطور المتسارع لتكنولوجيا المعلومات و وسائل الاتصال الحديثة و ما نتج عنه من ظهور أنماط إجرامية مستحدثة، من بينها جريمة الابتزاز الإلكتروني، كشف عن وجود قصور تشريعي في الإحاطة بمختلف صور هذه الجريمة. الأمر الذي دفع المشرع الجزائري إلى التدخل بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 ، بهدف تدارك هذا الفراغ التشريعي و تعزيز المنظومة الجزائية لمواجهة الجرائم المرتكبة في البيئة الرقمية. و عليه، جاء هذا القانون لتجريم بعض السلوكيات الإجرامية المستحدثة، و من بينها أفعال الابتزاز و ذلك وفقاً لما نصت عليه المادة 371 من ق.ع.ج .

2- التعريف الفقهي للابتزاز الإلكتروني:

قبل الشروع في تقديم التعريفات الفقهية المتعلقة بالابتزاز الإلكتروني، نرى أنه من المناسب تناول بعض التعريفات الفقهية لجريمة الابتزاز التقليدي، لأنها اللبنة الأساسية التي تطورت منها الجريمة محل الدراسة.

لقد تعددت التعريفات الفقهية لتعريف الابتزاز بحيث حظي هذا المصطلح باهتمام الفقهاء و مفسري القانون ، إذا عرف الابتزاز بأنه : " فعل يقوم به شخص بتهديد شخص آخر شفاهاً أو كتابة، و لا عبرة بنوع عبارة التهديد، ما دام من شأنها التأثير في نفس المجني عليه كتخويفه أو مجرد إزعاجه من خطر لم يتحقق بعد، بل قد يلحق بماله، أو بنفسه، أو بمال أو نفس أي شخص آخر له صلة بالمجني عليه"²، و بعضهم الآخر عرفه بأنه : "قيام المبتز بتهديد

¹ - ياسين بن عمر ، الابتزاز الإلكتروني للأطفال في التشريع الجزائري ، دفاثر السياسة و القانون ، المجلد 16، العدد 02، 2024، ص 172 .

² - زهراء عادل سلمي ، جريمة الابتزاز الإلكتروني (دراسة مقارنة) ، ط01 ، شركة دار الأكاديميون للنشر و التوزيع، عمان - الأردن ، 2020 ص 34 .

شخص بفضح أمره ما لم يستجيب المهدد إلى تنفيذ طلبات الجاني، و غالباً ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف أو الكرامة أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي يتم ابتزازه"¹، و قد عُرف أيضاً بأنه : " نوع من السلب الذي يقضي بالحصول على تسليم أموال، أو قيم، أو سندات، أو توافيق، تحت تهديد إفشاء مشين صحيح أو كاذب"²، في حين ذهب آخر في تعريفه إلى أن " الابتزاز هو أخذ المال من صاحبه جبراً، و بسبب غير مشروع، كالخوف من القتل و هتك العرض و الإيقاع في التهلكة و غيرها من وسائل التهديد و الإكراه"³.

و تماشياً مع ما تم ذكره و بعد استعراض بعض التعريفات الفقهية لجريمة الابتزاز في صورتها التقليدية، الآن سنتناول التعريفات الفقهية المتعلقة بها في سياقها الإلكتروني، حيث تعددت تعريفات هذا الجانب من الفقه للإبتراز الإلكتروني حيث سوف نحاول إيجازها فيما يلي: عُرف البعض الابتزاز الإلكتروني بأنه: " محاولة تحصيل مكاسب مادية أو معنوية من شخص أو أشخاص طبيعي أو إعتباري بالإكراه، و بالتهديد بفضح سر وقع عليه الابتزاز أو هي استغلال القوة مقابل ضعف إنسان آخر سواء كان هذا الضعف مؤقتاً أو دائماً " .⁴ ويعرف آخرون الابتزاز أنه: "محاولة الحصول على شيء ما عن طريق التهديد بالكلمات أو الإيحاءات أو الاتهام بشيء ما عن طريق العنف أو التخويف مثل طرد الشخص و الصراخ عليه و رمي و كسر الأشياء " .⁵

¹ - أميل جبار عاشور ، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي (دراسة مقارنة)،

مجلة أبحاث ميسان ، المجلد 16 ، العدد 31 ، 2020 ، ص 114 .

² - حسين طاهري ، الجرائم المعلوماتية الماسة بالشرف و الاعتبار و الحياة الخاصة و بالأخلاق و الآداب العامة ، د . ط ، دار العلا للطباعة و النشر للترجمة و التوزيع ، أم البواقي - الجزائر ، 2024 ، ص148 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 22 .

⁴ - زهراء عادل سلمي ، المرجع السابق ، ص 35 .

⁵ - حسين طاهري ، المرجع السابق ، ص153 .

يتبين من ما تم ذكره سابقاً أن جميع التعريفات المتعلقة بالابتزاز سواء كان تقليدياً أو إلكترونياً تتفق على اعتبار الابتزاز وسيلة للضغط أو التهديد التي يمارسها المبتز على إرادة الضحية، بهدف تحقيق غاياته و أهدافه المنشودة و يُعتبر الابتزاز مرتبطاً ارتباطاً وثيقاً بالتهديد حيث أنه في غياب التهديد لا يمكن للمبتز أن يحقق ما يسعى إليه.¹

" و يُعد التعريف الأقرب إلى العقل و المنطق هو التعريف الذي أورده جانب من الفقه، بأن الابتزاز هو محاولة الحصول على مكاسب مادية أو معنوية من خلال التهديد بإيقاع أذى سواء بكشف أسرار، أو معلومات خاصة، أو إلحاق أذى بنفس أو مال الضحية، أو شخص عزيز لديه ، معتمداً في ذلك على قوته و نفوذه لاستخراج ما يرغب من ضحيته، لأنه جمع كل صور الغاية من الابتزاز، و أنه جعل مضمون الابتزاز يشمل التهديد بالإيذاء المادي و التهديد بالإيذاء المعنوي".²

استناداً إلى ما ذكر سابقاً، يمكننا تقديم تعريف للابتزاز الإلكتروني بأنه " تهديد الجاني للمجني عليه عبر وسيلة إلكترونية، سواء كان مضمون ذلك التهديد إلحاق أذى بنفس أو مال الضحية، أو شخص يهمه أمره، أم كان نشر صور أو تسجيلات صوتية أو مواد فيلمية أو معلومات أو أسرار تخص الضحية أو شخص يهمه أمره، لحمله على القيام بفعل أو امتناع وسواء أكان هذا الفعل أو الامتناع مشروعاً أم غير مشروع".³

الفرع الثاني : مراحل الابتزاز الإلكتروني

نظراً لكون جريمة الابتزاز الإلكتروني تتميز عن غيرها من الجرائم سواء كانت تقليدية أم رقمية، فإنها تتكون من خمس مراحل تبدأ بجمع مادة الابتزاز، الطلب و التهديد، المقاومة، الإذعان، و تنتهي أخيراً بالتكرار و هذا ما سوف يتم تفصيله كالاتي:

¹ - زهراء عادل سلمي ، المرجع السابق ، ص 36 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 26 .

³ - المرجع نفسه ، ص 26 .

أولاً : الحصول على مادة الإبتراز

تتجسد هذه المرحلة في حصول الجاني على صورة أو تسجيل صوتي أو مقطع فيديو أو معلومات لا يريد المجني عليه أن تنشر علناً.¹

ففي بعض الحالات يتبع المجني عليه عدة طرق و وسائل سبيلاً لتحقيق غايته الدنيئة، ويتم ذلك من خلال غرف الدردشة عبر مواقع التواصل الاجتماعي حيث يمكن للأفراد تبادل الرسائل عبر كتابة النصوص باستخدام لوحة المفاتيح على أجهزة الكمبيوتر أو الهواتف الذكية، بحيث تتيح هذه المنصات للأشخاص رؤية ما تم كتابته، مما يؤدي إلى تلقي ردود فعل من الآخرين، كما يمكن للأفراد تحديد موضوعات معينة للتواصل مما يعزز من فعالية هذه الخاصية .

تعتبر هذه الوسيلة سواء كانت من خلال غرف المحادثة النصية أو المرئية، من أبرز أساليب الإبتراز حيث يقوم بعض الأفراد بالدخول إلى هذه الغرف تحت أسماء مستعارة أو صفات وهمية بهدف ابتزاز الشباب و الفتيات. ثم تتطور العلاقة بين المبتز و الضحية من خلال التواصل المستمر عبر تطبيقات الدردشة مثل إيمو، سكايب، إنستغرام، حيث يقوم المبتز بتسجيل الصور و مقاطع الفيديو التي يرسلها الضحية، بعد ذلك يبدأ المبتز في ممارسة الإبتراز من خلال التهديد بنشر مواد الإبتراز عبر شبكات التواصل الاجتماعي أو إرسالها إلى الأصدقاء و الأقارب، و غالباً ما تكوم الضحية في هذه الحالات من الشخصيات العامة مما يجعل تأثير الرأي العام على حياتهم العملية و الإجتماعية.²

و من زاوية أخرى يتسنى للجاني في بعض الأحوال إنتفاع من صفته الوظيفية للحصول على مواد الإبتراز، مثل كونه موظفاً يُسمح له بالإطلاع على الرسائل أو الاتصالات الهاتفية أو كونه يعمل في قسم الاستعلامات في جهة معينة حيث تُودع لديه هواتف المراجعين. كما يمكن أن يستغل الجاني مهارته الفنية أو المهنية، مثل كونه صاحب محل لصيانة الأجهزة

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص32.

² - أميل جبار عاشور ، المرجع السابق ، ص-ص 119-120.

الذكية أو المتاجرة في الأجهزة المستعملة، أو قد يكون مزوداً لخدمات الأنترنت. بالإضافة إلى ذلك، قد يلجأ الجاني إلى استخدام أساليب احتيالية للحصول على مواد الإبتراز فقد يدعي أنه يشغل منصباً سياسياً أو اجتماعياً مرموقاً، ويسعى لاستغلال هذا الإدعاء للتقرب من ضحاياه، يحاول إقناعهم بمشاركة ملفات شخصية تحت ذريعة الصداقة أو الحب بهدف الزواج بينما يكون الهدف الحقيقي هو ابتزازهم واستغلالهم.¹ تعتبر وسائل الإبتراز الإلكتروني الحديثة من الظواهر السلبية التي تتجلى في استغلال بعض المحتالين الذين يدعون أنهم محاربون ضد الإبتراز الإلكتروني، حيث يقوم هؤلاء الأفراد بالتواصل مع الضحايا و استدراجهم من خلال إنشاء مواقع إلكترونية تحمل عنوان " محاربي الإبتراز الإلكتروني " و يطلب من الضحايا تقديم بياناتهم الشخصية و صورهم.²

ثانيا : الطلب و التهديد

إن مضمون جريمة الإبتراز يتضمن تهديداً مرتبطاً بطلب محدد، و بالتالي لا يمكن اعتبار جريمة الإبتراز قائمة إذا لم يكن التهديد مصحوباً بطلب ففي هذه الحالة تظهر جريمة التهديد كجريمة مستقلة، و تجدر الإشارة إلى أن معظم التشريعات لم تحدد شكلاً معيناً لهذا الطلب، حيث يمكن أن يتمثل في القيام بعمل معين، أو الامتناع عن فعل ما، أو تكليف بأمر أو الحصول على منفعة بغض النظر عن طبيعتها.³

تبدأ هذه المرحلة بعد الانتهاء من المرحلة الأولى. أي بعد حصول الجاني على مادة الإبتراز حينها يبدأ الجاني في ممارسة التهديد و الضغط على الضحية⁴، و يتحقق ذلك من خلال نشر المعلومات بشكل علني مما قد يؤدي إلى إحراج الضحية و تشويه سمعتها، مما

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 34 .

² - أميل جبار عاشور ، المرجع السابق ، ص 119 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 35 .

⁴ - المرجع نفسه ، ص 35 .

يزيد من تعرض الضحية لابتراز الجاني.¹ وذلك من أجل أن يحقق هذا الأخير أهدافه الإجرامية التي تتمثل في الضغط على الضحية لتنفيذ رغباته²، سواء بدفع مبلغ مالي أو تقديم خدمة معينة مقابل عدم الكشف عن تلك المعلومات.³ و فضلاً عما سبق يجب أن يكون التهديد الذي يصدر عن الجاني حقيقياً و ذا طابع جاد و ليس مجرد مزاح حتى و إن كان المجني عليه من الأشخاص الذين لا يتأثرون بمحتوى التهديد.⁴

يجب أن نوضح أن هذه المرحلة قد تمثل البداية لعملية الابتراز الإلكتروني، حيث يتجلى مضمون الابتراز في التهديد بإلحاق الأذى الجسدي أو المالي، إذ يكفي أن يهدد الضحية بحدوث ضرر إذا لم يستجيب لمطالبه ليكون الابتراز قد تحقق بالفعل.⁵

ثالثاً : المقاومة :

في حالة عدم استجابة الضحية لمطالب المبتز تبدأ مرحلة جديدة تتمثل في التشهير من خلال فضح الأسرار الشخصية علناً عبر منصات رقمية مثل وسائل التواصل الاجتماعي أو اليوتيوب و قد يتم ذلك من خلال نشر المعلومات على الصفحة المخترقة للضحية، أو عبر حساب الجاني نفسه، أو حتى من خلال حساب مجهول يحمل اسماً مستعاراً " Pseudonyme"⁶.

و يزداد الأمر خطورة إذا كانت هذه المطالب تتعلق بأفعال غير قانونية مثل إقامة علاقة جنسية محرمة أو تنفيذ عمليات سرقة لصالح الجاني، أو ترويج للمخدرات و ما شابه ذلك.⁷

¹ - محمد عبد الرحمن عبد المحسن ، المواجهة الجنائية لجرائم الابتراز الإلكتروني و الاعتداء على الحياة الخاصة ، مجلة الدراسات القانونية و الاقتصادية - دورية علمية محكمة - ، المجلد 11 ، العدد 02 ، 2025 ، ص - ص 26-27.

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 35 .

³ - محمد عبد الرحمن عبد المحسن ، المرجع السابق ، ص 28 - 26 .

⁴ - حسين طاهري ، المرجع السابق ، ص 179 .

⁵ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 36.

⁶ - ياسين بن عمر ، المرجع السابق ، ص 175 .

⁷ - باقر غازي حنون الدراجي، المرجع السابق، ص 36.

رابعاً : الإذعان

يعني الإذعان الاستسلام و هو يتعارض مع مفهومي المقاومة و الممانعة¹ ، ففي حالة استجابة الضحية لمطالب المبتز فإن ذلك يشير إلى قدرة المبتز على إضعاف إرادة الضحية و استدراجها نحو المطالبة بمزيد من المنافع المادية أو الجنسية أو المعنوية².

خامساً : التكرار

إن بعض الجناة لا تقتصر مطامعهم على تحقيق مطالبهم من الضحية فحسب، بل تتجاوز ذلك خاصة عندما يشعر الجاني بضعف آليات الردع من جهة و وجود استجابة من المجني عليه من جهة أخرى. و بالنظر إلى المنافع التي جناها من عملية الابتزاز فإن الجاني قد يُعاود سلوكه الإجرامي المتمثل في ابتزاز المجني عليه مرة أخرى، سواء من خلال تكرار هذا السلوك بنفسه أو عبر إرسال أشخاص آخرين للقيام بعملية الابتزاز مجدداً³.

الفرع الثالث : صور الابتزاز الإلكتروني :

في ظل الارتفاع الملحوظ في معدلات جرائم الابتزاز الإلكتروني في الفترة الأخيرة، بات من الواضح أن لهذه الجريمة سمات فريدة تميزها عن باقي الجرائم التقليدية، بالإضافة إلى الأساليب و وسائل التي تمارس بها و قد أدى ذلك إلى تنوعها و تفرع أنواعها وفق معايير متعددة، و من هذا المنطلق سوف نتناول في هذا الفرع أهمها مع التركيز على تصنيفها من حيث المجني عليه، و من حيث الهدف المقصود .

أولاً :الابتزاز الإلكتروني من حيث المجني عليه

يتنوع الابتزاز الإلكتروني وفقاً للضحايا إلى أربعة أصناف و ذلك بالطريقة التالية :

1- باقر غازي حنون الدراجي ، المرجع السابق ، ص37.

2- ياسين بن عمر ، المرجع السابق ، ص175 .

3- باقر غازي حنون الدراجي ، المرجع السابق ، ص37 .

1- إبتراز النساء :

يعتبر هذا النوع من الإبتراز الإلكتروني الأكثر شيوعاً و انتشاراً بين الأنواع المختلفة للإبتراز الإلكتروني، حيث تمثل فئة النساء النموذج المثالي للضحايا في سياق الإبتراز عبر وسائل التواصل الاجتماعي و يتجلى ذلك بشكل خاص عندما يكون الجاني رجلاً و المجني عليه امرأة،¹ حيث يحدث الإبتراز نتيجة لعلاقة غير مشروعة تطورت بينهما من خلال التعارف على إحدى منصات التواصل الإجتماعي أو عبر وسائل أخرى. في هذه الحالة يتم استخدام صور أو مقاطع فيديو، بالإضافة إلى محادثات تمت بين الطرفين كوسيلة للإبتراز حيث يقوم الجاني باستغلال هذه المواد للحصول على أموال من الضحية أو لاستغلالها جنسياً مقابل عدم نشر تلك الصور.²

و تطبيقاً لذلك " تقدمت الفتاة (ز أ) ببلاغ تشكو فيه بأنها تتعرض لعملية إبتراز من أحد الشباب (و ن) و من خلال سابقة تعرفها الكترونياً بإحدى غرف المحادثة من فترة و نظراً لإقناعها بأنه سوف يتقدم لأسرتها للزواج منها تواصلت معه الكترونياً أكثر من مرة و قامت بفتح الويب كام حتى يراها مما مكنته من التقاط بعض اللقطات الخاصة بها، فوجئت المبلغة باتصال هاتفي من هذا الشاب يخبرها بحاجته إلى مبلغ عشرة آلاف جنيه لظروف خاصة به وحينما اعتذرت عن عدم تنفيذ طلبه هدهداً بأنه يحوز لقطات فاضحة لها و سيقوم بإرسالها وبثها على أحد المواقع الإباحية و قد عاود المذكور الاتصال بها و أخبرها برغبته في السلسلة الذهبية التي كانت ترتديها خلال محادثتها .

تم إجراء الفحص الفني لبلاغ الفتاة و التأكد من المراسلات الالكترونية بينهما و بين هذا الشاب الذي يداوم الاتصال بها تلفونياً و يطلب منها سرعة تسليمه السلسلة الذهبية الخاصة بها لإحدى الفتيات التي ستقابلها في إحدى محطات مترو الأنفاق.

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص38

² - محمد سعيد عبد العاطي ، رهوف عصام محمد الغانمي، جريمة الإبتراز الإلكتروني دراسة مقارنة ، مجلة قطاع الشريعة و القانون ، العدد 16 ، 2024 ، ص- ص 1636 - 1637 .

قيد المحضر برقم 7684 لسنة 2010 جنحتم العرض على النيابة العامة لاتخاذ الإجراءات القانونية نحو ضبط المذكور.

و في الموعد المحدد حضرت إحدى الفتيات (ل د) مع المكلفة باستلام السلسلة التي طلبها هذا الشاب و قد تبين أن تلك الفتاة (ل د) كانت إحدى ضحايا هذا الشاب و تمكن من ابتزازها مرارا و حصل منها على عدة مبالغ نقدية و يحوز بعض المقاطع الفاضحة لها و قد استغل ذلك مؤخرا في تكلفها لمقابلة المكلفة و الحصول على السلسلة ذهبية لتسليمها له حال مقابلتها و في الموعد المحدد للاستلام المذكور للسلسلة الذهبية تم ضبطه و بين أنه طالب بكلية الحقوق و يدعى (و ن) من محافظة الدفهلية من أسرة طيبة و والده رجل ميسور ماديا و برر ما أقدم عليه من أفعال من المبلغة و غيرها بسبب تعامله مع شبكة الأنترنت بدون وعي بمخاطرها و أضرارها و ما يمكنه أن تسببه له من مشاكل نتيجة جهله بقواعد الاستخدام الآمن للشبكة و ما توفر به من مواقع إباحية و غرف محادثة مشبوهة قادته دون أن يدري لعالم الجريمة".¹

2- ابتزاز الأحداث :

عُرف المشرع الجزائري الحدث في المادة 02 من قانون حماية الطفل رقم 15-12 لسنة 2015 إذ نصت على أنه : " الطفل كل شخص لم يبلغ الثامنة عشر (18) سنة كاملة ".² يعتبر هذا النوع من الابتزاز من أكثر الأنواع شيوعا و انتشاراً بعد ابتزاز النساء³، حيث يعد ابتزاز الأحداث من الحقائق المؤلمة في عالمنا المعاصر.⁴ في هذا السياق، يقوم المبتز بالتعرف على الحدث من خلال غرف الدردشة أو عبر منصات التواصل الاجتماعي، ثم يطلب من الضحية صوراً ذات طابع جنسي ممارساً ضغوطاً

¹ - حسين طاهري ، المرجع السابق ، ص- ص 174 - 175 .

² - راجع المادة 02 من القانون رقم 15-12 مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015 ، المتعلق بحماية الطفل ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 39، الصادرة في 19 جويلية 2015 .

³ - محمد سعيد عبد العاطي ، رهوف عصام محمد الغانمي ، المرجع السابق ، ص1637 .

⁴ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 41 .

عليه للحصول على تلك الصور و المقاطع¹، و عندما يتمكن المبتز من استمالة الضحية تبدأ أوامر الابتزاز الجنسي من هذه الشبكات الموجهة نحو الأطفال حيث يطلب منهم تقديم المزيد من الصور و الفيديوهات بالطريقة التي يفضلها المبتز، كما يمكن أن يطلب منهم التواصل إلكترونيا عبر صفحات أو مواقع أخرى ذات رقابة أقل و في حال رفض الضحية التواصل أو الإستمرار في هذا السلوك الخاطئ، يتعرض للتهديد بنشر معلوماته الشخصية على شبكات التواصل الاجتماعي مما قد يصل إلى المعارف أو من خلال تهديد بنشرها على صفحات الانترنت الخاصة بالوالدين.²

قد يحدث في بعض الأحيان أن يقوم الحدث بتسليم صورته أو معلوماته الشخصية بشكل طوعي و من هنا تبدأ المرحلة الأولى من الابتزاز، حيث يطلب الجاني من الحدث الانخراط في فعل جنسي معه أو تقديم مبالغ مالية مقابل عدم الكشف عن هذه الصور أو المعلومات السرية.³ اعتبر القانون الجزائري ابتزاز الأطفال جريمة يعاقب عليها بشكل أشد مقارنة بالجرائم الأخرى، و قد خصص المشرع الجزائري في قانون حماية الطفل عدة مواد لتحديد العقوبات المقررة على الأفراد الذين يرتكبون هذا الفعل نظراً للأهمية البالغة لهذه الفئة في المجتمع، و ما قد تقترب على هذه الجريمة من آثار سلبية سواء على الطفل المعني أو على المجتمع بشكل عام.

حيث نصت المادة 140 على أن " يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات و بغرامة من 150.000 دج إلى 300.000 دج، كل من ينال أو يحاول النيل من الحياة الخاصة للطفل بنشر أو ببث نصوص و/أو صور بأية وسيلة يكون من شأنها الإضرار بالطفل".

¹ - محمد سعيد عبد العاطي، رهوف عصام محمد الغانمي، المرجع السابق ص 41.

² - علي لطرش، مخاطر الأنترنت على حقوق الطفل في الخصوصية و النسيان في ظل التشريعات المقارنة (التشريع الأمريكي - البريطاني - الأوروبي و الجزائري)، د.ط، دار الخلدونية للنشر و التوزيع، الجزائر، 2023، ص 136.

³ - باقر غازي حنون الدراجي، المرجع السابق، ص 41.

كما نصت المادة 141 على أنه " دون الإخلال بالعقوبات الأشد ، يعاقب بالحبس من سنة (1) إلى (3) ثلاث سنوات و بغرامة من 150.000 دج إلى 300.000 دج، كل من يستغل الطفل عبر وسائل الإتصال مهما كان شكلها في مسائل منافية للآداب العامة و النظام العام ".

و علاوة على ذلك أيضا، تنص المادة 143 على أن : " يعاقب على الجرائم الأخرى الواقعة على الطفل ، لاسيما الاستغلال الجنسي للطفل و استعماله في البغاء و في الأعمال الإباحية و الاتجار به و التسول به أو تعريضه للتسول و اختطاف الطفل للتشريع الساري المفعول و لا سيما قانون العقوبات " ¹.

فمثلاً من أبرز النتائج التي نستخلصها من أحد التقارير المعدة سنة 2021، و الموسومة بالعنوان التالي : " معلومات غير مسبقة - عن خطر استغلال الأطفال و الإعتداء عليهم جنسيا عبر الأنترنت في كينيا " و المعد من طرف الإنتربول حيث أفاد التقرير أن خلال العام الماضي خضع 4 في المائة من الأطفال للتهديد أو الابتزاز على الإنترنت لحثهم على القيام بأنشطة جنسية، و تتعلق هذه التهديدات و الطلبات بالصبيان و البنات على حد سواء و عن طريق وسائل التواصل الاجتماعي في أغلب الأحيان ².

يعد استغلال الأطفال و المراهقين و ابتزازهم من أخطر أشكال الابتزاز حيث قامت العديد من القوانين الدولية بتشديد العقوبات المتعلقة بجرائم ابتزاز الأحداث، مصحوبة بالعديد من المطالبات والتحذيرات بشأن استخدام الأطفال في هذه الأفعال الإجرامية ³.

¹ - راجع المواد 140 و 141 و 143 من القانون رقم 15 - 12 المتعلق بحماية الطفل .

² - علي لطرش ، المرجع السابق ، ص 137 - 139 .

³ - دعاء سليمان عبد القادر التميمي ، جريمة الابتزاز الإلكتروني "دراسة مقارنة" ، رسالة ماجستير ، القانون العام ، كلية القانون - كلية الدراسات العليا - جامعة القدس - فلسطين ، 2019/07/07 ، ص 27.

3- ابتزاز الرجال:

يُعتبر هذا النوع من الجرائم من الأنواع الأقل شيوعاً مقارنةً بالأنواع السابقة، إذ يظهر الرجال الميسورون مالياً تعرضاً أكبر لهذه الجرائم، حيث تلجأ بعض النساء إلى إقامة علاقات غير شرعية معهم مستغلات تلك العلاقات في الاحتفاظ ببعض الصور و مقاطع الفيديو المخلة أو التسجيلات الصوتية التي تسجل خلال محادثاتهم في غرف الدردشة أو عبر وسائل التواصل الاجتماعي و تقوم المرأة بعد ذلك بطلب المال مقابل عدم نشر تلك المواد.¹

وتطبيقاً لذلك " تقدم أحد الأشخاص (أ ش) و كان يشغل منصبا إعلاميا هاما ببلاغ بتلقيه رسالة الكترونية من مجهول تتضمن بعض الصور الخاصة به في أوضاع غير لائقة مع التهديد ببث هذه الصور على شبكة الأنترنت بقصد الإضرار به ما لم يقيم بسداد مبلغ عشرة آلاف جنيه لحساب مرسل الرسالة .

بإجراء الفحص الفني و التحريات الأمنية تبين أن المبلغ دأب على استخدام شبكة الأنترنت و التعامل مع غرف المحادثة و قد تعرف من خلال ذلك على إحدى الفتيات وتطورت العلاقة الالكترونية بينهما و قاما بفتح الويب كام بينهما و قد نفذ ما طلبته منه هذه الفتاة من أفعال مشينة.

تم تحديد مصدر الرسائل الالكترونية و تبين أنها صورت من احدى الأشخاص و كان دائم التردد على غرف المحادثة منتحلاً اسم فتاة و يستعمل بعض الصور الفوتوغرافية و مقاطع الفيديو الخاصة بفتاة حسناء لإبهام المجني عليه بأن هذه الفتاة ثم يقوم بطلب فتح الويب كام مع المجني عليه و يطلب منه تنفيذ بعض الأمور الجنسية الفاضحة مع نفسه وخلال ذلك يقوم هو تسجيلها على جهاز الحساب الآلي الخاص به ثم يستخدمها عقب ذلك للتهديد و الربح غير المشروع .

¹ - محمد سعيد عبد العاطي ، رهوف عصام محمد الغانمي ، المرجع السابق ، ص1637 .

ثم ضبط المتهم و الأجهزة المستخدمة في الأفعال الإجرامية و يعرضها على النيابة المختصة أمرت بحبس المتهم و تحويل الأجهزة إلى الخبير المختص.¹

" و في قضية أخرى ، تعرف ضابط على فتاة عن طريق مواقع التواصل الاجتماعي، ثم جرى تبادل أرقام الهواتف و تطورت العلاقة بينهما إلى التحدث عن طريق الاتصال المرئي، و الذي من خلاله تمكنت الفتاة من تسجيل مقطع للضابط و هو بوضع مخل للأداب، وبحسب الأوراق التحقيقية تعرض الضابط للإبتراز إما بنشر المقطع أو تحويل مبالغ مالية ، مما اضطر معه إلى تحويل مبلغ (500) دولار إلى إحدى المكاتب المصرفية في البصرة، و تشير الأوراق التحقيقية إلى أن الفتاة قد حضرت مع شقيقها لاستلام المال المحول من قبل الضابط، و أثناء ذلك تم القبض عليها ".²

4- إبتراز الأشخاص المعنوية :

يُعرف الشخص المعنوي بأنه : " تكتل من الأشخاص، أو الأموال، يحظى بإعتراف القانون له بالشخصية، و الكيان المستقل".³

يُعد هذا النوع من الجرائم الإلكترونية من أخطر الأنواع و أكثرها تأثيراً، حيث يسجل حدوثه بشكل متكرر و يؤدي الى خسائر جسيمة للأفراد و المؤسسات على حد سواء. يشمل هذا النوع من الجرائم الأنشطة التي تتعلق بتعديل أو محو أو سرقة أو إتلاف أو تعطيل المعلومات و قواعد البيانات المخزنة إلكترونياً على الحواسيب ، سواء كانت متصلة أو غير متصلة بشبكات المعلومات و من أبسط هذه الأنشطة هو الدخول غير المشروع إلى أنظمة المعلومات و قواعد البيانات و الخروج منها دون إحداث أي تأثير سلبي، يقوم بهذا النوع من الأنشطة ما يعرف بأصحاب " الياقات البيضاء "، الذين يستغلون الثغرات في الأنظمة للدخول

¹ - حسين طاهري ، المرجع السابق ، ص-ص 175 - 176

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص - ص 42-43 .

³ - المرجع نفسه ، ص 43 .

بشكل غير قانوني إلى أنظمة الحواسيب أو شبكات المعلومات أو مواقع الإنترنت، مما يخالف سياسات و إجراءات أمن المعلومات التي يضعها مدراء تلك الأنظمة .

كما أشرنا، فإن دخول شخص غير مصرح له إلى غرفة الحواسيب المركزية في المؤسسة و خروجه دون إحداث أي أضرار يعتبر خرقا لسياسات و إجراءات أمن المعلومات المعمول بها في تلك المؤسسة.¹

" و من التطبيقات القضائية عن هذا النوع من الابتزاز، ماذهبت إليه محكمة النقض الفرنسية في إحدى قراراتها، حين قضت (..... إن السيد X متهم بحالة ابتزاز في نيس، في 20 أغسطس 2012، للحصول على تنازل من Y المحامي في نقابة محامين نيس، لممارسة الدفاع عن عقارات المجتمع المدني (marido,monclair)، من خلال التهديد بالكشف عن بعض الحقائق التي من المحتمل أن تمس الشرف أو الإعتبار ، أو أن يُنسب إليه حقائق من ذلك القبيل ، و هو ما يؤدي إلى الإضرار بالمحامي)".²

" كما تم القبض على المتهم (ع) في بغداد الذي إعترف باختراق حاسبة مدير أحد المراكز الإمتحانية و سحب النتائج منها، و من ثم ابتزاز مدير المركز بنشر النتائج إن لم يدفع له مبلغاً من المال".³

ثانيا :الابتزاز الإلكتروني من حيث الهدف

1- الابتزاز بهدف مادي : يعتبر هذا الهدف من أكثر الأهداف التي يسعى المبتز لتحقيقها، حيث يتمثل في الحصول على منافع مادية .

يقوم المبتز بطلب مبالغ مالية أو عينية من المجني عليه و ذلك في مقابل عدم نشر المعلومات الضارة على الملأ و في هذه الحالة يسعى المجني عليه إلى إسكات المبتز من خلال دفع مبلغ مالي لتفادي الأذى و الفضيحة كما تتفاوت القيمة المالية التي يطلبها المبتز

¹ - دعاء سليمان عبد القادر التميمي ، المرجع السابق ، ص 23 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 43 .

³ - المرجع نفسه ، ص 44 .

من المجني عليه بناء على الوضع الحالي للمجني عليه، بالإضافة إلى ما إذا كان شخصاً طبيعياً أو اعتبارياً تجارياً كان أو حكومياً ، و أيضاً بناء على جنس المجني عليه سواء كان امرأة أو رجل.¹

و مثال ذلك "عن الإبتراز الذي يكون الهدف منه الكسب المادي، ما قضت به المحكمة الجنائية المركزية (الهيئة الثانية) في رئاسة محكمة استئناف بغداد الرصافة الاتحادية، بالحكم على كل من المتهمين (ح. ص. ع) (ف.س.ع) و(س.م.ع) وفق أحكام المادة (1/4) و بدلالة المادة (1/2) من قانون مكافحة الإرهاب رقم 13 لسنة 2005، عن جريمة التهديد المشتكي (أ.ن.ي) و ابتزازه للحصول على منافع مادية، و قد جاء بقرار الإدانة (إن المتهمين وبالاتفاق و الاشتراك، قاموا بتهديد المشتكي بواسطة الاتصال به من رقم كورك و إجباره على دفع مبلغ من المال (مقداره خمسة ملايين دينار) و في حال عدم الدفع سيتم قتله أو رمي رمانة على داره، وقد قام المتهمون بذلك بهدف بث الرعب و الخوف في نفوس المواطنين ، و زعزعة الأمن والإستقرار في البلاد ، تحقيقاً لغايات مادية بطريقة غير مشروعة)".²

2- الإبتراز بهدف لا أخلاقي (جنسي) : يحدث هذا النوع من الابتراز عندما يطلب المبتز من ضحية القيام بأفعال جنسية أو ما يتعلق بها ، فينقسم الابتراز الجنسي إلى نوعين الأول هو الابتراز الجنسي الإلكتروني (الافتراضي) و الثاني هو الإبتراز الجنسي الواقعي، فالابتراز الجنسي الإلكتروني يتم عن بعد عبر منصات التواصل مثل (الفيس بوك، الفاير، و السكايب) و غيرها من وسائل الاتصال المرئية ، أما الابتراز الجنسي الواقعي فيتجلى في مطالبة المبتز للضحية بممارسة الجنس غير المشروع في العالم الحقيقي.³

يُعد هذا الهدف من الاهداف الأكثر شيوعاً حيث يستهدف غالباً النساء و الأحداث، ويتحقق هدف المبتز الجنسي عندما يقابل عدم نشر الصور و الفيديوهات بتمكينه من ممارسة

¹ - محمد سعيد عبد العاطي ، رهوف عصام محمد الغانمي ، المرجع السابق ، ص - ص 1637 - 1638 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 46 .

³ - المرجع نفسه ، ص - ص 46 - 47 .

الفاحشة مع الضحية مما يشبع رغبته الجنسية توافق الضحية على ذلك خوفاً من العار و الفضيحة، بالإضافة إلى ذلك قد يطلب المبتز من الضحية تكرار هذا الفعل أو حتى ممارسة الفاحشة مع أشخاص آخرين مثل أصدقائه.¹

و تطبيقاً لذلك " كما ذهبت محكمة النقض الفرنسية إلى هكذا نوع من الابتزاز، إذ قضت في إحدى قراراتها بأنه (.....قدم السيد Xشكوى ضد شخص غير معروف في 28 كانون الثاني (يناير) 2011، زاعماً أنه تلقى تهديداً بالكشف عن طبيعة حياته الجنسية (ميوله الجنسي) إذا لم يكن مستعداً لتلبية المطالب الجنسية لمراسله المجهول)".²

3- الابتزاز بهدف نفعي : يحدث الابتزاز الإلكتروني عندما يضغط الجاني على الضحية للقيام بفعل ضد إرادتها ، بغض النظر عن طبيعة هذا الفعل سواء كان قانونياً أو غير قانوني لصالح الجاني أو لصالح شخص آخر، قد يطلب الجاني من مسؤول في جهة حكومية تعيين شخص في وظيفة معينة أو قد يستخدم الضحية كأداة لتنفيذ جريمة معينة، و غالباً ماينتشر هذا النوع من الابتزاز بين العصابات المنظمة التي تسعى لتحقيق مخططاتهم الإجرامية حيث يتم استغلال الضحية لتكون وسيلة لتحقيق أهدافهم غير المشروعة.

" ومن التطبيقات القضائية عن هذا النوع من الابتزاز، ما قضت به محكمة إستئناف المثنى بصفتها التمييزية، عندما صدقت قرار محكمة جناح الرميثة المرقم 221/ج/2009 في 2009/12/04، عند إدانتها المتهم (ع.غ.ح) وفق أحكام المادة (431) ، بعد إعتدائه على المشتكي (ن.ب) و طعنه بشرف إبنته، في حال عدم إرجاعها إلى زوجها مستخدماً جهازه الموبايل.³

¹ - محمد سعيد عبد العاطي ، رهوف عصام محمد الغانمي، المرجع السابق ، ص 1638 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص ص 47-48 .

³ - المرجع نفسه ، ص 48 .

المطلب الثاني: خصائص الإبتراز الإلكتروني

تتمتع جريمة الإبتراز الإلكتروني بسمات فريدة تميزها عن الجرائم التقليدية، كما أن الجاني في هذا النوع من الجرائم يحمل خصائص خاصة تفرقه عن المجرم التقليدي، فهذه الجريمة تعتمد على المهارات الفنية و التقنية، و هناك نقاط تشابه بين الإبتراز الإلكتروني وأنواع أخرى من الجرائم رغم وجود اختلافات في بعض الجوانب¹، و بسبب الآثار الخطيرة التي تترتب على هذه الجريمة سنستعرض هذه الموضوعات في الفروع التالية :

الفرع الأول: سمات الإبتراز الإلكتروني

تتجلى خطورة جريمة الإبتراز الإلكتروني في كونها ترتكب من خلال وسائل إلكترونية وذلك نتيجة لتزايد دور الشبكة و ازدهارها في مختلف المجالات، و قد أسفر ذلك عن منح عن هذا النوع من الجرائم سمات و خصائص فريدة، لذا سنقوم في هذا الفرع بتوضيح هذه الخصائص.

أولاً : جريمة عابرة للحدود

يمكن الإشارة إلى أن من أبرز الخصائص التي تميز الجريمة الإلكترونية هي تجاوزها للحدود الجغرافية، إذ أنها لا تعترف بالحدود المكانية أو الزمانية. فالعالم بأسره يمكن أن يصبح مسرحاً لإرتكاب الجرائم ، كما أنها لا تقتصر على زمن معين على الرغم من الاختلاف في التوقيت بين الدول.²

إذ لا تحمل الحدود الجغرافية أي دلالة أمام الجرائم الإلكترونية بشكل عام و جريمة الإبتراز الإلكتروني بشكل خاص، حيث إنها لا تعترف بالفواصل بين الدول و يمكن تنفيذها بسهولة عن بعد³، بحيث يمكن أن يكون الجاني في قارة معينة بينما يكون الضحية في قارة أخرى و على سبيل المثال يمكن لشخص متواجد في الصين أن يرتكب جريمة الإبتراز

¹ -حسام منصورمحمد، جريمة الإبتراز الإلكتروني، بحث مقدم إلى مجلس المعهد القضائي وهو جزء من متطلبات نيل درجة الدبلوم العالي في العلوم القضائية، جامعة بغداد، 2024، ص 12.

² - الطاهر ياكور ، الجرائم الإلكترونية الأحكام الموضوعية و الإجرائية دراسة مقارنة ، د.ط ، دار بلقيس للنشر ، الجرائر ، 2024 ، ص 31 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 50 .

الإلكتروني باستخدام هاتف محمول متصل بشبكة الانترنت وفي حين يكون الضحية موجودا في الولايات المتحدة الأمريكية.¹

نظراً لأن جريمة الإبتراز الإلكتروني لا تقتصر على حدود جغرافية معينة و لا تعترف بعنصر المكان و تتميز بالتباعد الجغرافي بين الجاني و الضحية فإنها تثير العديد من الإشكالات القانونية مثل تحديد الدولة التي تملك الاختصاص القضائي و كذلك القانون الذي يجب تطبيقه بالإضافة إلى القضايا المتعلقة بإجراءات الملاحقة القضائية. و بسبب هذه الخصائص الفريدة لجريمة الإبتراز الإلكتروني و ما قد تسببه من خسائر ارتفعت الأصوات المنادية بضرورة التعاون الدولي لمواجهتها. إذ يتطلب انتشار الجريمة المنظمة على مستوى عالمي استجابة مماثلة في مكافحة هذه الظاهرة من خلال أشكال مختلفة من التعاون الدولي. و من أجل مواجهة ظاهرة الإبتراز الإلكتروني ينبغي أن يتمحور تعاون الدول حول إتجاهين رئيسيين، يتمثل الاتجاه الأول في التعاون على المستوى الداخلي من خلال سن تشريعات مناسبة لمكافحة الإبتراز الإلكتروني، أما الاتجاه الثاني فيتعلق بالتعاون على المستوى الدول و ذلك عبر إبرام الاتفاقيات و المعاهدات الدولية لضمان عدم إفلات مرتكبي جرائم الإبتراز الإلكتروني من العقاب و استغلالهم لنقص التشريعات الداخلية من جهة، و غياب الاتفاقيات الدولية التي تحمي المجتمع الدولي من جهة أخرى.²

ثانيا : جريمة جاذبة للجناة

تعتبر جريمة الإبتراز الإلكتروني واحدة من أخطر الجرائم في عصرنا الحالي، حيث تجذب المجرمين بشكل كبير فالمجرم هنا لا يحتاج إلى جهد بدني كما هو الحال في معظم الجرائم التقليدية ، إذ أن مسرح الجريمة افتراضي لا يتطلب وقتاً طويلاً لتنفيذه بالإضافة إلى

¹ - زهراء عادل سلمي ، المرجع السابق ، ص - ص 53 - 54 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 51 .

ذلك، فإن المخاطر المرتبطة به قليلة بينما العائد المالي كبير مما يجعلها بمثابة كنز للمجرمين أو للجريمة المنظمة و هذا يعزز من إغراء الجناة للانخراط في هذا النوع من الجرائم.¹

ثالثاً: جريمة هادئة

إن أبرز ما يميز هذه الجريمة هو أنها جريمة غير عنيفة لا تتطلب استخدام القوة أو العنف لتنفيذها على عكس جرائم مثل السرقة و القتل و الاعتداء و يعود ذلك إلى أن هذه الجريمة لا تحدث عادة من خلال مواجهة مباشرة بين الجاني و المجني عليه بل ترتكب عن بعد حيث يمثل مسرح الجريمة في بيئة افتراضية و ذلك من خلال الوسائل الالكترونية.²

رابعاً : جريمة صعبة الإثبات و الإبلاغ

تُعد جريمة الابتزاز الإلكتروني من الجرائم التي يصعب الكشف عنها و إثباتها، نظراً لأنها لا ترتكب في واقع ملموس يترك آثاراً مثل الدماء أو البصمات أو الجثث في مسرح الجريمة، بل تنفذ في فضاء افتراضي مما يسهل العبث بأدلة الإثبات. علاوة على ذلك تعتبر هذه الجريمة من الجرائم العابرة للحدود مما يبرز الأهمية الخاصة للأدلة الرقمية في هذا النوع من الجرائم و يستدعي الاعتراف بها كأدلة في سياق الإثبات الجنائي.³

و في الوقت نفسه، يتبوأ المجني عليه مكانة محورية في تعقيد عملية اكتشاف جريمة الابتزاز الإلكتروني، إذ يميل معظم ضحايا هذه الجريمة إلى الامتناع عن الإبلاغ عنها، خوفاً من الفضيحة و التشهير. فعندما يمتلك الجاني مواد مثل الصور أو مقاطع فيديو أو التسجيلات الصوتية يشعر المجني عليه بالقلق من تقديم بلاغ تجنباً لانكشاف أمره خصوصاً في المجتمعات المحافظة و بالتالي يلجأ المجني عليه غالباً إلى تلبية مطالب المبتز،

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 52 .

² - إيهاب عبد الغني عثمان المغربي ، المواجهة التشريعية لجريمة الابتزاز الإلكتروني " دراسة مقارنة " ، بحث متاح على الموقع الإلكتروني <https://jslem.journals.ekb.eg> تاريخ الزيارة 2026/02/28 على الساعة 02:11 ، ص 607 .

³ - رباب مصطفى عبد المنعم الحكيم ، جريمة الابتزاز الإلكتروني في التشريع المصري ، مجلة قطاع الشريعة و القانون ، العدد 17 ، 2025 ، ص 3185 .

و فضلا على ذلك، يتجلى تردد المجني عليه في الإبلاغ عن جريمة الإبتراز الإلكتروني بشكل أكبر عندما يكون المجني عليه مؤسسة مالية أو شركة خاصة، حيث تخشى هذه المؤسسات أن تؤدي الدعاية السلبية إلى فقدان الثقة من قبل المتعاملين معها، و بالإضافة إلى ذلك تتردد هذه المؤسسات في تقديم البلاغات تجنباً للإعلان عن إختراق أنظمتها مما قد يكشف عن مواطن الضعف في نظامها الإلكتروني، و بالتالي يؤدي إلى تكرار عمليات الاختراق والإبتراز.¹

خامساً : خصوصية مجرم الإبتراز الإلكتروني

يتميز الجاني الإلكتروني أو المعلوماتي بعدد من الصفات في جريمة الإبتراز الإلكتروني، مما يجعله مختلف عن الجاني التقليدي و من بين هذه الخصائص نذكر ما يلي :

1- مجرم ذكي : يمتاز مرتكبو جرائم الإبتراز الإلكتروني بقدر من الذكاء و المهارة²، حيث يمتلك هؤلاء الأفراد مهارات تؤهلهم لتعديل و تطوير الأنظمة الأمنية مما يجعل من الصعب ملاحظتهم أو تتبع أنشطتهم الإجرامية عبر الشبكات أو داخل أجهزة الحواسيب، لذا يعتبر الإجرام المعلوماتي نوعاً من الإجرام الذي يعتمد على الذكاء دون الحاجة إلى استخدام القوة أو العنف و يعد هذا الذكاء مفتاحاً لمرتكب الجريمة المعلوماتية لاكتشاف الثغرات و اختراق البرامج المحصنة.

يعتبر الإلمام بتكنولوجيا المعلومات و القدرة على تعديل و تغيير برامج الحاسوب من الصفات الأساسية للمجرم المعلوماتي، حيث تتطلب المهارات اللازمة لتنفيذ الأنشطة الإجرامية مستوى عال من الكفاءة، إن تنفيذ بعض الجرائم الإلكترونية يتطلب مهارة معينة يمتلكها الفاعل و التي يمكن اكتسابها من خلال الدراسة المتخصصة في هذا المجال أو من خلال الخبرة العملية في تكنولوجيا المعلومات أو من خلال التفاعل الاجتماعي مع الآخرين.³

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص 54.

² - المرجع نفسه ، ص 54 .

³ - الطاهر ياكور ، المرجع السابق ، ص - ص 34-35.

2- مجرم غير عنيف : لا يحتاج مجرم الإبتراز الإلكتروني الى استخدام القوة أو العنف في تنفيذ جريمة خاصة حيث أنه لا يتفاعل مع أشخاص حقيقين، بل يتعامل مع عناصر غير ملموسة تتمثل في البيانات و المعلومات المخزنة على جهاز الكمبيوتر لذا لا يوجد أي سبب يدفعه للجوء إلى العنف.¹

3- مجرم ذو طبيعة اجتماعية : تتمثل الصفة الثالثة التي يتميز بها مجرم الإبتراز الإلكتروني في كونه فرداً اجتماعياً، يمتلك القدرة على التكيف مع بيئته الاجتماعية و يمارس أنشطته بشكل طبيعي ضمنها، يتميز هذا المجرم بعدم وضع نفسه في حالة من العداء تجاه المجتمع المحيط به بل إنه قادر على التواصل و التفاعل مع أفراد مجتمعه، لذلك إن طبيعة الإبتراز الإلكتروني تتطلب أحيانا من الجاني الدخول في علاقات عاطفية مع الضحية مما يستلزم أن يكون الجاني متكيفاً اجتماعياً و قادراً على استدراج الضحية إلى شباكه.²

الفرع الثاني : الآثار المترتبة عن الإبتراز الإلكتروني :

تتعدد الآثار الناتجة عن جريمة الإبتراز الإلكتروني، حيث قد تقتصر هذه النتائج على المجني عليه ، مما يسبب له مشاعر الخوف و القلق النفسي كما يكمن أن تكون لها آثار اجتماعية تؤدي إلى تفكك المجتمع خصوصا في إطار الأسرة و العلاقات الزوجية، بالإضافة إلى ذلك قد تترتب آثار أمنية تهدد الأمن العام سنتناول هذه الجوانب بالتفصيل كالاتي :

أولا : الآثار النفسية

ينتج عن ارتكاب جريمة ابتزاز الإلكتروني آثار نفسية سلبية عميقة على الضحية، تتضمن القلق و التوتر و الشعور المستمر بالذنب، فضلاً عن صعوبات في النوم و عدم القدرة على التركيز و النوم المفرط، بالإضافة إلى زيادة الشك في الأشخاص المحيطين به يصبح الضحية حساساً تجاه سلوكيات الآخرين خصوصا أولئك الذين يمتلكون خبرة في مجالات

¹ - الطاهر ياكور ، المرجع السابق ، ص 35 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص - ص 55 - 56 .

التكنولوجيا و الحوسبة، علاوة على ذلك، قد يستمر الضحية في التفكير في كيفية التخلص من ظلم الجاني بطرق متعددة خاصة إذا استمر الجاني في ممارسة ضغوطه مما قد يؤدي إلى تفكير الضحية في إيذاء نفسه بما في ذلك التفكير في الانتحار.¹

ولتوضيح ذلك يمكننا تقديم أمثلة على حالات انتحار بعض الفتيات في مصر نتيجة خوفهن من انتشار الصور ففي 1 يناير 2022، صدم المجتمع المصري بخبر انتحار مراهقة مصرية تدعى (ن.ك) التي كانت في السابعة عشرة من عمرها بعد تعرضها لإبتراز إلكتروني من قبل شابين من قريتها حيث قام الشابان بنشر صور مزيفة لها على وسائل التواصل الاجتماعي، و قد بذلت الفتاة محاولات يائسة لإبعاد الشبهات عنها و التأكيد على أن الصور المنشورة لا تخصها و لكن دون جدوى مما دفعها إلى اتخاذ قرار الانتحار هرباً من العار. و بعد ذلك أقدمت فتاة أخرى تبلغ من العمر خمسة عشر عاماً على الانتحار أيضاً بعد أن تعرضت لإبتراز إلكتروني.²

ثانياً : الآثار الاجتماعية

أثرت وسائل التواصل الاجتماعي بشكل ملحوظ على الأسرة و المجتمع، حيث أفسحت المجال أمام أشكال متعددة من التعارف و التواصل سواء عبر الصوت أو الصورة و قد أدى ذلك إلى زيادة سهولة وقوع جريمة الإبتراز الإلكتروني و التي تعتبر من أكثر الجرائم الإلكترونية تأثيراً على سلامة المجتمع و الأسرة. إذ يترتب على هذه الجرائم إرهاب الضحية و وضعها تحت وطأة الخوف ، بالإضافة إلى قهر إرادتها و دفعها نحو القيام بأفعال لم تكن لتقوم بها لولا التهديد الموجه إليها .

و تجدر الإشارة إلى أن معظم ضحايا هذه الجريمة من النساء مما أدى إلى تفكك علاقاتهن الزوجية، كما أن العديد من الفتيات اللواتي يتعرضن للإبتراز يتجنبن تقديم شكاوى

¹ - وفاء محمد صقر، جريمة الإبتراز الإلكتروني (دراسة مقارنة) ، مجلة البحوث القانونية و الاقتصادية، المجلد 36، العدد 02 ، 2024 ، ص- ص 474 - 475 .

² - حسام منصور محمد ، المرجع السابق ، ص 34 .

ضد الجناة خشية من الفضيحة و تأثيرها السلبي على فرصهن في الزواج، حيث يتردد الشباب في التقدم للزواج منهن و قد تفضل الفتاة نفسها عدم الزواج خوفاً من أن يكشف أمرها أمام الزوج في المستقبل.¹

ثالثاً : الآثار الأمنية

تعد جريمة الابتزاز و غيرها من الجرائم الجنسية من العوامل المؤثرة بشكل مباشر على مستوى الأمن في الدولة، حيث تؤثر على شعور المجتمع بالأمان فيما يتعلق بغرضه و شرفه و ترتبط هذه الجرائم بجرائم أخرى مثل الاغتصاب و الزنا و تعاطي المسكرات و المخدرات و قد تصل إلى حد الدعارة و السطو على أموال الأفراد . كما أن جريمة الابتزاز قد تؤدي أحيانا إلى زيادة معدلات جرائم القتل التي تحدث بدافع الانتقام من المبتز الذي ارتكب الفاحشة بحق ضحيته ثم قام بنشر فضيحته عبر رسائل الهواتف المحمولة أو شبكة الأنترنت أو كليهما، وفي هذه الحالة قد تقدم الضحية أو أحد أقاربها على قتل المعتدي كنوع من الانتقام خاصة في بعض المجتمعات التي ترى أن غسل العار الذي لحق بها لا يتحقق إلا من خلال سفك دم المتسبب.²

الفرع الثالث : تمييز الابتزاز الإلكتروني عن الأفعال المشابهة له

يتميز الابتزاز الإلكتروني عن غيره من الجرائم التي قد تبدو مشابهة له مثل التهديد و استغلال النفوذ، لذا قررنا في هذا الفرع أن نتطرق لهذه الجرائم التي تتقارب مع الابتزاز الإلكتروني من خلال القواسم المشتركة التي تجمع بينها .

¹ - وفاء محمد صقر ، المرجع السابق ، ص - ص 475 - 476 .

² - أمير فرج يوسف ، المرجع السابق ، ص 72 .

أولاً : الفرق بين جريمة الإبتراز الإلكتروني و جريمة التهديد

قد يحدث تداخل و خلط في بعض الحالات بين جريمة الإبتراز الإلكتروني و جريمة التهديد، و ذلك بسبب طبيعة مضمون الجريمتين لذا من الضروري توضيح النقاط التي تتشابه و تختلف بها هاتان الجريمتان.¹

1 - أوجه التشابه : تتشارك جريمة التهديد مع جريمة الإبتراز في عدة جوانب أهمها:

أ- كلا الجريمتين تتحققان من خلال التهديد سواء كان هذا التهديد يتعلق بأذى مادي أو بأذى معنوي .

ب- تتشارك الجريمتان من حيث محل التهديد في عدم اشتراط توجيه التهديد مباشرة إلى المجني عليه، إذ يمكن أن تتحقق جريمة الإبتراز الإلكتروني من خلال التهديد سواء كان ذلك التهديد متعلقاً بالإيذاء أو بالنشر سواء كان موجهاً إلى المجني عليه نفسه أو إلى شخص قريب منه بهدف إرغامه على تنفيذ ما يطلب منه و ينطبق الأمر ذاته على جريمة التهديد المستقلة، حيث يمكن أن يتعرض شخص للتهديد بخطر ابنه أو بقتل والده أو بإفشاء أو إسناد أمور تضر بشرف زوجته أو ابنته أو بحرق منزله.

ج- لا يشترط في الجريمتين أو يقوم الجاني بتنفيذ تهديده إذ يمكن أن تتحقق جريمة التهديد بمجرد وصول التهديد إلى المجني عليه بغض النظر عن تنفيذ ذلك التهديد فالمشرع يعاقب على مجرد التهديد لما له من تأثير سلبي على أمن المجني عليه و ينطبق الأمر نفسه على جريمة الإبتراز الإلكتروني حيث لا يعتبر تنفيذ الجاني لتهديده شرطاً لتوافر الجريمة.²

2- أوجه الاختلاف : توجد فروق واضحة بين جريمة التهديد و جريمة الإبتراز الإلكتروني يمكننا توضيحها على النحو التالي :

أ- يهدف الإبتراز الإلكتروني إلى إجبار المجني عليه على القيام بفعل معين أو الامتناع عن القيام به، مما يعني أن جريمة الإبتراز ترتبط عادة بطلب محدد بالمقابل قد تكون جريمة

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 61 .

² - المرجع نفسه ، ص 62 .

التهديد مرتبطة بطلب أو قد تكون غير مرتبطة به، حيث يكون الهدف من التهديد هو إحداث حالة من الفزع و الخوف لدى الضحية دون وجود طلب مباشر.¹

ب- تتميز جريمة التهديد عن جريمة الابتزاز الإلكتروني من حيث الأساس القانوني للتجريم، ففي جريمة التهديد يقتصر الاعتداء على حق المجني عليه في الشعور بالهدوء و الأمان و الاستقرار النفسي، بينما في حالة الابتزاز الإلكتروني يمتد هذا الاعتداء بالإضافة إلى إزعاج المجني عليه ليشمل حقه في حرية الإرادة حيث يتم الضغط عليه للقيام بفعل لم يكن لينفذه لو كان متحفظاً بحرية إرادته و بالتالي فإن جريمة الابتزاز الإلكتروني تتضمن إلى جانب التهديد عناصر من القهر و الإكراه.²

ج- يجب اعتبار التهديد جريمة مستقلة حيث لا يتوافر التهديد إذا كان موضوعه لا يصل إلى درجة جريمة مثل مقاطعة أحد التجار في تجارته أو تهديد شخص آخر بأنه سيسلط عليه الجن بواسطة السحر و الشعوذة و في المقابل يشترط أن يرتقي التهديد في سياق جريمة الابتزاز الإلكتروني إلى درجة الجريمة فقد يكون موضوع التهديد جريمة وفقاً لقانون العقوبات أو قد لا يكون كذلك على سبيل المثال فإن التهديد بالحرمان من الترقية المستحقة لا يشكل جريمة تهديد مستقلة و لكن إذا اقترن هذا التهديد بطلب معين فإن ذلك يؤدي إلى تحقق جريمة الابتزاز.³

ثانيا : الفرق بين الابتزاز الإلكتروني و استغلال النفوذ

يعرف استغلال النفوذ بأنه : " استخدام النفوذ أي كان مصدره لدى جهة عامة أو خاصة، للحصول على منفعة مادية أو معنوية لمصلحة الفاعل أو الغير".⁴ وفقا للتعريف، فإن جريمة استغلال النفوذ تعتمد على ثلاثة عناصر أساسية على النحو التالي :

¹ - حسام منصور محمد ، المرجع السابق ، ص 23 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 64 .

³ - حسام منصور محمد ، المرجع السابق ، ص 25 .

⁴ - خميري رشدي ، مراد عمراني ، جريمة استغلال النفوذ في القانون الجزائري ، المجلة الجزائرية للحقوق و العلوم السياسية ، المجلد 06 ، العدد 02 ، 2021 ، ص 21 .

- 1- " النفوذ أي كان مصدره سياسيا، اجتماعيا، وظيفيا أو إقتصاديا.
 - 2 - استخدام النفوذ لدى جهة عامة أو خاصة.
 - 3- للحصول على منفعة مادية أو معنوية أو أية غاية مقابل لصالح الفاعل أو الغير".¹
- يعتبر استغلال النفوذ وفقاً للقانون الجزائري ، كما هو منصوص عليه في المادة 32 من القانون رقم 06 - 01 المتعلق بالوقاية من الفساد و مكافحته على أنه : " 1- كل من وعد موظفا عموميا أو أي شخص آخر بأية مزية غير مستحقة أو عرضها عليه أو منحه إياها ، بشكل مباشر أو غير مباشر ، لتحريض ذلك الموظف العمومي أو الشخص على استغلال نفوذه الفعلي أو المفترض بهدف الحصول من إدارة أو من سلطة عمومية على مزية غير مستحقة لصالح المحرض الأصلي على ذلك الفعل أو لصالح أي شخص آخر ،
- 2- كل موظف عمومي أو أي شخص آخر يقوم بشكل مباشر أو غير مباشر ، بطلب أو قبول أية مزية غير مستحقة لصالحه أو لصالح شخص آخر لكي يستغل ذلك الموظف العمومي أو الشخص نفوذه الفعلي أو المفترض بهدف الحصول من إدارة أو سلطة عمومية على منافع غير مستحقة " .²

1- أوجه التشابه :

أ- يتشابه الاحتزاز الإلكتروني مع جريمة استغلال النفوذ في كونهما ينتجان درجة من الإكراه التي تدفع الأفراد الذين يتعرضون للاستغلال أو الذين يُستخدم ضدهم النفوذ إلى الاستجابة بشكل دائم.

ب- يتفقان على أهمية وجود تعويض يكتسب نتيجة التهديد أو استغلال السلطة.³

¹ -حسين طاهري ، المرجع السابق ،ص- ص 162 - 163 .

² - راجع المادة 32 من القانون رقم 06 - 01 مؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006 ، يتعلق بالوقاية من الفساد و مكافحته ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 14، الصادرة في 08 مارس 2006 .

³ - ريهام عاطف معروف ، الاحتزاز الإلكتروني ، مجلة روح القوانين ، عدد خاص - المؤتمر العلمي الدولي الثامن- التكنولوجيا و القانون، دس ، ص 2005 .

2- أوجه الاختلاف :

أ- تتميز جريمة استغلال النفوذ عن جريمة الابتزاز الإلكتروني في أن السلوك الاجرامي المرتبط بجريمة استغلال النفوذ يتجلى في شكل رجاء أو توصية أو طلب دون أن يتضمن ذلك أي تهديد من جانب الجاني أو إيذاء كما يتطلب استغلال النفوذ أن يكون موجها نحو سلطة عامة و ذلك وفقا للمادة 32 من ق.ع.ج ، و على النقيض من ذلك تتطلب جريمة الابتزاز الإلكتروني حدوث تهديد بإلحاق الأذى بالمجني عليه أو بأحد الأشخاص المقربين له دون أن يشترط أن يكون هذا الشخص من ضمن السلطات العامة.¹

ب- تفترض جريمة استغلال النفوذ وجود ثلاثة أطراف و هي : الشخص الذي يمتلك النفوذ والشخص الذي يحتاج إلى المساعدة و الشخص الذي يشغل وظيفة معينة، بينما يمكن أن تحدث جرائم الابتزاز الإلكتروني بوجود طرفين فقط و هما الجاني و المجني عليه.²

¹ - حسين طاهري ، المرجع السابق ، ص 163 .

² - ريهام عاطف معروف ، المرجع السابق ، ص 2006 .

المبحث الثاني: التكيف القانوني لجريمة الإبتراز الإلكتروني

أصبحت ظاهرة الإبتراز الإلكتروني تمثل تهديداً متزايداً للمجتمع خاصة في ظل غياب الرقابة الفعالة على منصات التواصل الاجتماعي و ضعف الإشراف عليها، و قد ساهم ذلك في تفشي هذه الظاهرة التي تعكس نوعاً من الضغط و الإكراه الذي يمارسه الجاني على الضحية بهدف فرض السيطرة عليها و إجبارها على الامتثال لمطالبه مستخدماً في ذلك أساليب متعددة من بينها التهديد فيتمثل الإبتراز الإلكتروني في أي تهديد يوجهه الجاني يؤثر سلباً على نفسية الضحية أو أحد الأشخاص المقربين منها و يحدث ذلك عبر الوسائل الإلكترونية مما يدفع الضحية إلى تنفيذ ما يطلبه الجاني سواء كان هذا الطلب مشروعاً أو غير مشروع و قد تسارعت الجهود التشريعية لتجريم هذه الظاهرة¹، و من بينها التشريع الجزائري.

و استناداً الى ما سبق، سوف نناقش في هذا المبحث مطلبين نخصص الأول لمناقشة أركان جريمة الإبتراز الإلكتروني بينما سوف نتناول في المطلب الثاني العقوبة المقررة لهذه الجريمة .

المطلب الأول: أركان جريمة الإبتراز الإلكتروني

لقيام المسؤولية الجنائية عن جريمة الإبتراز الإلكتروني بوصفها فعلاً إجرامياً مستحدثاً، لا بد من توافر ثلاثة أركان أساسية لتصنيفها قانونياً كجريمة تستحق العقوبة و في حالة انقضاء أحد هذه الأركان تنتفي الجريمة كلياً و هو ما سوف نحاول التفصيل فيه من خلال هذا المطلب بالتطرق إلى الركن الشرعي في الفرع الأول ثم نتناول الركن المادي في الفرع الثاني ثم لنتطرق بعدها إلى الركن المعنوي في الفرع الثالث .

¹ - وفاء محمد صقر ، المرجع السابق ، ص 503 .

الفرع الأول : الركن الشرعي

يعتبر الركن الشرعي هو النص القانوني الذي يجرم الفعل بحيث يمثل النص القانوني مصدر التجريم و يشكل معيار الفاصل بين ما هو مباح و ما هو محظور تحت طائلة العقوبة¹، فلا بد أن يكون هذا النص سارياً سواء من حيث الزمان و المكان أو من حيث الأشخاص على مرتكب الفعل الإجرامي،² عملاً بمبدأ الشرعية حيث تنص المادة الأولى من قانون العقوبات الجزائري على أنه : " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون " ³، لذا لا يمكن اعتبار الجريمة موجودة قانونياً إلا في حال وجود هذا الركن و في حالة غيابه لا تكون هناك حاجة للبحث في الأركان الأخرى للجريمة.⁴

و بالتالي و نتيجة الإزدياد المستمر لظاهرة الابتزاز الإلكتروني و تأثيراتها السلبية العميقة على مختلف جوانب الحياة، قامت معظم دول العالم بتكثيف جهودها لوضع أسس قانونية تهدف إلى تجريم هذه الظاهرة⁵، من خلال تبني نصوص قانونية عقابية خاصة بالجريمة المعلوماتية و قد اختلفت الخيارات التشريعية المتبعة في هذا السياق حيث قامت بعض الدول بإدماج نصوص تتعلق بالجريمة المعلوماتية ضمن قانون العقوبات التقليدي في حين اتجهت دول أخرى نحو وضع قانون جنائي مستقل يختص بقضايا الإلكترونية.⁶

يتضح لنا أن المشرع الجزائري قبل عام 2024 لم يجرم جريمة الابتزاز الإلكتروني بشكل خاص، و عند الرجوع إلى قانون العقوبات نجد أنه لا يوجد نص تشريعي مباشر و مستقل يخص هذه الجريمة بل اكتفى المشرع بإدراجها ضمن جرائم التهديد بشكل عام في المواد 284،

¹ - أحسن بوسقيعة ، الوجيز في القانون الجزائري العام ، ط22 ، دار بلقيس للنشر و التوزيع ، دار البيضاء - الجزائر ، 2025 ، ص 51 .

² - مريم عراب ، جريمة التهديد و الابتزاز الإلكتروني ، مجلة الدراسات القانونية المقارنة ، المجلد 07 ، العدد 01، 2021، ص 1209 .

³ - راجع المادة 01 من الأمر رقم 66 - 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل و المتمم .

⁴ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 107 .

⁵ - المرجع نفسه ، ص 130 .

⁶ - مريم عراب ، المرجع السابق، ص 1209 .

286 و 371 من ق. ع. ج كما ذكرنا سابقاً بحيث كانت صالحة لتطبيقها على جريمة الابتزاز الإلكتروني و مع تزايد استخدام التقنيات الحديثة عموماً و ظاهرة الابتزاز الإلكتروني خصوصاً التي شهدت انتشاراً في المجتمع الجزائري في الآونة الأخيرة، أصبح من الضروري وجود تطور تشريعي مستمر يتماشى مع التقدم التكنولوجي و هذا ما دفع بالمشروع الجزائري لإيجاد إطار قانوني أكثر ملائمة لجريمة الابتزاز الإلكتروني و هو ما تم التطرق إليه في قانون العقوبات بموجب المادة 371 من القانون رقم 24 - 06 المؤرخ في 28 أفريل سنة 2024 التي نصت على أنه " كل من تحصل بطريق التهديد كتابة أو شفاهة أو بإفشاء أو نسبة أمور شائنة على أموال أو أوراق مالية أو على توقيع أو على المحررات المبينة في المادة 370 من هذا القانون أو على أية منفعة مادية أخرى أو لأي غرض آخر أو شرع في ذلك، يكون قد ارتكب بذلك جريمة الابتزاز يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات بغرامة من 200.000 دج إلى 500.000 دج و يجوز، علاوة على ذلك " ¹.

فقد أدخل هذا التعديل الأخير تغييرات جوهرية، حيث اعتبر التهديد العنصر الأساسي في جريمة الابتزاز و جعله وسيلة لتحقيق أهداف غير مشروعة مثل الحصول على أموال أو توقيعات أو مستندات، أو الاستفادة من منفعة مادية أخرى ، أو تحقيق أي غرض غير مشروع آخر. كما أكد التعديل على أن التهديد يمكن أن يتم بأي وسيلة كانت سواء كانت كتابية أو شفوية. ²

¹ - راجع المادة 371 من القانون رقم 24 - 06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، يعدل و يتم الأمر رقم 66 - 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 و المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 30، الصادرة في 30 أبريل سنة 2024.

² - نورة بن بو عبد الله ، وردة بن بو عبد الله ، تعزيز الحماية الجزائية للخصوصية المعلوماتية على ضوء تعديل قانون

العقوبات رقم 24-06 المؤرخ في 28 أفريل 2024، المجلة الدولية للبحوث الدولية والسياسية، المجلد 09 ، العدد 01، 2025 ، ص- ص 354-355.

أكدت الدساتير الجزائرية المتعاقبة على ضرورة احترام حرمة الحياة الخاصة، و ذلك تماشياً مع ما أقرته إعلانات الحقوق و المواثيق الدولية¹، و عند الرجوع إلى التعديل الدستوري لسنة 2020 نجد أن المادة 47 منه تنص على مايلي :

" لكل شخص الحق في حرية مراسلاته و اتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى و الثانية إلا بأمر معلن من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل إنتهاك لهذه الحقوق".²

و من جهة أخرى يعتبر إنتهاك حرمة الحياة الخاصة بأي شكل و خاصة من خلال الإبتراز عبر الوسائل الإلكترونية نوعاً خاصاً من المسؤولية التقصيرية، حيث إن المعتدي قد خالف إلزاماً قانونياً نص عليه المشرع الجزائري صراحة في المادة 47 من القانون المدني التي تنص على أنه : " لكل من وقع عليه إعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الإعتداء و التعويض عما يكون قد لحقه من ضرر". و هو المساس بحق من الحقوق الأساسية للشخصية.

بالتالي فإن أي إعتداء على هذه الحرمة، بأي صورة كانت يتيح للمضرور المطالبة بالتعويض المناسب و ذلك إستناداً إلى نصوص القانون المدني من المواد 131 إلى 134 و المواد 181 و 182 مكرر.³

¹ - عادل رزيق ، الحماية الجزائرية للحق في حرمة الحياة الخاصة في ظل التقنيات الحديثة ، مجلة القانون والعلوم السياسية، المجلد 03، العدد 01، 2017، ص 169 .

² - راجع المادة 47 من المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020 ، والمتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020، الجريدة الرسمية للجمهورية الجزائرية ، العدد 82.

³ - فاطمة العرفي ، الحماية القانونية للحق في الخصوصية للأطفال من جريمة التشهير عبر مواقع التواصل الاجتماعي في القانون الجزائري، مجلة الاجتهاد القضائي ، المجلد 12 ، العدد 04 ، 2020 ، ص 544.

الفرع الثاني : الركن المادي

يتمثل الركن المادي للجريمة إلى وجود فعل خارجي ملموس يمكن إدراكه بواسطة الحواس، و يعني الركن المادي بشكل خاص الواقعة الإجرامية التي تتكون منها السلوكيات المادية الخارجية التي ينص القانون على تجريمها ، أي كل ما يدخل في كيان الجريمة و يتميز بطبيعة مادية يمكن إدراكها حسياً و يعتبر هذا الركن ضرورياً لقيام الجريمة إذا لا يعترف القانون بوجود جرائم دون ركن مادي، و لهذا السبب أطلق عليه بعض الباحثين مصطلح ماديات الجريمة.¹

تمر جريمة الابتزاز الإلكتروني قبل إقترافها من قبل الجاني بمراحل متعددة، حيث تتشكل في البداية كفكرة في ذهنه ثم تتطور لتظهر في العالم الخارجي على شكل سلوك إجرامي يهدف إلى تهديد الضحية و الضغط عليها من أجل الحصول على مكاسب سواء كانت مشروعة أو غير مشروعة و الذي يؤدي إلى نتيجة إجرامية تثبت العلاقة بينها و بين السلوك الإجرامي و هذا ما يمثل الركن المادي لهذه الجريمة و الذي يتكون من ثلاث عناصر هي :

أولاً : السلوك الإجرامي

يتمثل السلوك الإجرامي في الفعل الصادر عن الجاني بتهديد المجني عليه سواء كان ذلك من خلال القول أو الكتابة أو إفشاء أو نسبة أمور شائنة عليه أو أي فعل آخر يتمثل في التهديد بنشر بيانات أو صور أو مقاطع فيديو تخص الضحية، و لا يهم المصدر الذي حصل منه الجاني على هذه المعلومات فقد يكون قد حصل عليها من خلال اختراق حساب الضحية أو من خلال العثور عليها في جهاز الضحية المسروق أو المفقود ، كما أنه لا يشترط أن يتم التهديد بطريقة معينة فقد يتم ذلك عبر غرف الدردشة أو البريد الإلكتروني أو من خلال تسجيل صوتي.²

¹ - الطاهر ياكّر ، المرجع السابق ، ص 39 .

² - مريم عراب ، المرجع السابق ، ص 1208 .

- و عليه تتجسد الأفعال المادية لجريمة الإبتراز الإلكتروني في مجموعة من التصرفات التي قد تختلف وفقاً لأسلوب و هدف الجاني و تتمثل هذه الأفعال في:
- جمع المعلومات أو الصور الشخصية: في العديد من الحالات يبدأ الجاني باختراق حسابات الضحية أو استدراجها للكشف عن معلومات حساسة أو صور غير مناسبة.
 - تهديد الضحية بنشر المعلومات : يعتبر التهديد بنشر البيانات الشخصية أو الصور المحرجة أحد الأساليب الرئيسية في الإبتراز الإلكتروني فيتم ذلك من خلال إرسال رسائل تهديدية إلى الضحية و غالباً ما ترسل عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي .
 - مطالبة الضحية للإمتثال لشروط الجاني: و هي المرحلة التي يطلب فيها الضحية دفع المال أو تقديم خدمات أو القيام بأفعال معينة مقابل عدم نشر الصور أو المعلومات و هو ما يعتبر جوهر جريمة الإبتراز الإلكتروني .
 - استغلال أساليب التشفير أو البرمجيات الخبيثة : في بعض الأحيان قد يلجأ الجاني إلى تقنيات متطورة مثل البرمجيات الضارة أو برامج الفدية لتهديد الضحية أو التسلل إلى معلوماتها.¹

تتجلى العناصر الأساسية للعنصر المادي في سياق الإبتراز في أن الفرد الذي يتعرض للإبتراز يكون في حالة من الاستحالة المطلقة لدفع الأضرار المهددة به في حال عدم استجابته لمطالب المبتز، إذ يجد الشخص نفسه في وضعية من الإعسار، حيث تفتقر لديه القدرة على مواجهة الخطر و لا يوجد من يضمن سلامته في حال رفضه لمطالب المبتز و لا يوجد أي ضمان لحمايته.²

¹ - أكرم ماجد خلف ، الحماية الجنائية للطالب الجامعي من جرائم الإبتراز الإلكتروني ، مجلة الشرق الأوسط للدراسات القانونية و الفقهية ، المجلد 05 ، العدد 02 ، 2025 ، ص 425 .

² - فاطمة العرفي ، حجية الدليل الرقمي في إثبات جريمة الإبتراز الإلكتروني في القانون الجزائري ، مجلة صوت القانون ، المجلد 08 ، العدد خاص 02 ، 2022 ، ص 498 .

- التهديد كركن مادي أساسي في جريمة الابتزاز الإلكتروني: يعتبر التهديد من أبرز سمات الركن المادي في جريمة الابتزاز الإلكتروني، حيث يستغل الجاني وسائل التواصل الاجتماعي بشكل خاص أو الفضاء الرقمي بشكل عام لابتزاز الضحية من خلال تهديدها بنشر معلومات أو صور خاصة بها.

فيحدث هذا التهديد ضغطاً نفسياً على الضحية، مما يجبرها على الاستجابة لمطالب الجاني سواء كانت مالية أو تتعلق بأي غرض آخر.¹ و عليه يتحقق التهديد إما من خلال كتابة أو شفاهة و ذلك على النحو التالي :

- التهديد الكتابي: حددته المادة 284 من ق.ع.ج، حيث يمكن أن يقوم الجاني بكتابة رسالة تهديد تتعلق بالقتل أو بإفشاء معلومات تمس الشرف تجاه شخص محدد و تنشر هذه الرسالة عبر وسائل التواصل الاجتماعي إذا لم يستجب المجني عليه لمطالب الجاني، و قد أعتبر المشرع الجزائري أن كل من يسهم في تسهيل الإذاعة أو النشر يعد فاعلاً أصلياً للجريمة.² و علاوة على ذلك يجب أن يكون التهديد واضحاً سواء كان صريحاً أو ضمنياً، بحيث يفهم منه أن الجاني يهدد الضحية بكشف أسرارها إذا لم تستجيب لرغابته، فالأهمية تكمن في الضغط و الإكراه المرتبطين بالتهديد مما يجبر المجني عليه على القيام بالفعل المطلوب.³

- أما التهديد الشفوي: أشارت إليه المادة 286 من ق.ع.ج و يعتبر أقل خطورة من التهديد الكتابي ، حيث يكون الجاني غالباً في حالة من الغضب كما أن تأثيره على نفسية المجني عليه يكون أقل مقارنة بالتهديد الكتابي و يشترط في التهديد الشفوي أن يكون مصحوباً بأمر أو شرط

¹- أكرم ماجد خلف، المرجع السابق، ص 425 .

²- سهام عكوش، الحماية القانونية لحق من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقاً للقانون الجزائري، مجلة السياسة العالمية، المجلد 06، العدد 01، 2022، ص 1301.

³- آمال برحال، جريمة الابتزاز عبر الوسائل الإلكترونية ، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر ، قانون جنائي وعلوم جنائية ، جامعة العربي التبسي - تبسة ، 2022/2019 ، ص 43 .

مثل أن يقوم الجاني بإرسال فيديو للمجني عليه عبر وسائل التواصل الاجتماعي يتضمن تهديداً له في حالة عدم استجابته لمطالبه.¹

ثانياً : النتيجة الإجرامية

النتيجة الإجرامية تعد الأثر الناتج عن السلوك الذي يهدف القانون إلى معاقبته، حيث تمثل هذه النتيجة حقيقة مادية تتجسد في كيان ملموس في العالم الخارجي أو يمكن اعتبارها حقيقة قانونية.²

و عليه تتحقق النتيجة الإجرامية في جريمة الابتزاز الإلكتروني عندما يقوم المبتز بإثارة الرعب و الخوف في نفسية الضحية من خلال التهديد بكشف أسرارها أو جزء من حياته الخاصة و ذلك مقابل الحصول على منفعة مادية أو معنوية أو جنسية، و ينتج عن ذلك قيام المسؤولية الجنائية للجاني حيث يتوافر الركن المادي للجريمة و حتى و إن لم تتحقق النتيجة الإجرامية المتمثلة في تنفيذ الجاني لتهديداته و نشر تلك المعلومات و الصور و المقاطع المرئية و جعلها متاحة للجمهور.³

ثالثاً : العلاقة السببية

لكي يتحقق الركن المادي بجميع عناصره يجب أن توجد صلة سببية بين السلوك الإجرامي الذي ارتكبه الجاني و النتيجة الناتجة عنه بحيث يمكن القول إن هذه النتيجة ناتجة عن ذلك السلوك، و إذا انعدمت العلاقة السببية فلا مجال لمسائلة الفاعل.⁴

يصعب تحديد العلاقة السببية في هذه الجريمة نظراً للتعقيدات المرتبطة بها حيث تحدث في بيئة إفتراضية يتضمن ذلك تداخل المراحل التي تمر بها الجريمة بدءاً من الدخول عبر جهاز الحاسوب، مروراً بالأوامر المدخلة وصولاً إلى النتيجة المراد تحقيقها سواء كانت قد

¹ - سهام عكوش ، المرجع السابق ، ص 1302 .

² - آمال برحال ، المرجع السابق ، ص 45 .

³ - أكرم ديب، نورة بن بو عبد الله، دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني، مجلة الحقوق و العلوم الانسانية، المجلد 16، العدد 01، 2023، ص 407.

⁴ - الطاهر ياكور ، المرجع السابق ، ص 41 .

تحققت بالفعل أم لا، و من هذا المنطلق تتمثل العلاقة السببية في جريمة الابتزاز الإلكتروني في خوف الضحية و استجابتها لمطالب الجاني نتيجة للتهديد الذي يمارسه الجاني بنشر معلومات و أسرار تتعلق بخصوصية الضحية في الفضاء الرقمي.¹

الفرع الثالث : الركن المعنوي

لا يكفي لقيام الجريمة أن يتم ارتكاب فعل مادي ينص عليه القانون الجنائي و يعاقب عليه بل يتعين أن يصدر هذا الفعل المادي عن إرادة الجاني، و تعد هذه العلاقة التي تربط الفعل المادي بالفاعل ما يعرف بالركن المعنوي.²

و عليه يعرف الركن المعنوي بأنه : " العلاقة التي تربط بين ماديات الجريمة و شخصية الجاني مرتكبها "، و تعتبر هذه العلاقة محورا لفهم استحقاق العقاب، و بالتالي يتم توجيه إليها اللوم من قبل القانون و عقوباته.³

تعتبر جريمة الابتزاز الإلكتروني من الجرائم العمدية التي تستلزم توفر القصد الجنائي والذي يتمثل في رغبة الجاني في تنفيذ فعل التهديد مع علمه لكافة أركان الجريمة القانونية، حيث يكون الجاني واعياً بمعاني عباراته أو أفعاله في لحظة ارتكاب التهديد، و تكون تلك العبارات أو الأفعال وفقاً لمفاهيمها اللغوية أو العرفية قادرة على إزعاج المجني عليه و إثارة الخوف و الرعب في نفسه، مما يؤثر بشكل ملحوظ على حالته النفسية، كما يشترط أن يكون الجاني مدركاً للنتائج المحتملة المترتبة على تهديده و أن تكون تلك النتائج مقصودة أو على الأقل متوقعة لديه ، مما يعكس نية جنائية واضحة في ارتكاب الجريمة و بالتالي في إطار جرائم الابتزاز يشترط أن تتجه إرادة الجاني نحو تحقيق هدفين أساسيين :

أ - الحصول على معلومات سرية تتعلق بالضحية .

¹ - فاطمة العرفي ، المرجع السابق ، ص 498

² - أحسن بوسقيعة ، المرجع السابق ، ص 112 .

³ - الطاهر ياكور ، المرجع السابق ، ص 42 .

ب- استعمال تلك المعلومات لابتزاز الضحية بغرض تحقيق مكاسب مادية أو الحصول على فوائد غير قانونية سواء كانت مالية أو معنوية.¹

المطلب الثاني : العقوبة المقررة لجريمة الابتزاز الإلكتروني

تعتبر النصوص القانونية بمثابة درع يحمي الفرد و يحيط به بمزيد من الأمان و الخصوصية، إذ فإن أي شخص يسعى لتجاوز هذه الحواجز أو اختراق هذا الدرع فهو مذنب و يستحق العقوبة المقررة على فعله.²

تنقسم العقوبات المقررة للجاني في جريمة الابتزاز الإلكتروني إلى نوعين أصلية وتكميلية، فتعرف العقوبات الأصلية في الفقه الجنائي بأنها تلك التي يحددها المشرع بشكل أساسي، حيث يمكن فرضها بشكل مستقل دون الحاجة إلى الحكم بعقوبة أخرى ، أما العقوبات التكميلية فهي تلك التي تترتب تلقائياً على العقوبات الأصلية بموجب القانون ، حيث تطبق حتى في حال عدم النص عليها في الحكم و بالتالي فإن النطق بالعقوبة الأصلية يتضمن ضمناً العقوبة التكميلية المنصوص عليها قانوناً سواء تم ذكرها صراحة في منطوق الحكم أم لا.³

وبناءً على ما تقدم، سيتناول هذا المطلب بيان العقوبة المقررة لجريمة الابتزاز الإلكتروني من خلال ثلاثة فروع، حيث خصصنا الفرع الأول للعقوبات الأصلية، بينما يتناول الفرع الثاني العقوبات التكميلية ثم نستعرض في الفرع الثالث حالات تشديد العقوبة.

الفرع الأول : العقوبات الأصلية لجريمة الابتزاز الإلكتروني

تحمل جريمة الابتزاز الإلكتروني وصف الجنحة و يعاقب عليها القانون بعقوبة سالبة للحرية و عقوبة مالية.

فبعد إثبات المسؤولية الجنائية للفرد عن ارتكاب جريمة الابتزاز الإلكتروني يواجه هذا الشخص عقوبات قانونية قد تتباين وفقاً للنظام القانوني في الدولة المعنية، و تستند هذه

¹ - نورة بن بو عبد الله، ورده بن بو عبد الله، المرجع السابق، ص- ص 355 - 356.

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 114 .

³ - رباب مصطفى عبد المنعم الحكيم ، المرجع السابق ، ص 3204 .

العقوبات على خطورة الجريمة و الظروف المحيطة بارتكابها¹، لذلك أقر المشرع الجزائري مثل العديد من الدول الأخرى فرض عقوبات أصلية لجريمة الإبتراز الإلكتروني التي تشمل:

أولاً: العقوبة السالبة للحرية

يعاقب الجاني في جريمة الإبتراز الإلكتروني بعقوبة سالبة للحرية و هي الحبس لمدة تتراوح بين سنتين (2) إلى خمس سنوات (5) ، ما يمكن ملاحظته أن المشرع حدد العقوبة السالبة للحرية بين حدين، حيث يتمثل الحد الأدنى في سنتين و الحد الأقصى خمس سنوات، مما يتيح للقاضي سلطة تقديرية في تقدير العقوبة ضمن هذين الحدين.

ثانياً: العقوبة المالية

رافق المشرع الجزائري العقوبة السالبة للحرية بعقوبة ذات طابع مالي تتمثل في الغرامة المالية و ذلك وفقاً لما نصت عليه المادة 1/371 من ق.ع.ج و يتراوح قدرها بين 200.000 دج إلى 500.000 دج، مما يجعل إعمال السلطة التقديرية للقاضي ممكناً بين الحد الأدنى والأقصى .

فيما يتعلق بعقوبة الشروع في جريمة الإبتراز الإلكتروني، فإن القانون الجزائري لم يفرد نصاً خاصاً لهذه الجريمة، و بالتالي تطبق عليها القواعد العامة المنصوص عليها في قانون العقوبات و تحديداً تطبق أحكام المادة 394 مكرر 7 من ق.ع.ج²، كما أقر المشرع المسؤولية الجزائية للشخص المعنوي عن هذه الجريمة بموجب المادة 394 مكرر 4 من ق.ع.ج³، وتطبق بخصوص هذه المسؤولية القواعد العامة المقررة لمسؤولية الشخص المعنوي بصورة عامة.

¹ - أكرم ماجد خلف ، المرجع السابق ، ص 427 .

² - راجع المادة 394 مكرر 7 من الأمر رقم 66-156 المتضمن قانون العقوبات المعدل و المتمم .

³ - راجع المادة 394 مكرر 4 من نفس القانون .

الفرع الثاني : العقوبات التكميلية لجريمة الإبتراز الإلكتروني

تنقسم العقوبات التكميلية إلى عقوبات تكميلية وجوبية و أخرى جوازية .

أولاً- العقوبات التكميلية الوجوبية

تتجلى في إصدار حكم بمصادرة الأشياء التي تم استعمالها في تنفيذ جريمة الإبتراز الإلكتروني و هذا وفقا لأحكام المواد 303 فقرة 02 مكرر 2 ، 394 مكرر 6 من ق.ع.ج¹ والمادة 333 مكرر 7 المستحدثة بموجب القانون رقم 24-06 السالف الذكر .

التي تنص على أنه " دون الإخلال بحقوق الغير حسن النية ، يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في المواد 333 مكرر 4 و 333 مكرر 5 و 333 مكرر 6 و الأموال المتحصلة منها و إغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة " .²

ثانياً-العقوبات التكميلية الجوازية

تتمثل في منع المحكوم عليه من ممارسة حق أو أكثر من الحقوق الوطنية و المدنية والعائلية لمدة لا تتجاوز 05 سنوات المنصوص عليها في المادة 19 مكرر 1 من ق.ع.ج³ والتي تتمثل في :

- العزل أو الإقصاء من جميع الوظائف و المناصب العمومية التي لها علاقة بالجريمة.
- الحرمان من حق الانتخاب أو الترشح و من حمل أي وسام .
- عدم الأهلية لأن يكون مساعد محلف أو خبيراً أو شاهداً على أي عقد ، أو شاهداً أمام القضاء إلا على سبيل الاستدلال .
- الحرمان من الحق في حمل الأسلحة، و في التدريس، و إدارة مدرسة أو الخدمة في مؤسسة التعليم بوصفه أستاذاً أو مدرساً أو مراقباً.
- عدم الأهلية لأن يكون وصياً أو قيماً.

¹- راجع المادتين 303 فقرة 02 مكرر 02 و 394 مكرر 6 من الأمر 66-156 المعدل و المتمم للقانون العقوبات .

²- راجع المادة 333 مكرر 7 من القانون رقم 24-06 المتضمن قانون العقوبات المعدل المتمم .

³- راجع المادة 19 مكرر 1 من الأمر 66-156 المعدل و المتمم للقانون العقوبات.

- سقوط حقوق الولاية كلها أو بعضها.

كما يجوز للمحكمة أن تأمر بنشر حكم الإدانة طبقاً لكيفيات المبنية في المادة 18 من ق.ع.ج.¹، كما يتعرض الشخص المعنوي لوحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر من ق.ع.ج.²

ثالثاً: المساهمة الجنائية في جريمة الابتزاز الإلكتروني

قد يقوم فرد واحد بارتكاب جريمة الابتزاز الإلكتروني فيتحمل المسؤولية الجزائية وحده، وقد يتعاون عدة أشخاص على ارتكابها، فيسهم كل منهم بقدر معين، و تتباين صور هذا التعاون بحسب ظروف الواقعة و الدور الذي يؤديه كل مساهم في تنفيذها وقد يتخذ هذا التعاون شكل اتفاق مسبق أو تداخل أدوار بين الفاعلين.

وتُعد المساهمة الجنائية في جريمة الابتزاز الإلكتروني صورة من صور الاشتراك في الجريمة، و تقوم على تعاون أكثر من شخص في ارتكابها، بما يفترض توافر شرطين أساسيين:

1- تعدد الجناة، بحيث لا تكون الجريمة ثمرة جهد فردي، و إنما نتيجة عمل جماعي

يساهم فيه كل شخص بدور محدد. وقد يكون هذا الدور رئيسياً فيعد صاحبه فاعلاً أصلياً أو مسهماً أصلياً، وقد يكون ثانوياً فيعد شريكاً أو مسهماً تبعياً في الجريمة.

2- وحدة الجريمة المرتكبة، أي أن الجريمة الناتجة عن هذا التعاون تعد جريمة واحدة،

ويستدل على وحدتها من خلال وحدة الركن المادي و الركن المعنوي.

فمن حيث الركن المادي، يتحقق عندما تكون النتيجة الإجرامية واحدة، سواء تحققت بفعل مادي واحد أو بأفعال متعددة صادرة عن المساهمين و مثال ذلك اتفاق شخصين على ابتزاز الضحية، حيث يقوم أحدهما بتوفير الوسيلة التقنية (الحاسوب أو الحساب الإلكتروني)، بينما يتولى الآخر التهديد و الابتزاز عبرها فتكون النتيجة المستهدفة واحدة و هي ابتزاز المجني عليه، أما وحدة الركن المعنوي، فتقوم على وجود رابطة ذهنية بين المساهمين تقتضى اتفاقاً

¹ - راجع المادة 18 من الأمر رقم 66-156 المتضمن قانون العقوبات المعدل و المتمم .

² - راجع المادة 18 مكرر من نفس القانون.

مسبقاً أو معاصراً على ارتكاب الجريمة، سواء كان هذا الاتفاق صريحاً أو ضمناً و يكفي تحقق هذا التفاهم لإثبات المساهمة الجنائية أما في حال غياب قصد الاشتراك، فإن كل شخص يسأل عن أفعاله على حدة دون قيام المساهمة الجنائية. و يتضح مما سبق أن المساهمة في جريمة الإبتراز الإلكتروني، سواء كانت مساهمة أصلية أو تبعية، لا تختلف في طبيعتها القانونية عن المساهمة في الجرائم التقليدية كالقتل و السرقة، من حيث صورها و أركانها¹، إذ تخضع لأحكام القواعد العامة المنصوص عليها في قانون العقوبات الجزائري، بما في ذلك الأحكام المتعلقة بتحديد مسؤولية الشريك و تقرير العقوبة المقررة له، إذ يخضع الشريك للأحكام القانونية ذاتها المنظمة للمساهمة الجنائية الواردة في المواد من 41 إلى 46 من ق.ع.ج²، بما في ذلك الأحكام الخاصة بالجزاء، حيث اتجه المشرع الجزائري إلى مساواة الشريك بالفاعل الأصلي من حيث العقوبة المقررة.

الفرع الثالث : حالات تشديد العقوبة

تتراوح العقوبات المنصوص عليها في التشريع الجزائري بين حدين أدنى و أقصى، باستثناء عقوبتي الإعدام و السجن المؤبد المقررتين للجنايات، يتمتع القاضي بسلطة مطلقة في تقدير العقوبة ضمن هذين الحدين دون الحاجة إلى تقديم مبررات أم أسباب، فإذا التزم القاضي بهذه الحدود فلا يوجد مبرر لتشديد العقوبة حتى و إن تم رفعها إلى الحد الأقصى للعقوبة المقررة قانوناً و التي تعرف بالظروف المشددة.³

¹ - حسام منصور محمد، المرجع السابق، ص- ص 52- 53.

² - راجع المواد من 41 إلى 46 من الأمر رقم 66-156 المتضمن قانون العقوبات المعدل و المتمم.

³ - أحسن بوسقيعة ، المرجع السابق ، ص338 .

فهناك حالات معينة يتم فيها تشديد العقوبة في جريمة الإبتراز الإلكتروني بشكل ملحوظ، الحالة الأولى هي عندما يكون التهديد يرمي إلى ارتكاب جرائم القتل أو التسمم أو أي اعتداء آخر على الأشخاص فتكون العقوبة الإعدام أو السجن المؤبد.¹

و الحالة الثانية هي عندما يكون التهديد بارتكاب جريمة ضد المال، أي أن الجاني يهدد الضحية بإيداع مبلغ من النقود في مكان معين أو تنفيذ أي شرط آخر.

و الحالة الثالثة هي عندما يكون التهديد بإفشاء أمور مخدشة بالشرف أي أن الجاني يهدد الضحية بكشف أسرار شخصية أو أمور حميمية أو معلومات محرجة، أما الحالة الرابعة عند المساس بحرمة الحياة الخاصة أي أن يقوم الجاني بالنقاط أو تسجيل أو نقل محادثات أو صور في مكان خاص بدون رضا صاحبها.

و علاوة على ذلك، يتم تشديد العقوبة بشكل ملحوظ، خاصة في حالات الإبتراز التي تتعلق بالقاصرين و استغلالهم في أنشطة قد تكون قانونية أو غير قانونية، و غالباً ما تكون هذه الأنشطة غير قانونية مثل ترويج المخدرات و ارتكاب عمليات السرقة، كما تزداد العقوبة على المبتز الذي يستغل منصبه أو معرفته بالضحية لتهديدها و في حال تكرار الجريمة و العود أي إذا قام الجاني بارتكاب جريمة الإبتراز أكثر من مرة، وكذلك في حالة استخدام حسابات وهمية لإخفاء هويته أو اختراق الأنظمة للوصول إلى المعلومات مثل الجرائم المتعلقة بالدخول غير المشروع و تخريب البيانات.

¹ - حسين طاهري، المرجع السابق، ص 229.

الفصل الثاني:

الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

تعد القواعد الإجرائية مجموعة من الأحكام والإجراءات التي تتبناها السلطة القضائية بهدف الوصول إلى الحقيقة وكشفها و جمع الأدلة التي تدين المشتبه فيهم، تهدف هذه الإجراءات إلى تنظيم ومتابعة سير التحقيق في جميع مراحله بدءاً من مرحلة جمع الاستدلالات مروراً بالتحقيق الابتدائي وصولاً إلى مرحلة المحاكمة، كل مرحلة من هذه المراحل تسعى لضبط الأدلة التي تكشف عن المتهمين بارتكاب الجريمة.

وبناءً على ذلك، فإن الجرائم التي ترتكب عبر الوسائل الإلكترونية تتطلب تأهيلاً فنياً وعملياً خاصاً يجب أن يتوفر في جميع الأفراد المعنيين بهذه الجرائم، بدءاً من مرحلة التحري وجمع الاستدلالات مروراً بالتحقيق الابتدائي وانتهاءً بالمحاكمة. إذ أن هذا النوع من الجرائم يتميز بطبيعته الفنية المعقدة و قدلاً يترك وراءه آثاراً واضحة تكشف عنه مما يتطلب خبرة معينة من جميع المعنيين، بما في ذلك عناصر الضبطية وقضاة التحقيق والنيابة وقضاء الحكم بالإضافة إلى هيئة الدفاع.¹ ونتيجة لذلك، أصبحت النصوص التقليدية لقانون الإجراءات الجنائية تمثل عائقاً يعرقل سير عمل الجهات المعنية بالتحقيق، وكذلك سير الدعوى في جميع مراحلها، بما في ذلك مرحلة التحقيق الابتدائي ففي هذه المرحلة تحديداً يواجه أفراد أجهزة العدالة العديد من التحديات سواء في ما يتعلق بالكشف عن حقيقة وقوع الجريمة أو في استخلاص الأدلة المتعلقة بها و يعود ذلك إلى سهولة محو أو تدمير الأدلة الناتجة عن الجريمة والتي تعرف بالأدلة الرقمية نظراً لطبيعتها التقنية .

بالإضافة إلى ذلك، يختلف مسرح جريمة الابتزاز الإلكتروني عن ما هو متعارف عليه في الجرائم التقليدية، حيث يتميز بطبيعة خاصة تتمثل في طابعه التقني ووجوده في البيئة الافتراضية، وهذا يتطلب من جهات التحقيق أن تكون على دراية علمية متقدمة بطبيعة العالم الافتراضي والأدلة الرقمية الناتجة عنه، حتى يتسنى لهم فهم هذا النوع من الجرائم وكشف الغموض الذي يكتنفها.²

¹ - الطاهر ياكور ، المرجع السابق ، ص 81 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 147 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

لذلك وبناءً على ما سبق، سيتم تقسيم هذا الفصل إلى مبحثين، نناقش في الأول التحقيق و الإثبات في جريمة الابتزاز الإلكتروني، فيما سيعنى المبحث الثاني بمكافحة جريمة الابتزاز الإلكتروني على المستوى المؤسساتي الوطني .

المبحث الأول : التحقيق والإثبات في جريمة الابتزاز الإلكتروني

تخضع جريمة الابتزاز الإلكتروني مثل غيرها من الجرائم لمرحلة الاستدلال و التحقيق الجنائي بعد وقوعها حيث يهدف هذا التحقيق إلى اكتشاف الجريمة وفاعلها وفهم جميع الوقائع والملابسات المرتبطة بها، فيتعين على المحققين تحديد ما إذا كان مرتكب الجريمة فردًا واحدًا أم مجموعة من الفاعلين ومن بين الأهداف الأساسية لهذا البحث والتحقيق هو الوصول إلى الحقيقة التي تتطلب بدورها أدلة تثبت نسبة التهمة إلى المتهم أو نفي الجريمة عنه، ولكي تكتمل خصوصية هذه الجريمة يجب الإقرار بأن الأدلة في الجرائم الإلكترونية وبالأخص في جريمة الابتزاز الإلكتروني هي أدلة غير تقليدية ترتبط بالحواسيب وأجهزة الهواتف المحمولة وملحقاتها بالإضافة إلى البرامج والتطبيقات التكنولوجية.

تتميز الجرائم التقنية بالتباعد الجغرافي بين الجاني والمجني عليه ، حيث يقوم المجرم بالمعلوماتي بارتكاب جريمته بعد تخطيط مسبق مستخدماً قدراته الفنية والعقلية ويحيط نفسه بتدابير أمنية ووقائية تعزز من صعوبة الكشف عنه وعن مخططاته، لذا يلجأ إلى التمويه من خلال استخدام التشفير وكلمات السر والأسماء المستعارة، بالإضافة إلى سهولة محو الأدلة والتلاعب بها و في ظل هذه الظروف تبرز صعوبة اكتشاف الجرائم الإلكترونية.¹

لذلك وتأسيساً على ما تقدم، سنقوم بتقسيم هذا المبحث المتمثل في التحقيق والإثبات في جريمة الابتزاز الإلكتروني إلى مطلبين، نخصص الأول لبيان إجراءات التحقيق في جريمة الابتزاز الإلكتروني، في حين سنناقش في المطلب الثاني الإثبات في جريمة الابتزاز الإلكتروني.

المطلب الأول : إجراءات التحقيق في جريمة الابتزاز الإلكتروني

عُرف التحقيق الجنائي في الجرائم الإلكترونية بأنه : " عمل قانوني يقوم به مأمور الضبط القضائي المختص و المتخصص لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل

¹ - مريم عراب ، المرجع السابق ، ص 1214 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

إلكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل".¹

ومن هذا المنطلق تتميز خصائص جريمة الابتزاز الإلكتروني عن الجرائم التقليدية، مما يفرض تحديات على الجهات المعنية بالتحقيق فيما يتعلق بملائمة الإجراءات المتبعة سواء بشكل عام أو فيما يخص جريمة الابتزاز الإلكتروني بشكل خاص، ومع ذلك تظل الإجراءات الجزائية في إطار قواعد التحقيق كما هي مع الأخذ بعين الاعتبار الفروقات الموضوعية المرتبطة بعمليات التحقيق وتتشابه هذه الإجراءات عبر مختلف أنواع الجرائم سواء كانت إلكترونية أو تقليدية حيث تتطلب جميعها عمليات المعاينة والتفتيش والاستجواب وجمع الأدلة وتحليلها والأهم من ذلك يتعين على المحقق اتخاذ الاحتياطات اللازمة للحفاظ على الأدلة المضبوطة في مسرح الجريمة من العبث أو فقدان.²

استناداً إلى ما تم ذكره، سنسعى في هذا المطلب إلى توضيح إجراءات التحقيق في جريمة الابتزاز الإلكتروني من خلال ثلاثة فروع في الفرع الأول، سنستعرض الإجراءات التقليدية المتبعة في التحقيق هذه الجريمة، بينما سنخصص الفرع الثاني، لمناقشة المعوقات التي تعترض تلك الإجراءات التقليدية، أما في الفرع الثالث، فسنتناول الإجراءات المستحدثة التي تم الإعتماد عليها للتحقيق في جريمة الابتزاز الإلكتروني .

الفرع الأول : التحقيق في جريمة الابتزاز الإلكتروني عن طريق الإجراءات التقليدية

عند تطرقنا لجريمة الابتزاز الإلكتروني وما تثيره من صعوبات إجرائية، سنركز على الجانب الإجرائي لهذه الجريمة، نظراً لخصوصية هذا الجانب في عدة صور من الإجراءات التحقيقية مثل المعاينة والتفتيش والضبط، والتي تتمتع بحضور بارز في هذا الإطار، أما

¹ - مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الالكترونية ، ط 01 ، مطابع الشرطة للطباعة و النشر و التوزيع ، القاهرة ، 2009 ، ص 166 .

² - عماد جواد موسى ، التحقيق و الصعوبات التي تواجه جريمة الابتزاز الإلكتروني ، مجلة كلية المعارف الجامعة ، المجلد 33 ، العدد 04 ، 2022 ، ص 237 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

بالنسبة للإجراءات التحقيقية الأخرى مثل الشهادة والاستجواب وما شابهها، فإنها تقع خارج نطاق هذا البحث حيث إنها ذات طبيعة شخصية وليست مادية، مما يعني أنها تتعلق بالأشخاص وليس بالأشياء وبطبيعة الحال فإن هذه الإجراءات التحقيقية هي ذاتها المتبعة وفقاً للمبادئ الإجرائية العامة التي تحكم أي جريمة أخرى سواء كانت جريمة الابتزاز الإلكتروني أو غيرها من الجرائم.¹

استكمالاً إلى ما تم ذكره، سنقوم في هذا الفرع بفتح نافذة لاستعراض الإجراءات التحقيقية المتعلقة بالمعينة و التفتيش والضبط، وذلك من ثلاث فقرات كما يلي :

أولاً : المعينة

تعرف المعينة بأنها : " الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص و الفحص الدقيق لكافة المحتويات تهدف كشف مخلفات و آثار الجاني بالمكان والتي تشير إلى شخصيته أو شركائه وما قد يفيد في إثبات ارتكاب الجريمة وتوضيح قدرا من الاستنتاجات المنطقية تشكل في حد ذاتها الأساس الذي تقام عليه عملية التحقيق و البحث والمعينة ".²

كما يطلق على المعينة في جريمة الابتزاز الإلكتروني بأنها : " معينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الأنترنت، وتشمل الرسائل المرسله منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر أو الانترنت".³

تعتبر المعينة إجراء لتحقيق أو إستدلال وهي تعد إجراءً جوازيًا للمحقق شأنها شأن باقي إجراءات التحقيق، ومع ذلك المعينة في مجال الجرائم الالكترونية الرقمية لا تتمتع بنفس الأهمية التي تلعبها في الجرائم التقليدية وذلك لسببين رئيسيين هما :

1- الجرائم التي تستهدف أنظمة المعلومات و الشبكات نادراً ما تترك آثار مادية واضحة.

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص 151 .

² - محمود أحمد القرعان، الجرائم الإلكترونية ، ط 01، دار وائل للنشر و التوزيع، الأردن - عمان، 2017، ص 249 .

³ - آمال برحال، المرجع السابق، ص 69 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

2- قد يتواجد عدد كبير من الأشخاص في مسرح الجريمة خلال الفترة الزمنية الفاصلة بين ارتكاب الجريمة واكتشافها، مما يتيح الفرصة لإحداث تغييرات أو إتلاف أو عبث بالآثار المادية المتبقية.¹

ولعل من المناسب أن نذكر لكي تثمر المعاينة وتحقق أهدافها المرجوة، نجد أن بعض القوانين الوطنية قد فرضت عقوبات جنائية على كل من يقوم بإجراء أي تغيير في مكان وقوع الجريمة أو ينزع أي شيء منه قبل البدء في الإجراءات الأولية للتحقيق القضائي، ولكن إذا كانت هذه التغييرات أو إزالة الأشياء من أجل السلامة و الصحة العامة فلا تفرض عقوبات.² وفي هذا المقام وبالرجوع إلى قانون الإجراءات الجزائية لسنة 2025 وبالتحديد في الفقرة الأولى المادة 74 منه نلاحظ أن المشرع الجزائري قد التفت إلى هذه المسألة و فرض جزاء جنائي لمن يحظر في مكان ارتكاب جنائية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي فيعاقب بغرامة مالية يتراوح قدرها من 20.000 دج إلى 100.000 دج.³ كما ورد على هذه القاعدة استثناء بحيث جاءت المادة المذكور أعلاه في فقرتها الثانية صريحة حيث جاء في محتواها " غير أنه يستثنى من هذا الخطر حالة ما إذا كانت التغييرات أو نزع الأشياء ضرورية للسلامة والصحة العمومية أو تستلزمها معالجة الضحايا".⁴

الهدف من المعاينة هو تحديد أثر الدليل المتبقي في مسرح الجريمة لمستخدمي شبكة الانترنت، حيث يترك مستخدمو هذه الشبكة أثراً واضحة، إذ يقوم الموقع المستخدم بتسجيل معلومات محددة تتضمن عنوان الموقع ونوع المتصفح المستخدم وعنوان IP الثابت والمتغير

¹ - مريم عراب ، المرجع السابق ، ص 1219 .

² - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01 ، دار الفكر الجامعي، الاسكندرية، 2009 ، ص150 .

³ - المادة 1/74 من القانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54، الصادرة في 13 غشت 2025 .

⁴ - المادة 74 / 2 من نفس القانون .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

لجهاز الكمبيوتر المتصل، وفي بعض الحالات يمكن أيضاً الوصول الى عنوان البريد الإلكتروني واسم المستخدم إن الآثار الرقمية المستخرجة من أجهزة الكمبيوتر تعتبر ذات أهمية كبيرة في عملية جمع الأدلة وضبطها، نظراً لما تحتويه من معلومات قيمة تشمل صفحات الويب، والبريد الإلكتروني، والفيديو الرقمي، وغرف الدردشة، والمحادثات، و الملفات المخزنة على الكمبيوتر و الصور المرئية، بالإضافة إلى معلومات الدخول إلى الخدمة والاتصال بالإنترنت عبر مزود الخدمة.¹

ولكن قد يثار تساؤل في هذا الإطار حول كيفية الانتقال إلى العالم الافتراضي للمعاينة في جريمة الابتزاز الإلكتروني ؟

وللإجابة عن التساؤل المتقدم، يجب الإشارة إلى أن المعاينة في جرائم الأنترنت تجرى كما هو الحال في أي جريمة أخرى من خلال الانتقال إلى مسرح الجريمة، إلا أن هذا الانتقال في سياق جرائم الأنترنت لا يتم إلى العالم المادي بل إلى العالم الافتراضي أي الفضاء الإلكتروني، فالمعاينة تتطلب الانتقال إلى موقع الجريمة كقاعدة إجرائية معروفة إلا أن هذا الانتقال في إطار جرائم الإلكترونيات يعد موضوعاً جديداً حيث لا يكون بالضرورة عبر العالم الافتراضي، ففي حالة جريمة الابتزاز يكون الانتقال محصوراً في الفضاء الرقمي وليس في مكان مادي، فهناك عدة طرق يمكن من خلالها لعضو سلطة التحقيق أو الضبط القضائي الانتقال إلى الفضاء الإلكتروني لإجراء المعاينة التي يمكن إيجازها كالآتي:

- 1- من مكتبه في المحكمة باستخدام جهاز الكمبيوتر الخاص به.
- 2- يمكنه أيضاً التوجه إلى مقر عمل مزود خدمة الأنترنت الذي يعد المكان الأمثل لإجراء المعاينة .
- 3- كما يمكن للمحقق الانتقال إلى العالم الافتراضي لإجراء المعاينة من خلال مكتب خبير تقني متخصص إذ كان لديه ما يتيح القانون.²

¹ - عماد جواد موسى ، المرجع السابق ، ص 240 .

² - أمير فرج يوسف ، المرجع السابق ، ص 130 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

ولكي تكون معاينة مسرح الجريمة الرقمية في جريمة الابتزاز الإلكتروني ذات فائدة في كشف الحقائق المتعلقة بها و بمرتكبها يجب الالتزام بعدد من الخطوات والإرشادات الفنية الأساسية ومن أبرزها ما يلي :

1- يتعلق الأمر بتصوير الحاسوب وما يرتبط به من أجهزة بدقة عالية، بالإضافة إلى جميع ملحقاته والأجهزة الطرفية المتصلة به، كما يتضمن ذلك توثيق المحتويات والأوضاع العامة في موقعه، مع التركيز بشكل خاص على تصوير الأجزاء الخلفية للجهاز مع مراعاة تسجيل الوقت و التاريخ و المكان الذي تم فيه القاط كل صورة.

2- يتطلب الأمر اهتماماً كبيراً بمراقبة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وخاصة السجلات الإلكترونية التي تزود بها شبكات المعلومات، وذلك بهدف تحديد موقع الاتصال ونوع الجهاز الذي تم من خلاله الوصول إلى النظام أو الموقع أو الدخول في حوار معه.

3- يجب الامتناع عن نقل أي معلومات من مسرح الجريمة قبل إجراء الفحوصات اللازمة للتأكد من خلو البيئة المحيطة بموقع الكمبيوتر من أي مجالات مغناطيسية قد تؤدي إلى المحو أو الإتلاف البيانات المسجلة.

4- إعداد مخطط تفصيلي للمنشأة التي وقعت فيها الجريمة مع تقديم كشف شامل بأسماء المسؤولين المعنيين ودور كل واحد منهم المكلف بهذه المهمة.

5- يقتصر إجراء المعاينة المباشرة على فئة محددة من الباحثين والمحققين الذين يمتلكون الكفاءة العلمية والخبرة الفنية في مجالات الحاسوب و الشبكات ونظم المعلومات واسترجاع المعلومات ويجب أن يكون هؤلاء الأفراد قد تلقوا تدريباً كافياً يمكنهم من التعامل مع نوعية الآثار والأدلة التي يحتوي عليها مسرح الجريمة الإلكترونية.¹

¹ - خالد ممدوح إبراهيم ، المرجع السابق ، ص-ص 172 ، 173 ، 174 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

و في ضوء ذلك نجد إن إجراء إعادة المعاينة المستمرة لمسرح الجريمة قد يكشف دائماً عن أدلة جديدة، حيث قد توجد أدلة مخفية من الجاني و من هنا نستخلص أن المعاينة في الجرائم الإلكترونية لمسرح الجريمة قد لا تكون فعالة بنفس القدر كما هو الحال في الجرائم التقليدية، نظراً لوجود صعوبات أثناء التنفيذ، إذ تتطلب هذه العملية تخصصاً في البحث داخل جهاز الكمبيوتر وملحقاته ويتعامل المحقق مع معلومات وبيانات مخزنة فيه.¹

ثانيا : التفتيش

يعد التفتيش من أهم وأخطر الحقوق الممنوحة للمحقق، نظراً لمساسه بالحريات الخاصة المكفولة دستورياً لذلك نجد أن المشرع يضع مجموعة من الضوابط المتعلقة بالسلطة المخولة لمباشرة هذا الإجراء وكذلك الجهة التي يسمح لها بممارسته، بالإضافة إلى الظروف التي يسمح فيها بالتفتيش والشروط الواجب توافرها لتنفيذه بما يضمن حماية الحرية الفردية أو حرمة المسكن.²

بعيداً عن التفتيش التقليدي في البيئة المادية، يعرف التفتيش في البيئة الإلكترونية بأنه: " إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني "³، فالتفتيش الإلكتروني هو إجراء من إجراءات البحث و التحقيق يهدف الى الوصول إلى أدلة ارتكاب الجريمة في بيئة افتراضية، حيث يتم تخزين هذه الأدلة بشكل إلكتروني ضمن نظام معلوماتي.⁴

ولعل من المناسب أن نذكر بأن المشرع الجزائري لم يعرف مفهوم التفتيش الإلكتروني بشكل صريح، إلا أنه أشار إليه في المادة 05 من القانون رقم 04-09 الذي يتضمن القواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، ويعتبر هذا

¹ - عماد جواد موسى ، المرجع السابق ، ص 241 .

² - عز الدين عثمانى ، إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الإتصال و المعلوماتية ، مجلة دائرة البحوث و الدراسات القانونية و السياسية - مخبر المؤسسات الدستورية و النظم السياسية ، العدد 04 ، 2018 ، ص 56 .

³ - أمير فرج يوسف ، المرجع السابق ، ص 133 .

⁴ - كمال حفصاوي ، عمر مخلوف ، التفتيش الإلكتروني بين ضرورة التحقيق و الحق في سرية المراسلات و الاتصالات ، مجلة الباحث للدراسات الأكاديمية ، المجلد 11 ، العدد 01 ، 2024 ، ص 332 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

الإجراء جزءاً من إجراءات التحقيق في الجرائم الإلكترونية أو الجرائم ذات الصلة ويعتمد عليه في الحالات التي يصعب فيها الوصول إلى نتائج تتعلق بالتحقيقات الجارية دون اللجوء إلى التفتيش الإلكتروني.¹

يعتبر التفتيش من أخطر إجراءات التحقيق، إذ يتضمن المساس بالحرية الشخصية ومع ذلك فإن مختلف التشريعات تسمح بهذا الإجراء بهدف الكشف عن الحقيقة مع الحرص على إحاطته بضوابط أو شروط معينة حيث قسم الفقه هذه الضوابط إلى نوعين ضوابط موضوعية تتعلق بنشوء السلطة في التفتيش و ضوابط شكلية تتعلق بالمتطلبات والإجراءات التي يجب أن يستوفىها أمر التفتيش أو حضور بعض الأشخاص أثناء تنفيذ عملية التفتيش.²

1- الضوابط الموضوعية لتفتيش نظم الحاسب الآلي:

أ- وجود سبب للتفتيش:

يُعزى سبب إجراء التفتيش في العالم الافتراضي إلى ضرورة وجود جريمة إلكترونية قد وقعت بالفعل سواء كانت جنائية أو جنحة مع توجيه الاتهام إلى شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، مع توفر أدلة قوية تشير إلى وجود أجهزة معلوماتية قد تسهم في كشف الحقيقة المتعلقة بالمتهم أو غيره، يعتبر تقديم مبررات كافية للجوء إلى إجراء التفتيش سواء في الجرائم التقليدية أو في الجرائم المعلوماتية من الأمور الأساسية التي يجب أن تتوفر من أجل تنفيذ هذا الإجراء من قبل قاضي التحقيق أو ضابط الشرطة القضائية وفي غياب هذه المبررات يعتبر ذلك تعسفاً وخطأً في إجراءات التحقيق.³

¹ - كمال حفصاوي ، عمر مخلوف المرجع السابق ، ص-ص 331-332 .

² - إلهام بن خليفة ، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، المجلة الدولية للبحوث القانونية و السياسية ، المجلد 02 ، العدد 01 ، 2018 ، ص 31 .

³ - يوسف صغير ، آليات مكافحة الجريمة المرتكبة عبر الإنترنت ، رسالة لنيل درجة دكتوراه في العلوم ، تخصص قانون ، جامعة مولود معمري - تيزي وزو ، 01 جويلية 2024 ، ص 123 .

ب- محل التفتيش:

يقصد بمحل التفتيش هو " المستودع الذي يحتفظ فيه الشخص بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك السر الذي يستودع في محل له حرمة، و من ثم قد يكون محل التفتيش إما شخصاً ، أو مسكناً، أو سيارة وما شاكل ذلك، مع مراعاة الضوابط القانونية المقررة. " ¹

إن محل التفتيش بالنسبة للجرائم الإلكترونية يتمثل في نظام الحاسب الآلي بجميع مكوناته المادية و المعنوية، بالإضافة إلى شبكات الاتصال التي تشمل مكونات الخادم و المزود الآلي والمضيف والملحقات التقنية أو الوسائط الإلكترونية بمختلف أنواعها ولا يختلف اثنان على أن الوصول إلى المكونات المادية للحاسب الآلي بغرض البحث عن أدلة تتعلق بجريمة معلوماتية قد وقعت، يعتبر أمراً مفيداً في كشف الحقيقة حول تلك الجريمة ومرتكبيها ويخضع هذا الإجراء للقواعد الإجرائية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكونات المادية يعتمد على طبيعة المكان الذي توجد فيه سواء كان من الأماكن العامة أو الخاصة سواء كان مسكن المتهم أو مسكن شخص آخر وفي أي وقت، و بشكل عام فإن صفة المكان تلعب دوراً مهماً جداً في مجال التفتيش. ²

ج- السلطة المختصة بالتفتيش:

نظراً لأن إجراء التفتيش يعتبر من إجراءات التحقيق الابتدائي التي تؤثر على الحرية الشخصية وتعد انتهاكاً لحرمة الحياة الخاصة للأفراد، فقد حرص المشرع الجزائري على إسناد مهمة التفتيش إلى جهة قضائية تضمن حماية تلك الحقوق والحريات، وقد حدد المشرع الجهة

¹ - باقر غازي حنون الدراجي ، المرجع السابق ، ص155.

² - مريم عراب ، المرجع السابق ، ص 1220 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

المختصة بالتفتيش في قاضي التحقيق الذي يعهد إليه بإجراء التفتيش بينما تتولى النيابة العامة مهمة متابعة الجرائم واتخاذ الإجراءات المناسبة بشأنها¹.

2- الضوابط الشكلية لتفتيش نظم الحاسب الآلي تتمثل في:

أ- إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون:

يشترط المشرع الجزائري لإجراء التفتيش بغض النظر عن الجهة القائمة به وفقاً للمادة 76 في فقرتها الأولى حضور صاحب المسكن الذي يشتبه في مساهمته في ارتكاب الجريمة وفي حال تعذر حضوره يلزم ضابط الشرطة القضائية بتكليف تعيين ممثل عنه و في حال امتناعه عن ذلك أو كونه هارباً يتعين على ضابط الشرطة القضائية استدعاء شاهدين من غير الموظفين الخاضعين لسلطته، فيما يتعلق بالجرائم المرتبطة بأنظمة معالجة البيانات الآلية والجرائم المنظمة العابرة للحدود الوطنية وغيرها من الجرائم المحصورة على سبيل الحصر، أورد المشرع استثناء في الفقرة الأخيرة من ذات المادة ينص على إمكانية إجراء التفتيش دون حضور الأفراد كما أسلفنا ويعزى سبب هذا الاستثناء إلى الخصائص التي تتطلبها أدلة الجرائم الإلكترونية والتي تتمثل في سهولة تعديلها وسرعة تبخرها، مما يستدعي ضرورة الحفاظ على سرية التفتيش والإسراع في جمع الأدلة قبل أن تمتد إليها أيدي العابثين².

ب- تحرير محضر التفتيش:

يجب إعداد محضر للتفتيش يتضمن جميع الإجراءات و الخطوات التي اتخذها القائم بالتفتيش أثناء عملية التنفيذ بالإضافة إلى النتائج التي أسفرت عنها تلك الإجراءات ولا يفرض القانون شروطاً أو أشكالاً محددة لمحتوى محضر التفتيش، وبالتالي فإن صحة محضر تفتيش نظام الحاسوب تتطلب فقط ما تقتضيه القواعد العامة المتعلقة بالمحاضر بشكل عام³، مثل أن

¹ - عزيزة رابحي ، التفتيش في نظم المعالجة الآلية للمعطيات ، مجلة القانون و العلوم السياسية ، المجلد 02 ، العدد 01 ، 2016 ، ص-ص 405- 406 .

² - إلهام بن خليفة ، المرجع السابق ، ص 37 .

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 158 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

يكون المحضر مكتوباً باللغة الرسمية، مؤرخاً وموقعاً عليه، علاوة على ذلك يجب أن يتضمن المحضر كافة الإجراءات المتبعة من قبل الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به لتقديم الخبرة الفنية اللازمة.¹

ج- وقت أو ميعاد إجراء التفتيش :

حرصاً على تقليص نطاق الاعتداء على الحرية الفردية وحرمة المسكن ، تسعى التشريعات الإجرائية إلى تحديد وقت معين لإجراء عمليات التفتيش²، بينما تترك بعض هذه التشريعات مسألة تحديد ذلك الوقت للجهة المنفذة للتفتيش سواء كان ذلك في الليل أو النهار وذلك ضمن المدة المحددة في الاذن ومن بين هذه التشريعات نجد القانون العماني والقانون العراقي.³

من الجدير بالذكر إن المشرع الجزائري قد تناول موعد إجراء التفتيش بموجب نص المادة 78 الفقرة الأولى من قانون إج.ج.ج التي جاءت تنص على أنه : " لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحاً، ولا بعد الساعة الثامنة (8) مساءً..... " ⁴، يتبين من خلال هذا النص أن المشرع الجزائري قد اعتبر فترة الليل هي تلك التي تسبق الساعة الخامسة صباحاً أو التي تلي الساعة الثامنة مساءً وهذا يشير إلى أن المشرع قد حظر إجراء التفتيش في الليل وبالتالي فإن الأصل في النظام الإجرائي الجزائري هو عدم دخول المساكن وتفتيشها خلال ساعات الليل ولا يجوز الخروج عن هذا الأصل بشكل عام ومع ذلك فقد حدد المشرع الجزائري بعض الحالات الاستثنائية على سبيل الحصر التي يحق فيها لضباط الشرطة القضائية تجاوز هذه القاعدة مما يتيح لهم إجراء التفتيش في أي

¹ - ليندا بن طالب ، التفتيش في الجريمة المعلوماتية ، مجلة العلوم القانونية و السياسية ، عدد 16، 2017 ، ص 494 .

² - عزيزة رابحي ، المرجع السابق ، ص 408.

³ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 158 .

⁴ - المادة 1/78 من القانون رقم 25 -14 المتضمن قانون الإجراءات الجزائية .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

وقت بما في ذلك الليل و تتمثل هذه الحالات في الجرائم المستحدثة¹، حسب ما أشارت إليه المادة 78 في فقرتها الثالثة من إ.ج.ج.ج.²

ثالثا : الضبط

يعتبر الضبط الهدف الأساسي من عملية التفتيش والنتيجة المباشرة المستهدفة، ولذلك يجب أن تتوفر في إجراءات الضبط القواعد ذاتها التي تنطبق على التفتيش كما أن بطلان التفتيش يؤدي إلى بطلان الضبط.³

و يقصد بالضبط هو " الحصول على أي دليل لمصلحة التحقيق ،لإثبات واقعة معينة، أو هو وضع اليد على شيء يتعلق بالجريمة ويسهم في كشف حقيقة تلك الجريمة وتحديد مرتكبها ".⁴

وتأسيسا لذلك، قد تناول المشرع الجزائري في القانون 09-04 القواعد المتعلقة بضبط البيانات المعلوماتية تحت مسمى " حجز المعطيات المعلوماتية " وهو بمثابة الخلاصة النهائية التي تؤدي إلى عمليات التفتيش وما ينتج عنها من آثار مباشرة، بما في ذلك جمع الأدلة في الجرائم الإلكترونية ويرتبط هذا الحجز عادة بالعناصر المادية مثل أجهزة الكمبيوتر وملحقاتها والأقراص الصلبة ، حيث لا تثير عملية حجز هذه المكونات أي إشكال، لكن الأمر يصبح معقداً عندما يتعلق بالحجز الإلكتروني للمكونات المعنوية للحاسب الآلي كالبرامج والبيانات المعالجة، التي تعتبر في جوهرها أشياء غير ملموسة، مما يثير العديد من الإشكالات.⁵

¹ - عزيزة رابحي ، المرجع السابق ، ص-ص 408-409 .

² - راجع المادة 3/78 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية .

³ - عبد القادر فلاح ، حجز و حفظ المعطيات في الجريمة الإلكترونية ، مجلة صوت القانون ، المجلد 08 ، العدد 01 ،

2021 ، ص 180 .

⁴ - باقر غازي حنون الدراجي ، المرجع السابق ، ص 161 .

⁵ - عبد القادر فلاح ، المرجع السابق ، ص 179 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الفرع الثاني : المعوقات التي تواجه جهات التحقيق

تواجه عملية التحقيق في جريمة الابتزاز الإلكتروني العديد من التحديات و العقبات التي قد تعيق المحققين عن الوصول إلى نتائج ايجابية تكشف عن هوية مرتكبي هذه الجرائم، بل إن هذه الصعوبات قد تؤدي أحياناً إلى نتائج سلبية مما يسبب فقدان الثقة في الأجهزة الأمنية من قبل المجتمع والضحايا على حد سواء، فضلاً عن تأثيرها على ثقة المحقق بنفسه نتيجة عجزه عن التعامل مع قضايا تمس أمن المجتمع بشكل كبير.¹ و سنتناول هذه الصعوبات أو المعوقات عبر الفقرات الآتية:

أولاً : حق الإنسان في الخصوصية

يعتبر الحق في الخصوصية من الحقوق الجوهرية للإنسان في العصر الحديث ، لذا قامت أغلب دول العالم بتجريم التعدي على حرمة الحياة الخاصة للإنسان باعتبار حق الإنسان في الخصوصية وحقه في حرمة حياته الخاصة من أبرز الحقوق الأساسية التي تتعلق بكرامة الإنسان وإنسانيته فضلاً عن قيم معنوية أخرى مثل الحق في المشاركة السياسية والحق في الرأي والتعبير وما شاكل ذلك من الحقوق.²

ومن أبرز العراقيل التي تعترض المحقق في قضايا الابتزاز الإلكتروني في مسألة حق الفرد في الخصوصية فيعود ذلك إلى التحدي المتمثل في إيجاد توازن بين حرمة الحياة الشخصية للأفراد و الاعتبارات القانونية التي تستدعيها تطبيقات القانون.³

ثانياً : قلة الخبرة لدى جهات التحقيق

تواجه جهات التحقيق تحديات تتعلق بنقص الخبرة الفنية و التدريب الكافي في التعامل مع الأدلة الرقمية، بما في ذلك كيفية البحث عنها و جمعها كما أن التحقيق مع مجرم ذكي يتطلب مهارات خاصة، حيث يسعى هذا المجرم الى التلاعب بالمحققين و محاولة الهروب

¹ - عماد جواد موسى ، المرجع السابق ، ص - ص 244 - 245 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص - ص 163 - 164 .

³ - عماد جواد موسى ، المرجع السابق ، ص 245 .

من جريمته ربما من خلال إغراقهم في تفاصيل قد تكون بعيدة عن معرفتهم لذا يجب أن يمتلك المحقق الجنائي في قضايا الابتزاز الإلكتروني بتكوين تقني متكامل يجمع بين مهارات استخدام التقنيات الحديثة وقدرة على تقييم الجريمة الإلكترونية ومدى خطورتها، بالإضافة إلى مهارات التعرف على المكونات المادية للأجهزة وملحقاتها مثل الطابعات والماسحات الضوئية والكاميرات للتأكد من ارتباطها بالجهاز الأصلي وتقييم الوسائط المستخدمة في تخزين الأدلة الرقمية لتحديد مدى ارتباطها بالانترنت وما إذا كانت تشكل جزءاً من أدوات الجريمة أم لا.¹

ثالثاً : سيادة القانون والحاجة لتطوير القوانين

تعتبر الحاجة إلى تأسيس اتفاق دولي و آلية موحدة للتعامل مع جريمة الابتزاز الإلكتروني أمراً بالغ الأهمية نظراً لحدثة هذه الجريمة و انتشارها في مختلف الدول، إن تباين التشريعات والقوانين بين الدول يشكل عائقاً أمام الكشف عن العديد من المجرمين، حيث توفر هذه الاختلافات بيئة ملائمة لهم لتنفيذ مخططاتهم الإجرامية لذا يتوجب توحيد الإجراءات الدولية لتسهيل متابعة مجرمي الحاسوب و توفير الدعم و التعاون اللازمين للإطاحة بهم و كشف جرائمهم و قد أكدت الأمم المتحدة في تقريرها المتعلق بأعمال الدورة التاسعة للمجلس الاقتصادي و الاجتماعي على أهمية وضع توصيات ذات توجه علمي تهدف إلى منع ومكافحة الجرائم المرتبطة بالحاسوب و تعزيز القدرات على التصدي لها و التحري عنها.

إن الدور الذي تلعبه الشرطة الدولية الإنتربول في مكافحة الجرائم الإلكترونية يتطلب مزيداً من التفاعل بين الدول و استمرار التعاون فيما بينها للحد من خطورة هذه الجرائم ، مما يستدعي تكثيف الجهود و تعزيز التعاون و العمل المستمر لوضع أسس فعالة لتحقيق التعاون الدولي في مواجهة الجرائم الإلكترونية بما في ذلك جريمة الابتزاز الإلكتروني.²

¹ - مريم عراب ، المرجع السابق ، ص - ص 1215 - 1216 .

² - عماد جواد موسى ، المرجع السابق ، ص 246 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الفرع الثالث : التحقيق في جريمة الابتزاز الإلكتروني عن طريق الإجراءات المستحدثة

في ظل التطور التكنولوجي أثرت شبكة الأنترنت على طبيعة الجرائم المرتكبة عبرها، حيث أفرزت هذه الشبكة العالمية جرائم جديدة لم تكن معروفة من قبل في الساحة القانونية وقد امتد هذا التأثير ليشمل الآليات المعتمدة لمكافحة هذه الجرائم، إذ نال الجانب الإجرائي النصيب الأكبر من تأثير هذه المتغيرات على النظم القانونية بشكل عام، مما جعل الإجراءات التقليدية كالفتيش و الشهادة و الخبرة غير كافية لمتابعة تطورات هذه الجرائم المستحدثة.¹

و نظراً لأن مرتكب جريمة الابتزاز الإلكتروني يترك آثاراً رقمية تتميز بطابع غير مادي، فإنه من الضروري تطوير إجراءات حديثة تتماشى مع طبيعة الأدلة الرقمية الناتجة عن هذه الجريمة و من بين هذه الإجراءات الحديثة هي اعتراض المراسلات و تسجيل الأصوات والنقاط الصور (المراقبة الإلكترونية) و التسرب الإلكتروني² ، و سوف نحاول التعرض إلى هذه الإجراءات عبر الفقرات الآتية مثلما هو موضح أدناه :

أولاً: اعتراض المراسلات و تسجيل و النقاط الصور (المراقبة الإلكترونية)

الاعتراض و التسجيل و الالتقاط هي مجموعة من المصطلحات يمكن اختزالها تحت مسمى واحد هو " المراقبة الإلكترونية "حيث هذه المراقبة تعتبر رقابة مشروعة تستهدف شخصاً أو مكاناً أو محادثات أو مراسلات مكتوبة أو مسموعة أو مرئية، وذلك نتيجة الاشتباه في تصرفات غير مشروعة و تتم هذه العملية بشكل سري بحيث لا يشعر الآخرون بوجودها نظراً للطابع السري الذي يميزها.³

1- اعتراض المراسلات :

" يقصد بمصطلح اعتراض في اللغة الفرنسية Interception و يعني الإطلاع على محتوى المحادثة أو الرسالة الموجهة لآخرين أثناء توصيلها ، ويقضي ذلك وجود جهة مرسله

¹ - يوسف صغير ، المرجع السابق ، ص 139 .

² - باقر غازي حنون الدراجي ، المرجع السابق ، ص 168 .

³ - فوزي عمارة ، اعتراض المراسلات و تسجيل الأصوات و النقاط الصور و التسرب كإجراءات تحقيق قضائي في المواد الجزائية ، مجلة العلوم الإنسانية ، عدد 33 ، 2010 ، ص236 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

و أخرى مستقبلية كما يجب أن تتم العملية سرا دون علم المعنيين و أن يتم الإطلاع على محتوى المرسل قبل وصوله وجهته و إلا عد ذلك تفتيش و ليس اعتراض¹.
أما مفهوم اعتراض المراسلات يقصد به : " عملية مراقبة سرية المراسلات السلكية و اللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة ، و تتم المراقبة عن طريق الاعتراض و التسجيل أو النسخ للمراسلات و التي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض "².

وبفضل التقدم الملحوظ في مجالات الاتصالات قد جاء نص المادة 114 الفقرة الثانية موسعا حيث لم يقتصر الاعتراض على المكالمات الهاتفية فحسب بل شمل أيضا جميع مختلف أنواع الاتصالات السلكية و اللاسلكية³، و هذا ما سعى إليه المشرع الجزائري من خلال أحكام القانون 04-09 السالف الذكر حيث منح المشرع الحق في وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية ، بالإضافة إلى إمكانية إجراء التفتيش و الحجز داخل المنظومة المعلوماتية و ذلك بموجب إذن من السلطة القضائية⁴.

2- تسجيل الأصوات و النقاط الصور :

يعرف تسجيل الأصوات و النقاط الصور بأنه : " تسجيل المحادثات الشفوية يتحدث بها الأشخاص بصفة سرية أو خاصة و في مكان عام أو خاص و كذلك النقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص "⁵.

¹ - الطاهر ياكور ، المرجع السابق ، ص 106 .

² - محمد شنه ، إجراءات البحث و التحري عن الجرائم في التشريع الجزائري ، ط01 ، ألفا للوثائق للنشر و التوزيع ، عمان الأردن ، 2024 ، ص109 .

³ - فوزي عمارة ، المرجع السابق ، ص237 .

⁴ - جميلة محلق ، اعتراض المراسلات ، تسجيل الأصوات و النقاط الصور في قانون الإجراءات الجزائية الجزائري ، مجلة التواصل في الإقتصاد و الإدارة و القانون ، عدد 42 ، 2015 ، ص178 .

⁵ - محمد شنه ، المرجع السابق ، ص 112 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

فيما يتعلق بتسجيل الأصوات و التقاط الصور ، نصت المادة 114 الفقرتان 5 و 6 على أنه يمكن لوكيل الجمهورية أو قاضي التحقيق إذا اقتضت الحاجة إلى البحث و التحري أو التحقيق في الجرائم المذكورة على سبيل الحصر في الفقرة الأولى من نفس المادة، أن يمنح الإذن لضباط الشرطة القضائية للقيام بشكل سري بتسجيل و توثيق و بث ما يقال من قبل الأشخاص المشتبه فيهم في الأماكن العامة أو الخاصة، بالإضافة إلى التقاط صورهم في تلك الأماكن الخاصة.¹

واستخلاصا لما تقدم تعد هذه الإجراءات من بين الأساليب الخاصة التي سمح بها المشرع الجزائري لضباط الشرطة القضائية في التعامل مع جرائم معينة و ذلك وفق شروط محددة منصوص عليها في المواد من 114 إلى 127 من ق.إ.ج.ج، كما أتاح أيضا المشرع استخدام هذه الأساليب بموجب قوانين خاصة عند إجراء البحث و التحري في جرائم أخرى منصوص عليها و معاقب عليها في هذه القوانين الخاصة على سبيل المثال الجرائم الماسة بالمعلومات و الوثائق الإدارية المنصوص و المعاقب عليها في الأمر رقم 21 - 09 المؤرخ في 8 يونيو 2021 المتعلق بحماية المعلومات و الوثائق الإدارية بمقتضى المادة 27 منه وجرائم عصابات الأحياء المنصوص و المعاقب عليها في الأمر رقم 20-03 المؤرخ في 30 أوت 2020 المتعلق بالوقاية من عصابات الأحياء و مكافحتها بمقتضى المادة 20 منه وغيرها من الجرائم.²

ثانيا : ضوابط المراقبة الإلكترونية

كأصل عام، لا يسمح بالتدخل في اعتراض المراسلات واستراق الأصوات أو تسجيلها أو التقاط الصور دون الحصول على موافقة مسبقة ممن يكون محلا لها، و مع ذلك فقد أتاح المشرع الجزائري لضباط الشرطة القضائية القيام بهذه العمليات عند الضرورة خلال التحقيقات

¹ - الطاهر ياكور ، المرجع السابق ، ص 108 .

² - محمد حزيط ، الوجيز في قانون الاجراءات الجزائية الجزائري قانون رقم 25-14 مؤرخ في 3 غشت 2025 ، ط 02 ، دار بلقيس للنشر و التوزيع ، الجزائر ، 2026 ، ص 244 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

الأولية أو القضائية و ذلك في الجرائم المحددة على سبيل الحصر في الفقرة الأولى من المادة 114 من ق.إ.ج.ج كما ذكرنا سابقا و حتى يمكن تحقيق التوازن بين المصلحة العامة في كشف الحقيقة و حماية الحق في الخصوصية وضع المشرع مجموعة من الضوابط أو الشروط التي يجب الالتزام بها و التي تتمثل أساساً في ما يلي :

1- قيد المشرع الجزائري إجراءات اعتراض المراسلات و تسجيل الأصوات و التقاط الصور في حالة التلبس أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر حسب ما أشارت إليه المادة 114 الفقرة 2 من ق.إ.ج.ج، و إذا تم اكتشاف جرائم أخرى أثناء إجراءات التحري الخاصة فإن ذلك لا يعتبر سببا لبطلان الإجراءات العارضة وفقاً لأحكام المادة 115 الفقرة 2. إن تحديد المشرع لفئة معينة من الجرائم يقيد من حرية السلطة القضائية في استخدام أساليب التحري الخاصة ، نظراً لصعوبة وصف الجريمة و تكييفها قبل انتهاء إجراءات التحقيق، مما قد يؤدي إلى إفلات العديد من الجرائم الخطيرة من العقاب.¹

2- جعل المشرع الجزائري بموجب المادة 114 الفقرة 5 و 6 من ق.إ.ج.ج الإختصاص بالإذن بإجراء هذه العمليات لوكيل الجمهورية المختص و في حالة فتح تحقيق قضائي تتم العمليات المذكورة بناءً على إذن من قاضي التحقيق و تحت مراقبته المباشرة². كما يجوز لوكيل الجمهورية أو قاضي التحقيق المختص بناءً على المادة 114 أن يأذن لضابط الشرطة القضائية باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية ، و وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

و يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 78 من هذا القانون وبغير علم أو رضا الأشخاص

¹ - جميلة محلق ، المرجع السابق ، ص 179 .

² - المادة 5/114 و 6 من القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

الذين لهم حق على تلك الأماكن . غير أن العمليات المحددة في المادة 114 أعلاه يراعى فيها عدم المساس بالسّر المهني المنصوص عليه في المادة 76 من ذات القانون.¹

و تستوجب المادة 116 من ق.إ.ج.ج في الإذن الشروط التالية :

أ- يجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الإتصالات المطلوب التقاطها و الأماكن المقصودة ، سكنية أو غيرها و الجريمة التي تبرر اللجوء إلى التدابير و مدتها .

ب- يجب أن يسلم الإذن مكتوباً لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق القضائي ضمن نفس الشروط الشكلية و الزمنية.²

3- إستوجب المشرع الجزائري في المادة 118 أن يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض و تسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية و عمليات الإلتقاط و التثبيت و التسجيل الصوتي أو السمعي البصري، و يذكر بالمحضر أيضا تاريخ و ساعة بداية هذه العمليات و الإنهاء منها . كما أوجب عليه في المادة 119 أن يصف أو ينسخ المرسلات أو الصور أو المحادثات المسجلة و المفيدة في إظهار الحقيقة في محضر يودع بالملف، و ترفق به الدعامة الالكترونية إذا طلبها وكيل الجمهورية، كما تنسخ و تترجم المكالمات التي تتم باللغة الأجنبية عند الإقتضاء بمساعدة مترجم يسخر لهذا الغرض.³

ثالثا: التسرب الإلكتروني

أشار المشرع الجزائري إلى التسرب الإلكتروني بمقتضى القانون رقم 20-05 المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها في نص المادة 26 منه حيث نصت على أنه: " يمكن لوكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن، تحت

¹ - المادتين 114 / 2 و 3 و 4 و 115 / 1 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية.

² - المادة 116 من نفس القانون.

³ - المادتين 118 و 119 من نفس القانون .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

رقابته، لضابط الشرطة القضائية، بالتسرب الإلكتروني إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بايهاهم أنه فاعل معهم أو شريك لهم.¹ وبالرجوع إلى نص المادة 16 من القانون رقم 15-20 المتعلق بالوقاية من اختطاف الأشخاص و مكافحتها نجد أن المشرع الجزائري أعطى تعريف متطابق للتعريف الذي تبناه بموجب القانون رقم 05-20 المذكور أعلاه.²

وتأصيلاً لما سبق يعرف التسرب الإلكتروني على أنه: "هو التوغل إلى منظومة معلوماتية أو نظام الاتصالات الإلكترونية باستعمال اسم مستعار بقصد مراقبة الأشخاص المشتبه في ارتكابهم لجريمة من الجرائم عن طريق التواصل معهم و القيام ببعض الأعمال لايهاهم أنه فاعل معهم أو شريك لهم قصد الحصول على أدلة ضدهم".³

أما التسرب المادي عرفه المشرع الجزائري طبقاً للمادة 121 من ق.إ.ج.ج على أنه: "قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنائية أو جنحة بايهاهم أنه فاعل معهم أو شريك أو خاف".⁴

وفي هذا المقام، نلاحظ من خلال التعريفات المعروضة أن المشرع الجزائري قد اكتفى بذكر صورتين فقط للمتسرب حيث يمكن أن يكون هذا الأخير فاعلاً أصلياً أو شريكاً في الجريمة و لم يتطرق المشرع إلى الصورة الثالثة للمتسرب كخاف و الأمر هنا يتعلق بالتسرب الإلكتروني، أما بالنسبة للتسرب المادي الذي تم الإشارة إليه في نص المادة 121 من القانون

¹ - راجع المادة 22 من القانون رقم 05-20 المؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 25، الصادرة في 29 أبريل 2020.

² - راجع المادة 16 من القانون رقم 15-20 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، يتعلق بالوقاية من جرائم اختطاف الأشخاص و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 81، الصادرة في 30

ديسمبر سنة 2020.

³ - محمد حزيط، المرجع السابق، ص 250.

⁴ - المادة 121 من القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

رقم 25-14 السالف ذكره فإن المتسرب يمكن أن يتخذ ثلاثة صور إما أن يكون فاعلاً أصلياً أو شريكاً في الجريمة أو خاف.¹

إلى جانب ذلك يتميز التسرب الإلكتروني عن المراقبة الالكترونية بأنه يتجاوز حدود المراقبة حيث يتفاعل و يتواصل مع المشتبه بهم، بينما يقتصر دور الضابط في المراقبة الالكترونية على المراقبة فقط و النقاط الاتصالات الالكترونية و توثيقها في الوقت المناسب، كما أن المراقبة الإلكترونية تعتبر إجراءً وقائياً في حين أن التسرب الإلكتروني يجمع بين الوقاية والردع إذ يستخدم لجمع الأدلة و إفشال خطط المشتبه بهم الإجرامية قبل تنفيذها. بالإضافة إلى ذلك، يعتمد عليه أيضاً في جمع الأدلة و ضبط المشتبه بهم و تحديد هويتهم و معاقبتهم بعد ارتكاب الجرائم.²

وفي ضوء ذلك نجد أن المشرع الجزائري قد نص بشكل صريح على نطاق تطبيق التسرب الإلكتروني و الولوج إلى الأنظمة المعلوماتية أو نظم الاتصالات الالكترونية حيث قصر هذا النطاق على جرائم التمييز و خطاب الكراهية بالإضافة إلى الجرائم المتعلقة باختطاف الأشخاص، كما أشار إلى بعض الجرائم الخطيرة التي حددها في سياق تعريفه لمجال التسرب المادي و ذلك وفقاً لما ورد في المادة 120 التي أحالتنا إلى المادة 114 من القانون رقم 25-14 السالف ذكره حيث تم تحديد نطاق اللجوء إلى التسرب في مجموعة من الجرائم الخطيرة، بما في ذلك الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال، و نرى أن هذا النوع من الجرائم هو الأكثر ملائمة لتطبيق التسرب الإلكتروني نظراً لتوافقه مع طبيعة الاجراءات التي تتعلق بالعالم الافتراضي بدلاً من العالم المادي.³

¹ - سارة قريمس، التسرب الإلكتروني كآلية إجرائية مستحدثة للتحري و التحقيق الجنائي الرقمي على ضوء التشريع الجزائري، المجلد 09، العدد 02، 2025، ص 1237.

² - كريمة تاجر، التسرب الإلكتروني كآلية لمكافحة الجريمة الإلكترونية (دراسة مقارنة بين القانون الجزائري و الفرنسي)، المجلة النقدية للقانون و العلوم السياسية، المجلد 19، العدد 02، 2024، ص 480.

³ - سارة قريمس، المرجع السابق، ص 1243.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

و يمكن تجسيد عملية التسرب الإلكتروني في جريمة الابتزاز الإلكتروني من خلال مشاركة الشخص المعني في محادثات غرفة الدردشة أو الانضمام إلى مجموعاتهم الخاصة، ويتم ذلك عبر استخدام المتسرب لأسماء مستعارة مما يتيح له الظهور بمظهر طبيعي و كأنه أحد الجناة مثلهم محاولاً الاستفادة من معرفتهم و خبراتهم حول كيفية الايقاع بضحايا الابتزاز، أو كيفية اختراق الهاكرز لمواقع معينة و سحب محتوى الابتزاز منها، أو الدخول مباشرة للحديث عن عمليات الابتزاز التي قاموا بها بهدف اكتشاف و ضبط الجرائم سواء التي تمت بالفعل أو التي لاتزال في مرحلة التخطيط.¹

و لقد وضع المشرع الجزائري مجموعة من الشروط لتنظيم عملية التسرب الإلكتروني كما أوجب الإلتزام بها و إلا كانت هذه العملية باطلة، و قد قسم الفقه هذه الشروط إلى شكلية وموضوعية و تتلخص الأولى فيما يلي:

1- استصدار إذن مكتوب بعملية التسرب الإلكتروني:

يتعين على المشرع الجزائري أن يلزم ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب بالحصول على إذن قضائي مسبق من وكيل الجمهورية المختص إقليمياً أو من قاضي التحقيق، و ذلك بعد إبلاغ وكيل الجمهورية و يأتي هذا الاجراء كضمانة لشرعية عملية التسرب و حتى يتجنب استخدامه بشكل يضر بحقوق الآخرين، و هو ما نصت عليه المادة 120 و أكدته المادة 124 من القانون رقم 25-14 السالف الذكر²، على أن يكون الإذن مكتوب و مسبب و ذلك تحت طائلة البطلان و تذكر فيه الجريمة التي تبرر اللجوء إلى هذا الاجراء و هوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته.³

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص 176.

² - سارة قريمس، المرجع السابق، ص 1241.

³ - المادة 124 / 1 و 2 من القانون رقم 25-14 المتضمن قانون الاجراءات الجزائية.

2- تحرير تقرير حول عملية التسرب الإلكتروني:

يجب أن يحزر ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب تقريراً مسبقاً يتضمن العناصر الضرورية لمعينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط أو العون المتسرب و كذا الأشخاص المسخرين حسب ما أشارت إليه المادة 122 من ق.إ.ج.ج.¹

وهنا يطرح التساؤل حول الطبيعة القانونية للفعل الذي قام به المتسرب، وذلك بعد إثبات مسؤولية المجموعة التي تسرب إليها؟

قام المشرع الجزائري بالإجابة عن هذا التساؤل في المادة 127 من ق.إ.ج.ج. لسنة 2025، إذ نص فيها على أن: "يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهداً عن العملية".²

و يستفاد من هذا النص أن المشرع قد أوجب أن تتم مراحل عملية التسرب تحت مسؤولية الضابط المكلف بها، بل و ذهب إلى أبعد من ذلك بإجازته الاستماع إلى الضباط المكلفين بالعملية كشهود دون غيرهم لأنهم يتحملون المسؤولية الأولى عن كل ما حدث أثناء تنفيذ عملية التسرب، حتى و إن كان من قام بالتسرب هو ضابط آخر أو عون.³

كما أجاز المشرع الجزائري، بعد إتمام عملية التسرب بأن تودع الرخصة في ملف الاجراءات الخاص بضابط الشرطة القضائية المعني بتنسيق عملية التسرب، و ذلك وفقاً لما ورد في المادة 6/126 من ق.إ.ج.ج.⁴

¹ - المادة 122 من من القانون رقم 25-14 المتضمن قانون الاجراءات الجزائية.

² - باقر غازي حنون الدراجي، المرجع السابق، ص 176.

³ - سارة قريمس، المرجع السابق، ص 1243.

⁴ - المرجع نفسه، ص 1242.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

3- مدة عملية التسرب الإلكتروني:

وفقاً لنص المادة 124 من ق.إ.ج.ج.ج تم تحديد المدة الزمنية لعملية التسرب التي يسمح بالعمل فيها بناءً على إذن كتابي صادر عن وكيل الجمهورية في مرحلة التحريات الأولية أو من قبل قاضي التحقيق في مرحلة التحقيق الابتدائي تنفيذاً لإنابة قضائية، بعد إخطار وكيل الجمهورية قانونياً بفترة لا تتجاوز أربعة أشهر كحد أقصى، مع إمكانية تجديد العملية وفقاً لمتطلبات التحري و التحقيق مع الالتزام بنفس الشروط الشروط الشكلية و الزمنية.¹

كما منح القانون للقاضي الذي رخص بإجراء التسرب السلطة لإصدار أمر بوقف العملية قبل انتهاء المدة المصرح بها، و مع ذلك في حالة اتخاذ هذا الاجراء يسمح للعون المتسرب بمواصلة نشاطاته لفترة كافية حتى يتم وقف عملية المراقبة، وهو نفس الاجراء الذي أقره القانون في حالة انتهاء مدة الترخيص و عدم تجديدها، و ذلك لحماية سلامة العنصر المتسرب و توفير الظروف المناسبة له للتوقف عن هذا النشاط دون أن يتحمل مسؤولية جزائية، شريطة ألا تتجاوز هذه الفترة أربعة أشهر كحد أقصى و إذا انقضت هذه المهلة دون أن يتمكن العون المتسرب من إنهاء نشاطه في ظروف تضمن أمنه، كما يمكن للقاضي أن يرخص بتمديد هذه الفترة إضافية لا تتجاوز أربعة أشهر.²

أما بالنسبة للشروط الموضوعية فإنها تتمثل كالاتي:

1- الأعمال التي يأذن القانون الجزائري للمتسرب القيام بها:

أعفى المشرع الجزائري ضباط و أعوان الشرطة القضائية المرخص لهم بأجراء عملية التسرب و كذا الأشخاص الذين يتم تسخيرهم من المسؤولية الجزائية عند قيامهم بالأفعال التالية:

- حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها.

¹ - المادة 3/124 و 5 من القانون رقم 25-14 المتضمن قانون الاجراءات الجزائية.

² - المادة 1/126 و 2 من نفس القانون.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- اقتناء أو من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الايواء أو الحفظ أو الاتصال.¹
- و لتوضيح ذلك نشير في هذا الخصوص بأن المشرع الجزائري قد أعفى أعوان و ضباط الشرطة القضائية و المسخرين لعملية التسرب الإلكتروني من المسؤولية الجزائية تسهила للعملية و إنجاحها حيث أخرج هذه الأفعال من دائرة التجريم إلى دائرة الأفعال المبررة الغير المعاقب عليها و هذا ماورد في نص المادة 39 من ق.ع.ج.²

1- أن تتم عملية التسرب الإلكتروني تحت رقابة وكيل الجمهورية أو قاضي التحقيق:

إذا كانت عملية التسرب الإلكتروني تتم تحت إشراف ضابط الشرطة القضائية المكلف بتنسيق العملية، فإن هذه العملية برمتها تخضع لرقابة وكيل الجمهورية أو قاضي التحقيق كما هو منصوص عليه في المادة 120 من ق.إ.ج.ج. و قد أكدت ذلك المادتان 26 من القانون 05-20 المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها و المادة 16 من القانون رقم 15-20 المتعلق بالوقاية من جرائم اختطاف الأشخاص و مكافحتها، و بالتالي لا يجوز اتخاذ أي خطوة تتعلق بعملية التسرب دون علم و موافقة وكيل الجمهورية أو قاضي التحقيق.³

و عند الرجوع إلى نص المادة 125 من القانون رقم 14-25 السالف ذكره، يتبين أن المشرع الجزائري قد قام بتجريم و فرض عقوبات صارمة على من يقوم بكشف هوية ضباط أو أعوان الشرطة القضائية فيعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات و بغرامة من 200.000 دج إلى 500.000 دج.

¹ - المادة 123 من القانون رقم 14-25 المتضمن قانون الاجراءات الجزائية.

² - راجع المادة 39 من الأمر رقم 156-66 المتضمن قانون العقوبات المعدل و المتمم.

³ - سارة قريمس، المرجع السابق، ص - ص 1243-1244.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

و تشدد العقوبة في حالة تسبب الكشف عن الهوية في أعمال عنف أو ضرب و جرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس (5) إلى عشر (10) سنوات و الغرامة من 500.000 دج إلى 1000.000 دج. أما إذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص تشدد العقوبة أكثر لتصبح تتراوح ما بين الحبس من عشر (10) سنوات إلى عشرين (20) سنة و الغرامة من 1000.000 دج إلى 2000.000 دج دون الإخلال عند الاقتضاء تطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.¹

المطلب الثاني : الإثبات في جريمة الابتزاز الإلكتروني

يكتسب موضوع الإثبات مكانة بارزة و أهمية كبيرة في ميدان القانون الجنائي، حيث يرتبط بالجهود التي تبذلها الجهات المعنية قانونياً لكشف حقيقة الجريمة و ظروفها، كما أنه يساهم في توضيح الأمور أمام الهيئات القضائية التي لم تشهد وقوع الجريمة من خلال توفير معلومات حول الظروف المحيطة بها بناءً على نتائج التحريات و التحقيقات يمكن تحديد معالم الجريمة و مرتكبيها و الظروف المحيطة بها و بالتالي فإن الأدلة تلعب دوراً مهماً في إعادة تمثيل الجريمة التي تعتبر حدثاً من الماضي، مما يساعد على تقريب صورتها و كأنها وقعت في الحاضر.²

يقصد بالإثبات الجنائي " إقامة الدليل على وقوع الجريمة و من ثم نسبتها إلى المتهم بارتكاب الجريمة."³

بمجرد أن تبدأ إجراءات التحقيق بعد أن تتلقى الجهات المعنية بلاغاً عن وقوع جريمة ابتزاز إلكتروني ضد أحد الأفراد، تبدأ مرحلة البحث عن أدلة لإثبات تلك الجريمة، تعتبر

¹ - المادة 125 / 2 و 3 و 4 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية .

² - جمال دريسي، الإثبات الجنائي بالأدلة العلمية، المجلة النقدية للقانون و العلوم السياسية، المجلد 17، العدد 02، 2022 ، ص 420.

³ - أمير فرج يوسف، المرجع السابق، ص 97.

الجرائم الإلكترونية بشكل عام و جريمة الابتزاز الإلكتروني بشكل خاص من الجرائم التي يصعب إثباتها، حيث تواجه المحققين عدة عقبات و صعوبات في عملية الإثبات فتتجلى هذه الصعوبات في عدم توفر دليل مادي في معظم الأحيان، إذ غالباً ما تكون الأدلة الناتجة عنها رقمية مما يسهل محوها أو العبث بها، كما يمكن أن ترتكب هذه الجريمة عبر دول متعددة، حيث يقوم شخص في دولة معينة بابتزاز شخص آخر في دولة مختلفة، مما يستدعي ضرورة وجود تعاون دولي لمكافحة هذه الجريمة.

و من الجدير بالذكر أن أدلة جريمة الابتزاز الإلكتروني عادة ما تكون على شكل معلومات نصية أو صور أو مقاطع صوتية، و تعتبر هذه الأدلة سندات إلكترونية أو بيانات ثبوتية يمكن استخراجها رقمياً باستخدام بعض الأساليب الحديثة في الإثبات، ثم طباعتها على ورق أو حفظها على أقراص مدمجة أو عبر وسائل أخرى لتخزين الأدلة الرقمية بهدف الاستفادة منها في إثبات الجريمة.¹

و تفريعاً على ما تقدم ومن أجل الإحاطة بأغلب جوانب اثبات جريمة الابتزاز الإلكتروني سيتم تقسيم هذا المطلب على ثلاثة فروع، نتناول في الأول الدليل الجنائي الرقمي، في حين سيعنى الفرع الثاني ببيان معوقات الوصول إلى الدليل الرقمي، ثم نتطرق إلى معالجة الاشكالات التي يثيرها الدليل الرقمي في الفرع الثالث.

الفرع الأول : الدليل الجنائي الرقمي في جريمة الابتزاز الإلكتروني

يعد الدليل الرقمي نتاج من نتاجات التكنولوجيا الحديثة، و يعد من الناحية العملية وسيلة فعالة لا يمكن أن تخطيء في إثبات وقوع الجرائم المعلوماتية، فيمكن القول بأن الدليل الرقمي يمثل قرينة قاطعة على حدوث الجريمة المعلوماتية خاصة عند تكرار التجارب و ارتفاع دقتها

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص- ص 179 - 180.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

و مهارة الخبراء المعنيين، و مع ذلك يبقى في كثير من الأحيان محدوداً في قدرته على ربط الجريمة بشخص معين.¹

فما هو التعريف لهذا النوع المستحدث من الأدلة و خصائصه و ما هي تقسيماته؟ وما موقف المشرع الجزائري من قبول الدليل الرقمي في جريمة الابتزاز الإلكتروني؟.

أولاً : مفهوم الدليل الرقمي

تعرف الأدلة الرقمية بأنها " المعلومات التي يمكن قبولها منطقاً و عقلاً، و التي تعتمد عليها النظريات العلمية المحكمة يتم الحصول عليها من خلال اجراءات علمية و قانونية دقيقة تشمل ترجمة البيانات و المعلومات المخزنة في أجهزة الحاسوب، و كذلك في ملحقاتها وشبكات الاتصال، و تعد هذه الأدلة قابلة للاستخدام في مختلف مراحل التحقيق و المحاكمة لاثبات الوقائع أو الأشخاص المرتبطين بالجريمة، بما يساهم في الوصول إلى الحقيقة القانونية على نحو دقيق و موثوق."²

و تعرف أيضاً بأنها " الأدلة المأخوذة من أجهزة الكمبيوتر أو أي جهاز إلكتروني آخر ترتكب من خلال جريمة الابتزاز الإلكتروني، و تكون في شكل نبضات أو مجالات مغناطيسية، ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيات خاصة، وهي مكون رقمي لتقديم معلومات و بيانات بأشكال متنوعة كالنصوص المكتوبة، والصور، والأصوات، ومقاطع الفيديو، والرسوم و الأشكال، وذلك من أجل تقديمها و اعتمادها أمام أجهزة انفاذ وتطبيق القانون."³

و في هذا المقام، لم تتضمن التشريعات المقارنة بما في ذلك التشريع الجزائري تعريفاً للدليل الرقمي، إذ إن تحديد التعريف ليس من اختصاص المشرع و هو أمر يعتبر نهجاً طبيعياً

¹ - عبد القادر عمير، التحديات القانونية لإثبات الجريمة لنشر الجامعي الجديد، تلمسان- الجزائر، 2021، ص 103.

² - سليم درابلة العمري، حجية الدليل الرقمي في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة دكتوراه، تخصص القانون الجنائي و العلوم الجنائية، جامعة الجزائر 01، 2025/2024، ص 29.

³ - باقر غازي حنون الدراجي، المرجع السابق، ص- ص 181 -182.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

خاصة بالنظر إلى الخصائص الفريدة التي يتمتع بها الدليل الرقمي، مما يجعل محاولة تعريفه مغامرة قد تترتب عليها آثار سلبية متعددة في الممارسة العملية.

و علاوة على ذلك، لم يشر المشرع الجزائري إلى هذا المصطلح في أي من النصوص القانونية ذات الصلة، سواء في قانون العقوبات أو في القانون رقم 04-09 الذي يتضمن القواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام و الاتصال و مكافحتها، أو في المرسوم رقم 21-439 المتعلق بالهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال.¹

و نظراً لظهور الدليل الرقمي في بيئة افتراضية ديناميكية و متطورة، فقد أصبح هذا الدليل يكتسب مميزات تقنية و فنية تميزه عن الدليل الجنائي التقليدي²، لذا سنقوم بتلخيص هذه المميزات على النحو التالي :

1- الطابع التقني للدليل الرقمي :

تتطلب الطبيعة العلمية للأدلة أن يتعامل معها تخصصون في الفضاء الافتراضي، فالتعقيد التقني يستدعي ضرورة وجود تناغم بين الأدلة المستخلصة والبيئة المحيطة بها، فالتكنولوجيا لا تقدم لنا أداة تقليدية مثل السكين للكشف عن الجاني بل تتيح لنا نبضات أو مجالات مغناطيسية أو كهربائية.³

2- الطابع العلمي للدليل الرقمي:

يتسم الدليل الرقمي بكونه دليلاً علمياً، إذ يتكون من بضات و معطيات إلكترونية غير ملموسة، يتم استخراجها من الطبيعة الإلكترونية ذات البنية العلمية، و ما ينطبق على الدليل العلمي ينطبق أيضاً على الدليل الرقمي، و بالتالي يخضع الدليل العلمي لقاعدة ضرورة تعبيره

¹ - عبد القادر عمير، المرجع السابق، ص 105 .

² - أكرم ديب، نورة بن بو عبد الله، المرجع السابق، ص 402 .

³ - أحمد بن مالك، ابراهيم الخال، دور الأدلة الرقمية في الاثبات الجنائي، مجلة العلوم الانسانية، المجلد 05، العدد 01 ،

2021، ص 109 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

عن الحقيقة الكاملة، وفقاً لمبدأ أن القانون يسعى لتحقيق العدالة، بينما يسعى العلم لتحقيق الحقيقة لذلك فإن للدليل الرقمي طبيعة مماثلة لتلك التي يتمتع بها الدليل العلمي.¹

3-الدليل الرقمي ذو طبيعة متطورة و متنوعة:

تتميز الأدلة الجنائية الرقمية بطبيعة يناميكية سريعة الحركة، حيث تنتقل من مكان إلى آخر عبر شبكات الاتصال، متجاوزة الحدود الزمنية و المكانية و تظهر ميزة التنوع في الأدلة الرقمية من خلال قدرتها على اتخاذ أشكال متعددة تحمل بيانات و معلومات قابلة للتداول². أما كونها أدلة متطورة فهي ميزة شبه تلقائية، نتيجة لارتباطها بالطبيعة الديناميكية لحركة الاتصال عبر الإنترنت و العالم الافتراضي، اللذين لم يبلغا بعد ذروتها القصوى من التطور، إذ لا يزالان في مرحلة البداية و لم يصلا إلى نهايتهما و بالتالي سيكون من الصعب احتواؤهما.³

ثانياً: تقسيمات الدليل الرقمي في جريمة الابتزاز الإلكتروني

لا يتجلى الدليل الرقمي الناتج عن جرائم الإنترنت في شكل واحد فحسب، بل يتنوع في أشكال و صور متعددة و قد قام البعض بتصنيفه إلى أربع تقسيمات هي:

- الأدلة الرقمية الخاصة بأجهزة الكمبيوتر و شبكاتها.
- الأدلة الرقمية الخاصة بالإنترنت.
- الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.
- الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات⁴.

كذلك قسم الدليل الرقمي في إطار تصنيفين رئيسيين، يتمثل التصنيف الأول في تصنيف الدليل الرقمي وفقاً لهيئته، حيث يتنوع إلى أدلة عرض مرئي و أدلة صوتية و مرئية و أخيراً الأدلة المكتوبة. أما التصنيف الثاني فيتعلق بقيمته الاستدلالية، حيث يمكن تقسيم الأدلة

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص 182 .

² - أكرم ديب، نورة بن بو عبد الله، المرجع السابق، ص 403 .

³ - باقر غازي حنون الدراجي، المرجع السابق، ص 183 .

⁴ - أمير فرج يوسف ، المرجع السابق، ص 172 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الرقمية من حيث قيمتها الاستدلالية إلى أدلة تم إعدادها لتكون وسيلة إثبات، و تشمل الأدلة التي تم إنشاؤها تلقائياً دون تدخل من الشخص مثل سجلات المكالمات و فواتير الأجهزة. أما النوع الثاني، فهو الأدلة التي لم تعد تعتبر وسيلة إثبات، و هي تلك التي نشأت دون إرادة الشخص و لكن بمساهمته، مما يجعلها مجرد آثار يتركها الجاني دون رغبة في وجودها، و تعرف بالبصمة الرقمية أو الآثار الإلكترونية. هذه الآثار تتجلى في المخلفات التي يتركها مستخدم الأنترنت مثل المواقع التي تم تصفحها، و الملفات التي تم زيارتها، بالإضافة إلى رسائل البريد الإلكتروني، سواء كانت المرسلة أو المستلمة، الموجودة أو التي تم حذفها.¹

ثالثاً: موقف المشرع الجزائري من قبول الدليل الرقمي في جريمة الابتزاز الإلكتروني

يعد الدليل الرقمي من الوسائل الحديثة في مجال الإثبات، و يقصد بقبوله اعتراف المشرع به كوسيلة إثبات يمكن للقاضي الاستناد إليه في إصدار أحكامه و تكوين اقتناعه الشخصي، و يختلف هذا القبول باختلاف النظام القانوني المعتمد في الإثبات، ففي نظام الإثبات القانوني أو نظام الأدلة القانونية السائد في الدول الأنجلوسكسونية مثل إنجلترا و الولايات المتحدة الأمريكية و كندا و أستراليا لا يجوز للقاضي الاستناد إلى الدليل الرقمي ما لم يرد النص عليه صراحة ضمن وسائل الإثبات المحددة قانوناً. و على النقيض من ذلك، يقوم نظام حرية الإثبات المعتمد في العديد من الدول اللاتينية كفرنسا و ألمانيا و تركيا و اليونان و البرازيل على عدم تقييد القاضي بوسائل إثبات محددة على سبيل الحصر بل يمنحه سلطة تقديرية واسعة في تكوين اقتناعه الشخصي استناداً إلى أي دليل يراه مناسباً بما في ذلك الدليل الرقمي و يعد هذا الإتجاه هو الذي تبناه المشرع الجزائري.²

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص 184 .

² - عبد القادر عمير، المرجع السابق، ص 153.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

وهذا ما يستشف من خلال نص المادة 349 من ق.إ.ج.ج.ج بقولها: "يجوز إثبات الجرائم بأي طريق من طرق الإثبات، بما فيها الإلكترونية، ما عدا الأحوال التي ينص فيها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص. ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".¹

الفرع الثاني : المعوقات التي يثيرها الدليل الرقمي

إن الجرائم الإلكترونية لا تترك آثارا مادية تشير إلى مرتكبيها كما هو الحال في الجرائم التقليدية، حيث لا يوجد كسر أو دم أو أي من الآثار التقليدية المرتبطة بالجريمة، فالجريمة المعلوماتية تتمركز أنشطتها في فضاء افتراضي مما يجعل الأدلة الناتجة عنها ذات طبيعة خاصة و تختلف وسائل اكتشافها عن الوسائل التقليدية المستخدمة في الكشف و جمع الأدلة الجنائية². و تتمحور هذه المشكلات أساساً حول النقاط التالية:

أولاً: سهولة محو الدليل الرقمي

عادة ما يسعى الجناة في جرائم الابتزاز الإلكتروني إلى إخفاء أفعالهم و إزالة جميع آثارها من خلال التلاعب بقواعد البيانات في البرامج، دون أن يتركوا أي أثر للجريمة، و يزداد الأمر تعقيداً لأن عملية التخزين الإلكتروني غير مرئية، حيث تكتب البيانات بلغة رقمية غير ملموسة مما يتطلب عرضها على الشاشة لتمكين الأفراد من قراءتها و هذا يشكل عائقاً أمام إقامة الدليل على جريمة الابتزاز الإلكتروني.³

و في ضوء ذلك نجد أن المشرع الجزائري قد جرم الدخول إلى النظام أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات بموجب نص المادة 349 مكرر/2 حيث نصت

¹ - راجع المادة 349 من القانون رقم 25-14 المتضمن قانون الإجراءات الجزائية .

² - عبد القادر عمير، المرجع السابق، ص 118 .

³ - باقر غازي حنون الدراجي، المرجع السابق، ص 186 .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

على أنه: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة من 1000.000 دج، كل من يقوم عمدا و عن الغش بما يأتي:

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".¹

ثانيا: إعاقة الوصول إلى الدليل الرقمي

إن مرتكبي الجرائم المعلوماتية يتخذون تدابير لحماية أنفسهم، مما يعوق جهود أجهزة البحث و التحري في الوصول إلى الأدلة التي قد تدينهم، يتم ذلك من خلال استخدام تقنيات التشفير و كلمات المرور، بالإضافة إلى هويتهم أو انتحال شخصيات أخرى مما يجعل التعرف عليهم في حال اكتشاف الجريمة أمراً صعباً، هناك العديد من البرامج التي تتيح للمستخدمين إخفاء هويتهم أثناء إرسال الرسائل أو تصفح الإنترنت مما يجعل عملية استعادة الأدلة أو إعادة تشكيلها مهمة معقدة تتطلب خبرة و جهداً و وقتاً و أدوات دقيقة قد تكون غير متاحة في كثير من الأحيان للجهات المعنية بالتحقيق.²

ثالثا: ضعف التعاون بين الدول و اختلاف الأنظمة الاجرائية بينها

يلعب التنسيق و التعاون الدولي دوراً حيوياً في إثبات الجرائم الإلكترونية و الحد منها، خاصة في مجال جمع الأدلة الرقمية و تعقب المجرمين. و على النقيض من ذلك، فإن غياب سياسة فعالة للتنسيق و التعاون بين الدول في مكافحة الجرائم الإلكترونية يترافق مع تعاون ملحوظ بين محترفي الجريمة الإلكترونية، حيث يتبادل الجناة الخبرات و النصائح المتعلقة

¹ - راجع المادة 394 مكرر/2 من الأمر رقم 66-156 المتضمن قانون العقوبات المعدل و المتمم.

² - عبد القادر عمير، المرجع السابق، ص- ص 120 - 121 .

بأنشطتهم مما يزيد من فعالية تلك الأنشطة و يعزز من خطورتها في ظل قصور وعدم فعالية سياسات الدفاع المقررة ضد هذا النوع من الجرائم.

وعلى الرغم من تزايد المناشدات بضرورة تفعيل سياسة التعاون الدولي لمكافحة الجرائم الإلكترونية، إلا أن هناك العديد من المعوقات التي تحول دون تحقيق هذا التعاون، يأتي في مقدمتها اختلاف الأنظمة الإجرائية بين الدول، إذ إن تنوع الأنظمة القانونية الاجرائية بين الدول يعني أن طرق التحري التي أثبتت فعاليتها في دولة معينة قد تكون غير مجدية في دولة أخرى، أو قد لا يسمح بإجرائها أساساً على سبيل المثال، فإن إجراءات مثل التسرب الإلكتروني والمراقبة الإلكترونية و اعتراض المراسلات قد تعتبر قانونية في دولة ما، بينما تعد غير مشروعة في دولة أخرى. و بالتالي، فإن ذلك يفقد الدولة الأولى القدرة على جمع الأدلة وتطبيق قوانينها في الدولة الثانية باستخدام اجراءات تعتبر مشروعة و قانونية. علاوة على ذلك، قد ترفض الدولة الثانية قبول أي دليل تم جمعه بطرق أو اجراءات تعتبرها غير مشروعة، حتى وإن كان هذا الدليل قد تم استخلاصه بشكل قانوني في نطاق اختصاص قضائي للدولة التي قامت بجمعه.¹

رابعاً: نظم تشغيل أجهزة الكمبيوتر النشطة و النظم الساكنة

من المعروف أن عملية إيقاف تشغيل جهاز الكمبيوتر قد تؤدي إلى فقدان كمية ضئيلة من البيانات التي لا يمكن استعادتها، و ذلك في حالة عدم تخزينها في الذاكرة و مع ذلك، فإن ذلك لن يؤثر على سلامة الأدلة الموجودة بالفعل. و بالإضافة إلى ذلك، فإن انقطاع التيار الكهربائي المفاجيء عن جهاز الكمبيوتر ينطوي على العديد من المخاطر حيث يمكن أن يؤدي إلى محو المعلومات المخزنة في الذاكرة نتيجة إيقاف تشغيل الجهاز، مما يعني فقدان جميع العمليات النشطة، و الاتصالات الشبكية، و أنظمة الملفات الثابتة و فضلاً على ذلك، قد يؤدي

¹ - باقر غازي حنون الدراجي، المرجع السابق، ص- ص 187-188 .

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الإيقاف المفاجيء إلى تشويه بيانات هامة أو التسبب في أضرار للأجهزة مما يمنع نظام التشغيل من إعادة التحميل بشكل صحيح.¹

الفرع الثالث: معالجة الإشكالات المرتبطة بالدليل الرقمي في جريمة الابتزاز الإلكتروني

يمثل التعامل مع الإشكالات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني التي سبق الحديث عنها تحدياً معقداً، غير أن التطور المتسارع في مجال تكنولوجيات المعلومات والاتصال أتاح جملة من الآليات الكفيلة بمعالجتها بفعالية. وفي هذا السياق تبرز أهمية الاستعانة بالخبرة الفنية والتقنية، حيث أصبح من الضروري الاعتماد على مختصين في نظم المعلومات يمتلكون مهارات متقدمة في التحليل الرقمي وفك التشفير واسترجاع البيانات، بما يمكنهم من تتبع الآثار الرقمية والتحقق من سلامة الأدلة وأصالتها، فضلاً عن إعادة تركيبها في حال تعرضها للإتلاف، كما تلعب هذه الخبرة دوراً محورياً في استخدام أدوات التتبع وأنظمة كشف الاختراق لتحديد هوية الجناة. إلى جانب ذلك، يشكل تسخير التكنولوجيا الحديثة ركيزة أساسية في تعزيز فعالية أجهزة الضبط القضائي، من خلال تطوير برمجيات متخصصة لاستخلاص الأدلة الرقمية وتحليلها، مع الحرص على تحديثها المستمر لمواكبة تطور الأساليب الإجرامية، ويزداد هذا الدور أهمية مع إدماج تقنيات الذكاء الاصطناعي، التي تتيح إمكانيات متقدمة كالتعرف الآلي على الوجوه وتحليل الأصوات.²

¹ - أمير فرج يوسف، المرجع السابق، ص 186.

² - أكرم ديب، نورة بن بو عبد الله، المرجع السابق، ص 414 .

المبحث الثاني: مكافحة جريمة الابتزاز الإلكتروني على المستوى المؤسساتي الوطني

تعتبر الجرائم الإلكترونية من بين أكثر الجرائم التي تشكل هاجسًا يورق المواطن في حياته الشخصية، وكذلك الدول في سيادتها وأمنها ويعود ذلك إلى التطور التكنولوجي والرقمي الهائل وما نتج عنه من تأثيرات طالت جميع المستويات من جهة، ومن جهة أخرى باتت تداعيات هذه الثورة التكنولوجية تهدد خصوصية الأفراد و حقوقهم، مما دفع بالتشريعات المقارنة بما في ذلك التشريع الجزائري إلى العمل بجد على مكافحتها سعيًا نحو تحقيق الأمن السيبراني من خلال اتخاذ مجموعة من الآليات سواء من الجانب المؤسساتي أو الأمني للتصدي لهذه الجرائم بصورة عامة و جريمة الابتزاز الإلكتروني بصورة خاصة.¹

و إنطلاقًا من هذه المعطيات، و لغرض الوقوف على مكافحة جريمة الابتزاز الإلكتروني على المستوى المؤسساتي الوطني، فقد ارتأينا تقسيم هذا المبحث على مطلبين نوضح في الأول: دور المؤسسات الوطنية في مكافحة جريمة الابتزاز الإلكتروني ، ونبين في المطلب الثاني دور الضبطية القضائية في مجابهة الجرائم الإلكترونية.

المطلب الأول : دور المؤسسات الوطنية في مكافحة جريمة الابتزاز الإلكتروني

إلى جانب الآليات التشريعية أو القانونية التي أصدرتها الحكومة الجزائرية لمجابهة الجريمة الإلكترونية، توجد هناك أيضا آليات هيكلية أو مؤسساتية أنشأتها الحكومة لتعمل بالتوازي أو لتدعم الإطار القانوني القائم²، وعليه سنقوم بتسليط الضوء على أهم هذه الهيئات الوطنية الفاعلة.

¹ - نور الهدى قادري، الجريمة السيبرانية وآليات مكافحتها، مواجهة تحديات الأمن السيبراني، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 08، العدد 01، 2023، ص 329.

² - فاطمة خرشف، الآليات القانونية والمؤسساتية الخاصة بمكافحة الجريمة السيبرانية في الجزائر، مجلة سوسيلوجيا الجريمة للبحوث والدراسات في الظواهر الإجرامية، المجلد 04، العدد 02، 2023، ص 74.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

و تأسيسًا على ما تقدم، سنحاول في هذا المطلب بيان مدى دور المؤسسات الوطنية في مكافحة جريمة الابتزاز الإلكتروني من خلال ثلاثة فروع نتناول في الأول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، فيما نخصص الفرع الثاني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ثم سنتطرق بعدها إلى المنظومة الوطنية لأمن الأنشطة المعلوماتية في الفرع الثالث.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تعد الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إحدى أهم الآليات المؤسسية التي استحدثتها المشرع الجزائري لمواجهة التهديدات السيبرانية والجرائم الإلكترونية، والتي قد تم إنشاؤها بموجب القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالتحديد في نص المادة 13 منه التي تنص على أنه: " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحدد تشكيلة الهيئة و تنظيمها و كفاءات سيرها عن طريق التنظيم.¹

لكنه تدارك أمر تشكيلة الهيئة وتنظيمها و كفاءة سيرها للتنظيم الصادر بموجب المرسوم الرئاسي رقم 261/15 الملغى الخاص بإنشاء الهيئة، إلا أن هذا الكيان القانوني رغم أهميته البالغة لم يدخل حيز الوجود إلا بتاريخ 8 أكتوبر 2015، أي بعد أكثر من ست (6) سنوات من التنصيب عليه، الأمر الذي يعكس تماطلاً واضحاً في تنفيذ مقتضيات المادة 13 المشار إليها أعلاه.²

¹ - راجع المادة 13 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بتكنولوجيا الإعلام والاتصال ومكافحتها.

² - لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، د.ط، النشر الجامعي الجديد ، تلمسان -الجزائر، 2018، ص 80.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

والملاحظ أن الهيئة الوطنية طرأت عليها عدة تعديلات مست جوهر تشكيلها بعد تنصيبها لأول مرة بموجب المرسوم الرئاسي رقم 15-261، والذي ألغي بموجب المرسوم الرئاسي رقم 19-172 ، وأخيرا أعيد تنظيمها بموجب المرسوم الرئاسي رقم 21-439 1 الساري المفعول. كيف المرسوم الرئاسي رقم 21-439 الصادر بتاريخ 7 نوفمبر سنة 2021 الهيئة بسلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى رئيس الجمهورية ومقرها مدينة الجزائر العاصمة مع إمكانية نقلها إلى مكان آخر من التراب الوطني بموجب قرار من وزير الدفاع الوطني.²

من خلال استقراءنا للمرسومين الرئاسيين الملغيين يتبين أن المشرع الجزائري كان كيف الهيئة الوطنية في المرسوم الرئاسي رقم 15-261 بسلطة إدارية موضوعة تحت إشراف وزير العدل إلا أنه بعد صدور المرسوم الرئاسي رقم 19-172 يلاحظ أن المشرع الجزائري تراجع عن تكييف الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها من سلطة إدارية مستقلة لصالح مؤسسة عمومية كما تم تحويل تبعيتها من وزير العدل إلى وزارة الدفاع الوطني.

وهنا يبرز التساؤل المطروح كيف تم تشكيل الهيئة وكيف تم تنظيمها؟ وماهي المهام التي أوكلت لها في مجال مكافحة الجريمة الإلكترونية في ظل المرسوم الرئاسي رقم 21-439 ؟

¹ - المرسوم الرئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 86، الصادرة بتاريخ 11 نوفمبر 2021.

² - المادتين 02 و 03 من نفس المرسوم الرئاسي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

أولاً: تشكيل الهيئة الوطنية و تنظيمها:

تتكون الهيئة من مجلس توجيه و مديرية عامة، يوضعان تحت سلطة رئيس الجمهورية ويقدمان له عرضاً عن نشاطاتهما.¹

1- مجلس التوجيه :

يتألف مجلس التوجيه الأمين العام لرئاسة الجمهورية ويتشكل من الأعضاء الآتي ذكرهم:

- الأمين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج.
- الأمين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية.
- الأمين العام لوزارة العدل.
- الأمين العام لوزارة البريد والمواصلات السلكية واللاسلكية.
- قائد الدرك الوطني.
- المدير العام للأمن الداخلي.
- المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي.
- المدير العام للأمن الوطني.
- رئيس مصلحة الدفاع السبيرياني و مراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي.
- ممثل عن رئاسة الجمهورية يعينه رئيس الجمهورية.

ويتولى المدير العام للهيئة أمانة مجلس التوجيه.²

وقد نص المشرع على أن يجتمع مجلس التوجيه في دورة عادية مرة واحدة في السنة بناء على استدعاء من رئيسه، كما أنه يمكن أن يجتمع في دورة غير عادية كلما كان ذلك ضرورياً بناءً

¹ - المادة 05 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال ومكافحتها.

² - المادة 06 من نفس المرسوم الرئاسي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة¹، ويكلف مجلس التوجيه على الخصوص بما يأتي:

- توجيه عمل الهيئة والاشراف عليه ومراقبته.
- دراسة كل مسألة تخضع لمجال اختصاص الهيئة، والبت فيها، لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الالكترونية المنصوص عليها في المادة 4 من القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.
- المداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- دراسة مخطط عمل الهيئة و الموافقة عليه.
- القيام بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها و الأهداف المنشودة بدقة.
- اقتراح كل نشاط يتصل بالبحث و تقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- دراسة مشروع ميزانية الهيئة والموافقة عليه.
- المداولة حول مسائل التطوير و التعاون مع المؤسسات و الهيئات الوطنية و الأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- دراسة مشروع النظام الداخلي للهيئة و الموافقة عليه.
- تقديم كل اقتراح مفيد يتصل بمجال اختصاص الهيئة و إبداء رأيه في كل مسألة تتصل بمهامها.

¹ - المادة 08 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- دراسة التقرير السنوي لنشاطات الهيئة و الموافقة عليه¹.

2- المديرية العامة:

يدير المديرية العامة مدير عام بموجب مرسوم رئاسي، و تنهي مهامه حسب الأشكال نفسها، و تعد وظيفة المدير العام وظيفة عليا في الدولة.

ويسهر المدير العام على حسن سير الهيئة، ويتولى في هذا المجال:

- اقتراح عناصر لإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و السهر على تنفيذها.
- إعداد مشروع ميزانية الهيئة.
- اقتراح مخطط عمل الهيئة السهر على تنفيذه.
- تنشيط أعمال هياكل الهيئة وتنسيقها ومتابعتها و مراقبتها.
- تحضير اجتماعات مجلس توجيه الهيئة .
- تمثيل الهيئة لدى القضاء و في جميع أعمال الحياة المدنية .
- ممارسة السلطة السلمية على مستخدمي الهيئة .
- السهر على احترام قواعد حماية السر المهني في الهيئة .
- إعداد التقرير السنوي لنشاطات الهيئة ورفعها إلى رئيس الجمهورية.
- إعداد التقارير الدورية لنشاطات الهيئة ورفعها إلى رئيس مجلس التوجيه.
- إعداد مشروع النظام الداخلي للهيئة.
- المساهمة في تحسين المعايير القانونية في مجال اختصاصه.
- التوظيف على مستوى هياكل المديرية العامة.
- تعيين المستخدمين الذين لم تحدد كفاءات أخرى لتعيينهم.

¹ - المادة 07 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

و تجدر الإشارة إلى أن هناك مهام جديدة للمديرية العامة تم استحداثها بموجب المرسوم رقم 439-21 لم تكن موجودة في ظل المرسومين الملغيين و هما المرسوم الرئاسي رقم 261-15 و المرسوم الرئاسي رقم 19-172 ، وهي كالآتي:

- تمثيل الهيئة لدى السلطات الوطنية والدولية
- السهر على القيام بإجراءات التأهيل و أداء اليمين فيما يخص المستخدمين المعيّنين للهيئة.
- ضمان التسيير الإداري والمالي للهيئة.
- و يخطر المدير العام للهيئة رئيس الجمهورية فورا عن كل حادثة من شأنها المساس بأمن الدولة أو تلك المرتبطة بالأعمال الإرهابية أو التخريبية، كما يخطر أيضا رئيس أركان الجيش الشعبي عندما يتعلق الأمر بمسائل تخص الدفاع الوطني.¹
- و تضم المديرية العامة كل من :
- مديرية المراقبة الوقائية و اليقظة الإلكترونية.
- مديرية الإدارة و الوسائل.
- مديرية الدراسات و التلخيص.
- مصلحة للتعاون و اليقظة التكنولوجية.
- ملحقات جهوية.
- و تعد كل من وظائف مدير المراقبة الوقائية و اليقظة الإلكترونية و مدير الإدارة والوسائل و نواب المديرين ورئيس مصلحة الدراسات و التلخيص و رئيس مصلحة التعاون واليقظة التكنولوجية و رؤساء الملحقات الجهوية وظائف عليا في الدولة.

¹ - المادة 10 من المرسوم الرئاسي رقم 439-21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

بحيث يتم تعيينهم في هذه الوظائف بموجب مرسوم رئاسي بناء على اقتراح من المدير العام للهيئة، وتنتهي مهامهم حسب الأشكال نفسها .

كما يحدد التنظيم الداخلي لهيكل الهيئة بموجب قرار من المين العام لرئاسة الجمهورية بناء على اقتراح من المدير العام للهيئة.¹

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

تمارس الهيئة المهام المنوطة بها تحت رقابة السلطة القضائية، طبقت لأحكام قانون الإجراءات الجزائية والقانون رقم 09-04- المؤرخ في 14 شعبان الموافق 5 غشت سنة 2009 و المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و بهذه الصفة تكلف الهيئة على الخصوص بما يأتي:

- تحديد الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و وضعها حيز التنفيذ.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ضمان المراقبة الوقائية للاتصالات الالكترونية، تحت سلطة القاضي المختص، قصد الكشف عن الجرائم المتصلة بالعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة
- كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني، المراقبة الالكترونية عندما يتعلق الأمر بأمن الجيش، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول.

¹ المواد 11، 12، و 13 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- تجميع وتسجيل و حفظ المعطيات الرقمية للأنظمة المعلوماتية و تحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية.
- المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحسين المعايير القانونية في مجال اختصاصها.
- مساعدة السلطات القضائية والشرطة القضائية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ن عن طرق جمع المعلومات والتزويد بها و إنجاز الخبرات القضائية.
- تطوير التعاون مع المؤسسات و الهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية و تطوير تبادل المعلومات و التعاون على المستوى الدولي في مجال اختصاصها، وفقا لأحكام المادتين 17 و 18 من القانون 04-09 المذكور أعلاه.¹

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

لقد استحدث المشرع الجزائري بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالج المعطيات ذات الطابع الشخصي هيئة جديدة تدعى " السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي" كآلية لحماية الحق في الخصوصية وتعرف على أنها سلطة وطنية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي والإداري تنشأ من رئيس الجمهورية ويقع مقرها بالجزائر العاصمة، تعمل على حماية المعطيات ذات الطابع الشخصي. كما تم تزويد هذه السلطة بأمانة تنفيذية يديرها أمين تنفيذي بمساعدة مستخدمين بعد تأديتهم لنص اليمين المذكور في المادة 27 منه أمام مجلس قضاء الجزائر.

¹ - المادة 04 من المرسوم الرئاسي رقم 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

كما يلزمون بالمحافظة على سرية المعلومات التي يطلعون عليها أثناء أو بمناسبة ممارسة مهامهم¹، كما أيضا تزود السلطة بأقطاب جهوية تتكفل بمهام المراقبة والتدقيق على مستوى الهيئات و الأشخاص المعالجين للمعطيات ذات الطابع الشخصي.²

أولا: تشكيلتها

تتكون السلطة الوطنية من مجموعة من الأعضاء يتم اختيارهم حسب اختصاصهم القانوني و/أو التقني في مجال المعطيات ذات الطابع الشخصي، كما يمكن للسلطة أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أشغالها، وتحدد عضوية الرئيس والأعضاء لمدة 5 سنوات قابلة للتجديد، وتتشكل السلطة الوطنية من³:

- ثلاث (3) شخصيات من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية.
- ثلاث (3) قضاة يقترحهم المجلس الأعلى للقضاة من بين قضاة المحكمة العليا ومجلس الدولة.
- عضو عن كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية.
- ممثل (1) عن المجلس الوطني لحقوق الإنسان.
- ممثل (1) عن وزير الدفاع الوطني.

¹ - المادتين 22 و 27 من القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة في 10 يونيو 2018.

² - المادة 27 مكرر من القانون رقم 11-25 مؤرخ في 28 محرم 1447 الموافق 24 يوليو سنة 2025، يعدل ويتم القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادرة في 24 يونيو سنة 2025.

³ - المادة 23 من القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- ممثل(1) عن وزير الشؤون الخارجية.
 - ممثل(1) عن وزير المكلف بالداخلية.
 - ممثل(1) عن وزير العدل وحافظ الأختام.
 - ممثل(1) عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيا الرقمنة.
 - ممثل(1) عن الوزير المكلف بالصحة.
 - ممثل(1) عن وزير العمل والتشغيل والضمان الاجتماعي.
- ويلزم أعضاء السلطة الوطنية قبل تنصيبهم في وظائفهم تأدية اليمين أمام مجلس قضاء الجزائر في الصيغة الآتية: " أقسم بالله العظيم أن أؤدي مهمني كعضو في السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بكل استقلالية وحياد وشرف ونزاهة، وأن أحافظ على سرية المداولات ".¹

يتضح من خلال هذه التشكيلة تكاملها وحرص المشرع على التأكيد على ضرورة توافر شرط الاختصاص القانوني و التقني في مجال معالجة البيانات ذات الطابع الشخصي، وهذا يعكس مدى اهتمام المشرع بهذا الجهاز ودوره الحيوي في حماية البيانات الشخصية. وفي هذا المجال يمكن الاستفادة من خبرات الهيئات الدولية الرائدة مثل مجلس أوروبا الذي أنشأ لجنة من الخبراء في مجال حماية البيانات الشخصية والتي أصدرت مجموعة من الأدلة الإرشادية في مجالات متعددة لحماية البيانات خاصة تلك المتعلقة بالنشاطات الطبية والشرطة، الضمان الاجتماعي والبيانات الجنائية.² كما تجدر الإشارة أيضا إلى أن التشكيلة تتميز بطابع مختلط

¹ - المادة 24 من القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

² - عبد الهادي كحلوي، عبد الهادي بن زينة، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون رقم والعلوم السياسية، المجلد 07، العدد 02، 2021، ص 120.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

حيث تمثل السلطات الثلاث وهي التشريعية،القضائية والتنفيذية مما يعزز من كفاءة هذه السلطة ويزيد من فعاليتها.¹

ثانيا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تكلف السلطة الوطنية بالسهر على معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال أي على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة. و تتمثل مهامها في :

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين و المسؤولين عن المعالجة بحقوقهم وواجباتهم.
- تقديم الاستشارات للأشخاص و الكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.
- تلقي الاحتجاجات والطعون والشكاوي بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.
- تقديم أي اقتراح شأنه تبسيط و تحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.
- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون.

¹ - المهدي صدوق، محمد غريبي، فعالية دور السلطة الوطنية لحماية المعطيات الشخصية في البيئة الرقمية، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 07، العدد 02، 2023، ص 1543.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون.
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.
- وضع قواعد السلوك و الأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

و في إطار ممارسة السلطة الوطنية لمهامها تُخطر النائب العام فوراً في حالة معاناة وقائع تحتمل الوصف الجزائي، كما تقوم السلطة الوطنية بإعداد تقريراً سنوياً حول نشاطها و يرفع إلى رئيس الجمهورية.¹

يتوجب على رئيس و أعضاء السلطة الوطنية المحافظة على الطابع السري للمعطيات ذات الطابع الشخصي و المعلومات التي اطلعوا عليها بهذه الصفة و لو بعد انتهاء مهامهم، إلا في حالة وجود نص قانوني يقضي بخلاف ذلك.

كما منع المشرع على رئيس السلطة الوطنية و أعضائها امتلاك مصالح بصفة مباشرة أو غير مباشرة في أي مؤسسة تمارس نشاطاتها في مجال معالجة المعطيات ذات الطابع الشخصي.

كما يستفيد أيضا رئيس السلطة الوطنية و أعضائها من حماية الدولة ضد التهديدات أو الإهانات أو الاعتداءات من أي طبيعة كانت التي قد يتعرضون لها بسبب أو خلال تأديتهم مهامهم أو بمناسبتها.²

وتمسك السلطة الوطنية السجل الوطني لحماية المعطيات ذات الطابع الشخصي و تقيّد

فيه:

1- الملفات التي تكون السلطات العمومية مسؤولة عن معالجتها.

¹ - المادة 25 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

² - المادة 26 من نفس القانون.

- 2- الملفات التي يكون الخواص مسؤولين عن معالجتها.
 - 3- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية.
 - 4- التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها.
 - 5- المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في القانون.
- كما تعفى من التقييد في السجل الوطني الملفات التي يكون الغرض الوحيد من معالجتها مسك سجل موجه بموجب مقتضيات تشريعية أو تنظيمية.¹

الفرع الثالث: المنظومة الوطنية لأمن الأنظمة المعلوماتية

في ظل التطورات التكنولوجية المتسارعة، تبرز أهمية تحقيق أمن المعلومات والبيانات، حيث يسعى جميع المستفيدين من الخدمات الالكترونية سواء كانوا أفرادًا أو شركات إلى حماية معلوماتهم من جميع أنواع الاعتداءات خاصة في ظل تزايد الجرائم الالكترونية بمختلف أنواعها.²

و ذلك بناءً على أحكام المرسوم الرئاسي 05-20 لاسيما المادة الثالثة منه التي نصت على أنه: " تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، ما يأتي: مجلس وطني لأمن الأنظمة المعلوماتية، يدعى في طلب النص " المجلس " ويكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، و الموافقة عليها و توجيهها، وكالة لأمن الأنظمة المعلوماتية تدعى في طلب النص "الوكالة"، و تكلف بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

¹ - المادة 28 من القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

² - صونيا مقري، وليد بن لعامر، المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسسية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي 05-20، مجلة البحوث في العقود و قانون الأعمال، المجلد 10، العدد 02، 2025، ص 137.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

و لممارسة مهامه يتوفر المجلس، بالإضافة إلى الوكالة ، على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال.¹

لذا سنسعى من خلال هذا الفرع إلى توضيح مهام و تشكيلة كل من الهيئتين من خلال العنصرين المواليين.

أولاً: المجلس الوطني لأمن الأنظمة المعلوماتية

يعتبر المجلس الوطني لأمن الأنظمة المعلوماتية هيئة مستحدثة تم إنشاؤها على غرار هيئات التصديق الإلكتروني التي نص عليها القانون 04-15 المتعلق بالتوقيع والتصديق الإلكتروني.²

1- تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية:

يتألف تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية وزير الدفاع الوطني أو ممثله و يتكون من ممثل عن:

- رئاسة الجمهورية.
- الوزير الأول.
- الوزير المكلف بالشؤون الخارجية.
- الوزير المكلف بالداخلية.
- الوزير المكلف بالعدل.
- الوزير المكلف بالمالية.
- الوزير المكلف بالطاقة.
- الوزير المكلف بالاتصالات.

¹ المادة 03 من المرسوم الرئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، العدد 04، الصادر 26 جانفي 2020.

² فتية حزام، حماية الأنظمة الرقمية بين الآليات التقنية و اجهزة الحماية- قراءة في أحكام المرسوم الرئاسي 20-05، مجلة الحقوق والعلوم الانسانية، المجلد 13، العدد 03، 2020، ص 181.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- الوزير المكلف بالتعليم العالي.
- كما يمكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله.¹
- كما يتوفر المجلس على أمانة تقنية لأداء مهامه على أكمل وجه يسيرها أمين عام يعين طبقا لتنظيم المعمول به على مستوى وزارة الدفاع الوطني وتتهي مهامه حسب الأشكال نفسها، توضع تحت سلطة رئيس المجلس ويكلفها لقيام بعدة مهام كالآتي:
- إعداد مشروع النظام الداخلي للمجلس.
- التنسيق مع الوكالة.
- جمع الوثائق اللازمة لتحضير أشغال المجلس الوطني و استغلالها.
- جمع أي معلومة أو وثيقة ذات صلة بمهام المجلس، من الوكالة و من أي إدارة أو مؤسسة أو هيئة.
- كما تتولى الأمان التقنية للمجلس الوطني ما يأتي:
- أشغال الأمانة.
- حفظ الوثائق و الرشيف.
- تسيير الموارد البشرية والمادية.²
- 2- مهام المجلس الوطني لأمن الأنظمة المعلوماتية:
- يتولى المجلس في إطار إعداد الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتية:
- البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.
- دراسة مخطط عمل الوكالة و تقرير نشاطاتها و الموافقة عليهما.

¹ المادة 05 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² المواد 07 و 08 و 09 من نفس المرسوم الرئاسي.

- دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.
- الموافقة على اتفاقات التعاون و الاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على سياسة والتصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني.
- الموافقة على تصنيف الأنظمة المعلوماتية.
- اقتراح ملاءمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة.
- ويبدي المجلس رأياً مطابقاً في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.¹

3- سير المجلس الوطني لأمن الأنظمة المعلوماتية:

- يصادق المجلس الوطني لأمن الأنظمة المعلوماتية على نظامه الداخلي، بحيث يجتمع المجلس كلما دعت الضرورة إلى ذلك بناء على استدعاء من رئيسه كما يتولى رئيس المجلس إعداد جدول أعمال اجتماعات المجلس و يحدد تاريخها.
- ترسل الاستدعاءات و جدول الأعمال إلى الأعضاء قبل خمسة (5) أيام على الأقل من تاريخ الاجتماع، و في حالات الاستعجال، يمكن تبليغ جدول الأعمال خلال انعقاد الجلسة.
- وتتخذ قرارات المجلس بالأغلبية، وفي حال تساوي عدد الأصوات يكون صوت الرئيس مرجحاً. لذا تدون نتائج أشغال اجتماعات المجلس في محضر، كما تتوج أعمال المجلس حسب الحالة بقرارات و توصيات و آراء و تقارير.
- كما تفرد و تسجل الاعتمادات اللازمة لسير المجلس في ميزانية وزارة الدفاع الوطني.²

¹ - المادة 04 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - المواد من 11 إلى 16 من نفس المرسوم الرئاسي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

ثانيا: وكالة أمن الأنظمة المعلوماتية

تبنى المشرع الجزائري بموجب المرسوم الرئاسي رقم 05-20 وكالة أمن الأنظمة المعلوماتية و اعتبرها حسب نص المادة 17 منه مؤسسة عمومية ذات طابع إداري تتمتع الشخصية المعنوية والاستقلالية المالية يقع مقرها في مدينة الجزائر.¹

و ما تجدر الإشارة إليه في هذا الصدد أن المشرع التونسي كان الأسبق في إنشاء الوكالة الوطنية للسلامة المعلوماتية مقارنة مع المشرع الجزائري من خلال القانون الذي أصدره عام 2004 المتعلق بالسلامة المعلوماتية، حيث يهدف هذا القانون إلى تنظيم مجال السلامة المعلوماتية ووضع القواعد الأساسية لحماية الأنظمة المعلوماتية والشبكات وتعمل الوكالة تحت إشراف الوزارة المعنية بتكنولوجيا الاتصال، بينما يتم تنظيم إدارتها وطرق إدارتها بموجب أمر خاص.²

1- تنظيم وسير وكالة أمن الأنظمة المعلوماتية :

تدير الوكالة لجنة توجيه و تزود بلجنة علمية، كما يكلف بتسييرها مدير عام وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية و مديريات ومصالح تقنية و إدارية موضوعة تحت سلطته.³

أ- تشكيلة لجنة التوجيه:

تتشكل لجنة التوجيه من رئيس يعين طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وتتكون لجنة التوجيه من ممثلي: وزارة الدفاع الوطني - الوزارة المكلفة بالشؤون الخارجية - الوزارة المكلفة بالداخلية-الوزارة المكلفة بالعدل- الوزارة المكلفة بالمالية - الوزارة المكلفة بالطاقة- الوزارة المكلفة بالتعليم العالي - الوزارة المكلفة بالصناعة - الوزارة المكلفة بالاتصالات - الوزارة المكلفة بالتجارة-مصالح الأمن - سلطة ضبط البريد و الاتصالات الإلكترونية - السلطة الوطنية للتصديق الإلكتروني - الهيئة الوطنية لحماية البيانات ذات

¹ - المادة 17 من المرسوم الرئاسي رقم 05-20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - صونيا مقري، وليد بن عامر، ص 139.

³ - المادة 20 من المرسوم الرئاسي رقم 05-20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

الطابع الشخصي - السلطة الحكومية للتصديق الإلكتروني و المدير العام للوكالة على سبيل الاستشارة .

أما مصالح الوكالة تتولاها أمانة لجنة التوجيه بحيث يمكن أن تستعين لجنة التوجيه بأي شخص أو مؤسسة من شأنها تنويرها في أعمالها.¹

ويتم تحديد القائمة الإسمية لأعضاء لجنة التوجيه بموجب قرار من وزير الدفاع الوطني بناء على اقتراح السلطات التي ينتمون إليها، و في حالة غيابهم لا يمكن للأعضاء انتداب من يمثلهم.²

ب- مهام لجنة التوجيه:

تكلف لجنة التوجيه، على الخصوص بالمهام الآتية :

- دراسة و اقتراح عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.
- دراسة البرامج السنوية و المتعددة السنوات لتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، و المصادقة عليها .
- تقييم نتائج مجموع الأعمال التي قامت بها الوكالة.
- تحديد الطرق و الوسائل اللازمة للاستجابة للحاجات الوطنية في مجال أمن الأنظمة المعلوماتية .
- ضبط الطرق و الوسائل اللازمة لترقية البحث و التطوير في مجال أمن الأنظمة المعلوماتية و التطبيقات ذات الصلة بالاحتياجات الوطنية.
- التداول في كل المسائل التي تتعلق بتنظيم وسير الوكالة، و لاسيما منها حصائل الأنشطة و التسيير المالي للسنة المالية المنصرمة و البيانات التقديرية للإيرادات و النفقات و مخطط توظيف و تكوين المستخدمين و كذا مرتبات مستخدمي الوكالة.

¹ - المادتين 21 و 22 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - المادة 23 من نفس المرسوم الرئاسي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

- الموافقة على النظام الداخلي للوكالة.¹

ج- سير لجنة التوجيه:

تجتمع لجنة التوجيه في دورة عادية أربع مرات في السنة بناء على استدعاء من رئيسها و يمكنها أن تجتمع في دورة غير عادية كلما دعت الضرورة إلى ذلك حسب الكيفيات التي يسطرها النظام الداخلي.

كما تقوم لجنة باعداد نظامها الداخلي و تصادق عليه في دورتها الأولى كما أيضا تدون نتائج أعمالها في محضر و يرسل في شكل تقرير إلى وزير الدفاع الوطني.²

2- المدير العام لوكالة أمن الأنظمة المعلوماتية:

يعين المدير العام للوكالة طبقا للتنظيم المعمول به في وزارة الدفاع الوطني و تنهى مهامه حسب الأشكال نفسها.

أما فيما يتعلق بمهام المدير العام لوكالة أمن الأنظمة المعلوماتية فهو يسهر على تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية و ينفذ المخططات و البرامج المسطرة من طرف لجنة التوجيه.

كما أنه مسؤول على سير الوكالة، و يتولى تسييرها ضمن احترام التشريع و التنظيم المعمول بهما بهذه الصفة :

- يعد مخطط عمل و برامج نشاط الوكالة و يعرضها على لجنة التوجيه للموافقة عليها.
- يحضر مشروع الميزانية التقديرية و يعرضه على لجنة التوجيه للمداولة و يتولى تنفيذ ذلك.
- يبرم الصفقات و يوقع العقود و الاتفاقيات و الانفاقات ذات الصلة بمهام الوكالة طبقا للتنظيم المعمول به.
- يتصرف باسم الوكالة و يمثلها أمام الهيئات القضائية.
- يمارس السلطة السلمية على جميع مستخدمي الوكالة.

¹ - المادة 24 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - المادتين 25 و 26 من نفس المرسوم الرئاسي.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

يعد النظام الداخلي للوكالة.

- يسهر على القيام بإجراءات تأهيل مستخدمي الوكالة.
- هو الأمر بصرف ميزانية الوكالة.
- يعد المدير العام للوكالة تقريراً سنوياً عن نشاطات الوكالة، و يرسله إلى رئيس المجلس.¹

3- اللجنة العلمية للوكالة:

إلى جانب لجنة التوجيه و المدير العام لوكالة أمن الأنظمة المعلوماتية تم استحداث بموجب المرسوم الرئاسي 20-05 اللجنة العلمية التي تتكون من عشرة (10) أعضاء يتم إختيارهم لمدة ثلاث سنوات (03) قابلة للتجديد، من قبل لجنة التوجيه من بين الأساتذة والباحثين و الخبراء في مجال أمن الأنظمة المعلوماتية، بحيث ينتخب رئيس اللجنة العلمية من طرف زملائه الأعضاء، كما تتولى مصالح الوكالة أمانة اللجنة العلمية.²

أما مهام اللجنة العلمية فهي ذات طابع استشاري، حيث يستشير المدير العام للجنة العلمية في كل مسألة ذات طابع علمي تتدرج ضمن إطار مهام الوكالة المتعلقة بنشاطات البحث و التطوير في مجال أمن الأنظمة المعلوماتية.

وتبدي اللجنة رأيها و توصياتها فيما يأتي :

-تجانب البرامج والمشاريع المقترحة من المدير العام للوكالة، كفاءات تنفيذ برامج ومشاريع البحث والتطوير، اختيار و اقتناء المراجع العلمية ، التنظيم والمشاركة في الأحداث والتظاهرات العلمية المتعلقة بأمن الأنظمة المعلوماتية، نشاطات التكوين العلمي والإتقان و إعادة التأهيل لفائدة مستخدمي الوكالة، وكذا المستخدمين المكلفين بأمن الأنظمة المعلوماتية في الإدارات والمؤسسات والهيئات العمومية، كل المسائل ذات الطابع العلمي التي يعرضها عليها المدير العام للوكالة.

-كما تصادق اللجنة العلمية على نظامها الداخلي خلال دورتها الأولى .

¹ - المادة 28 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - المادة 31 من نفس المرسوم الرئاسي .

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

وفضلا عن ذلك، يمكن للجنة العلمية الاستعانة بأي شخصية علمية أو خبير بإمكانه المساهمة مساهمة مفيدة نظرا لكفاءاته في مجال أمن الأنظمة المعلوماتية.¹

ثالثا: مهام وكالة أمن الأنظمة المعلوماتية

- كلف الشرع الجزائري وكالة أمن الأنظمة المعلوماتية بمجموعة من المهام تتمثل في:
- تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية و عرضها على المجلس، تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس، اقتراح كفاءات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
 - إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السببرانية التي تستهدف المؤسسات الوطنية، السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية، متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية، تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية، ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية، مرافقة الإدارات والمؤسسات والهيئات بالتشاور مع الهياكل المختصة في هذا المجال، في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، جرد الأنظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها، إعداد و تحسين خارطة للأنظمة المعلوماتية للمصنفة .
 - اقتراح مشاريع نصوص تشريعية في مجال أمن الأنظمة المعلوماتية بعد الرأي المطابق للمجلس، إعداد و تحديث المرجعيات والإجراءات و الأدلة العلمية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية، اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها.
 - اعتماد منظومة إنشاء وفحص الإيمضاء الإلكتروني، تحديد معايير وإجراءات منح علامة الجودة و/أو التصديق و/أو اعتماد المنتجات و مقدمي الخدمات في مجال أمن الأنظمة

¹ - المادتين 32 و 33 من المرسوم الرئاسي 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

المعلوماتية طبقا للتشريع والتنظيم المعمول بهما، القيام بنشاطات التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية، تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال أمن الأنظمة المعلوماتية، اقتراح تدابير الترقية والبحث والتطوير للحلول الوطنية في مجال أمن الأنظمة المعلوماتية، تنشيط و توجيه أنشطة البحث والتطوير للحلول الوطنية في مجال أمن الأنظمة المعلوماتية، اقتراح مشاريع اتفاقات التعاون والاعتراف المتبادل مع الهيئات الدولية في مجال اختصاصها.

- إبرام مشاريع شراكة في مجال أمن الأنظمة المعلوماتية بعد موافقة المجلس .
- تعزيز ثقافة تأمين الأنظمة المعلوماتية .
- إعداد تقارير دورية وحصيلة سنوية عن نشاطها.
- إعداد وتحسين خارطة حالات هشاشة الأنظمة المعلوماتية على المستوى الوطني .
- ضمان تبادل المعلومات مع الأمانة التقنية للجنة الوطنية لتصنيف النقط الحساسة .
- التنظيم والمشاركة في الأحداث والتظاهرات العلمية والتقنية المتعلقة بأمن الأنظمة المعلوماتية.¹

المطلب الثاني : دور الضبطية القضائية في مجابهة الجرائم الإلكترونية

تشكل الجرائم الإلكترونية تحديًا متزايدًا دفع الحكومة الجزائرية إلى جعل مكافحتها من أولويات استراتيجياتها، لضمان مواجهة المخاطر الأمنية المتزايدة والحفاظ على الأمن العام في الفضاء الرقمي . وفي هذا الإطار تم إنشاء وحدات متخصصة تتوزع بين جهاز الشرطة والدرك الوطني تعمل بتنسيق تام لمواجهة مختلف أشكال هذا النوع من الإجرام.²

وتفريعًا على ما تقدم سنحاول في هذا المطلب ببيان دور الضبطية القضائية في مجابهة الجرائم الإلكترونية وذلك في إطار ثلاثة فروع نتناول في الأول دور جهاز الشرطة الجزائرية في

¹ - المادة 18 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

² - رضوان علي، رزق الله العربي بن مهدي، المكافحة المؤسسية للجريمة الإلكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 09، العدد 02، 2025، ص-ص 1383-1384.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

مكافحة الجريمة الإلكترونية فيما نخصص الفرع الثاني لبيان دور الدرك الوطني في التصدي للجريمة الإلكترونية أما في الفرع الثالث سنتناول فيه دور الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني.

الفرع الأول: دور جهاز الشرطة الجزائرية في مكافحة الجريمة الإلكترونية

عملت الجزائر إلى تفعيل جهاز الشرطة الجزائرية كآلية فعالة تعتمد عليها في الوقاية من الجريمة الإلكترونية ومكافحتها، فيعهد إلى جهاز الشرطة مسؤولية التحري عن الجرائم وضبطها وتلقي البلاغات و إجراء التحقيقات الأولية و تقديم القضايا إلى الجهات القضائية المختصة لمباشرة الدعوى الجزائية.¹

وفي إطار الجرائم الحديثة المرتبطة بالفضاء الرقمي قامت المؤسسة الشرطية بإعادة هيكلة مواردها البشرية والتنظيمية بشكل مبتكر، حيث تم دمج كفاءات متخصصة تلقت تدريبات متعمقة في القيادة الميدانية و إدارة الحالات الحساسة. بالإضافة إلى ذلك، تم إنشاء وحدات نوعية من أبرزها المديرية للعامة للشرطة القضائية والمصلحة المركزية لتصدي الجريمة الإلكترونية التي تأسست في عام 2015 ، و توسعت لتشمل فصائل جهوية في 48 ولاية، وقد أتاح هذا التطور للمواطنين الحصول على خدمات أقرب و أكثر فعالية في مجال مكافحة الجرائم المعلوماتية، كما تم تعزيز هذه الجهود من خلال إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي، الذي يشرف على شبكة من خمسة مختبرات جهوية في وهران، قسنطينة، ورقلة، بشار، و تمنراست والتي تتولى مهام التحليل الجنائي الرقمي و تقديم الدعم التقني

¹ - مريم عراب، المرجع السابق، ص 1228.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

للقضايا المعروضة أمام القضاء، فضلاً عن تكوين الكفاءات العلمية و التقنية المتعلقة بسلسلة العدالة الجنائية، وفي وقت لاحق تم إنشاء معهد الدراسات العليا للأمن الوطني.¹ و نستخلص مما تقدم، أن التحدي الذي تعمل عليه الشرطة الجزائرية لا يقتصر فقط على الجوانب المادية أو التقنية بل يتجاوز ذلك إلى إنشاء قاعدة بشرية مؤهلة و مؤسسات معرفية متخصصة، مما يجعلها أكثر استعداداً لمواجهة التحديات المعقدة المرتبطة بالجريمة الإلكترونية ومن بينها جريمة الابتزاز الإلكتروني و ضمان حماية الفضاء السبراني بما يتوافق مع متطلبات الأمن الوطني.²

الفرع الثاني: دور الدرك الوطني في التصدي للجريمة الإلكترونية

يعتبر الدرك الوطني أحد العناصر الأساسية في مواجهة الجرائم الإلكترونية في الجزائر، حيث اعتمدت استراتيجية على دمج البعد الوقائي مع الجانب العلمي. بدأت أولى خطوات هذه المهمة في عام 2004، لتتجسد بشكل مؤسسي من خلال إنشاء مركز الوقاية من الجرائم المعلوماتية و مكافحتها في عام 2008 ، والذي أصبح نقطة محورية لرصد التهديدات السيبرانية و متابعة مرتكبيها، مما يضمن تطبيق القوانين في فضاء رقمي سريع التطور.

كما يعزز دوره العلمي من خلال المعهد الوطني للأدلة الجنائية و علم الاجرام في بوشاوي الذي يقوم بمهام الخبرة المخبرية وتحليل البصمات الجينية والبيانات الرقمية، مما يوفر للمحققين والقضاة أدوات دقيقة لتفكيك الشبكات الإجرامية و كشف الروابط بينها، ولا يقتصر دور المعهد على الجانب التقني فحسب، بل يمتد ليشمل البحث التطبيقي و المساهمة في صياغة سياسات جنائية فعالة، مع انفتاح على التجارب الدولية واستخدام أحدث مناهج الشرطة العلمية .

و بناءً على ذلك، فإن الدرك الوطني لا يقتصر على كونه جهازاً تقليدياً لتطبيق القانون، بل يتجاوز ذلك ليصبح مؤسسة متكاملة تجمع بين البحث العلمي والتكوين المتخصص والعمل الوقائي و

¹ - رضوان علي، رزق الله العربي بن مهدي، المرجع السابق، ص 1384

² - المرجع نفسه، ص 1384.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

الميداني، مما يجعله فاعلاً رئيسياً في حماية الأمن السيبراني الوطني ومواكبة التحديات المرتبطة بالجريمة الإلكترونية ذات الطابع العابر للحدود.¹

الفرع الثالث: دور الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني

ظهر الذكاء الاصطناعي في خمسينات القرن الماضي، حيث تم استخدام هذا المصطلح لأول مرة خلال مؤتمر جامعة دارتموث (Dartmouth) حول الذكاء الاصطناعي الذي عقد في عام 1956، و منذ ذلك الحين قام المبتكرون و الباحثون بنشر حوالي 1,6 مليون منشور يتعلق بالذكاء الاصطناعي، بالإضافة إلى تقديم طلبات للحصول على براءات اختراع لنحو 340000 ابتكار في مجال الذكاء الاصطناعي.²

" يتكون مصطلح الذكاء الاصطناعي من كلمتين، الذكاء وتعني القدرة على الفهم و إدراك المفاهيم الجديدة، و الاصطناعي فترتبط بالأشياء التي نتجت عن عناصر معينة على عكس الأشياء الطبيعية التي ظهرت نتيجة تدخل الإنسان".³

و يعتبر الذكاء الاصطناعي أحد فروع علوم الحاسوب، حيث يسعى إلى تطور أنظمة و برامج قادرة على محاكاة الذكاء البشري، مما يمكنها من التفكير بطريقة مشابهة للبشر.⁴ وعليه سنسلط الضوء فيما يلي على تعريف الذكاء الاصطناعي أولاً و ثم تبيان دور الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني ثانياً.

¹ - رضوان علي، رزق الله العربي بن مهدي، المرجع السابق، ص- ص 1384-1385.

² - سعاد بوبجة، الذكاء الاصطناعي، تطبيقات وانعكاسات، مجلة إقتصاد المال و الأعمال، المجلد 06، العدد 04، 2022، ص 91 .

³ - خديجة رملي، سلسيل دزيري، استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية و تحقيق الأمن السيبراني، حاجة وافي، تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني، د.ط، دار لايمة للنشر والتوزيع، تيبازة - الجزائر، 2025، ص 70.

⁴ - رشيدة هاشمي، عبد الوهاب ملياني، الإطار المفاهيمي للذكاء الاصطناعي، مجلة التراث، المجلد 14، العدد 02، 2024، ص 49.

الفصل الثاني: الإطار الإجرائي لجريمة الإبتزاز الإلكتروني

أولا : تعريف الذكاء الاصطناعي

تتعدد التعريفات الفقهية المتعلقة بالذكاء الاصطناعي، إلا أنه لا يوجد تعريف شامل و موحد له، لذا سنحاول إيجازها على النحو التالي:

عرف جون مكارثي وهو أول حدد مصطلح الذكاء الاصطناعي بأنه : " وسيلة لصنع جهاز كمبيوتر، أو روبوت يتم التحكم فيه عن طريق الكمبيوتر، أو برنامج يفكر بذكاء و بنفس الطريقة التي يفكر بها البشر الأذكىاء، و يتم تحقيق الذكاء الاصطناعي من خلال دراسة كيف يفكر الدماغ البشري، وكيف يتعلم البشر ويقررون ويعملون أثناء محاولة حل مشكلة ما، ثم استخدام نتائج هذه الدراسة كأساس لتطوير برامج وأنظمة ذكية ".¹

كما عرفه عرنوس بشير بأنه : " علم الحاسبات الذي يهتم بأنظمة الحاسوب التي تمتلك خصائص مرتبطة بالذكاء البشري والقدرة على اتخاذ القرارات بدرجة مشابهة إلى حد ما للسلوك البشري في مختلف المجالات ، و أنظمة الذكاء الاصطناعي هي تلك الأنظمة المهمة بتطوير من الحاسوب ليقوم بالمهام التي تتطلب ذكاء بشريا من خلال جعل الآلات تقوم بأعمال تعتمد على الذكاء البشري في أدائها في الواقع".²

كما تم تعريفه بأنه : " الذكاء المرتبط بكافة الأجهزة الرقمية والتقنيات الحديثة المتداولة مثل الروبوتات والأجهزة الخلوية والكمبيوتر والتي تعبر عن قدرة الذكاء الاصطناعي في إجراء التجارب العلمية".³

بصفة عامة يمكن تعريف الذكاء الاصطناعي بأنه : " مجموعة من الجهود المبذولة لتطوير نظم المعلومات المحوسبة بطريقة تستطيع أن تتصرف فيها و تفكر بأسلوب مماثل للبشر، هذه النظم تستطيع أن تتعلم اللغات الطبيعية، وانجاز مهام فعلية بتنسيق متكامل، أو استخدام صور وأشكال

¹ - علي بن عوالي ، استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية و تحقيق الأمن السبيرياني، حاجة وافي ، الذكاء الاصطناعي ودوره في تعزيز الأمن السبيرياني ،د.ط، دار لايمة للنشر والتوزيع، تيبازة - الجزائر، 2025، ص 252.

² - رشيدة هاشمي، عبد الوهاب ملياني، المرجع السابق، ص 50.

³ - محمد عبد الرحمن عبد المحسن، المرجع السابق، ص 2680.

الفصل الثاني: الإطار الإجرائي لجريمة الابتزاز الإلكتروني

إدراكية لترشيد السلوك المادي، كما تستطيع في نفس الوقت خزن الخبرات والمعارف الإنسانية المتراكمة و استخدامها في عملية اتخاذ القرارات".¹

ثانيا : الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني

يمثل الذكاء الاصطناعي أداة ذات أهمية متزايدة في مكافحة جرائم الابتزاز الإلكتروني، لما يوفره من إمكانيات متقدمة في تحليل البيانات الضخمة بهدف رصد الأنماط الإجرامية وتحديد الأشخاص المعرضين للاستهداف. كما يُسهم في دعم وسائل الإثبات الرقمي من خلال تطوير تقنيات قادرة على كشف التزييف العميق و تمييز المحتوى الرقمي المصطنع عن الحقيقي، الأمر الذي يعزز من حجية الأدلة أمام الجهات القضائية.

إضافة إلى ذلك، يعزز الذكاء الاصطناعي من فعالية أنظمة الأمن السيبراني عبر الكشف المبكر عن محاولات الاختراق و عمليات التصيد الاحتيالي، بما يحد من وقوع الجريمة أو تفاقم آثارها، غير أن هذا التقدم التقني يطرح في المقابل تحديات قانونية معقدة، إذ يمكن استغلاله من قبل الجناة في ابتكار أساليب أكثر تطوراً للابتزاز، مما يزيد من صعوبة عمليات التحقيق والملاحقة القانونية.²

¹ - رشيدة هاشمي، عبد الوهاب ملياني، المرجع السابق، ص 50.

² - محمد عبد الرحمن عبد المحسن، المرجع السابق، ص - ص 2683 - 2684.

خاتمة

يعد الابتزاز الإلكتروني من أخطر الظواهر الاجتماعية التي تهدد المجتمع في ظل التطور الهائل في عالم التكنولوجيا الحديثة والمعلومات، فقد أتاح هذا التطور للمبتزين استخدام أساليب إجرامية متعددة للحصول على المعلومات الشخصية والصور الخاصة من خلال وسائل التواصل المختلفة، كما يستغل الجاني الفضاء الإلكتروني الواسع للتواصل مع الضحية والتسلل إلى بياناته الخاصة بهدف تحقيق غايته غير المشروعة كالتشهير أو التهديد أو الحصول على الأموال، ولذلك أصبح الابتزاز الإلكتروني يشكل خطراً حقيقياً على الأفراد والمجتمع، مما يستوجب نشر الوعي وتعزيز الحماية الرقمية للحد من هذه الظاهرة.

وعليه توصلنا إلى طائفة من النتائج و المقترحات التي نجلها كالآتي:

أولاً- النتائج:

- 1- جريمة الابتزاز الإلكتروني هي صورة من صور الجرائم الإلكترونية، إذ تتم باستخدام شبكة الانترنت و أجهزة الاتصال الحديثة و تطبيقاتها المختلفة كوسائل التواصل، و التي بلغت خطورتها على الافراد و المجتمعات حداً كبيراً.
- 2- لم يتناول المشرع الجزائري في قانون العقوبات نصوصاً صريحة و متخصصة تجرم الابتزاز الإلكتروني كجريمة مستقلة،انما نص عليها ضمناً مع جريمة التهديد و جعلها مجرد نموذج اجرامي خاص مع جريمة التهديد إلا انه بعد صدور آخر تعديل لقانون العقوبات رقم 06-24 عالج القضاء الجزائري هذه الجريمة في المادة (371) بغية عدم افلات مرتكبها من العقاب.
- 3- تعد جريمة الابتزاز الإلكتروني من الجرائم ذات الطبيعة العابرة للحدود، لما تتميز به من خصوصية ناتجة عن ارتكابها باستعمال الشبكة العنكبوتية و وسائل الاتصال الالكترونية، حيث قد يتواجد الجاني في دولة بينما توجد الضحية في دولة أخرى، الأمر الذي إشكالات قانونية و إجرائية تتعلق بالاختصاص القضائي و التعاون الدولي.
- 4- إن جريمة الابتزاز الإلكتروني لا تختلف في أحكامها العامة عن غيرها من الجرائم، إذ يشترط لقيامها توافر الركنين المادي و المعنوي. كما تعد من الجرائم العمدية التي

يتطلب تحققها توافر القصد الجنائي، و يكفي لقيامها توافر القصد العام المتمثل فياتجاه

إرادة الجاني إلى ارتكاب الفعل المجرم مع علمه بطبيعته غير المشروعة.

5- تتسم هذه الجريمة بخصوصية تتمثل في صعوبة إثباتها، نظراً لإمكانية طمس آثارها بسهولة، الأمر الذي يجعل التصدي لها تحدياً معقداً يقتضي تبني آليات حديثة و غير تقليدية لمواجهتها.

ثانياً- المقترحات:

بناءً على النتائج التي تم التوصل إليها نقترح بما يلي:

1- نرجو المشرع الجزائري إلى التدخل من أجل تعديل قانون مكافحة جرائم تكنولوجيا الإعلام و الاتصال، وذلك من خلال إدراج نص قانوني خاص و مستقل يجرم جريمة الابتزاز الإلكتروني بكافة صورها و أشكالها مع تشديد العقوبات المقررة لها بالنظر إلى ما تخلفه من آثار خطيرة و انعكاسات سلبية على أمن و استقرار المجتمع الجزائري.

2- نقترح بإطلاق حملات توعية وطنية شاملة عبر مختلف وسائل الإعلام و منصات التواصل الاجتماعي، بهدف توعية جميع فئات المجتمع خاصة الجامعات و المدارس بوصف هذه الفئات العمرية هي الأكثر عرضة بمخاطر الابتزاز الإلكتروني و سبل الوقاية منه، مع تشجيع الضحايا على تجاوز حاجز الصمت و الخوف و الإبلاغ عن هذه الجرائم، من خلال توفير آليات إبلاغ آمنة و سرية تكفل حماية المبلغين و تعزيز الثقة في الجهات المختصة.

3- إنشاء منصات رقمية رسمية متخصصة لاستقبال شكاوى الابتزاز الإلكتروني، تمكن المواطنين من الإبلاغ عن الجرائم بسرية تامة، مع ضمان حماية بياناتهم الشخصية و هويتهم مع توفير المرافقة القانونية و الدعم النفسي للضحايا ضماناً لحمايتهم من التعرض لمزيد من الضغوط أو الأذى النفسي و الاجتماعي.

4- تطوير برامج تدريبية متخصصة لفائدة القضاة و المحامين و رجال الأمن، تُعنى بأحدث التقنيات المرتبطة بالجرائم الإلكترونية و أساليب التحقيق الرقمي الحديثة، بهدف تعزيز

- معارفهم و خبراتهم العملية، بما يضمن رفع كفاءتهم و قدرتهم على التعامل مع القضايا المتعلقة بالابتزاز الإلكتروني بكفاءة و فعالية عالية.
- 5- يجب على الأسرة توعية أبنائها بمخاطر الابتزاز الإلكتروني و تعزيز التكافل الأسري و تقديم الدعم اللازم لهم خاصة للفتيات لحمايةهن من الوقوع في شباك المبتزين.
- 6- تفعيل آليات الحماية على مواقع التواصل الاجتماعي للحد من جريمة الابتزاز الإلكتروني، من خلال تشديد الرقابة على هذه المنصات و تعزيز إجراءات الأمن الرقمي من جهة، و من جهة أخرى فرض شروط قانونية لتنظيم الولوج إليها، كالإزام المستخدمين بتأكيد هوياتهم الحقيقية و عدم السماح بإنشاء حسابات بأسماء وهمية دون تقديم وثائق رسمية تثبت هوية المستخدم.
- 7- العمل الجاد في مجال التحقيق بين الدول من خلال إبرام الاتفاقيات و المعاهدات الثنائية و متعددة الأطراف.
- 8- نرجو المشرع الجزائري إلى أن يوضح الشروط الواجب توافرها في الدليل الرقمي بصورة دقيقة، حتى يتمتع بالحجية في إثبات جريمة الابتزاز الإلكتروني.
- 9- انشاء وحدات متخصصة داخل الجهات الأمنية و القضائية تتولى حصريا متابعة قضايا الابتزاز الإلكتروني، بحيث يتم تزويدها بأحدث التقنيات و الموارد البشرية المدربة لضمان سرعة التحقيق و الكشف عن المبتزين و اتخاذ الاجراءات القانونية اللازمة بكفاءة أكبر.

قائمة المصادر والمراجع

أولاً: النصوص التشريعية

- 1- قانون رقم 06 - 01 مؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006 ، يتعلق بالوقاية من الفساد و مكافحته ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 14، الصادرة في 08 مارس 2006 .
- 2- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 47، الصادرة في 16 غشت 2009.
- 3- قانون رقم 15-12 مؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015 ، المتعلق بحماية الطفل ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 39، الصادرة في 19 جويلية 2015 .
- 4- القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة في 10 يونيو 2018.
- 5- القانون رقم 20-15 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020 ، يتعلق بالوقاية من جرائم اختطاف الأشخاص و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 81، الصادرة في 30 ديسمبر سنة 2020.
- 6- القانون رقم 20-05 المؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020 ، يتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 25، الصادرة في 29 أبريل 2020.
- 7- قانون رقم 24-06 مؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024 ، يعدل و يتم الأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 و المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 30، الصادرة في 30 أبريل سنة 2024.
- 8- قانون رقم 25-11 مؤرخ في 28 محرم 1447 الموافق 24 يوليو سنة 2025 ، يعدل ويتم القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 ، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع

الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، الصادرة في 24 يوليو سنة 2025.

9- قانون رقم 25-14 مؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 54 ، الصادرة في 13 غشت 2025 .

10- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل و المتمم .

ثانيا: النصوص التنظيمية

11- المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020 ، والمتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020، الجريدة الرسمية للجمهورية الجزائرية ، العدد 82.

12- المرسوم الرئاسي رقم 20-05 مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، العدد 04، الصادر 26 جانفي 2020.

13- المرسوم الرئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 86، الصادر بتاريخ 11 نوفمبر 2021.

ثالثا: الكتب

أ- الكتب المتخصصة

14- أمير فرج يوسف ، المسؤولية الجنائية عن جريمة الإبتزاز الإلكتروني دراسة مقارنة، د.ط ، دار المطبوعات الجامعية ، الإسكندرية، 2023.

15- باقر غازي حنون الدراجي ، المسؤولية الجنائية الناشئة عن الإبتزاز الإلكتروني ، د.ط ، دروب المعرفة للنشر و التوزيع ، الإسكندرية ، جمهورية مصر العربية ، 2024.

16- زهراء عادل سلمي ، جريمة الابتزاز الإلكتروني (دراسة مقارنة) ، ط01 ، شركة دار الأكاديميون للنشر و التوزيع، عمان- الأردن ، 2020.

ب- الكتب العامة

- 17- أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، ط22 ، دار بلقيس للنشر والتوزيع، دار البيضاء - الجزائر ، 2025.
- 18- الطاهر ياكور ، الجرائم الإلكترونية الأحكام الموضوعية و الإجرائية دراسة مقارنة ، د.ط، دار بلقيس للنشر ، الجزائر ، 2024.
- 19- حسين طاهري ، الجرائم المعلوماتية الماسة بالشرف و الاعتبار و الحياة الخاصة و بالأخلاق و الآداب العامة ، د . ط ، دار العلا للطباعة و النشر للترجمة و التوزيع ، أم البواقي - الجزائر ، 2024.
- 20- خديجة رملي، سلسيل دزيري، استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية وتحقيق الأمن السيبراني، حاجة وافي، تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني، د.ط، دار لايمه للنشر والتوزيع، تيبازة - الجزائر ، 2025.
- 21- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط01 ، دار الفكر الجامعي، الاسكندرية، 2009.
- 22- عبد القادر عمير، التحديات القانونية لإثبات الجريمة المعلوماتية، د.ط، النشر الجامعي الجديد، تلمسان - الجزائر، 2021.
- 23- علي بن عوالي ، استخدامات الذكاء الاصطناعي في تعزيز السيادة الرقمية و تحقيق الأمن السيبراني، حاجة وافي ، الذكاء الاصطناعي ودوره في تعزيز الأمن السيبراني، د.ط، دار لايمه للنشر والتوزيع، تيبازة - الجزائر، 2025.
- 24- علي لطرش ، مخاطر الأنترنت على حقوق الطفل في الخصوصية و النسيان في ظل التشريعات المقارنة (التشريع الأمريكي - البريطاني - الأوروبي و الجزائري) ، د.ط ، دار الخلدونية للنشر و التوزيع ، الجزائر ، 2023.
- 25- لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، د.ط، النشر الجامعي الجديد ، تلمسان -الجزائر ، 2018.
- 26- محمود أحمد القرعان ، الجرائم الإلكترونية ، ط01، دار وائل للنشر و التوزيع، الأردن - عمان -، 2017 .
- 27- محمد حزيط ، الوجيز في قانون الاجراءات الجزائية الجزائري قانون رقم 25-14 مؤرخ في 3 غشت 2025 ، ط02 ، دار بلقيس للنشر و التوزيع ، الجزائر ، 2026 .

28- محمد شنه ، إجراءات البحث و التحري عن الجرائم في التشريع الجزائري ، ط01 ، ألفا للوثائق للنشر و التوزيع ، عمان- الأردن ، 2024.

29- مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الالكترونية ، ط 01 ، مطابع الشرطة للطباعة و النشر و التوزيع ، القاهرة ، 2009.

رابعاً: الرسائل الجامعية

أ - الأطروحات

30- سليم درابلة العمري، حجية الدليل الرقمي في الاثبات الجنائي، أطروحة مقدمة لنيل شهادة دكتوراه، تخصص القانون الجنائي و العلوم الجنائية، جامعة الجزائر 01، 2024/2025.

31- يوسف صغير ، آليات مكافحة الجريمة المرتكبة عبر الإنترنت ، رسالة نيل درجة دكتوراه في العلوم ، تخصص قانون ، جامعة مولود معمري - تيزي وزو ، 01 جويلية 2024.

ب-رسائل ماجستير

32- دعاء سليمان عبد القادر التميمي ، جريمة الابتزاز الالكتروني "دراسة مقارنة" ، رسالة ماجستير ، القانون العام ، كلية القانون - كلية الدراسات العليا -،جامعة القدس - فلسطين ، 2019/07/07.

33- محمد علي أحمد أبو علي ، جريمة الابتزاز الالكتروني في التشريع الفلسطيني ، ماجستير ، العلوم الجنائية ، الجامعة العربية الأمريكية -كلية الدراسات العليا ، 2022/9 .

ج-مذكرات الماستر

34- آمال برحال، جريمة الابتزاز عبر الوسائل الإلكترونية ، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر ، قانون جنائي و علوم جنائية ، جامعة العربي التبسي - تبسة ، 2022/2019.

خامساً: المقالات العلمية

35- أحمد بن مالك، ابراهيم الخال، دور الأدلة الرقمية في الاثبات الجنائي، مجلة العلوم الانسانية، المجلد 05، العدد 01 ، 2021.

36- أكرم ماجد خلف ، الحماية الجنائية للطلاب الجامعي من جرائم الابتزاز الإلكتروني ، مجلة الشرق الأوسط للدراسات القانونية و الفقهية ، المجلد 05 ، العدد 02 ، 2025.

37- المهدي صدوق، محمد غريبي، فعالية دور السلطة الوطنية لحماية المعطيات الشخصية في البيئة الرقمية، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 07، العدد 02، 2023.

- 38- أماني هاشم لطيف ، الابتزاز الإلكتروني و تداعياته على الواقع السياسي و الاجتماعي العراقي ، مجلة دراسات دولية ، العدد 98 ، 2024.
- 39- أميل جبار عاشور ، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي (دراسة مقارنة) مجلة أبحاث ميسان ، المجلد 16 ، العدد 31 ، 2020.
- 40- إسمهان بوضياف ، الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، العدد 11 ، 2018.
- 41- إلهام بن خليفة ، التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، المجلة الدولية للبحوث القانونية و السياسية ، المجلد 02 ، العدد 01 ، 2018.
- 42- جمال دريسي، الإثبات الجنائي بالأدلة العلمية، المجلة النقدية للقانون و العلوم السياسية، المجلد 17، العدد 02، 2022.
- 43- جميلة محلق ، اعتراض المراسلات ، تسجيل الأصوات و التقاط الصور في قانون الإجراءات الجزائية الجزائري ، مجلة التواصل في الإقتصاد و الإدارة و القانون ، عدد 42 ، 2015.
- 44- حسام منصور محمد، جريمة الابتزاز الإلكتروني، بحث مقدم إلى مجلس المعهد القضائي وهو جزء من متطلبات نيل درجة الدبلوم العالي في العلوم القضائية، جامعة بغداد، 2024.
- 45- رباب مصطفى عبد المنعم الحكيم ، جريمة الابتزاز الإلكتروني في التشريع المصري، مجلة قطاع الشريعة و القانون ، العدد 17 ، 2025.
- 46- رشدي خميري ، مراد عمراني ، جريمة استغلال النفوذ في القانون الجزائري ، المجلة الجزائرية للحقوق و العلوم السياسية ، المجلد 06 ، العدد 02 ، 2021.
- 47- رشيدة هاشمي، عبد الوهاب ملياني، الإطار المفاهيمي للذكاء الاصطناعي، مجلة التراث، المجلد 14، العدد 02، 2024.
- 48- رضوان علي، رزق الله العربي بن مهدي، مكافحة المؤسساتية للجريمة الالكترونية في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 09، العدد 02، 2025.
- 49- ريهام عاطف معروف ، الابتزاز الإلكتروني ، مجلة روح القوانين ، عدد خاص - المؤتمر العلمي الدولي الثامن ، التكنولوجيا و القانون، د.س.

- 50- سارة قريمس، التسرب الإلكتروني كآلية إجرائية مستحدثة للتحري و التحقيق الجنائي الرقمي على ضوء التشريع الجزائري، المجلد 09، العدد 02، 2025.
- 51- سعاد بوبجة، الذكاء الاصطناعي، تطبيقات وانعكاسات، مجلة اقتصاد المال و الأعمال، المجلد 06، العدد 04، 2022.
- 52- سهام عكوش، الحماية القانونية لحق الخصوصية من جريمة التهديد عبر مواقع التواصل الاجتماعي وفقا للقانون الجزائري، المجلد 06، العدد 01، 2022.
- 53- صونيا مقري، وليد بن لعامر، المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي 20-05، مجلة البحوث في العقود و قانون الأعمال، المجلد 10، العدد 02، 2025.
- 54- عادل رزيق ، الحماية الجزائرية للحق في حرمة الحياة الخاصة في ظل التقنيات الحديثة ، مجلة القانون والعلوم السياسية، المجلد 03، العدد 01، 2017.
- 55- عبد القادر سعد حاتم الحبيب ، الإطار القانوني لمكافحة الابتزاز الإلكتروني في العراق و لبنان: دراسة مقارنة ، مجلة العلوم الإنسانية و الطبيعية ، المجلد 06 ، العدد 01، 2025.
- 56- عبد القادر فلاح ، حجز و حفظ المعطيات في الجريمة الإلكترونية ، مجلة صوت القانون ، المجلد 08 ، العدد 01، 2021 .
- 57- عبد الهادي كحلاوي، عبد الهادي بن زيطة، آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون رقم والعلوم السياسية، المجلد 07، العدد 02، 2021.
- 58- عز الدين عثمانى ، إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الإتصال و المعلوماتية ، مجلة دائرة البحوث و الدراسات القانونية و السياسية - مخبر المؤسسات الدستورية و النظم السياسية ، العدد 04 ، 2018.
- 59- عزيزة رابحي ، التفتيش في نظم المعالجة الآلية للمعطيات ، مجلة القانون و العلوم السياسية ، المجلد 02 ، العدد 01 ، 2016.
- 60- عماد جواد موسى ، التحقيق و الصعوبات التي تواجه جريمة الابتزاز الإلكتروني ، مجلة كلية المعارف جامعة ، المجلد 33 ، العدد 04 ، 2022.

61- فاطمة العرفي ، الحماية القانونية للحق في الخصوصية للأطفال من جريمة التشهير عبر مواقع التواصل الاجتماعي في القانون الجزائري، مجلة الاجتهاد القضائي ، المجلد 12 ، العدد 04 ، 2022.

62- فاطمة العرفي، حجية الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري ، مجلة صوت القانون ، المجلد 08 ، العدد خاص 02 ، 2022 .

63- فاطمة خرشف، الآليات القانونية والمؤسسية الخاصة بمكافحة الجريمة السيبرانية في الجزائر، مجلة سوسيولوجيا الجريمة للبحوث والدراسات في الظواهر الإجرامية، المجلد 04، العدد 02، 2023.

64- فتيحة حزام، حماية الأنظمة الرقمية بين الآليات التقنية و اجهزة الحماية- قراءة في أحكام المرسوم الرئاسي 20-05، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد 03، 2020.

65- فوزي عمارة ، اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب كإجراءات تحقيق قضائي في المواد الجزائية ، مجلة العلوم الإنسانية، عدد 33، 2010.

66- كريمة تاجر، التسرب الإلكتروني كآلية لمكافحة الجريمة الإلكترونية (دراسة مقارنة بين القانون الجزائري و الفرنسي)، المجلة النقدية للقانون و العلوم السياسية، المجلد 19، العدد 02، 2024.

67- كمال حفصاوي ، عمر مخلوف ، التفتيش الإلكتروني بين ضرورة التحقيق و الحق في سرية المراسلات و الاتصالات ، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد 01، 2024.

68- ليندا بن طالب ، التفتيش في الجريمة المعلوماتية ، مجلة العلوم القانونية و السياسية ، عدد 16، 2017.

69- مريم عراب، جريمة التهديد و الابتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد 01، 2021.

70- نور الهدى قادري، الجريمة السيبرانية وآليات مكافحتها، مواجهة تحديات الأمن السيبراني، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 08، العدد 01، 2023.

71- نورة بن بو عبد الله ، وردة بن بو عبد الله ، تعزيز الحماية الجزائية للخصوصية المعلوماتية على ضوء تعديل قانون العقوبات رقم 24-06 المؤرخ في 28 أفريل 2024 ، المجلة الدولية للبحوث الدولية والسياسية، المجلد 09 ، العدد 01، 2025.

72- وفاء محمد صقر، جريمة الابتزاز الإلكتروني (دراسة مقارنة) ، مجلة البحوث القانونية و الاقتصادية ، المجلد 36 ، العدد 02 ، 2024.

73- ياسر مهيبوب عبد العزيز المليكي، جريمة الابتزاز الإلكتروني إشكالية الحماية الموضوعية والإجرائية في التشريع اليمني مجلة العلوم التربوية و الدراسات الإنسانية، العدد 36، د.س.

74- ياسين بن عمر، الابتزاز الإلكتروني للأطفال في التشريع الجزائري، دفاتر السياسة و القانون ، المجلد 16 ، العدد 02 ، 2024.

سادسا: المواقع الإلكترونية

75- إيهاب عبد الغني عثمان المغربي ، المواجهة التشريعية لجريمة الابتزاز الإلكتروني "دراسة مقارنة " ، بحث متاح على الموقع الإلكتروني <https://jslem.journals.ekb.eg>.

76- متاح على الموقع الإلكتروني www.almaany.com.

فهرس المحتويات

	الإهداء
	شكر وتقدير
	قائمة المختصرات
6-2	مقدمة
-	الفصل الأول: الإطار المفاهيمي للابتزاز الإلكتروني
9	المبحث الأول : ماهية جريمة الابتزاز الإلكتروني
9	المطلب الأول: مفهوم الابتزاز الإلكتروني و مراحل ارتكابه و صورته
10	الفرع الأول : تعريف الابتزاز الإلكتروني لغة و اصطلاحا
11-10	أولا : التعريف اللغوي للابتزاز الإلكتروني
11	ثانيا : التعريف الاصطلاحي للابتزاز الإلكتروني
15-11	1-التعريف التشريعي للابتزاز الإلكتروني
17-15	2-التعريف الفقهي للابتزاز الإلكتروني
17	الفرع الثاني : مراحل الابتزاز الإلكتروني
19-17	أولا : الحصول على مادة الابتزاز
19	ثانيا : الطلب و التهديد
20	ثالثا : المقاومة
21	رابعا : الإذعان
21	خامسا : التكرار
21	الفرع الثالث : صور الابتزاز الإلكتروني
21	أولا :الابتزاز الإلكتروني من حيث المجني عليه
22	1-ابتزاز النساء
25-23	2-ابتزاز الأحداث
27-26	3-ابتزاز الرجال
28-27	4-ابتزاز الأشخاص المعنوية
28	ثانيا :الابتزاز الإلكتروني من حيث الهدف
29-28	1-الابتزاز بهدف مادي

30-29	2-الابتزاز بهدف لا أخلاقي (جنسي)
30	3-الابتزاز بهدف نفعي
31	المطلب الثاني: خصائص الابتزاز الإلكتروني
31	الفرع الأول: سمات الابتزاز الإلكتروني
32-31	أولا : جريمة عابرة للحدود
33-32	ثانيا : جريمة جاذبة للجناة
33	ثالثا: جريمة هادئة
34-33	رابعا : جريمة صعبة الإثبات و الإبلاغ
34	خامسا : خصوصية مجرم الابتزاز الإلكتروني
34	1- مجرم ذكي
35	2- مجرم غير عنيف
35	3- مجرم ذو طبيعة اجتماعية
35	الفرع الثاني : الآثار المترتبة عن الابتزاز الإلكتروني
36-35	أولا : الآثار النفسية
37-36	ثانيا : الآثار الاجتماعية
37	ثالثا : الآثار الأمنية
37	الفرع الثالث : تمييز الابتزاز الإلكتروني عن الأفعال المشابهة له
38	أولا : الفرق بين جريمة الابتزاز الإلكتروني و جريمة التهديد
38	1 - أوجه التشابه
39-38	2- أوجه الاختلاف
39	ثانيا : الفرق بين الابتزاز الإلكتروني و استغلال النفوذ
40	1- أوجه التشابه
41	2- أوجه الاختلاف
42	المبحث الثاني: التكييف القانوني لجريمة الابتزاز الإلكتروني
42	المطلب الأول: أركان جريمة الابتزاز الإلكتروني
45-43	الفرع الأول : الركن الشرعي

49-46	الفرع الثاني : الركن المادي
49-46	أولا : السلوك الإجرامي
49	ثانيا : النتيجة الإجرامية
50	ثالثا : العلاقة السببية
51-50	الفرع الثالث : الركن المعنوي
51	المطلب الثاني : العقوبة المقررة لجريمة الابتزاز الإلكتروني
52-51	الفرع الأول : العقوبات الأصلية لجريمة الابتزاز الإلكتروني
52	أولا: العقوبة السالبة للحرية
52	ثانيا: العقوبة المالية
53	الفرع الثاني : العقوبات التكميلية لجريمة الابتزاز الإلكتروني
53	أولا- العقوبات التكميلية الوجوبية
54-53	ثانيا-العقوبات التكميلية الجوازية
54	ثالثا: المساهمة الجنائية في جريمة الابتزاز الإلكتروني
56-55	الفرع الثالث : حالات تشديد العقوبة
58	الفصل الثاني: الإطار الإجرائي لجريمة للابتزاز الإلكتروني
61	المبحث الأول : التحقيق والإثبات في جريمة الابتزاز الإلكتروني
61	المطلب الأول : إجراءات التحقيق في جريمة الابتزاز الإلكتروني
62-61	الفرع الأول : التحقيق في جريمة الابتزاز الإلكتروني عن طريق الإجراءات التقليدية
66-62	أولا : المعاينة
67-66	ثانيا : التفتيش
67	1-الضوابط الموضوعية لتفتيش نظم الحاسب الآلي
67	أ - وجود سبب للتفتيش
68	ب- محل التفتيش
68	ج- السلطة المختصة بالتفتيش
69	2-الضوابط الشكلية لتفتيش نظم الحاسب الآلي

69	أ - إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون
70-69	ب- تحرير محضر التفتيش
71-70	ج- وقت أو ميعاد إجراء التفتيش
71	ثالثا : الضبط
72	الفرع الثاني : المعوقات التي تواجه جهات التحقيق في جريمة الابتزاز الإلكتروني
72	أولا : حق الإنسان في الخصوصية
73-72	ثانيا : قلة الخبرة لدى جهات التحقيق
73	ثالثا : سيادة القانون و الحاجة لتطوير القوانين
74	الفرع الثالث : التحقيق في جريمة الابتزاز الإلكتروني عن طريق الإجراءات المستحدثة
74	أولا : اعتراض المراسلات و تسجيل و التقاط الصور (المراقبة الإلكترونية)
75-74	1- اعتراض المراسلات
76-75	2- تسجيل الأصوات و التقاط الصور
78-76	ثانيا : ضوابط المراقبة الإلكترونية
81-78	ثالثا: التسرب الإلكتروني
81	1- استصدار إذن مكتوب بعملية التسرب الإلكتروني
82	2- تحرير تقرير حول عملية التسرب الإلكتروني
83	3- مدة عملية التسرب الإلكتروني
	4- الأعمال التي يأذن القانون الجزائي للمتسرب القيام بها
	5- أن تتم عملية التسرب الإلكتروني تحت رقابة وكيل الجمهورية أو قاضي التحقيق
86-85	المطلب الثاني: الإثبات في جريمة الابتزاز الإلكتروني
87-86	الفرع الأول : الدليل الجنائي الرقمي في جريمة الابتزاز الإلكتروني
89-87	أولا : مفهوم الدليل الرقمي
89	ثانيا: تقسيمات الدليل الرقمي في جريمة الابتزاز الإلكتروني

91-90	ثالثا: موقف المشرع الجزائري من قبول الدليل الرقمي في جريمة الابتزاز الإلكتروني
91	الفرع الثاني : المعوقات التي يثيرها الدليل الرقمي في جريمة الابتزاز الإلكتروني
92-91	أولا: سهولة محو الدليل الرقمي
92	ثانيا:إعاقة الوصول إلى الدليل الرقمي
93-92	ثالثا: ضعف التعاون بين الدول و اختلاف الأنظمة الإجرائية بينها
94-93	رابعا: نظم تشغيل أجهزة الكمبيوتر النشطة و النظم الساكنة
94	الفرع الثالث: معالجة الاشكالات المرتبطة بالدليل الرقمي في جريمة الابتزاز الإلكتروني
95	المبحث الثاني: مكافحة جريمة الابتزاز الإلكتروني على المستوى المؤسسي الوطني
96	المطلب الأول: دور المؤسسات الوطنية في مكافحة جريمة الابتزاز الإلكتروني
97-96	الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
98	أولا: تشكيل الهيئة الوطنية و تنظيمها
100-98	1-مجلس التوجيه
102-100	2-المديرية العامة
103-102	ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها
109-103	الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي
106-109	أولا: تشكيلتها
108-106	ثانيا: مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي
108	الفرع الثالث: المنظومة الوطنية لأمن الأنظمة المعلوماتية
109	أولا: المجلس الوطني لأمن الأنظمة المعلوماتية
110-109	1-تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية

111-110	2-مهام المجلس الوطني لأمن الأنظمة المعلوماتية
111	3-تسيير المجلس الوطني لأمن الأنظمة المعلوماتية
112	ثانيا: وكالة أمن الأنظمة المعلوماتية
112	1- تنظيم وسير وكالة أمن الأنظمة المعلوماتية
113-112	أ-تشكيلة لجنة التوجيه
114-113	ب- مهام لجنة التوجيه
114	ج-سير لجنة التوجيه
115-114	2- المدير العام لوكالة أمن الأنظمة المعلوماتية
116-115	3-اللجنة العلمية للوكالة
116	ثالثا: مهام وكالة أمن الأنظمة المعلوماتية
118-117	المطلب الثاني : دور الضبطية القضائية في مجابهة الجرائم الإلكترونية
119-118	الفرع الأول : دور جهاز الشرطة الجزائرية في مكافحة الجريمة الالكترونية
120-119	الفرع الثاني : دور الدرك الوطني في التصدي للجريمة الإلكترونية
120	الفرع الثالث: دور الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني
122-121	أولا : تعريف الذكاء الاصطناعي
122	ثانيا : الذكاء الاصطناعي في مكافحة الابتزاز الإلكتروني
126-124	خاتمة
135-128	قائمة المراجع والمصادر
142-137	فهرس المحتويات
	الملخص

الملخص:

تناولت هذه الدراسة الأكاديمية جريمة الابتزاز الإلكتروني التي تعد من الجرائم الحديثة التي نشأت مع دخول التكنولوجيا كونه سلوك اجتماعي مضاد للقيم و ثقافة المجتمع الجزائري و مخالف للقانون خصوصا بعدما اتخذت منحني أكثر خطورة بسبب الثورة الحديثة في عالم التكنولوجيا و المعلوماتية حيث استغل البعض هذه التكنولوجيا للاعتداء على خصوصية الآخرين و تهديدهم بما يحقرهم أو يضعهم في موقف صعب في المجتمع.

و قد تعرضنا في بداية الدراسة لماهية جريمة الابتزاز الإلكتروني في مبحث أول و عرضنا من خلاله تعريف هذه الجريمة و خصائصها و صورها، مع إبراز أوجه التشابه و الاختلاف بينها و بين بعض الجرائم المشابهة لها كجريمة التهديد و استغلال النفوذ، و ما لها من طبيعة خاصة كونها تمر بعدة مراحل ثم تناولنا في المبحث الثاني التكييف القانوني لجريمة الابتزاز الإلكتروني و قمنا بعرض الأركان المكونة لها و العقوبات المقررة لها، أما الفصل الثاني فقد خصصناه لدراسة الإطار الاجرائي لجريمة الابتزاز الإلكتروني، حيث تناول المبحث الأول اجراءات التحقيق و الإثبات المتعلقة بها بالنظر إلى خصوصيتها و طبيعتها التقنية في حين تم تخصيص المبحث الثاني لدراسة دور المؤسسات الوطنية و الأمنية في مجابهة هذه الجريمة و الحد من انتشارها. و تنتهي الدراسة بتقديم نتائج و اقتراحات تهدف إلى تحسين الإطار القانوني لمواجهة هذه الجريمة الخطيرة و المتنامية بما في ذلك تشديد العقوبات و اصدار نصوص متخصصة و تطوير آليات التحقيق و الإثبات.

الكلمات المفتاحية: الجريمة الإلكترونية، جريمة الابتزاز الإلكتروني، التهديد، التحقيق، الإثبات، الدليل الرقمي

Abstract:

This academic study addressed the crime of electronic blackmail, which is considered one of the modern crimes that emerged with the advancement of technology. It represents a social behavior that is contrary to the values and culture of Algerian society and violates legal provisions, particularly after it became more dangerous due to the modern revolution in the fields of technology and information systems. Some individuals have exploited these violate the privacy of others and threaten them in ways that humiliate them or place them in difficult situations within society.

At the beginning of this study, the first chapter was devoted to examining the concept and nature of electronic blackmail the first section presented the definition, characteristics, and various forms of this crime, while highlighting the similarities and differences between electronic blackmail and certain related crimes such as traditional blackmail and abuse of authority. It also discussed its particular nature as a crime that passes through several stages. The second section addressed the legal characterization of electronic blackmail by presenting its constituent elements and the penalties prescribed for it. The second chapter was devoted to studying the procedural framework of electronic blackmail. The first section focused on investigation and evidentiary procedures related to this crime in light of its specific characteristics and technical nature, while the second section examined the role of national institutions and security agencies in combating this crime and limiting its spread. The study concluded by presenting findings and recommendations aimed at improving the legal framework for confronting this serious and growing crime, including strengthening penalties, enacting specialized legal provisions, and developing investigation and evidentiary mechanisms.

Keywords: cybercrime, electronic, blackmail crime, threat, investigation, evidence, digital evidence .