Ministère de l'Enseignement supérieur
et de la Recherche Scientifique

Université de Ghardaïa

Faculté des Sciences et des Sciences Appliquées
Département de Droit

شهادة تصحيح

يشهد ... الأستاذ فيصل رمون .....

بصفته رئيسا ... الأستاذ فيصل رمون ..... في لجنة المناقشة لمذكرة

الماستر

الطالب(ة): ميمونة ناصر ..... رقم التسجيل: 239307394.48

الطالب(ة): ..... رقم التسجيل: .....

تخصص: قانون جنائي وعلوم جنائية دفعة: 2023 - 2024 م ... لنظام ل م د

أن المذكرة المعنونة بـ: آليات القانونية لحماية الأشخاص في الجزائر الإلكتروني -

.....

.....

تم تصحيحها من طرف الطالب الطالبين وهي صالحة للإيداع

غرداية في .....

إمضاء الأستاذ رئيس اللجنة المكلف بمتابعة التصحيح

الأستاذ فيصل رمون

رئيس القسم

جامعة غرداية
كلية الحقوق والعلوم السياسية
قسم الحقوق

الآليات القانونية لحماية الأشخاص من جريمة الإبتزاز الإلكتروني

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق
تخصص القانون الجنائي والعلوم الجنائية

إعداد الطالبة
ميمونة ثامر

إشراف الدكتور
عبد الكريم بوحميدة

لجنة المناقشة

إسم ولقب الأستاذ	الرتبة	الجامعة	الصفة
فيصل رمون	أستاذ دكتور	جامعة غرداية	رئيسا
عبد الكريم بوحميدة	أستاذ محاضر أ	جامعة غرداية	مشرفا مقررا
صفاء هاجر خالدي	أستاذ محاضر أ	جامعة غرداية	عضوا مناقشا

السنة الجامعية: 1444-1445هـ / 2023-2024م

أعوذ بالله من الشيطان الرجيم

﴿..وَأَن لَّيْسَ لِلْإِنسَانِ إِلَّا مَا سَعَى..﴾

"الآية 39 سورة النجم"

إذا غامرت في شرف مروم

فلا تقنع بما دون النجوم

فطعم الموت في أمر صغير

كطعم الموت في أمر عظيم.

أبو الطيب المتنبي

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات. الحمد لله الذي وفقني لإتمام هذا العمل.

بداية أتقدم بأسمى آيات الشكر والامتنان والتقدير والعرفان بالجميل إلى الأستاذ الفاضل الدكتور عبد الكريم بوحميدة، الذي قبل الإشراف على هذه المذكرة، ولم يدخر جهدا ولا وقتا في توجيهي وإرشادي لإخراج هذا العمل إلى حيز الوجود، فشكرا على سعة صدره ورحابة نفسه ولا يسعني إلا أن أجزل في الشكر له فأقول: آتاك الله من فضله العظيم وجزاك المولى الجنة.

كما أتقدم بالامتنان والشكر الموصول للسادة الأساتذة: أعضاء لجنة المناقشة، لتفضلهم على قبول مناقشة هذه المذكرة، لسد خللها وتبيان مواطن القصور فأستدرك النقائص فيها، بإبداء ملاحظاتهم القيمة.

وأتقدم بالشكر لكل من قدم لي العون خاصة أساتذتي من الطور الإبتدائي إلى الجامعي، وكذا الوالدين الكريمين وزوجي وكافة الأهل مصداقا لقول المصطفى عليه أفضل الصلاة والسلام «لا يَشْكُرُ اللَّهَ مَنْ لا يَشْكُرُ النَّاسَ» حديثُ صحيح صححه الألباني.

إهداء

إلى زهرة فؤادي ومنبع الحب والحنان، أمي الحبيبة. حفظك الله ورعاك وجعلك سيدة من سيدات الجنة.

إلى تاج الرأس وفخري في الحياة، أبي الغالي. ألبسك الله لباس العافية ورزقك الفردوس الأعلى.

إلى من أشد عضدي بهم إلى رفاق دربي وشركاء طفولتي إخوتي وأختي الأعزاء. إلى كل أفراد عائلتي، حفظكم الله ووفقكم لما يحب ويرضى.

إلى شقيق روحي، زوجي الغالي آتاك الله من فضله العظيم.

إلى ألماستاي أشواق ريحانة وريتاج تماضر وقرة عيني بشير إقبال جعلكم الله ذخرا للإسلام

إلى كل من دعمني وأنار دربي إلى كل من أحب.

اهدي ثمرة جهدي وعملي المتواضع هذا.

قائمة المختصرات

المختصر	المدلول.
ج.ر	الجريدة الرسمية.
د.س.ن	دون سنة النشر.
ص	الصفحة.
ط	طبعة.
ق	قانون.
ق.ع	قانون العقوبات.
ق.إ.ج	قانون الإجراءات الجزائية.
م	المادة.

مقدمة

لقد تردد على ألسنة البعض القول بأن :"من يملك اليوم حاسوبا أو وسيلة تقنية ذكية وخدمة أنترنت، فإنه يملك من القوة والنفوذ ما قد يضاهي قوة ونفوذ قائد عسكري لفيلق من مئات الجنود والمعدات العسكرية إبان الحرب العالمية الأولى! ولأول مرة في تاريخ البشرية تغدو المعرفة الباب الأوسع والأقرب للنفوذ وكسب المال سواء المشروع: من خلال الاقتصاد المعرفي، ذلك أن ما يميز هذا العصر أنه عصر المعلومة والمعرفة والمهارة العقلية والإبداعية، أو الكسب غير المشروع. فالأنترنت منجم حقيقي يزخر بدرر كثيرة جديدة ومتنوعة وهو أيضا قمامة كبيرة تفوح بنتن رائحة القاذورات الأخلاقية والجرائم الإلكترونية والتي ينبغي التفطن لها والاحتراز من شرورها."[1]

وفي ظل الإنفجار المعلوماتي والإتصالات التي شهدها العالم خلال العقود الأخيرة، عرفنا تطورا كبيرا ومتسارعا في استخدام الأنترنت ووسائل التواصل الإجتماعي من جميع الفئات العمرية في مختلف نواحي الحياة، مما فتح آفاقا واسعة للتفاعل والتواصل بين أفراد العالم وكأنه بيت يتسامر فيه أفراده بشتى الأحاديث دون مراعاة لأي حدود.

وكما هو الحال في أي تقدم تكنولوجي، ظهرت مع هذه التطورات بعض التحديات والمخاطر، ولدت من رحم التقنية، وأضحت البيئة الإفتراضية مهدا لها، ومن بينها الجرائم الإلكترونية عامة، والإبتزاز الإلكتروني خاصة.

هذه الجريمة أوكما يحلو للبعض تسميتها جريمة "أصحاب الياقات البيضاء" حديثة نسبيا، تقوم فيها مجموعة من الفئات باستغلال التقنية العالية، وتوجيهها لتنفيذ إجرامهم قصاد فئة أخرى، جعلت منها سلعة لاستغلالهم، عن طريق التهديد عبر وسائل التواصل الاجتماعي، بإرسال رسائل تهديد أو نشر صور، مقاطع فيديو محرجة، اختراق حسابات التواصل أو استخدام برامج التجسس لمراقبة الضحية. والمشكل أن الأشخاص يتباهون

[1] عبد الباقي دعماش، ثراء الفكر وفكر الثراء، موقع الألوكة، عبر الرابط التالي:ثراء الفكر وفكر الثراء ((alukah.net تاريخ الإطلاع يوم2024/07/02 على الساعة 16:30.

بنشر خصوصياتهم وصورهم، ومارس الأطفال التقليد الأعمى دون علم بالمخاطر المحدقة بهم، مما يسبب ضررا نفسيا ومعنويا للضحايا. ففي ظل التطورات التكنولوجية المتسارعة، وتطور انتشار جرائم الإبتزاز الإلكتروني بشكل مرعب عبر الشبكة المعلوماتية، ووسائل التواصل الإجتماعي تظهر أهمية الموضوع العلمية والعملية، حيث تحمي الآليات حق خصوصية الفرد من خلال تجريم أفعال الإبتزاز التي تهدد أمن الضحية، فيجبرها على القيام بأفعال تهدد سلامتها أو سلامة الآخرين. كما تقوم بردع المجرمين من خلال وضع أحكام جزائية رادعة تحرمهم من تحقيق أهدافهم الدنيئة، إضافة إلى أنها تساعد على نشر الوعي حول مخاطر هذه الجريمة والحد من انتشارها، وتتيح للمجني عليهم الإستشارة القانونية اللازمة حول كيفية التعامل مع المبتز، وتعزز الثقة بالتكنولوجيا من خلال إلتزام الدولة بحماية مستخدمي الأنترنت. ونظرا لانتشارها المتزايد ورغبتي الشديدة في الوقوف على هذه الجريمة "الناعمة" والتي من الممكن أن أكون أنا أو أحد أفراد عائلتي أو أقاربي من ضحاياها أردت التزود بالمعرفة في هذا الجانب، هذا من الأسباب الذاتية لاختيار الموضوع. أما عن الأسباب الموضوعية فالمجتمع العربي المعروف بالعادات والتقاليد والأعراف الاجتماعية المحافظة على السمعة والشرف بات مهددا بانتشار هذه الجريمة التي تهدم أمنه واستقراره. –ولسنا بمنأى عن هذا التهديد– فحري بنا أن نتسم بالفضول لمعرفة ولو الجزء البسيط من خفاياها.

ولما كان تفشي الجريمة بل انفجارها في المجتمع بطريقة مخيفة كانت الحاجة الملحة لدراسة الآليات القانونية لحماية الأشخاص من هذه الجريمة ومن بين أهداف الدراسة:

- فهم طبيعة وخطورة جريمة الإبتزاز الإلكتروني.
- الوصول إلى معرفة الجناة.
- طرق ارتكاب الجريمة وتأثيرها على الضحايا.
- التعرف على كيفية التحقيق وإثبات الجريمة.

- مدى كفاية القوانين التشريعية والموضوعية الحالية في مكافحة ومواجهة جريمة الإبتزاز الإلكتروني.
- الهيآت المخولة بحماية الأشخاص من الإبتزاز الإلكتروني.

وأثناء البحث عن الدراسات السابقة لاحظت ندرة في الدراسات التي تناولت جريمة الإبتزاز الإلكتروني، وإن وجدت فأغلبها يركز على الجريمة الإلكترونية بصفة عامة أكثر المسؤولية "من تركيزه على الإبتزاز الإلكتروني، ومن هذه الدراسات: دراسة سارة حنش الجزائية عن التهديد عبر الوسائل الإلكترونية" حيث هدفت الدراسة إلى البحث في الإطار القانوني للمسؤولية الجزائية عن جريمة التهديد عبر الأنترنت والرسائل الإلكترونية، ومدى كفاية القوانين الحالية في مواجهة الجريمة في التشريع الأردني والعراقي وفي التشريعات المقارنة. وتضمنت الأطروحة أربع فصول: تناولت في الفصل الأول عرض مشكلة الدراسة وأهدافها، أهميتها وحدود دراستها، محدداتها ومصطلحات الدراسة، فضلا عن الدراسات السابقة والمنهجية المتبعة. أما الفصل الثاني فتضمن ماهية الجريمة ومدى خطورتها وأركانها. ليكرس الفصل الثالث صور التهديد عبر وسائل التكنولوجيا الحديثة ومدى انطباق أحكام جريمة التهديد على الوسائل الإلكترونية. ليختم الفصل الرابع بإجراءات التحري والتحقيق والمحاكمة. واعتمدت المنهج التحليلي والمقارن، وكانت الحدود الزمانية من2015 أي بعد نفاذ قانون الجرائم الإلكترونية في الأردن إلى 2019 م، وأما الحدود المكانية فشملت النصوص الجزائية في الأردن والعراق، واستعملت النصوص القانونية وأحكام المحاكم والتشريعات المقارنة كأدوات للدراسة. وخلصت إلى مجموعة من النتائج والتوصيات: أن الجرائم الإلكترونية متجددة ومتطورة لذا يجب استعمال نفس وسائل الجريمة، قبول الدليل الرقمي أمام المحاكم الجزائية، وضرورة امتلاك القاضي خلفية عن الوسائل التقنية والأنترنت.

استفدت من هذه الدراسة في إثراء الجانب النظري لدراستي، اتباع الخطوات المنهجية اللازمة للتحليل، والحصول على معلومات لإثراء بحثي.

أثناء بحثي عكفت على التنقيب على كل ما له صلة بالبحث سواء كتب أو لقاءات أو مواقع إلكترونية لأكتشف صعوبات في ندرة الكتب والمراجع التي تتكلم عن الآليات القانونية لمواجهة الإبتزاز الإلكتروني بصفة خاصة مستقلة، وخاصة الجزائرية منها، وإذا وجد مرجع عن الإبتزاز فمعظمه يتكلم عن الجريمة الإلكترونية عموما، وتختلف وجهات النظر عن بعضها البعض.

وللإجابة على الإشكالية المحورية التي طرحتها:

هل تعتبر الآليات القانونية لحماية الأشخاص من جريمة الإبتزاز الإلكتروني كفيلة للحد من هذه الظاهرة؟

وتتفرع عن هذه الإشكالية الأسئلة الفرعية التالية:

ماهي جريمة الإبتزاز الإلكتروني؟ ماهي صورها وطرق ارتكابها؟ ما أسبابها، وما مدى خطورتها؟ ما هي الهيآت المكلفة بمتابعة الأشخاص من الابتزاز الإلكتروني؟ كيف يكون التحقيق والإثبات في هذه الجرائم؟ وما الجزاءات المترتبة عنها؟

ولمعالجة هذه التساؤلات سأعتمد على المنهج الوصفي في تعريف الجريمة وتحديد بعض المفاهيم التي تقوم عليها، ووصف ماهيتها وأسبابها، وسأتبع المنهج التحليلي في تحليل بعض النصوص القانونية ذات الصلة بالموضوع، من قانون الإجراءات الجزائية الجزائرية وقانون العقوبات، إضافة إلى قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، وتحليل بعض مواد قانون العقوبات الفرنسي والمصري. إضافة إلى بعض قرارات الجمعية العامة، ومواد اتفاقية بودابست، وكذلك تحليل بعض المفاهيم والتعمق في جزئياتها وطرحها بشيء من التفصيل لما بدا لي

من أهميتها. وسيكون لزاما أن أدخل المنهج المقارن في بعض جزئيات البحث لأقارن مع القانون المصري والفرنسي والأمريكي.

تتناول حدود الدراسة الموضوعية في البحث ماهية الإبتزاز الإلكتروني وآليات حماية الأشخاص والمتمثلة في الهيآت والأشخاص المكلفين بالحماية وما يعتريهم من صعوبات في التحقيق والإثبات، والصعوبات التي تواجه السلطات القضائية والأمنية، والعقوبات المقررة بشأنها، والحدود المكانية تركز على التشريع الجزائري مع الإشارة الخفيفة للعقوبات المقررة في التشريع الفرنسي والمصري.

وللتعمق في الإشكالية أقترح خطة مقسمة إلى مبحث تمهيدي و فصلين، يتناول الفصل الأول: النظام القانوني للإبتزاز، وينقسم بدوره إلى مبحثين، حيت يتكلم المبحث الأول عن مواجهة الإبتزاز الإلكتروني في التشريع الجزائري، ويتضمن المبحث الثاني الهيآت والأشخاص المكلفة بمتابعة الإبتزاز، ليصل الحديث إلى الإجراءات القانونية في حماية الأشخاص من الإبتزاز الإلكتروني في الفصل الثاني، ويكرس المبحث الأول منه، التحقيق والإثبات وصعوبات إجراءهما، وأما المبحث الثاني فيخصص لصعوبات تحديد القانون الواجب التطبيق والمحكمة المختصة والعقوبات المترتبة في مطلبين .

مبحث تمهيدي

الأطر الدولية لمواجهة الإبتزاز الإلكتروني

يعد التواصل عبر الأنترنت وسيلة فعالة من وسائل الإتصال، وهو أحد الدعائم الأساسية في عصر المعلومات، لكن حرية استعمال الشبكة العنكبوتية يجب أن تتوازن مع الحقوق والحريات الأخرى، فمقابل الإقرار بالحرية هناك مسؤولية عند إساءة استعمالها[2]. ومع الطفرة التكنولوجية التي أدت بالعالم ان يكون مدينة صغيرة، ظهرت أنماط جديدة من الجرائم نتيجة الخدمات اللامتناهية للأنترنت والتي لا يمكن الإستغناء عنها[3].

ومن الصعوبة مواجهة الجرائم الإلكترونية بنظام قانوني لدولة منفردة بتشريعه، ما يستوجب تطوير البنية التشريعية الدولية بتطوير الآليات التقليدية، أو استحداث أخرى جديدة، وأضحى التعاون الدولي أمرا حتميا بل ضروريا.

ومن أبرز المنظمات والمجموعات التي لعبت دورا في مكافحة هذه الجريمة ووصلت لوضع آليات تعاون دولي تمخض في تشريعات عالمية أو اتفاقيات دولية: منظمة الأمم المتحدة، الشرطة الدولية، واتفاقية بودا بست، هذا في المطلب الأول تحت إسم الهيئات الدولية. والمطلب الثاني تفرد بالهيئات الإقليمية واللجان وتفرع: في الفرع الأول، للجنة الإقتصادية والإجتماعية لغرب آسيا (الإسكوا)، والجامعة العربية في الفرع الثاني.

[2] سمير عالية، الجرائم الإلكترونية ،في القانون الجديد رقم 2018/81 والمقارن، (حرية التواصل الإلكتروني والقواعد العقابية والإجرامية)، الطبعة الأولى منشورات الحلبي الحقوقية بيروت، (لبنان)، سنة 2020، ص20.

[3] عبد القادر زرقين – مصطفى قزران، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، الجزائر، المجلد الثامن، العدد2، سنة2002، ص1223.

المطلب الأول: الهيئات الدولية

نظرا لخطورة الجرائم الإلكترونية بكافة صورها وتأثيرها على كافة نواحي الحياة الاجتماعية، الاقتصادية، الأمنية والسياسية للدولة، كان جديرا بالأمر تعاون الدول وتكاثف الجهود، سواء دوليا أو إقليميا، لأجل الوصول إلى تشريعات عالمية، أو اتفاقيات دولية من شأنها التصدي للجريمة الإلكترونية بصورة عامة، ومنها جريمة الإبتزاز الإلكتروني بوصفها أحد أنواع الجرائم الإلكترونية، التي تنتهك الحياة الخاصة. ومن أبرز هذه المنظمات التي لعبت دورا لا يستهان به:

الفرع الأول: منظمة الأمم المتحدة:

عكفت منظمة الأمم المتحدة للوصول إلى توافق دولي، بوضع معايير توفير الحماية لمستخدمي الأنترنت، على إصدار العديد من القرارات لمواجهة الجريمة السيبرانية وتأمين استخدام التكنولوجيا وشبكات المعلوماتية بمشاركة وكالاتها في مختلف المفاوضات[4]، ومن أهم قراراتها:

- قرار المؤتمر الثامن المنعقد بهافانا سنة 1990 حول منع الجريمة السيبرانية ومعاملة المجرمين. توصلت منظمة الأمم المتحدة إلى إصدار قانون خاص بالجرائم المتعلقة بالحاسوب، وأشار القانون إلى:

1. تحديث القوانين وإدخال التعديلات في الجرائم الإلكترونية إذا تطلب الأمر[5].
2. رفع الوعي لدى الجماهير وتدريب القضاة من خلال إقحامهم في تكوينات ذات صلة بالجرائم المعلوماتية[6].

[4] محمد موسى جابر، المواجهة الجنائية للابتزاز الإلكتروني، مجلة الجامعة العراقية، العراق، المجلد2، العدد49، د.س.ن ص373.

[5] مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، الجزائر، المجلد12 العدد02،2019م، ص 707.

[6] نفس المرجع والصفحة.

3. التعاون مع المنظمات المهتمة بالموضوع وتدريس التعامل بالحاسوب في المناهج التعليمية [7].
4. تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة الخصوصية وحقوق الإنسان[8].
5. حماية مصالح الدولة وحقوق ضحايا جرائم الحاسوب [9].
6. ضرورة حل مشكل الإختصاص القضائي التي تثيره الجرائم المعلوماتية العابرة للحدود[10].
7. حث الدول الأعضاء على مضاعفة الأنشطة لمكافحة الجريمة، بدخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة بطريقة حديثة تتلاءم والجريمة الإلكترونية[11].
8. تعزيز الشراكة بين القطاع العام والخاص في مجال منع الجريمة الحاسوبية ومكافحتها[12].

لكن مع تزايد الجريمة ناقش مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية في جلسته المنعقدة في البرازيل من 12 إلى 19 أبريل 2010 وتوصل في هذا المؤتمر لمجموعة من الإستنتاجات منها: تحسين التعاون الدولي، سد الثغرات في التشريعات

[7] مراد مشوش، المرجع السابق، ص707.

[8] فاطمة الزهراء قرينح، كمال راشد، حماية الطفل من جريمة التهديد الإلكتروني بين التشريعين الدولي والجزائري، مجلة القانون والمجتمع، الجزائر، المجلد09، العدد 02، سنة2021، ص156.

[9] مراد مشوش مرجع سابق ص 707..

[10] ليندة شرابشة – السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية الإتجاهات الدولية في مكافحة الجريمة الإلكترونية، منصة المجلات العلمية الجزائرية، الجزائر، المجلد 01، العدد01، سنة 2009، ص245.

[11] ليندة شرابشة، المرجع نفسه، ص 245.

[12] محمد موسى جابر، مرجع سابق، ص 375.

القائمة، والنظر في توافق القوانين لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[13] .

ويعزز مكتب الأمم المتحدة المعني بالمخدرات والجريمة قدرات مكافحة الجريمة على المدى الطويل وذلك بدعم الهياكل الوطنية وتقديم المساعدة التقنية:

– الوقاية والتوعية. وجمع البيانات والبحث وتحليل جرائم الإنترنت[14] .

كما دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية، لدراسة شاملة لمواجهة الجريمة السيبرانية، بتحليلها ودراسة تحدياتها ومدى مواءمة التشريعات لها: التعاون الدولي – الأدلة الإلكترونية – مسؤولية متعهدي خدمات الإنترنت – إجراءات التحقيق – جمع المعلومات والإحصائيات المتعلقة بها – التصدي للجريمة خارج دائرة التدابير القانونية – دور القطاع الخاص في الحد من الجريمة – المساعدة التقنية الدولية[15] .

---

[13] نفس المرجع والصفحة.

[14] فاطمة الزهراء قرينح، كمال راشد، مرجع سابق ص 157.

[15] محمود محمد صفاء الدين علي شرشر – الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مجلة البحوث القانونية والإقتصادية، المنوفية، المجلد 54 العدد 03، سنة 2021، ص 535.

قرارات الجمعية العامة: لأجل سلامة استخدام التكنولوجيا وشبكات الأنترنت، تشارك وكالات الأمم المتحدة في مختلف المفاوضات لإيجاد توافق في الآراء ومن أبرز قرارات الجمعية العامة في مجال الجريمة المعلوماتية: القرار 121/45 عام 1990

- نشر دليل منع الجرائم المتصلة بأجهزة الكومبيوتر: القرار 49/54 1 ديسمبر 1999،القرار70/53 في 4 ديسمبر 28/55 في 20 نوفمبر 2000، القرار63/55 في 4 ديسمبر 2000،القرار 19/56 في 29 نوفمبر 2001.

القرار 121/56 في ديسمبر 2001. بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات، يدعو هذا القرار الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات الأخذ بعين الإعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار 53/57 في 22 نوفمبر 2002 ،القرار 32/58 في 18 ديسمبر 2003 حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي.
- قرار الجمعية العامة 239/57 في 31 جانفي 2003.القرار 199/58 في 30 جانفي 2004 الذي يدعو الدول الأعضاء إلى التعاون وإنشاء ثقافة عالمية للأمن السيبراني.

الفرع الثاني: دور الشرطة الدولية (الإنتربول).

تعتبر منظمة الشرطة الجنائية الدولية من أهم الآليات للتعاون الشرطي الدولي لمكافحة الجرائم العابرة للحدود، والتي من ضمنها الجريمة الإلكترونية وتكمن مهمتها في تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء في المنظمة[16] .

تجدر الإشارة أن الإنتربول وضعت برنامجا خاصا لمكافحة الإجرام الإلكتروني وهذا بتوفير دورات تدريبية لوضع معايير مهنية والتقيد بها ومنها:

- توحيد إجراءات التسليم وتجميع البيانات[17].
- المساعدة الدولية عند تلقي الهجمات الإلكترونية، تطوير النظم القادرة على مكافحة الجريمة والوقاية منها وتعزيز تبادل المعلومات لتيسير خدمات التحقيق والملاحقة وتسليم المجرمين[18] .

وفي ظل التطور المستمر لأساليب عمل المجرمين السيبرانيين، وضعف العمل الشرطي التقليدي في مواجهته، وجب على الشرطة الجنائية الدولية تقديم برامج تدريبية، ومشاريع وأدوات ومنصات لبناء القدرات السيبرانية، التي تتيح للشرطة مكافحة الجريمة بشكل فعال، بتزويد المركز المتعدد الإختصاصات لمكافحة الجريمة السيبرانية التابع للمنظمة بمختصين في مجال الأمن السيبراني، الذي يزود الدول بمعلومات استخبارية يمكن ترجمتها إلى تحرك عملي[19].

- القرار 29 مارس 2019 جاء بالعديد من التوصيات لمواجهة الجريمة الإلكترونية إما بحث الدول الأعضاء على التعاون وإصدار التشريعات لذلك أو تشريع صك دولي.

[16] فاطمة الزهراء قرينح، مرجع سابق، ص 158.

[17] مراد مشوش، مرجع سابق، ص 711.

[18] فاطمة الزهراء قرينح، مرجع سابق، نفس الصفحة.

[19] نفس المرجع، ص159.

وينشر المركز تقارير لتنبيه الدول إلى تهديدات جديدة وشيكة أو متطورة، وبالتالي يحمي الأشخاص من جريمة الإبتزاز الإلكتروني سواء قبل ارتكاب الجريمة أو بعدها. [20]

الفرع الثالث: دور اتفاقية بودابست في حماية الأشخاص من الإبتزاز الإلكتروني.

تعد "اتفاقية بودابست" من الإتفاقيات المهمة التي تم إبرامها لمكافحة الجرائم الإلكترونية، بل هي الإتفاقية الوحيدة المعروفة بالإتفاقية الدولية لمكافحة الجرائم التي ترتكب عبر الإنترنت[21]. وهذا لما أدركت الدول خطورة الجريمة السيبرانية وأثرها على كل المجالات بوصفها جريمة عابرة للحدود[22]، قامت بالتوقيع على المعاهدة التي كانت في العاصمة المجرية بودابست في 23 نوفمبر 2001. وقد تمت صياغة هذه الإتفاقية من قبل العديد من الأشخاص الذين يمتلكون خبرة قانونية في مجلس أوروبا، وبالتعاون مع دول أخرى، مثل اليابان، وأمريكا، وكندا، وجنوب إفريقيا، وحكومات الدول الأعضاء، وأجهزة الشرطة ،وقطاع الكومبيوتر على مستوى العالم[23] .

جاءت الإتفاقية لتكوين أرضية قانونية تعمل على:

- دعم الكفاح الدولي المشترك ضد الجريمة عبر الأنترنت و تعاون الدول الأعضاء الموقعة فيما بينها[24].
- تتبع المجرمين والمساعدة على الإستدلال عليهم وضبطهم، ورسم كيفية التحقيق في الجريمة[25].

---

[20] فاطمة الزهراء قرينح، المرجع السابق، ص 160.

[21] حسين عبد الكريم يونس خليل يونس الجندي، الإبتزاز الإلكتروني والجرائم الإلكترونية، ط1، دار كفاءة المعرفة عمان (الأردن) 2021 ص105.

[22] ليندة شرابشة، مرجع سابق، ص247.

[23] حسين عبد الكريم يونس–خليل يونس الجندي مرجع سابق ،ص105.

[24] نفسالمرجع ،ونفس الصفحة.

[25] ليندة شرابشة، مرجع سابق، ص247.

ومما يجدر الإشارة إليه أن المعاهدة ركزت على ثلاث ركائز:

1. أهمية نصوص التجريم[26].
2. أهمية النصوص الإجرائية.
3. أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم[27] .

تعد هذه المعاهدة أكثر تنوعا وإدراجا لقوانين جديدة وأنواع الجرائم.

الجهود الوقائية

مع تزايد الجرائم المعلوماتية وتشعبها فرضت العديد من الشركات ما يلي:

الحجر الصحي على أجهزتها المعلوماتية وهو منع الإتصال بالأجهزة خارج الشركة الذي يلغي العديد من الفوائد التي توفرها المعلوماتية. وفي المقابل هناك فيروسات لا تزرع في البرامج وإنما تزرع في الجهاز مباشرة. مع عدم استخدام البرامج المسروقة والمجانية، للتقليل من احتمال العدوى في الفيروس، وإعداد نسخ احتياطية[28] .

صعوبة التعاون الدولي لمكافحة الجريمة

قدمت الأنترنت خدمات متنوعة لجميع المجالات، مما زاد من حالات الإعتداءات على خصوصية وسرية المعلومات، ما يستدعي ضرورة التعاون الدولي، ذلك أن التشريع الوطني لا يكفي وحده، وتبادل الخبرات والمعلومات حول هذه الجريمة حتمية ضرورية[29].

لكن هناك عوائق تجعله صعبا مثل:

- تسارع وتيرة تطور الجريمة وعدم وجود مفهوم متفق عليه لتبيان هذه الجريمة، قصور التشريع في كافة الدول في العالم وخاصة الدول العربية، صعوبة الحصول على الدليل وعدم وجود تنسيق في الإجراءات الجنائية المتبعة بين الدول، تداخل وترابط بين شبكات المعلومات ومشكلة الإختصاص[30] .

---

[26] مراد مشوش، مرجع سابق، ص772.

[27] مراد مشوش، المرجع السابق، ص712.

[28] ليندة شرابشة، مرجع سابق، ص248.

[29] نفس المرجع، ص249.

[30] نفس المرجع، ص250.

- سهولة إخفاء الجريمة، عدم وجود توصيف موحد لجريمة الإنترنت، تعدد النظم القانونية الإجرائية بحيث يكون مسموحا في دولة وغير مسموح في دولة أخرى، الطبيعة الدولية للجريمة ومشكلة الإختصاص القضائي[31] .

سبل التغلب على المعوقات:

وجب إيجاد حلول عملية للتغلب على الصعوبات التي تواجه التعاون الدولي لمكافحة جريمة الإبتزاز الإلكتروني، ومنها:

- عقد إتفاقيات ثنائية وجماعية لمكافحة جريمة الإبتزاز الإلكتروني. ورغم ذلك تبقى غير كافية لخصوصية الجريمة واحتيال وذكاء مرتكبيها[32] .
- تكوين الإطارات تكوينا فنيا متخصصا كل حسب اختصاصه والإستعانة بخبراء الكومبيوتر عند التحقيق والمتابعة والتقاضي[33].
- إقرار التعاون الدولي والقواعد الإتفاقية وتعزيزها بالإجراءات التي تكفل ولو نسبيا مواجهة الجريمة[34] .

---

[31] عبد القادر زرقين، مصطفى قزران، مرجع سابق، ص1237.

[32] ليندة شرابشة، مرجع سابق، ص250.

[33]عبد القادر زرقين، مصطفى قزران، مرجع سابق، ص1241.

[34] انظر جاسم محمد جندل، الجرائم الإلكترونية، ط1، دار المعتز للنشر والتوزيع، عمان (الأردن)سنة 2022، ص180 وما بعدها.

وكذلك حسين عباس حميد، جريمة الإبتزاز الإلكتروني، مجلة القانون للدراسات والبحوث القانونية، جامعة ذي قار كلية القانون، العراق،المجلد 23، العدد22 سنة 2021، ص593.

المطلب الثاني

الهيئات الإقليمية واللجان في مواجهة الإبتزاز الإلكتروني

كما سبق الذكر عن خطورة جريمة الإبتزاز الإلكتروني التي تمس خصوصيات الشخص الطبيعي والمعنوي، عكفت التشريعات لسن قوانين ونهجت الدول عقد مؤتمرات واتفاقيات دولية وإقليمية لمواجهة هذه الجريمة التي امتدت آثارها لمختلف جوانب الحياة. ومن بين هاته الهيئات نذكر منها على سبيل المثال لا الحصر: اللجنة الإقتصادية والإجتماعية لغرب آسيا وجامعة الدول العربية.

الفرع الأول: دور اللجنة الإقتصادية والإجتماعية لغرب آسيا في مواجهة الإبتزاز الإلكتروني:

أعدت اللجنة الإقتصادية والإجتماعية لغرب آسيا (الإسكوا) إرشادات الإسكوا للتشريعات السيبرانية والتي تضمنت 6 محاور أساسية[35]:

1. الجرائم السيبرانية.
2. معالجة البيانات ذات الطابع الشخصي.
3. المعاملات الإلكترونية والتوقيع الإلكتروني.
4. التجارة الإلكترونية وحماية المستهلك.
5. الإتصالات الإلكترونية وحرية التعبير.
6. الملكية الفكرية في المجال المعلوماتي والسيبراني.

وقد تضمنت هذه الإرشادات نصوصا مقترحة لجملة من الجرائم عالجت فيها حماية الخصوصية وحددت جرم الإطلاع على معلومات سرية وحساسة أو إفشائها (المواد 12 – 30–31–32). وبينت العقوبات في الباب الثالث من الإرشادات بما فيها السجن والغرامة المالية ومصادرة الأجهزة الإلكترونية المستعملة في ارتكاب الجرم (المواد 52 – 53 – 54)[36].

[35] محمد موسى جابر، مرجع سابق، ص375.

[36] المرجع نفسه، ص376.

كما حددت المصطلحات ومفاهيمها مثل جريمة سيبرانية، جريمة إفشاء معلومات ذات طابع شخصي[37] .

الفرع الثاني: دور جامعة الدول العربية في مواجهة الإبتزاز الإلكتروني:

صدر القانون العربي النموذجي الإسترشادي بخصوص مكافحة الجرائم الإلكترونية (قانون الإمارات الإسترشادي لمكافحة جرائم تقنية المعلومات) كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب [38] .واعتمدت جامعة الدول العربية هذا القانون المقترح من طرف دولة الإمارات ذلك أن المجتمعات العربية على غرار بقية المجتمعات ليست بمنأى عن تهديدات الجريمة الإلكترونية. وتم اعتماد هذا القانون من قبل مجلس وزراء العدل العرب، في دورته التاسعة عشر بالقرار رقم 495 بتاريخ 8 أكتوبر 2003. واعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين، والملاحظ أنه أشار لأنواع الجرائم الإلكترونية بصفة عامة وأركانها والعقوبات التي تطبق عليها وأحال إلى التشريعات الداخلية.

كما أشار إلى حماية خصوصية الأشخاص من خطر الجرائم وكيفية تتبع المجرمين[39] . فجامعة الدول العربية حرصت على تنسيق سياستها الجنائية وإرساء آليات قانونية لتنظيم التعاون القانوني والأمني والقضائي بين أعضائها.

يذكر أن الجامعة ساهمت في جميع مراحل صياغة إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية من خلال الإقتراحات المقدمة في اجتماعات الخبراء الحكوميين[40] .

---

[37] أنظر نفس المرجع ونفس الصفحة.

[38] الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والإتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، الجزائر، المجلد 4، العدد 4، سلة 2022، ص24.

[39] يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، مخبر أثر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، الطبعة الأولى مطبعة الرمال، الوادي (الجزائر)سنة 2019، ص47.

[40] الطاهر ياكر، مرجع سابق، ص23.

الفصل الأول

النظام القانوني للإبتزاز الإلكتروني

ظهرت جريمة الإبتزاز الإلكتروني حديثا بظهور تقنيات الإتصال الحديثة، لكن هناك مظاهر سلبية نتجت عن سوء استعمال الوسائل الإلكترونية التي من المفروض أنها وجدت لخدمة البشر لا سببا في تعاستهم[41]. ونظرا لخطورة الجريمة سعى المشرع الجزائري على غرار التشريعات الدولية العربية منها والأجنبية الى مواكبة التطور التكنولوجي –الذي رافقه بروز مختلف الجرائم المعلوماتية –بصياغة نصوص قانونية لحماية الأشخاص، وخول لهيئات متابعة هذه الجريمة. فكيف تصدى المشرع الجزائري لجريمة الإبتزاز الإلكتروني؟

المبحث الأول:

مواجهة الإبتزاز الإلكتروني في التشريع الجزائري:

إن استجابة المشرعين في الدول المختلفة لمواجهة الجرائم الإلكترونية الحديثة والإبتزاز الإلكتروني والذي يعتبر من صور هذه الجرائم تختلف باختلاف درجة التقدم العلمي في هذه الدول[42].

فنجد في الدول المتقدمة مواجهة هذه الجرائم بقوانين خاصة متناسبة مع درجة الخطورة، متكيفة مع المستجدات في مجال تقنية المعلومات مثل الولايات المتحدة الأمريكية التي أصدرت مجموعة من التشريعات بداية من سنه 1984، ولحقتها فرنسا سنه 1994، البحرين 2002، الإمارات العربية 2006، السودان 2007، المملكة العربية السعودية 2008، وكما سبق الذكر في المبحث التمهيدي جامعة الدول العربية سنة 2003 [43].

أما في الجزائر فقط أعطى المشرع الجزائري حماية لحرية الأشخاص وحياتهم الخاصة في دستور 1996، والبدايات الأولى كانت في سن التشريعات لمجموعة من النصوص القانونية التي تخص الجرائم المعلوماتية عامة سنة2004 بصدور القانون 04/ 15المؤرخ في 10

[41] سعيد زيوش، ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها ،قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الإجتماعية،الجزائر، المجلد 11، العدد 01، سنة جانفي2017، ص70.

[42] سمير عالية، مرجع سابق، ص31.

[43] نفس المرجع، ص32.

نوفمبر 2004 المعدل والمتمم للأمر رقم156/66 المتضمن قانون العقوبات، ولما انتشرت الجرائم الإلكترونية خصه بتعديل سنة 2006[44].

يذكر أن قانون الوقاية رقم 04/09 أدرج جرائم المعالجة الآلية للمعطيات ضمن جرائم الإنترنت[45].

لكن ما هو الإبتزاز الإلكتروني؟ وما مدى خطورته؟ كيف يتم ارتكابه؟ وماهي صوره واركانه؟ ما هي الهيئات والأشخاص المكلفة بمتابعته حين ارتكابه؟ للإجابة عن هذه الأسئلة تدرجت في الإجابة كالآتي:

المطلب الأول:

مفهوم جريمة الإبتزاز الإلكتروني، مدى خطورتها، صورها وطرق ارتكابها.

من أكبر المخاطر التي تواجه مستخدمي شبكه الإنترنت والأجهزة الذكية عدم درايتهم عن أمن المعلومات، وفي المقابل استغلال مجموعة إجرامية هذه التقنيات لتنفيذ مبتغاهم، بجعل المجني عليه سلعة لاستغلاله، عن طريق التهديد والإبتزاز الذي يؤدي بالوضع النفسي السيء للضحية. فالإبتزاز مشابه لعملية سرقة البيوت وإجبار الضحايا على جلب اموالهم جميعا تحت التهديد بالقتل، ولكن إلكترونيا تهديد بنشر صور أو معلومات سرية وفضحها مقابل مبالغ مالية[46].

---

[44] اية لوصيف، قراءة قانونية هامة في جنحة الإبتزاز حسب القانون الجزائري، موقع محاماة نت عبر الرابط التالي: قراءة قانونية هامة في جنحة الإبتزاز حسب القانون الجزائري 2024 ((mohamah.net تاريخ الإطلاع 01 فيفري 2024، الساعة 16:00.

[45] بجاد عبد الرؤوف بوديسة، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الإبراهيمي برج بوعريريج، السنة الجامعية 2021-2022، ص أ.

[46] حسين عبد الكريم يونس، خليل يونس الجندي، مرجع سابق، ص50.

الفرع الأول مفهوم جريمة الإبتزاز الإلكتروني ومدى خطورتها:

تعد جريمة الإبتزاز الإلكتروني من الجرائم التي تمثل ضربا من ضروب الذكاء الإجرامي وهي من أكثر الجرائم المعلوماتية انتشارا، وهي جريمة غير أخلاقية.

اولا: تعريف جريمة الإبتزاز الإلكتروني:

I. لغة: البز وهو السلب، فالإبتزاز هو الحصول على المنافع والمال من شخص تحت الإكراه والتهديد بفضح بعض أسراره، أو أخباره أو صوره حيث لا يرغب بنشرها وتكون بغرض التشهير[47].

بزَ وتطلق على أمور منها الثياب والسلاح والنزع وأخذ الشيء بجفاء وقهر وتجريد، وفي المثل من عز بزَ أي قهر واغتصب، وبز ثوبه عنه وبز قرينه بزا أي غلبه وسلبه[48].

II. اصطلاحا: ونتطرق هنا للتعريف التشريعي والفقهي

1) التعريف التشريعي: لم يتطرق المشرع الجزائري لتعريف جريمة التهديد الإلكتروني كما عرفها المشرع الفرنسي والمصري والإماراتي والسعودي[49]، ونظرا لتزايد الجرائم الإلكترونية حاول تطوير المنظومة القانونية وإصدار تشريعات تواكب التطور التكنولوجي مثل تعديل القانون 15/04 سابق الذكر، والقانون04/09 المؤرخ في05 سبتمبر2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وإصدار القانون 07/18 المؤرخ بتاريخ 10 جوان 2018 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[50].

---

[47] منصور عبد السلام عبد الحميد حسان، جريمة الإبتزاز الإلكتروني، دراسة مقارنة بين القانون المصري والفرنسي والإماراتي والنظام السعودي، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، المجلد17، العدد5، اوت2023، ص878 و879.

[48] وائل سليم عبد الله شاطر، الإطار القانوني لجريمة الإبتزاز الإلكتروني في الألعاب الإلكترونية، دراسة مقارنة وفق النظام السعودي والقانون الكويتي، المجلة العربية للنشر العلمي، جدة، المملكة العربية السعودية، العدد 16، 2شباط2020، ص428.

[49] أنظر منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص880 وما بعدها.

[50] مريم عراب، جريمة التهديد الإلكتروني، مجلة الدراسات القانونية، الجزائر، المجلد07، العدد01، سنة2021، ص1206.

2) التعريف الفقهي: اجتهد الفقهاء في إيجاد تعريف لجريمة الإبتزاز الإلكتروني وعموما نقول: "الإبتزاز الإلكتروني هو تهديد الجاني للمجني عليه عبر وسيلة إلكترونية، سواء أكان 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، لحمله على القيام بفعل أو امتناع، وسواء كان هذا الفعل أو الإمتناع مشروعا أم غير مشروع ."[51]

"كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخدشة للشرف وقد يحمله التهديد تحت تأثير ذلك الخوف إلى استجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب ."[52]

ثانيا: مدى خطورة جريمة الإبتزاز الإلكتروني:

ظهرت جريمة الإبتزاز الإلكتروني نتاج تقنية المعلومات التي أكسبتها لونا وطابعا خاصا يختلف عن الجرائم التقليدية ومن بين خصائصها[53]:

- سهولة وسرعة التنفيذ، وسهولة الوقوع في فخها بسبب غياب الرقابة الأمنية [54].
- صعوبة اكتشافها إلا باستخدام وسائل أمنية ذات تقنية عالية.[55]
- عابرة للحدود مما يترتب عليها تنازع الإختصاص[56].
- صعوبة قياس الضرر المترتب عليها كونه يمس الكيان المعنوي[57].

---

[51] باقر غازي حنون، حسن حماد حميد، جريمة الإبتزاز الإلكتروني (دراسة مقارنة)، مجلة دراسات البصرة، جامعة البصرة مركز دراسات البصرة والخليج العربي، العراق، المجلد 16 العدد42، ديسمبر 2021، ص53.

[52] مريم عراب، مرجع سابق، ص1207.

[53] الغديان سليمان بن عبد الرزاق، خطاطبة يحيى بن مبارك وآخرون، صور جرائم الإبتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية كلية الملك فهد الأمنية – مركز البحوث والدراسات، السعودية، المجلد27، العدد69، 2018/01/31، ص180.

[54] جاسم محمد جندل، مرجع سابق، ص86.

[55] حسين عبد الكريم يونس، خليل يوسف الجندي، مرجع سابق، ص74.

[56] جاسم مجمد جندل، مرجع سابق، ص.

[57] حسين عبد الكريم يونس، خليل يوسف الجندي نفس المرجع والصفحة.

- تعد جرائم دون عنف (جرائم ناعمة)[58].
- ذكاء وحرفية الجاني وتزوده بالعلم والثقافة التكنولوجية[59].
- سهولة إتلاف الأدلة من طرف الجناة[60].
- قلة الإبلاغ عن الجريمة إما لعدم اكتشاف الضحية لها، أو خوفا من التشهير[61].

إن عدوى التواصل الإجتماعي عبر شبكة الأنترنت من خلال مواقع الدردشة وموضة التباهي بالصور والفيديوهات، وجعل الحياة الخاصة ملكا لكل رواد الشبكة العنكبوتية، في المقابل وجود مستغلي التقنية بدهاء كما تم ذكره، أوجد آثارا خطيرة نذكر منها على سبيل المثال:

الآثار النفسية:

- عدم قدرة المجني عليه طلب المساعدة بسبب الإحراج أو الجهل بأساليب الوقاية، قلق، اضطرابات النوم، خوف، عدم التركيز، الشعور الدائم بالذنب، فقد الثقة في الآخرين، العدوانية.[62]
- العزلة وربما الهجرة من بلاده، وكردة فعل يمكن أن يتحول من ضحية إلى مجرم يمارس ما مورس عليه على آخرين.
- ومن أشد آثار الإبتزاز الإلكتروني أن يقدم الضحية على الإنتحار.

الآثار الاجتماعية:

- التفكك الأسري: قد تنصاع الفتيات خوفا من الفضيحة لرغبة المجرم (اغتصاب، فحمل، فإجهاض او قتل لطفل غير شرعي أو التخلي عنه وحيدا او قتلها من ذويها.
- تشويه السمعة.

---

[58] علي ابراهيم بن دراج، محاضرات في الجرائم المعلوماتية، مقدمة للسنة الثانية ماستر تخصص جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي آفلو، الأغواط، لعام2020 /2021، ص8.

[59] سمير عالية، مرجع سابق، ص70.

[60] محمد موسى جابر، مرجع سابق، ص373.

[61] سمير عالية، مرجع سابق، ص70.

[62] زينب محمود حسين، المواجهة الجنائية للابتزاز الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية كركوك، العراق، المجلد 10، العدد 37، العام 2021، ص580.

الآثار الأمنية[63] :

- تفشي الفساد وانهيار القيم والإخلاق.
- العبث بأمن المجتمع مثل السرقة والنصب والقتل لعدم حصول الضحية على المال المطلوب من الجاني.
- انتشار الفوضى وعدم الطمأنينة.

الآثار الشرعية:

وهي من أعظم الآثار وتتلخص في معصية الخالق وسخطه[64].

الفرع الثاني: صورها وطرق ارتكابها:

يتخذ الإبتزاز الإلكتروني عدة صور متشعبة بحسب الزاوية المنظور منها إليه، ووفقا للنموذج الإجرامي فإن الجريمة لا تقع حتى تجتمع أركانها.

أولا: صور التهديد والإبتزاز الإلكتروني: قبل التطرق لصور الإبتزاز الإلكتروني يجدر بنا ذكر طريقته وهي إما كتابيا أو شفهيا.

التهديد الإلكتروني الكتابي: وهو إرسال الجاني للضحية رسالة إلكترونية عبر وسائل الإتصال الحديثة تتضمن عبارات تهديد أو صور ورموز وشعارات تحمل مشاهد عنف كصورة خنجر على الصدر أو خنجر يقطر دما تبث في نفسيته القلق والرعب[65].

التهديد الإلكتروني الشفهي: ويكون إما مكالمة هاتفية عبر النقال، أو إرسال تسجيل صوتي أو فيديو عبر غرف الدردشة بأسماء مجهولة، أو حتى معروفة لدى المجني عليهم، لكنهم يهددونهم بعدم الإفصاح عن شخصيتهم لأي أحد حتى لا ينكشف أمرهم[66]. والجدير بالذكر أن هذا الجاني صديق مفترض للضحية استدرجها المبتز للقيام بأفعال مخلة بالحياء مصورة

---

[63] برحال امال، جريمة الإبتزاز عبر الوسائل الإلكترونية، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي التبسي، تبسة 2019 /2020، صفحة 32.

[64] الغديان سليمان بن عبد الرزاق، خطاطبة يحيى بن مبارك وآخرون، مرجع سابق، ص179.

[65] فاطمة الزهراء قرينح، كمال راشد، مرجع سابق، ص152.

[66] نفس المرجع، ص153.

وتهديدها بها للحصول على المال أو الإستمرار بالقيام بالأفعال المشينة أو إرغام المجني عليه على أفعال يقوم بها لصالح الجاني[67].

وتكون صور الإبتزاز الإلكتروني:

- بحسب شخص الضحية: يكون للإبتزاز صورا تبعا لشخصية المجني عليه فقد تكون الضحية[68]:

1. شخصية اعتبارية من الحكومات والشركات والمؤسسات: تتم الجريمة عن طريق تطفل، أو دخول على مواقع مهمة للحصول على معلومات سرية، والسطو عليها، والتهديد بإعلان أو نشر هذه المعلومات للآخرين[69].
2. الأحداث: يختلف تعريف الأحداث حسب التشريعات، وهذا لاختلاف تحديد السن القانونية، والأحداث يسهل استدراجهم، لأنهم أكثر الفئات ولعا وارتباطا بالتكنولوجيا ووسائل التواصل الإجتماعي ولصغر سنهم وقله خبرتهم. يقوم المبتز بالضغط على الحدث بتهديده بنشر صور، أو تسجيل مرئي، أو محادثات على مواقع الدردشة ،أو وقائع لا يريد الحدث إطلاع أحد عليها[70]،أو من شأنها تحقيره أمام أهله ومحيطه الإجتماعي[71].
3. النساء: وهن أكثر الأنواع شهرة وانتشارا، خاصة إذا كان الجاني رجلا، فغالبا ما يكون تهديد المبتز للمرأة بنشر صور فاضحة، أو محادثات خادشة للحياء، أو فيديو لعلاقة غير شرعية جمعت المرأة بالمبتز[72]، فيهددها ويبتزها بطلب مبالغ مالية أو الإستمرار في أفعال يطلبها منها، فتضطر المرأة للإذعان لهذه الأوامر، وخاصة إذا كانت من الأحداث فتتجاوب

[67] نفس المرجع ونفس الصفحة.

[68] محمد موسى جابر، مرجع سابق، ص372.

[69] مريم عراب، مرجع سابق، ص1210.

[70] محمد موسى جابر، مرجع سابق، ص372.

[71] مريم عراب، مرجع سابق، ص 1210.

[72] محمد موسى جابر، مرجع سابق، ص372.

معه خوفا من العار[73]، وقد يفضح عملها التجاري بسبب كونها سيده أعمال، أو يقوم بفضح محادثات سرية أو إتفاقات معينة كونها سياسية [74].

4. الرجال: يكون الرجل عرضة للإبتزاز نتيجة عمله ومركزه الإجتماعي أو السياسي، أو نتيجة وجود أسرار في عائلته، ويكون نشر هذه الأسرار يمس بسمعته وشرفه، أو يثير احتقاره في مجتمعه ويؤثر سلبا على مركزه المالي[75]، كما قد يكون ضحية الإبتزاز إذا كان ميسور الحال من طرف محترفات بيع الهوى على المواقع الإلكترونية، وتهدده بنشر صور أو إذاعة مقاطع مصورة تهدد مركزه[76].

- بحسب الغاية:

يختلف الهدف الذي يسعى المبتز إلى تحقيقه من الإبتزاز باختلاف كل جريمة كما يلي:

1. هدف مادي: من أهم الأهداف التي يسعى إلى تحقيقها المبتز الهدف المالي أو العيني مقابل عدم نشر الأسرار وتختلف القيمة المادية حسب نوع الضحية إما شركة أو فرد وحسب غنى الضحية أيضا[77].
2. هدف جنسي: قد يكون الهدف من الإبتزاز جنسيا وهو الشائع إن كانت الضحية امرأة أو طفلة (حدث)، فمقابل عدم نشر الأسرار يكون الطلب من المبتز إما ممارسة الجنس معه أو القيام بهذه الأفعال مع شخص آخر غيره ولمرة واحدة أو لعدة مرات[78].

[73] مريم عراب، مرجع سابق، ص1211.

[74] محمد موسى جابر، مرجع سابق، ص372.

[75] نفس المرجع السابق ونفس الصفحة.

[76] مريم عراب، مرجع سابق، ص1211.

[77] نفس المرجع ونفس الصفحة.

[78] محمد موسى جابر، مرجع سابق، ص372.

3. هدف نفعي: كأن يطلب المبتز من الضحية القيام بأفعال لصالحه كالسرقة، أو ترويج مخدرات، أو التوسط لدى شخص لإتمام عمل، سواء كان هذا العمل مشروعا ام غير مشروع[79].

- بحسب وسائله المستعملة:

1. إبتزاز مادي إلكتروني: يستعمل المبتز التهديد بوسائل إلكترونية مادية ملموسة (صور، مستندات، مقاطع صوتية أو مرئية) عبر الأسلاك، أو الألياف البصرية، أو بطريقة كهرومغناطيسية [80].
2. إبتزاز معنوي إلكتروني: باستعمال عبارات شديده التهديد والوعيد.

ثانيا: طرق جريمة الإبتزاز الإلكتروني: هناك عده طرق يستعملها المجرم الإلكتروني للحصول على الهدف المبتغى.

- استعمال الحاسب الآلي وملحقاته وبرامجه: كل فعل غير مشروع يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية مثل:

1. الدخول غير المصرح به إلى النظام[81]، ويسمى أسلوب الولوج غير المشروع إلى المعلومات بقصد الإبتزاز، ويتكون من فعلين، الفعل الأول: الولوج غير المشروع، والفعل الثاني: الحصول على المعلومات بقصد الإبتزاز[82]، مثال قيام أحد الموظفين بالدخول على الحاسب الآلي التابع للشركة، ثم الدخول إلى المستند الخاص ببيانات الموظفين، والحصول على معلومات سرية عنهم للقيام بابتزازهم[83].
2. الاستيلاء على البيانات المخزنة.

---

[79] مريم عراب، مرجع سابق، ص1211.

[80] نفس المرجع، ونفس الصفحة.

[81] جاسم محمد جندل، مرجع سابق، ص109.

[82] منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص887.

[83] مريم عراب، مرجع سابق، ص1212.

3. استعماله كبيئة للجريمة، كجعله مخزن للمواد الإباحية والبرامج المقرصنة[84].

- الأنترنت : تعتبر الأنترنت شبكة دولية إلكترونية متعددة الأبعاد والخدمات، وهي أضخم شبكة معلومات لحواسيب منتشرة في العالم، كما تعد أداة تواصلية بين شبكات المعلوماتية دونما اعتبار للحدود الفاصلة بين الدول، فهي تحتوي على آلاف من شبكات الحواسيب المحلية والدولية المرتبطة ببعضها البعض، إما بطريق خطوط الهاتف، أو الأقمار الصناعية، وتمتد عبر العالم لتؤلف شبكة هائلة، بحيث يمكن للمستخدم الولوج إليها في أي مكان وزمان، شرط توافر حاسب آلي مزود بموديم أو هاتف نقال، متصل بشبكة الأنترنت، مع تحميل وسائط الإتصال لتلقي وإرسال البيانات[85].

1. الهاتف النقال وبرامجه: يستخدم المبتز الهاتف للقيام بجريمته مستعملا برامج التجسس المحملة، أو التصوير بالكاميرا، أو سرقة المعلومات بالبلوتوث، أو التسجيل الصوتي.
2. خدمة الدردشة: يسمح هذا البرنامج بتجمع الأشخاص من مختلف أنحاء العالم، وقد يكون من ضمن الأشخاص من يمتهن الإبتزاز الإلكتروني، فيتصيد فريسته عبر هذه الدردشات، مثل غرف ومواقع الدردشات الصوتية والكتابية.
3. البريد الإلكتروني: قد يكون البريد الإلكتروني بيئة لارتكاب جريمة الإبتزاز، عن طريق إرسال روابط مفخخة على سبيل المثال، أو سرقة الرمز السري [86].

ومن طرق الإبتزاز الإلكتروني الجديدة استغلال الدين في التواصل مع الشخص، حيث يقوم المبتز بانتحال صفة شيخ راقي يقوم بفك سحر المجني عليه، ويطلب منه إرسال صور له ومقاطع ليجعلها ماده ابتزاز لاحقا[87].

ومن بين الأساليب لكيفية حصول المبتز على المعلومات:

- أسلوب الولوج غير المشروع إلى المعلومات (سبق ذكره).

---

[84] جاسم محمد جندل، مرجع سابق، ص109.

[85] سمير عالية، مرجع سابق، ص 22 و23.

[86]مريم عراب، مرجع سابق، ص 1213.

[87] هند علي حنون، وسائل حماية الأسرة من الإبتزاز الإلكتروني، مجلة جامعة دهوك، العراق، المجلد26، العدد1، سنة2023م، ص81. وحسين عبد الكريم يونس، خليل يوسف الجندي، مرجع سابق، ص 55.

- أسلوب السرقة المعلوماتية وهو الإستيلاء على المعلومات والبيانات دون علم وإرادة صاحبها الشرعي، سواء أكانت على أسطوانات مدمجة أو أشرطة ممغنطة فيستولي عليها بتوجيهها ونقلها ونسخها إلى حاسوبه الشخصي دون رضا المجني عليه[88].
- خيانة الأمانة كوسيلة للإبتزاز الإلكتروني: وتكون بين مقدمي خدمات الإنترنت والمستفيدين منها مثل:

1) الدخول إلى شبكة الأنترنت وتقديم المساعدة الفنية. إنشاء المواقع مثل مواقع الزواج والتوظيف والتراسل عبر الماسنجر، الفايسبوك والسكايب[89].
2) تقديم خدمة البريد الإلكتروني. إنشاء المتجر الافتراضي، بيع البرامج وتأجيرها واستعمالها. عقود خدمات الهواتف النقالة[90].

المطلب الثاني

[88] منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص885.

[89] ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الإبتزاز الإلكتروني، المجلة العربية للدراسات الأمنية الرياض، السعودية، المجلد33، العدد80، سنة2017، ص 203 و204.

[90] منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص886.

أركان جريمة الإبتزاز الإلكتروني أسبابها ومراحلها

الفرع الأول: أركان جريمة الإبتزاز الإلكتروني:

يعتبر الإبتزاز الإلكتروني وسيلة من وسائل الضغط والإكراه، يقوم بها الجاني على المجني عليه بالمساس بحياته الخاصة أو التشهير به[91]، وبمعنى آخر المخالفات المرتكبة ضد أفراد أو مجموعات لإيذاء سمعة الضحية، أو إيذاءها ماديا مباشرا أو غير مباشر، باستخدام الأنترنت (البريد الإلكتروني، الحاسوب، الهاتف النقال، الألعاب الإلكترونية، مواقع التواصل الإجتماعي ...)[92].

وتقوم جريمة الإبتزاز على أركان أساسية، بدونها لا يمكن أن تكون لا جريمة ولا عقوبة. فيجب توفر الركن المادي والمكون من السلوك والنتيجة والعلاقة السببية، كما يجب توافر الإرادة الحرة الواعية والمتمثلة في الركن المعنوي.

أولا: الركن المادي لجريمة الإبتزاز الإلكتروني

يقصد بالركن المادي للجريمة السلوك الخارجي المادي الذي يجرمه القانون[93]، ويتكون من السلوك الإجرامي والنتيجة والعلاقة السببية:

- السلوك الإجرامي: يكون الركن المادي في جريمة الإبتزاز الإلكتروني بدخول الجاني بطريقة متعمدة إلى موقع إلكتروني، أو نظام معلوماتي لا يملك الجاني حق الدخول فيه، ويهدد المجني عليه للقيام بفعل أو الإمتناع عنه، سواء أكان هذا الفعل أو الإمتناع مشروعا أو غير مشروع.[94] ويتمثل الركن المادي في التهديد المقترن بطلب، وشرطه أن يكون إيذاء أو

  يترك أثرا في نفس المجني عليه، يدفعه إلى تنفيذ طلب المبتز دون إرادته. كأن يكون الطلب ماديا أو جنسيا وإذا رفض المجني عليه ينفذ الجاني تهديده.[95]

  قد يكون السلوك الإجرامي تهديدا أو تشهيرا أو إلحاق الضرر بالمجني عليه:

---

[91] منصور عبد السلام عبد الحميد حسان، المرجع السابق، ص899.

[92] مريم عراب، مرجع سابق، ص 1207.

[93] برحال آمال، مرجع سابق، ص42.

[94] ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص 207 و208.

[95] باقر غازي حنون وحسن حماد حميد، مرجع سابق، ص63.

1) التهديد: هو فعل إجرامي من الجاني إلى المجني عليه ينال من حريته وطمأنينته، وقد يمتد إلى حواشي المجني عليه الذين يهمه أمرهم كزوجته وأبنائه[96]. والتهديد الإلكتروني لا يختلف عن التهديد التقليدي سواء شفاهة أو كتابة أو رموزا أو شعارات. إما بنشر بيانات أو صور أو مقاطع فيديو حصل عليها بطريق الإختراق، أو سرقة جهاز الضحية، وسواء أكان التهديد عن طريق البريد الإلكتروني، أو غرف الدردشة، أو التسجيل الصوتي أو المنتديات، ما من شأنه أن يكون المجني عليه تحت رحمة الجاني، ولا يهم هذا الأخير أن ينوي تنفيذ الأمر المهدد به أم لا، المهم ألا يكون التهديد هزليا[97]. فيكفي لتحقيق التهديد أن يكون من شأنه ترويع المجني عليه، بحيث يحمله على تنفيذ طلبات المبتز. بل ويعتبر أيضا تهديدا إخبار شخص آخر وقام هذا الأخير بنقل التهديد للمجني عليه[98].

2) التشهير بالآخرين: لكل فرد الحق في إخفاء حياته الخاصة التي يحميها القانون باعتبارها ملكا له، ولا يجوز الإطلاع عليها دون رضاه. إلا أنه نتيجة التقدم التكنولوجي في الأجهزة المستحدثة، أصبح من السهل اجتياز أي حاجز من تسجيل أو تصوير أو نقل الأحاديث ونسخها، لقذف وتشويه سمعة الأشخاص، أو طبيعة عملهم، أو التعرض لأسرهم بهدف الإبتزاز أو الإنتقام أو لمجرد الضرر[99]. وقد حصل أن قام تلميذ في الثانوية بتصوير أستاذته التي منحته علامة صفر في مادة مهمة وأطلق الشائعات في صفحة فيسبوك مزيفة باسمها.

3) مدى توافر ركن الضرر في جريمة الإبتزاز الإلكتروني: الضرر هو ما يصيب الإنسان في حق من حقوقه أو في مصلحة مشروعة له، وهو إما ضرر مادي يلحق الإنسان في ماله أو جسده[100]:

---

[96] ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص208.

[97] مريم عراب، مرجع سابق، ص 1208.

[98] ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص209.

[99] نفس المرجع والصفحة.

[100] نفس المرجع، ص211.

- التهديد الذي يكون محله الجسد ويكون بالعنف ضد الجسد مثل القتل أو الضرب[101].
- التهديد الذي يكون محله المال كأن يهدد المجني عليه بترك وظيفته وإلا سيقوم الجاني بحرق منزله[102].

أو ضرر معنوي، كأن ينصب الإيذاء على الشرف والسمعة أو المكانة الإجتماعية أو المركز الوظيفي، كمن يسند له أنه يتردد على محلات الدعارة أو فار من مستشفى الأمراض العقلية[103].

وبالتالي الضرر المتطلب هو الضرر المحتمل حتى ولو يلحق ضررا، باعتبار أن الفعل بحد ذاته جريمة مثل التصنت، والإلتقاط ،والدخول غير المشروع إلى موقع إلكتروني[104]، أو عن طريق استدراج الضحية في مراسلات وأحاديث للحصول على معلومات أو صور لاستخدامها فيما بعد للإبتزاز، وإجبار المجني عليه لتنفيذ رغباته، ولخشية الفضيحة ينفذها هذا الأخير[105].

- النتيجة: تقع النتيجة الجرمية في جريمة الإبتزاز الإلكتروني لمجرد قيام المبتز بتهديد الضحية بإفشاء سر من أسرارها سواء فعل المجني عليه ما طلب منه أو لم يفعل.[106]
- العلاقة السببية: وهو أن يكون تنفيذ الضحية لطلب المبتز نتيجة التهديد الذي أثر في نفسية المجني عليه وترك خوفا ورعبا[107].

---

[101] باقر غازي حنون، حسن حماد حميد، مرجع سابق، ص63 و64.

[102] نفس المرجع والصفحة.

[103] نفس المرجع، ص 65.

[104] ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص212.

[105] منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص906.

[106] بوالشعير الحسن، حداد شعيب، جريمة الإبتزاز الإلكتروني – دراسة مقارنة –مذكرة مقدمة لاستكمال متطلبات شهادة الماستر مهني في القانون العام، تخصص قانون الإعلام الآلي والأنترنت، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الإبراهيمي برج بوعريريج سنة 2022/ 2023، ص59.

[107] أنظر باقر غازي حنون وحسن حماد حميد، مرجع سابق، ص 68.

ثانيا: الركن المعنوي: هو الركن الثاني الذي تقوم عليه جريمة الإبتزاز الإلكتروني والجانب النفسي للجاني، باعتبار الجانب المادي هو السلوك المكون للجريمة. ويعبر عنه بالقصد الجنائي (العلم والإرادة)[108].

- العلم: أن يعلم الجاني وقت اقتراف فعله أن المنفعة التي حصل عليها هي ثمرة التهديد الذي صدر عنه، وأنه ليس له الحق فيما يلزم الضحية بتنفيذه[109]. فلا بد أن يعلم الجاني بنتيجة السلوك المرتكب، والحصول على صور فاضحة، مقابل الحصول على منفعة جريمة يعاقب عليها القانون[110]. وقد أكد القضاء الفرنسي ذلك حينما قررت محكمة النقض الفرنسية " أن القصد الجنائي يتوافر حين يدرك الشخص أنه يحصل بالقوة أو بالعنف أو الإكراه ما كان لا يمكن الحصول عليه من خلال إتفاق طوعي .[111]"
- الإرادة: يجب أن تتجه إرادة الجاني في جريمة الإبتزاز الإلكتروني إلى تهديد المجني عليه لإرغامه على تنفيذ طلباته، كما أكدت ذلك محكمة النقض الفرنسية. "إن توافر القصد الجنائي يشترط أن تتجه نية الشخص إلى استخدام تهديدات غير مشروعة لإلزام الآخرين بالدخول في التزامات أو تحويل أموال دون إرادتهم أو لا مبرر لها"[112]. ولكي تقوم المسؤولية الجنائية يجب أن تكون إرادة الفاعل قد اتجهت إلى القيام بالفعل المجرم دون أن يكون هناك عيب في هذه الإرادة. كأن يكون الجاني مكرها على القيام بالفعل المجرّم[113]. كما يجب أن تتجه إرادة المبتز إلى تحقيق النتيجة من سلوكه المجرّم، كالحصول على منفعة مالية أو جنسية، ولا عبرة للباعث أن يكون نبيلا أو غير ذلك في قيام المسؤولية الجنائية، كأن يكون الباعث الحصول على أموال لأمه المريضة، فبتوافر القصد الجنائي العام تقوم جريمة الإبتزاز

---

[108] أنظر منصور عبد السلام عبد الحميد حسان، مرجع سابق، ص906 و907.

[109] باقر غازي حنون، حسن حماد حميد، مرجع سابق، ص69.

[110] مريم عراب، مرجع سابق، ص 1208.

[111] باقر غازي حنون، حسن حماد حميد، مرجع سابق، ص70.

[112] نفس المرجع والصفحة.

[113] مريم عراب، مرجع سابق، ص 1208 و1209.

الإلكتروني التي تعتبر من الجرائم التي تحتاج إلى احتراف تكنولوجيا المعلومات بمهارة من أجل تنفيذها، فلا يمكن تصور حصولها من دون قصد، ولا حاجة لشرط توفر القصد الجنائي الخاص لأنها جرائم عمدية. كما يجب أن يكون التهديد جدّي بدرجة كافية للتأثير في نفسية الضحية[114].

ثالثا: الركن الشرعي لجريمة الإبتزاز الإلكتروني

يعتبر الركن الشرعي في الجريمة هو نص التجريم والعقاب، ومبدأ الشرعية يقتضي في جميع التشريعات أن "لا جريمة ولا عقوبة إلا بنص". فالنصوص القانونية هي جدار حماية لأمن الإنسان وخصوصيته. وأي شخص يحاول كسر هذه الحواجز أو اختراقها يعد مدانا ويستحق العقاب المقرر لفعله[115]. ومع تزايد الجرائم الإلكترونية، باشرت معظم الدول لمواجهتها إما بسن تشريع قانون مستقل، أو الإكتفاء بتطبيق النصوص التقليدية أو إدخال تعديلات عليها وذلك بحسب قدراتها وظروفها ومصالحها[116]. فالركن الشرعي هو تجريم الفعل ووضع العقوبة المقررة له، ومعظم الدول سنت تشريعا جنائيا للجريمة الإلكترونية والتهديد الإلكتروني.

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

ففي المادة 39 من دستور 1996 نصت على ما يلي" : لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه[117]"، والمادة 24 من المرسوم الرئاسي المتعلق بالمنظومة الإحصائية» لا يحق للمصلحة المؤتمنة أن تكشف أو تنشر المعلومات الفردية الواردة في الإستمارات التي تنص على التسجيل الإحصائي ولها علاقة بالحياة الشخصية والعائلية وعلى العموم الوقائع والتصرفات الخصوصيةِ ، ورتبت العقاب عند استعمال المعلومات الشخصية المتحصل عليها

---

[114] مريم عراب، المرجع السابق، ص 1209.

[115] باقر غازي حنون، حسن حماد حميد، مرجع سابق، ص71.

[116] مريم عراب، مرجع سابق، ص 1209.

[117]عدلت في التعديل الدستوري01/16 بالمادة1/40–2. والمادة 3/46 والتي تنص على "... حماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".

من طرف أجهزة المنظومة الإحصائية بهدف المساس بالحق في الحياة الخاصة، وذلك بموجب المادة 3/25 من نفس المرسوم.[118]

كما نص المشرع الجزائري من خلال المواد 284 – 285– 286 و287 في قانون العقوبات الجزائري على جريمة التهديد وطرقها والعقوبة المقررة لكل طريقة:

المادة 284 ق.ع.ج أشارت إلى التهديد الكتابي، وهو أشد وأخطر من التهديد الشفهي المشار إليه في المادة 286 ق ع ج، كونه يصدر عن تصميم وتفكير مسبق عكس التهديد الشفهي الصادر عن انفعال عارض (تشديد العقوبة في التهديد الكتابي)[119].

الملاحظ في المادة 285 ق.ع.ج أن التشديد في العقوبة في التهديد المصحوب بأمر أو شرط، وهذا لأنه يمتد إلى حرية المجني عليه، والتأثير على إرادته وحمله على القيام بأمر لا يلزمه القانون أو منعه من عمل مشروع، إضافة إلى تكدير أمنه وسكينته وإلقاء الخوف والرعب في نفسه. أما التهديد غير المصحوب بأمر فيلقي الرعب في نفس المجني عليه ويكدر أمنه وسكينته دون طلب القيام بفعل أو طلب الإمتناع عن القيام بفعل آخر[120]. (فالمشرع الجزائري وسع في التهديد الكتابي وقلص في التهديد الشفهي حيث جعله مقترنا بأمر أو شرط).

المادة 287: جاءت المادة 287 ق.ع.ج لتوسع من حالات التهديد بعد الحصر في المادة 284 ق ع ج لكن مع الإبقاء على نفس الطرق المذكورة في المواد 284،285 و286 من

ق ع ج. مثال على الحالات المنصوص عليها في المادة 287 ق ع ج: التهديد بالضرب أو الجرح أو التعذيب أو الإعتداء الجنسي ...الخ. والأجدر أن ينص المشرع الجزائري على جريمة

[118] بن حيدة محمد، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 01/16، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر، لمجلد الأول، العدد 10، جوان2018، ص45.

[119] فاطمة الزهراء قرينح، كمال راشد، مرجع سابق، ص162.

[120] نفس المرجع، ص163.

الإبتزاز الإلكتروني ويوليها عناية خاصة ذلك أن التواصل الإلكتروني في تزايد كثيف وتكثر معه الجرائم والتهديدات الإلكترونية.[121]

ونصّ المشرّع في المواد من 296 إلى 303 مكرر2 في قانون العقوبات الجزائري تحت إسم الإعتداءات على شرف واعتبار الأشخاص وعلى حياتهم الخاصة وإفشاء الأسرار من الفصل الأول من الباب الثاني تحت عنوان "الجنايات والجنح ضد الإفراد[122].

المادة 303 مكرر و303 مكرر1 من قانون العقوبات الجزائري والمستوحى من قانون العقوبات الفرنسي الجديد لسنة 1992 في المادة 2/226 قانون العقوبات الفرنسي والتي تجرم نشر صور وفيديوهات ومواد مخلة بالحياء أو حيازتها بأي طريقة كانت أو تداولها علنا بأي طريقة متوقعة ومنها النشر عبر مواقع التواصل الإجتماعي[123] .

جاء النص في المادة 303 عام إذ شمل الرسائل والمراسلات بما في ذلك رسائل البريد الإلكتروني أو السكايب أو أي تقنية أخرى[124].

لم يشدد المشرع في المادة 303 مكرر في الجريمة المرتكبة بالتقنية رغم أن كل الحواسيب والهواتف النقالة مجهزة بكاميرات ولواقط الصوت. وجرم في المادة 303 مكرر 1 الأفعال التالية: التسجيلات السمعية أو السمعية البصرية، صور، وثائق، بيانات شخصية والمتحصل عليها بواسطة الإلتقاط أو النقل أو التسجيل (م303 مكرر) إضافة إلى الإحتفاظ أو الوضع

---

[121] فاطمة الزهراء قرينح، كمال راشد المرجع السابق، ص164.

[122] قانون رقم 06-23. مؤرخ في 29 ذي القعدة 1427 الموافق ل 20 ديسمبر 2006. يعدل ويتمم الإمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق ل 8 جوان 1966 والمتضمن قانون العقوبات. ج.ر العدد84، الصادر في 4 ذي الحجة 1427هـ الموافق ل 24 ديسمبر 2006.

[123] فاطمة العرفي، الحماية القانونية للحق في الخصوصية للأطفال من جريمة التشهير عبر مواقع التواصل الإجتماعي في القانون الجزائري، مجلة الإجتهاد القضائي، مخبر الإجتهاد القضائي على حركة التشريع، بسكرة، الجزائر، المجلد12، العدد 02، أكتوبر 2020، ص543.

[124] مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، الجزائر المجلد السابع، العدد01، سنة 2018 م، ص475.

في متناول الجمهور أو الغير أو الإمتناع عن منع وضعها في متناول الجمهور أو الغير أو الإستخدام بأي وسيلة كانت.

لم يلتفت المشرع الجزائري إلى الوسيلة المستخدمة في ارتكاب الجريمة بل جعلها عامة وبالتالي تدخل الجرائم المرتكبة بالتقنية ضمن هذه المادة[125].

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

تبنى المشرع الجزائري الشمولية في تجريمه للأفعال التي يكون مسرحها إلكتروني من خلال القانون رقم04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. وأحالنا إلى القواعد التقليدية المطبقة على جريمة التهديد الكلاسيكية (الماد 02 من قانون 04/09)[127]. والابتزاز الإلكتروني صورة مستجدة من الإبتزاز العادي المنصوص عليه في قانون العقوبات المادة 371[128].

الفرع الثاني: أسباب الإبتزاز الإلكتروني ومراحله:

أولا:أسباب الإبتزاز الإلكتروني:

[125] المرجع السابق ص476.

[126]فاطمة العرفي، مرجع سابق، ص544.

[127] بوالشعير الحسن، حداد شعيب، مرجع سابق، ص54.

[128] قانون 06-23 سابق الذكر.

أسباب الإبتزاز الإلكتروني كثيرة ومتنوعة، وما يتفق عليه أن من يمارسه إنسان غير سوي، بل قد يكون المجني عليه أيضا متواطئ في الجريمة ومسؤول مسؤولية مباشرة في الإبتزاز الموجه إليه. من بين الأسباب:

1) ضعف الوازع الديني والفراغ الروحي سواء عند المبتز أو الضحية[129].
2) قلة الوعي بوسائل التكنولوجيا[130].
3) عدم المراقبة الأبوية، وعدم الشعور بالإنتماء إلى الأسرة أو الأصدقاء أو المحيطين بالشخص الضحية أو حتى المبتز[131].
4) هوس الشباب بالتقليد ومحاولة عيش المغامرات[132].
5) سوء التنشئة الإجتماعية وضعف الضبط الإجتماعي[133].
6) رغبة الجاني في الحصول على منفعة مادية أو معنوية أو جنسية.
7) التفكك الأسري[134]
8) الفقر والبطالة والظروف الإقتصادية الصعبة ومن جانب آخر قد يكون الترف والغنى سببا للإبتزاز أيضا[135].
9) انتشار الرذيلة وعدم وجود القدوة.

---

[129] محمد سعيد عبد العاطي محمد، محمد أحمد المنشاوي محمد، دور القانون الجنائي في حماية الطفل من الإبتزاز الإلكتروني (دراسة مقارنة)، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون، قرع جامعة الأزهر، دمنهور، محافظة البحيرة، المجلد 33، العدد 36، سنة2021، ص 137.

[130] الغديان، سليمان بن عبد الرزاق ومؤلفون آخرون، مرجع سابق، ص176.

[131] زينب محمود حسين، مرجع سابق، ص 577.

[132] هيئة التحرير، جرائم إلكترونية، موقع النجاح عبر الرابط www.ennajah.net، تاريخ الإطلاع 2023/12/22 الساعة 23:00.

[133] الغديان، سليمان بن عبد الرزاق ومؤلفون آخرون، مرجع سابق، ص176.

[134] زينب محمود حسين، مرجع سابق، ص 577.

[135] يوسف علي حسن الداودي، حكم الإبتزاز الإلكتروني دراسة مقارنة بين الشريعة والقانون، دون ذكر بلد النشر ،سنة 2022، ص 645

10) الحب في الإنتقام[136].

11) الإعلام الهابط وانتشار القنوات الفضائية والمواقع الإلكترونية التي تسوق للأفكار والثقافات المنحرفة وتبث المسلسلات التي تؤجج النزوات[137].

12) دخول التكنولوجيا في حياة الأفراد والتي ألغت الستر والحياء وكسرت الحواجز وخلقت الإختلاط غير المشروع[138].

ثانيا: مراحل الإبتزاز الإلكتروني:

عموما تبدأ جريمة الإبتزاز الإلكتروني[139]ب:

1) طلب صداقة مع الشخص المستهدف، التواصل عبر برامج المحادثات (صوتية، كتابية أو عن طريق الفيديو)، استدراج الضحية وتسجيل أي محتوى مسيء وفاضح (صورة، نص، صوت أو فيديو)[140].

2) الطلب (إما مادي أو جنسي أو....)، المقاومة من الضحية، الضغط من الجاني ثم التكشير عن الأنياب والتهديد، الإذعان من الضحية فترفع الراية وتستسلم، إمكانية تكرار الفعل من الجاني [141].

---

[136] ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص 202

[137] الغديان، مرجع سابق، ص176.

[138] هند علي حنون، مرجع سابق، ص81.

[139] سبخاوي خديجة، جريمة الإبتزاز الإلكتروني دراسة ميدانية على عينة من طلبة جامعة البليدة 2، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور بالجلفة . الجزائر المجلد09، العدد01، السنة مارس 2024، ص461.

[140] حسين عبد الكريم يونس، خليل يوسف الجندي، مرجع سابق، ص52.

[141] هيئة التحرير، معنى الإبتزاز الإلكتروني وتداعياته مع10 نصائح هامة للحماية والتخلص منه في السعودية، موقع بصمة أمان عبر الرابط ،WWW.SECPRINT.SA/EXTORTION-MEANINGتاريخ الإطلاع 22 /04//2024 على الساعة18:00.

المبحث لثاني

الهيآت والأشخاص المكلفة بمتابعة الإبتزاز الإلكتروني

أدرك المشرع الجزائري على غرار التشريعات العربية والغربية أن المواجهة الفعالة تكون بمصاحبة القواعد القانونية الموضوعية ذات الطبيعة الردعية بقواعد إجرائية وقائية وتحفظية، وللقيام بهذه المهمات أوكل متابعة هذه الجريمة لهيئات ولأشخاص يتسلمون مهامهم من ضحايا هذه الجريمة، فمن هم هؤلاء الأشخاص وكيف تم تسلمهم للمهمة؟ لكن تجدر الإشارة أولا لمن أقدم على إسقاط الضحية في فخه.

المطلب الأول

المبتز إلكترونيا وطرق التبليغ عنه.

رمى مهندس الجريمة الإلكترونية (المبتز الإلكتروني) حباله الخبيثة لضحيته راسما بذلك بداية إجرامية وتاركا المجني عليه في حيرة بين الصمت أو الإذعان أو التبليغ عنه.

الفرع الأول: المبتز الكترونيا:

يتميز المبتز إلكترونيا بمجموعة من السمات تميزه عن المجرم التقليدي:

1. الذكاء: يتمتع المجرم الإلكتروني بالذكاء لكي يتعامل بالحاسوب ويحترف الشبكات المعلوماتية فهو يرغب في إثبات الذات وتجربة ما يتمتع به من قدرة علمية من أجل

اختراق النظم الإلكترونية واستدراج الضحية بالأساليب المخادعة للحصول على الأشياء التي يحولها إلى أدوات ابتزاز[142].

2. المهارة في مجال تكنولوجيا المعلومات: يستطيع المبتز الدخول إلى البيانات الشخصية والصور والفيديوهات الخاصة بالضحية ليستعملها بعد ذلك للابتزاز عبر استخدام برامج المعلومات والإنترنت فيرتكب الجريمة ويطمس آثارها وأدلتها[143].

3. المبتز إنسان اجتماعي بطبعه. مسؤول عن أفعاله بإرادة حرة موجهة لاقتراف الجرم. فهو إجتماعي لا تظهر عليه علامات الإجرام لذا يستدرج الضحية ببساطة.[144]

الفرع الثاني: طرق التبليغ عن المبتز:

عند سقوط الضحية في فخ الإبتزاز الإلكتروني، البعض تصمت ويتم إجبارها على تنفيذ مطالب الجاني تجنبا للفضيحة. وبعض الضحايا تدفع أموالا للحصول على محل الإبتزاز والتخلص منه، ولكن هذا لا يضمن توقف الجاني على فعله وإعادة الكرة ابتغاء الوصول إلى الهدف من الإبتزاز، والقلة تقوم بالإبلاغ عن المبتز وتترك القانون يأخذ مجراه وهي أفضل طريقة للتعامل مع الإبتزاز ذلك أن الجهات المختصة مدربة وحريصة بشكل تام على التعامل مع هذه الجريمة[145].

---

[142] عبد العزيز بن حمين، الإبتزاز ودور الرئاسة العامة لهيئة الإمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الإبتزاز: المفهوم، الأسباب والعلاج، مكتبة الملك فهد الوطنية، الرياض 1432هـ ص58.

[143] بوالشعير الحسن، حداد شعيب، مرجع سابق، ص29.

[144] نفس المرجع والصفحة.

[145] هيئة التحرير، لا يفوتك عقوبة الإبتزاز الإلكتروني في الجزائر ونص المادتين 287 و303 ،موقع إستشارات قانونية أون لاين عبر الرابط: لا يفوتك عقوبة الإبتزاز الإلكتروني في الجزائر ونص المادتين 287 و303 2024-legal advice.online)، تاريخ الإطلاع2024//05/01.الساعة09:20.

يمكن للمجني عليه الإتصال بعدة جهات لمباشرة التبليغ عن المبتز[146]:

- التواصل مع محام متخصص في قضايا الإبتزاز لمتابعة القضية.
- اللجوء إلى القضاء.
- التوجه إلى أقرب مركز للشرطة لتقديم شكوى.
- التوجه إلى الشركات التقنية في حال نشر أي محتوى عبر الإنترنت لطلب الحجب ومنع التداول.

توجد عدة أرقام للتواصل مع الهيئات المختصة لمكافحة الإبتزاز الإلكتروني في الجزائر:

- الإتصال بالشرطة على الرقم 17[147].
- الإبلاغ عبر رقم وحدة مكافحة جرائم الإبتزاز في الجزائر 48 15 [148].
- التواصل على الرقم المحدد من جهة أمن الولايات 9642 [149]149.

وبسبب الإحتكاك الدائم عبر الإنترنت والعلاقات المستمرة ، يمكن للمواطن الجزائري أن يتعرض للإبتزاز من خارج الدولة الجزائرية فيتقدم بشكوى لدى الجهات الحكومية في الجزائر بغية الحصول على وجهات النظر والخبرات في موضوع الإبتزاز الدولي حتى تحدد دولة المجرم ثم

[146] هيئة التحرير، رقم مكافحة الإبتزاز الإلكتروني في الجزائر وكيفية التبليغ ،(secprint.sa)بصمة أمان عبر الرابط: https://www.secprint.sa/blackmail-number-algeria/، تاريخ الإطلاع 01 ماي 2024 الساعة:02:45.

[147] الموقع نفسه.

[148] الموقع نفسه.

[149] الموقع نفسه.

التوجه لسفارته في الجزائر لتقديم شكوى باعتبار السفارة جزء من دولته[150].

في حال وقوع شخص ضحية للابتزاز الإلكتروني:

- قطع التواصل مع الشخص المبتز[151].
- عدم الاستجابة للمبتز وإخبار الأهل للوقوف معك[152].
- عدم طلب المساعدة من أي شخص لاختراق حساب المبتز، فمن الممكن أن يكون عضوا في منظمة أو عصابة كبيرة محترفة لأساليب الإختراق، وبالتالي تزويد الإنتقام منك وتوسيع دائرة الإبتزاز ليشمل من ساعدك، فالمبتز سيتواصل معك بحساب وهمي آخر واختراق حسابه لا يجدي نفعا[153].
- الإتصال بالشرطة أو هيئة مكافحة الجرائم الإلكترونية لحجب ما تم نشره[154].
- يجب على الضحايا الإحتفاظ بجميع الاتصالات والرسائل النصية والإلكترونية وجعلها أدلة رقمية في المحكمة[155].

علاوة على ذلك يجب:

---

[150] هيئة التحرير، رقم مكافحة الإبتزاز في الجزائر وتبليغ الشرطة المسؤولة عن الشكاوى، موقع إستشارات قانونية مجانية، محاماة نت عبرا الرابط:www.mohamat.net/law/.تبليغ-و-الجزائر-في-الإبتزاز-مكافحة-رقم/#3: lawyer تاريخ الإطلاع2024//05/01، الساعة الإطلاع09:40.

[151] حسين عبد الكريم يونس، خليل يوسف الجندي، مرجع سابق، ص53.

[152] هيئة التحرير، جرائم الكترونية، موقع النجاح عبر الرابط، كيف تحمي نفسك من الإبتزاز الإلكتروني؟ ،(annajah.net) تاريخ الإطلاع 2024/05/01، الساعة 09:52

[153] المرجع نفسه ص54.

[154] الموقع السابق عبر نفس الرابط

[155] هيئة التحرير، رقم مكافحة الإبتزاز في الجزائر وتبليغ الشرطة المسؤولة عن الشكاوى، استشارات قانونية مجانية، محاماة نت عبرا الرابط:www.mohamat.net/law/، تبليغ-و-الجزائر-في-الإبتزاز-مكافحة-رقم/#3: lawyer تاريخ الإطلاع2024//05/01،الساعة 09:44.

- الإعتماد على كلمة سر قوية والقيام بتغييرها بشكل دوري وعدم حفظها.
- عدم الثقة بمعارف التواصل الإجتماعي وعدم إجراء محادثات صوتية أو فيديو مع الغرباء، عدم استخدام شبكة الإنترنت في الأماكن العامة إلا في حدود وبحذر[156].
- صلح هاتفك أو حاسوبك عند تقني ثقة.
- تجنب مشاركة صورك ومعلوماتك الشخصية في فضاء الإنترنت، التوعية التقنية عن طريق التزود بمعلومات الحاسوب والهواتف الذكية، مراقبة الأطفال وتوعيتهم عن مخاطر الإبتزاز، لا تدخل إلى روابط مريبة تطلب منك تسجيل الدخول[157].
- تنظيف الهاتف قبل بيعه وملء الذاكرة مرة أخرى بالقرآن أو بمناظر طبيعية أو مقاطع دينية ثم حذفها مرة أخرى لأن هناك برامج إعادة الأشياء المحذوفة[158].
- استخدام برامج مكافحة الفيروسات الأصلية دائما مثبتة ومحينة[159].
- فصل الأنترنت عن الأجهزة المتصلة في البيت كي لا يقوم المبتز بالسطو عليها[160].
- إغلاق جميع الحسابات المقدمة من طرفك لهذا المبتز[161].
- الإبتعاد عن المواقع المشبوهة[162].

---

[156] هيئة التحرير،كيفية مكافحة الإبتزاز،منصة معك عبر الرابط – معك.(m3k.net)

[157] هيئة التحرير، أبرز 8 طرق الوقاية من الابتزاز الالكتروني في السعودية، موقع محامي الرياض، عبر الرابط https://yalawyer.sa

[158] هيئة التحرير، جرائم الكترونية، موقع النجاح عبر الرابط، كيف تحمي نفسك من الإبتزاز الإلكتروني؟ ،(annajah.net) تاريخ الإطلاع 2024/05/01، الساعة 09:52

[159] ابتسام كريم وآخرون، انتشار ظاهرة الإبتزاز الإلكتروني في المجتمع العراقي، استطلاع آراء عينة من المجتمع العراقي حول التعامل مع هذه الظاهرة، شبكة المؤتمرات العرب، مركز التطور الإستراتيجي الأكاديمي، جامعة دهوك العراق، 11 و12 فيفري 2019، ص166.

[160] بوالشعير الحسن، حداد شعيب، مرجع سابق، ص70.

[161] ابتسام كريم وآخرون، مرجع سابق، ص166.

[162] بوالشعير الحسن، حداد شعيب، مرجع سابق، ص65.

- وضع شريط لاصق على كاميرا الحاسوب تجنبا لتصوير المستخدم عند اختراق الحاسوب[163].

المطلب الثاني

الهيئات المكلفة بحماية الأشخاص من جريمة الإبتزاز الإلكتروني.

الفرع الأول: دور جهازي الأمن والدرك الوطني والمعهد الوطني للأدلة الجنائية على الإجرام في حماية الأشخاص من جريمة الإبتزاز الإلكتروني:

توفر الدولة الأمن لمواطنيها باتخاذ كل السبل للقضاء على الجريمة، لكنها لا تستطيع بجهودها المنفردة مواجهة الجريمة الإلكترونية عامة والإبتزاز الإلكتروني خاصة، لذا سعت الدول لإيجاد كيان دولي تتعاون من خلاله أجهزة الشرطة التابعة للدول لتبادل المعلومات وتتبع المجرمين[164].وجهازي الأمن والدرك الوطني ليسا بمنأى عن هذه المستجدات بل يوكل إليهم دور هام في الوقاية والمكافحة للجريمة الإلكترونية.

أولا: دور جهازي الأمن والدرك الوطني

I. على مستوى جهاز الشرطة:

يهتم جهاز الشرطة بالتحري عن الجرائم وضبطها وتلقي البلاغات وإجراء التحقيقات الأولية وتقديمها للجهات القضائية المختصة لمباشرة الدعوى الجزائية إذا صحت البلاغات أو توافرت الأدلة الكافية للسير في إجراءاتها[165]. حيث شاركت إطارات الشرطة الجزائرية سنة 2001 (تاريخ إبرام اتفاقية بودابست) في الملتقيات الدولية الأوروبية لأخذ الخبرة، وقامت المديرية العامة للأمن الوطني سنة 2003بإرسال إطارات للتكوين في فرنسا في إطار محاربة الإجرام الإلكتروني.

---

[163] ابتسام كريم وآخرون، مرجع سابق، ص166.

[164] عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون جنائي، جامعة وهران، الجزائر، سنة 2012-2013، ص244.

[165] نفس المرجع، ص245.

كما تم استحداث مصالح مختصة على مستوى مخابر الشرطة العلمية والتقنية المتواجدة في العاصمة بشاطوناف، ومخبرين جهويين بوهران وقسنطينة بها أقسام مختصة في الأدلة الرقمية لمساعدة السلطة المكلفة بالتحقيق[166].

قسم استغلال الرقمية الناتجة عن الحواسيب والشبكات[167].

- ✔ قسم استغلال الأدلة الناتجة عن الهواتف النقالة[168].
- ✔ قسم تحليل الأصوات، وذلك بالإستعانة بأجهزة مادية للكشف عن الجرائم[169].

وتم تنصيب 23 خلية عملياتية (جانفي 2010) على مستوى المصالح الولائية للشرطة القضائية لأمن الولايات مقسمة على ولايات الوسط والشرق والغرب والجنوب على أن يكون المحققون التابعون لهذه الخلايا مختارين وفق شروط معينة[170]..

II. على مستوى جهاز الدرك الوطني:

تم إعادة تنظيم هياكل الدرك الوطني الجزائري حسب الإختصاصات المستجدة إلى:

1. المصلحة المركزية للتحريات الجنائية **SCIC:** اختصاصها وطني مكلف بمكافحة الجريمة المنظمة، القضايا الإقتصادية الكبرى والإجرام المرتبط بتكنولوجيا الإعلام والإتصال[171].
2. المصالح الجهوية للشرطة القضائية:

مهمتها تنسيق النشاطات بين وحدات الشرطة القضائية وتدعيمها بوسائل التحريات والأبحاث[172].

---

[166] عائشة بوخبزة، المرجع السابق، ص247.

[167] عبد القادر فلاح، نادية أيت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري. مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر، المجلد 04، العدد 02، السنة 2019، ص1696.

[168] نفس المرجع والصفحة.

[169] نفس المرجع والصفحة.

[170] عائشة بوخبزة، مرجع سابق، ص248.

[171] نفس المرجع والصفحة

[172] نفس المرجع، ص250.

ثانيا: المعهد الوطني للأدلة الجنائية وعلم الإجرام:

تم بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004 إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام في بوشاوي. وهو هيئة مختصة في إجراء الخبرة والمعاينة في الجرائم المعلوماتية[173]. يذكر أن قيادة الدرك الوطني[174] استحدثت مشروع إنشاء مركز لمحاربة جرائم الإعلام الآلي، ليساهم في تقديم المساعدة التقنية بتقديم أسماء الخبراء المختصين المنتمين للمعهد الوطني للأدلة الجنائية وعلم الإجرام على مستوى المحاكم والمجالس، للاستفادة من خبراتهم في مجال الإعلام الآلي ومساعدة القضاة تقنيا[175].

الفرع الثاني: دور الهيئة الوطنية للوقاية من جرائم الإعلام والإتصال ومكافحتها ومساعدة مقدمي الخدمات:

أولا: دور الهيئة الوطنية للوقاية من جرائم الإعلام والإتصال ومكافحتها:

تم إنشاء هيئة وطنية للوقاية من جرائم الإعلام والإتصال ومكافحتها بموجب المرسوم الرئاسي رقم 15 -261 ومقرها بئر مراد رايس[176](تأخر إنشاؤها من2009 إلى2015)، نظمها القانون04/09المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها[177]، مهامها طبقا للمادة 14 من هذا القانون:

1. "تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

[173] يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة.

[174] مريم عراب، مرجع سابق، ص1228.

[175] نفس المرجع ص1229.

[176] عبد القادر فلاح، نادية أيت عبد المالك، مرجع سابق، ص1696.

[177] المادة13 من القانون04/09 المؤرخ في 05 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الصادر في ج.ر عدد 47، المؤرخ في 16 أوت 2009.

2. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والإتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.
3. تبادل المعلومات مع نظيراتها في الخارج قصد جمع المعلومات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم."

ثانيا: مساعدة مقدمي الخدمات:

تشتغل الأنترنت بتضافر جهود العديد من الأشخاص، والتي تختلف مهامهم بين تخزين المعلومات، ونقلها أو استضافتها ونشرها وبثها عبر شبكة الإنترنت[178].

ويعدّ مقدم خدمة الأنترنت بوابة الوصول إلى المعلومات أو محتوى الإنترنت[179]. وعرفه المشرع الجزائري في المادة 2/د من القانون 09-04 على أنه: "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات و/أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها[180]". ويكون إما مورد الخدمة أو متعهد الإيواء (أو مستضيف البيانات) أو مؤلف الرسائل أو متعهد الوصول أو ناقل المعلومات[181].

أشار المشرع الجزائري إلى التزامات مقدمي خدمة الأنترنت في المواد 10، 11 و12 من الفصل الرابع من القانون 09-04 في مساعدة السلطات. م 10 "... يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات

[178] عبد الله شيباني، وداد بن سالم، النظام القانوني لمقدمي خدمة الإنترنت في ظل القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مجلة الإجتهاد للدراسات القانونية والاقتصادية، الجزائر، المجلد13، العدد01 سنة 2024، ص62.

[179] نفس المرجع، ص.63

[180] نفس المضمون أخذه المشرع في القانون 18-07 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[181] أنظر عبد الله شيباني، وداد بن سالم، مرجع سابق، ص64. وكذلك سمير عالية، مرجع سابق، ص84 إلى 99.

المتعلقة بمحتوى الاتصالات في حينها ويوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11أدناه تحت تصرف السلطات المذكورة"[182].

م 11 "... يلتزم مقدمو الخدمات بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت وحدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليهم...[183]".

"التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموضوعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.[184]"

ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات لأغراض التحري والتحقيق نظرا لأهميتها وصعوبة الحصول عليها من قبل الجاني للتغيير منها أو حذفها، كما يجب على مقدمي الخدمات الإلتزام بالسرية التامة بطلب من المحققين، تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[185]."وتحدد مدة حفظ المعطيات بسنة واحدة ابتداء من تاريخ التسجيل"[186] .

---

[182] المادة 10 من القانون 09-04 السابق الذكره.

[183] المادة 11 من القانون 09-04 السابق ذكره.

[184] المادة 12 من القانون 09-04.

[185] عبد الله شيباني، وداد بن سالم، مرجع سابق، ص65.

[186] المادة11-هـ الفقرة 3 من القانون 09-04.

خلاصة الفصل الأول

أختم في نهاية الفصل الأول بذكر النقاط التي تناولتها من خلاله، بداية بالتطرق لمواجهة الإبتزاز الإلكتروني في التشريع الجزائري حيث تم التعريف بالجريمة وصورها وطرق ارتكابها وكذا مدى خطورتها. أساليبها ومراحل ارتكابها وتجريمها وهذا بذكر أركانها.

ثم الهيآت والأشخاص المكلفين بحماية ضحايا الجريمة والمتمثلة في الشرطة، الدرك الوطني، مقدمي الخدمات، المعهد الوطني للأدلة الجنائية على الإجرام والهيئة الوطنية للوقاية من جرائم الإعلام والإتصال ومكافحتها.

الفصل الثاني

الإجراءات القانونية لحماية الأشخاص من الإبتزاز الإلكتروني

تمر جريمة الإبتزاز الإلكتروني كغيرها من الجرائم، ولاكتشاف الجريمة وفاعلها، والوقوف على وقائعها وملابساتها، يتطلب التحقيق والاستدلال، لنسبة التهمة إلى المتهم بها أو نفيها عنه. وفي هذه الجريمة يجب توفر دليل غير تقليدي، دليل يرتبط بالحاسوب والأجهزة الذكية والبرامج والتطبيقات التكنولوجية، والمشرع هو الذي يحدد للقاضي الأدلة المقبولة أو غير المقبولة[187].

وكما هو الحال في القصور التشريعي لتحديد كل جريمة معلوماتية على حدى لإزالة الغموض الذي يحيط بها، فإن الفراغ التشريعي واضح للعيان أيضا في التهديد الإلكتروني[188].

والمشرع العربي والجزائري لم يتدخلا جديا لمواجهة الجرائم الإلكترونية بنصوص إجرائية خاصة، مما يصعب جمع الأدلة وعدم ملاءمة الإجراءات التقليدية وتطبيقها عليها[189].

حاول المشرع الجزائري التطرق للجريمة الإلكترونية في خطوة متأخرة نوعا ما لمسايرة ركب أغلب الدول[190] بموجب القانون 04-15[191]، وخصها بقانون 09-04 سابق الذكر، وساير الإتفاقيات الدولية بموجب القانون 04-14[192] والمرسوم التنفيذي رقم 06-348 المؤرخ في

---

[187] داليا عبد العزيز، المسؤولية الجنائية عن جريمة الإبتزاز الإلكتروني في النظام السعودي، دراسة مقارنة، مجلة جيل للأبحاث القانونية المعمقة، مركز جيل البحث العلمي بالجزائر / فرع لبنان، المجلد 03، العدد25، سنة 31 ماي 2018، من ص27 الى ص76.

[188] مريم عراب، مرجع سابق، ص1214.

[189] نفس المرجع ونفس الصفحة.

[190] عائشة بوخبزة، مرجع سابق، ص122.

[191] المؤرخ في 27 رمضان1425 الموافق ل 10نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، ج. ر 2004/71.

[192]المؤرخ في 27 رمضان1425 الموافق ل 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155المتضمن قانون الإجراءات الجزائية، ج.ر 2004/71.

2006/10/05 المتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[193]،واستحداث أساليب جديدة في البحث والتحري.

فكيف تكون متابعة الجناة وكيف يكون التحقيق والإثبات في هذه الجريمة المستحدثة، وكيف عاقب المشرع فاعليها؟

المبحث الأول

التحقيق والإثبات في جريمة الإبتزاز الإلكتروني والصعوبات التي تواجهها

وجب على المحققين بمجرد وقوع الجريمة جمع الإستدلالات بهدف إقامة الدليل واكتشاف الجاني[194]، لكن جرائم الإبتزاز الإلكتروني تنشأ في وسط افتراضي وترتكب بأساليب متطورة وحديثة دون ترك أثر لها، مما يصعب الحصول على الدليل الإلكتروني باعتباره الوسيلة الوحيدة للإثبات وعند استخلاصه تعترض جهات التحري والتحقيق عدة صعوبات نتيجة الطبيعة التقنية الرقمية التي يتكون منها والوسط المتواجد فيه[195].

[193] مريم عراب، نفس المرجع ونفس الصفحة.

[194] داليا عبد العزيز، مرجع سابق، من ص27 الى ص76.

[195] بن شهرة الشول، هانية بوشارب، صعوبة عملية استخلاص الدليل الإلكتروني، مجلة الدراسات القانونية والسياسية، الجزائر، المجلد09، العدد 01 جانفي 2023، ص68.

المطلب الأول

التحقيق والصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني

الفرع الأول: التحقيق في جريمة الإبتزاز الإلكتروني

تتشابه إجراءات التحقيق في الجرائم الإلكترونية مع إجراءات التحقيق في الجرائم التقليدية لأن كليهما يحتاجان إلى (المعاينة – التفتيش – الإستجواب وجمع الأدلة وفحصها)[196]رغم خصوصية جريمة الإبتزاز الإلكتروني.

ويعرف التحقيق على أنه: "مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومرتكبها تمهيدا لتقديمه إلى المحاكمة كي ينال عقابه، وقد تكون الإجراءات عملية كالتفتيش، أو فنية كمضاهاة البصمات، أو برمجية لتحديد كيفية الدخول إلى المعطيات المخزنة في أجهزة الحاسوب[197]". ذكره المشرع الجزائري بالتعبير عنه بقاضي التحقيق وعرفه في المادة 68 من قانون الإجراءات الجزائية.[198]

أولا: الإجراءات التي يجب على المحقق التقيد بها:

1. مراعاة حرمة الحياة الخاصة والحرص على عدم انتهاكها بالمحافظة على الأسرار الموجودة في الحاسوب[199].

---

[196] داليا عبد العزيز، مرجع سابق، ص27ص76.

[197] نفس المرجع، من ص27 الى ص76.

[198]عبد القادر فلاح، نادية أيت عبد المالك، مرجع سابق، ص1695.

[199]عماد جواد مرسي، التحقيق والصعوبات التي تواجه جريمة الإبتزاز الإلكتروني، مجلة كلية المعارف الجامعة، الأنبار، العراق، المجلد33، العدد4 سنة 2022، ص238.

2. المحافظة على الأدلة بالحالة التي ضبطت عليها وتقديمها للمحكمة[200].
3. تجنب ضياع الوقت في التحقيق بالجرائم الإلكترونية التي لا يمكن اكتشافها أو أن تكون أدلتها قد تم تدميرها أو إتلافها[201].
4. الحصول على إذن مسبق من الجهات المختصة عند تفتيش الأجهزة[202].
5. تدوين جميع إجراءات التحقيق في محاضر، وتتم المصادقة عليها في محضر رسمي لتكون دليل إثبات.[203]
6. طلب التعاون والإستشارة من جهة الإختصاص كمركز الإتصالات وخبراء التقنية والبحث الجنائي[204].
7. وضع خطة للتحقيق تبدأ بجمع الأدلة بالإستعانة بفريق فني مؤهل[205].

ثانيا: إجراءات التحقيق في جريمة الإبتزاز الإلكتروني في الجزائر

يبقى نظام الإجراءات الجزائية في قواعد التحقيق هو السائد، مع ضرورة اعتبار الفوارق الموضوعية فيه، حيث أن هناك صعوبات تثار أثناء التحقيق ناتجة عن طبيعة جريمة الإبتزاز الإلكتروني[206]،

[200] عماد جواد مرسي، نفس المرجع، ص239.
[201] داليا عبد العزيز، مرجع سابق، ص27.
[202] عماد جواد مرسي، نفس المرجع ونفس الصفحة.
[203] عبد القادر فلاح، نادية أيت عبد المالك، مرجع سابق، ص1695.
[204] وائل سليم عبد الله شاطر، مرجع سابق، ص 438.
[205] عبد القادر فلاح، نادية أيت عبد المالك، مرجع سابق، ص1695.
[206] داليا عبد العزيز، مرجع سابق، من ص27 إلى ص 76.

تنص المادة 40[207]: على أن اختصاص قاضي التحقيق محليا يتعين بمكان وقوع الجريمة، أو محل إقامة أحد الأشخاص المشتبه فيهم، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

كما أن ضباط الشرطة القضائية يمارسون اختصاصهم المحلي في الدائرة التي يباشرون فيها وظائفهم المعتادة.و يجوز للقاضي المختص في حالة الاستعجال أمرهم بمباشرتها في كافة دائرة اختصاص المجلس القضائي التابعين له، أوعلى كافة إقليم الوطن،شرط إعلام وكيل الجمهورية التابعين له، وهذا وفقا للمادة 16 من قانون الإجراءات الجزائية

I. إجراءات التحري والتحقيق العامة: (التقليدية)

يمر التحقيق في الجرائم الإلكترونية بمرحلتين:

1. المرحلة الأولى: وهي الإجراءات المنفذة في مسرح الجريمة، وتتمثل في:

- إغلاق أو تجميد مسرح الجريمة لمنع فقدان الأدلة والحفاظ على مسرح الجريمة ومنع العبث به.[208]

2. المرحلة الثانية: وتشمل:

- توثيق حالة مسرح الجريمة (هل الجهاز مفتوح وقت ضبطه؟ هل هو موصول بالأنترنت، ...)، تحديد هوية الجهاز والأجهزة الملحقة به وتوثيقIP الذي يحدد

[207] (الأمر رقم 69-73 المؤرخ في 16 سبتمبر 1969) من قانون الإجراءات الجزائية المعدل بموجب القانون رقم 14-04 المؤرخ في 10نوفمبر 2004 والمرسوم التنفيذي رقم 06/348 المؤرخ في 2006/10/05 المتضمن تمديد الإختصاص لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق

[208] مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، دراسة مقارنة، مجلة علوم الشريعة والقانون، الأردن، المجلد45، العدد4، سنة 2018، ص286.

موقع المشتبه به، تحديد هوية وتوثيق أجهزة التخزين (CD DVD...) وتصوير وحفظ الأدلة والوثائق المطبوعة واسترجاع الوثائق الملغاة[209].

على أن يتم تسجيل وقت وتاريخ ومكان الصورة، كذلك ملاحظة الطريقة التي تم بها إعداد النظام[210]، وعدم نقل أي معلومة في مكان ارتكاب الجريمة إلا بعد إجراء الإختبار الخاص بخلو المحيط الخارجي لموقع الحاسوب من المجالات المغناطيسية التي تسبب مسح البيانات المسجلة[211].

اعتمد المشرع الجزائري كما سبق ذكره على النصوص الجزائية التقليدية:

1) الانتقال للمعاينة: الهدف من المعاينة هو الوصول إلى دليل أو آثاره المتبقية في مسرح الجريمة، وفي جريمة الإبتزاز الإلكتروني يقصد بها معاينة الآثار التي يخلفها مستخدم الأنترنت أو الشبكة العنكبوتية، وتتضمن الرسائل المرسلة أو المستقبلة وكافة الاتصالات التي تمت بالأجهزة التقنية، ومستخدم الشبكة يترك أثرا لأن الموقع المستخدم يسجل عنوان المكان ونوع المتصفح المستخدم وعنوان IP الدائم والمتغير للكومبيوتر الذي يستخدمه وعنوان وإسم المستخدم[212].

وعرفها أحدهم بأنها: "إجراء ينتقل المحقق بمقتضاه إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة"[213].

---

[209] نفس المرجع ونفس الصفحة.

[210] سارة حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، (دراسة مقارنة) رسالة للحصول على ماجستير في القانون العام، كلية الحقوق، قسم القانون العام، جامعة الشرق الأوسط،ا لأردن، سنة 2020، ص59.

[211] عماد جواد مرسي، مرجع سابق، ص241.

[212] نفس المرجع، ص240.

[213] سارة محمد حنش، مرجع سابق، ص57.

تعتبر المعاينة في الجرائم الإلكترونية جوازية، ولا تتمتع في مجال كشفها بنفس درجة الأهمية في الجرائم التقليدية، ذلك لأنها قد تتلف أو تمحى من طرف الجناة وتدمر في زمن وجيز يصعب تتبع أثرها. إضافة إلى تردد عدد كبير من الناس على مسرح الجريمة[214]. رغم أن بإمكان الآثار المعلوماتية المستخلصة أن تكون ثرية فيما تحتويه من معلومات (البريد الإلكتروني، الصوت الرقمي، الملفات المخزنة، الفيديو الرقمي، ...)[215].فالمعاينة تستهدف التعرف على أبعاد الجريمة، وأركانها، وظروفها، وكشف الحقيقة بشأنها، لذا لا يجوز لأي خصم أو طرف أن يعترض على إجرائها أو على أسلوب تنفيذها، لأنها ليست موجهة ضد شخص معين ماسا بحرمة مستودع سره[216].

2) التفتيش:

يعرف أحدهم التفتيش على أنه" :إجراء من إجراءات التحقيق تباشره سلطة مختصة بهدف البحث في مستودع سر فرد معين عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة، وذلك لغرض إثبات وقوعها ونسبتها إلى المتهم وفقا للضمانات والضوابط المقررة قانونا[217]". وهو من أخطر الإجراءات الجنائية التي تمس حريات الناس، لأنه يبحث في مستودع أسرارهم[218]. فالتفتيش وسيلة للإثبات المادي، غايته ضبط الأدلة المادية الخاصة بالجريمة، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي ومعطيات شبكة

[214] مريم عراب، مرجع سابق، ص1219.

[215] عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبوبكر بلقايد، تلمسان، سنة 2017-2018، ص277.

[216] المرجع نفسه، ص277.

[217] أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني، (دراسة مقارنة) كلية الحقوق، قسم القانون الجنائي، جامعة المنصورة، مصر، المجلد الثامن عدد يونيو 2022، ص13.

[218] مريم عراب، مرجع سابق، ص1219.

الأنترنت الخالية من أي مظهر مادي محسوس في العالم الخارجي[219].التفتيش في الجريمة الإلكترونية يعني التفتيش في المكونات المادية والمكونات المعنوية (الحاسب الآلي مثلا...) كما له شبكات اتصال بعدية سلكية ولاسلكية محلية أو دولية[220].

- تفتيش المكونات المادية للحاسوب:

لا تثار مشكلة بشأن التفتيش لتطابقها مع الإجراءات التقليدية، وهنا نفصل بين وجود الحاسب في مكان عام أو خاص[221]. فإذا كانت المكونات المادية موجودة في أماكن عامة، كالحدائق أو عامة بالتخصيص، كمقاهي الأنترنت، فتكون إجراءات التفتيش وفقا للأصول الخاصة بتلك الأماكن[222]. أما إذا كانت موجودة في مكان خاص كمسكن المتهم، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وفق المادة44 و64 من قانون الإجراءات، وذلك بالحصول على إذن للتفتيش مكتوب من وكيل الجمهورية وبحضور صاحب المسكن أو شاهدين لا علاقة لهما (م45 ق.إ.ج.) وأن يكون التفتيش بعد الخامسة صباحا وقبل الثامنة مساء، إلا إذا طلب صاحب المسكن. لكن هناك استثناءات –وهنا المشرع رجع عن القاعدة العامة في المادة 64 لينص[223]– في المادة 3/47 ق.إ.ج: ."..عندما يتعلق الأمر بالجرائم الماسة بأنظمة ممارسة المعالجة الإلية للمعطيات.....فإنه يجوز إجراء التفتيش والمعاينة والحجز في

[219] جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، سنة 2018، ص 14.

[220] عزيزة رابحي، مرجع سابق، ص279.

[221] أنظر جمال براهيمي، مرجع سابق، ص15، وعزيزة رابحي، مرجع سابق، ص280 وأحمد لطفي السيد مرعي، مرجع سابق، ص13.

[222] جمال براهيمي، مرجع سابق، ص16.

[223] مريم عراب، مرجع سابق، ص1220.

كل محل سكني في كل ساعة من ساعات النهار، أو الليل بناء على إذن مسبق من وكيل الجمهورية المختص.[224]"

- تفتيش المكونات المعنوية للحاسوب:

ثار خلاف فقهي بشأن جواز تفتيش المكونات المعنوية للحاسوب لأنه لا يحتوي على ماديات. فمنهم من ذهب إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب، باعتباره وسيلة للإثبات المادي، بهدف ضبط أدلة مادية للكشف عن الحقيقة، وهذا يتعارض مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي[225]. وهذا ما أخذ به الفقه الفرنسي والمشرع الألماني والياباني الأمريكي[226]، حينما اعتبروا البيانات والبرامج مجرد مكونات غير مرئية، كونها نبضات أو ذبذبات إلكترونية أو موجات كهرومغناطيسية غير محسوسة ماديا، لا يرد عليها تفتيش إلا بعد تحويلها إلى كيان مادي محسوس، مثل طبعها على الورق أو تخزينها في دعامة مادية مثل الأقراص المغناطيسية أو تصويرها على الشاشة أو نقلها على حافظة بيانات[227].

ولم يبق المشرع الجزائري بعيدا عن المستجدات التي انتهجتها القوانين الغربية والعربية، بل حذا حذوهم واستحدث نصوصا قانونية جديدة، أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب[228] طبقا للمادة 5 من القانون 09-04، وطبقا للإحالات المنصوص عليها في المادة 4 من قانون الإجراءات الجزائية، مما يسمح

---

[224] عزيزة رابحي، مرجع سابق، ص280.

[225] مريم عراب، مرجع سابق، ص1220.

[226] فصلت بعدها التشريعات المعاصرة حل الخصوصية التشريعية وأقرت التفتيش في جميع الأماكن في سبيل كشف الحقيقة. وحذا حذوهم المشرع المصري سنة 2018.

[227] أحمد لطفي السيد مرعي، مرجع سابق، ص15.

[228] جمال براهيمي، مرجع سابق، ص19 و20.

للسلطات القضائية المختصة وضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد[229] إلى منظومة معلوماتية أو جزء منها والمعطيات المخزنة فيها[230].

يذكر أن المشرع الجزائري خطى خطوة لتجاوز مسألة تفتيش المنظومة المعلوماتية عن بعد بصفة نهائية (المادة 47 من ق.إ.ج) بتمديد اختصاصات ضباط الشرطة القضائية في أي وقت وفي أي مكان من التراب الوطني (المادة 2/5 من القانون 09-04).

أما إذا كان خارج الإقليم الجزائري (المادة 3/5 من نفس القانون) فيمكن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة...[231].

فيما يخص السلطة المختصة بالتفتيش هي قاضي التحقيق وتساعده النيابة العامة (المواد 81، 82 ومن 83 من ق.إ.ج) واستثناء أحد ضباط الشرطة القضائية عن طريق تفويض من قاضي التحقيق لاستحالة قيامه بالمهمة (المادة 84 من ق.إ.ج) وطبقا للشروط المنصوص عليها في المواد 138، 139، 140، 141 و142 من نفس القانون[232].

3) الضبط في مجال الجريمة الإلكترونية:

ينتهي التفتيش بضبط الأدلة المتحصل عليها ووضع اليد على الأشياء المتصلة بالجريمة التي تؤدي إلى كشف حقيقتها والتعرف على مرتكبيها[233].

تتصف الأشياء المضبوطة في الجرائم التقليدية بالمادية فكيف يكون الضبط في الجرائم الإلكترونية؟ خاصة عند عدم وجود دليل مرئي. إنقسم الفقه إلى قسمين في هذا الإجراء

[229] نصت الإتفاقية الأوروبية حول الجرائم الإلكترونية صراحة حق الدول الأعضاء تفتيش مكونات الحاسب المنطقية.

[230] جمال براهيمي، مرجع سابق، ص20.

[231] أنظر عزيزة رابحي، مرجع سابق، ص281 وما بعدها.

[232] نفس المرجع، ص 286.

[233] مريم عراب، مرجع سابق، ص 1221.

مثله مثل التفتيش[234]. أما المشرع الجزائري حل هذه المسألة في المواد 6، 7 و8 من القانون 09-04 تحت عنوان حجز المعطيات المعلوماتية[235].والحجز عن طريق منع الوصول الى المعطيات [236].

فالقاعدة العامة: الضبط لا يرد إلا على الأشياء المادية (جهاز الحاسوب وملحقاته، أقراص الليزر، البطاقات المضغوطة، ...)، أما ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج ومحتويات صناديق البريد الإلكتروني، ففيه من ينفي إجراء الضبط وفيه من يقبله إذا ما حول إلى كيان مادي كتسجيل البيانات المراد ضبطها على ورق أو نسخها في ملفات[237] .

4) الخبرة التقنية:

تعرف الخبرة بأنها: "إجراء من إجراءات التحقيق يتم بموجبه الإستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع الجريمة أو نسبتها إلى المتهم.[238]"

فإذا كان للخبرة دور كبير وأهمية قصوى في الجرائم التقليدية، فإن أهميتها تزداد بل وتصبح حتمية في الجرائم الإلكترونية[239]. يقصد بالخبرة المعلوماتية الشرعية: "عملية البحث التي يقوم

[234] عزيزة رابحي، مرجع سابق، ص292 وما بعدها.

[235] عبد القادر فلاح، نادية عبد المالك، مرجع سابق، ص9 و10.

[236] أنظر فحوى المواد 6.7.8.من القانون09 -04.

[237] مريم عراب، مرجع سابق، ص1221.

[238] جمال براهيمي، مرجع سابق، ص68.

[239] مريم عراب، مرجع سابق، ص1219.

بها الخبير المعلوماتي من أجل الحصول على الدليل الرقمي بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة وهذه العملية تشبه تشريح الجثة في الطب الشرعي ."[240]

والخبير شخص يتمتع بمؤهلات علمية، وقدرة في التحكم في مجال الإعلام الآلي تلجأ اليه السلطات المكلفة بالتفتيش قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاح مهمتها[241] .

تخضع الخبرة لمجموعة من الضوابط لتكون لها نتائج أمام القضاء وهي:

اختيار الخبير من جدول الخبراء على أداء اليمين القانونية، والتزامه بأداء مهامه بنفسه، واعتماد هذا الأخير على وسائل علمية متطورة لإنجاز الخبرة"[242].

5) تدريب الكوادر: تقتضي جريمة الإبتزاز الإلكتروني معرفة متميزة بنظم المعلوماتية وكيفية تشغيلها ووسائل إساءة استعمالها من قبل مستخدميها، ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري والمباشرين للتحقيق[243] إما في مراكز تابعة لوزارة الداخلية، أو وزارة العدل، كما يجب استقطاب الكفاءات في المجال المعلوماتي وضمهم إليها[244]، وتنظيم التكوينات، والإنضمام للدورات في الخارج للاستفادة من الخبرات الدولية عن طريق التعاون الدولي[245].

---

[240] نفس المرجع ونفس الصفحة.

[241] أنظر المادة 5 الفقرة الأخيرة من القانون.

[242] عبد القادر فلاح، نادية عبد المالك، مرجع سابق، ص1698.

[243] عزيزة رابحي مرجع سابق، ص273.

[244] نفس المرجع والصفحة

[245] أهم مشروع: مشروع فالكون 2001، وبرنامج أجيس 2004/2003 الذي أعده مركز التدريب الوطني عن الجرائم التقنية NSLEC في الإتحاد الأوربي.

6) سماع شهادة الشهود: في جريمة الإبتزاز الإلكتروني يسمى الشاهد المعلوماتي أو الخبير.[246] وهم مشغلو الحاسب الآلي، وخبراء البرمجة، والمحللون، ومهندسو الصيانة والاتصالات، ومديري النظام.[247]

7) الإستجواب: وهو مساءلة المتهم ومواجهته بالأدلة وسماع أقواله لنفي التهمة، ومن حقه الإستعانة بمحامي، ومن حق هذا الأخير الإطلاع على التحقيق.[248]

والهيئات المتخصصة في مواجهة الجرائم الإلكترونية والمساعدة للسلطات القضائية: هي مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها الذي أنشأته قيادة الدرك الوطني سنة 2009، والمعهد الوطني للبحث في علم التحقيق الجنائي الذي أنشئ بالمرسوم الرئاسي 04-432 سنة 2004. والذي يتضمن مخابر وأقسام. ومصلحة الخبرات الخاصة بالدلائل التكنولوجية سنة 2007. والقسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرة العامة للأمن الوطني وتمتد مصالحها إلى بعض الولايات. والمخابر الجهوية الجنائية والتي تضم عدة أقسام متخصصة بما فيها قسم الأدلة الإلكترونية والرقمية. والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وهي منوطة بتقديم المساعدات القضائية والتحريات والتحقيق وتقديم الخبرة[249] .

II. إجراءات التحقيق المستحدثة:

قام المشرع الجزائري باستحداث آليات تحقيق خاصة بموجب قانون الإجراءات الجزائية الجديد 06-22 والقانون 09-04 ، وذلك لأن الإجراءات التقليدية لم تعد تسع

[246] فاطمة العرفي، مرجع سابق، ص 503.

[247] سارة محمد حنش، مرجع سابق، ص 64.

[248] سارة محمد حنش، المرجع السابق، ص64.

[249] جمال براهيمي، مرجع سابق، ص71، 72 و73.

الجرائم الإلكترونية التي تطورت وتنامى خطرها، ومن هذه الإجراءات التسرب الإلكتروني، إعتراض المراسلات وتسجيل الأصوات والتقاط الصور(المراقبة الإلكترونية).

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

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

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

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

تكون عملية التسرب في الجرائم الإلكترونية في ولوج ضابط الشرطة القضائية إلى العالم الإفتراضي، ومشاركته في محادثات غرف الدردشة، أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الإتصال أو بث الفيروسات، أو انخراطه في نوادي الهاكر مستخدما إسما مستعارا لاستدراجهم والكشف عن أعمالهم[251].

[250] مريم عراب، مرجع سابق، ص1224.

[251] جمال براهيمي، مرجع سابق، ص85.

شروط التسرب: حسب المادة 65 مكرر 11 ق.إ.ج، يجب أن تكون أدلة كافية تدعم الإشتباه واشترط المشرع الجزائري أنواع الجرائم التي يتم فيها التسرب وهي المذكورة في المادة 65 مكرر 5 ومن ضمنها الجرائم الماسة بأنظمة المعالجة الإلية للمعطيات[252].

وليكون التسرب مشروعا يجب:

1- صدور إذن قضائي: م65 مكرر 15 من وكيل الجمهورية وتكون العملية تحت إشرافه أو من قاضي التحقيق بإخطار وكيل الجمهورية ومنح إذن مكتوب لضابط الشرطة القضائية[253].

2-أن يكون الإذن مكتوبا ويذكر أسباب إقراره[254]. (م65 مكرر 15 ق إ ج)

3-تحديد المدة المطلوبة لعملية التسرب (لا يتجاوز 4 أشهر قابلة للتجديد واسم ضابط الشرطة ونوع الجريمة[255].

2) إعتراض المراسلات وتسجيل الأصوات والتقاط الصور (المراقبة الإلكترونية)

كان المشرع الفرنسي سباقا في تبني عملية اعتراض ومراقبة الإتصالات الإلكترونية ضمن إجراءات التحري والتحقيق الجنائي سنة 1991 في قانون إجراءاته الجزائية، ثم المشرع الأمريكي سنة 2000 بتوسيع مجال تطبيق إجراء الإعتراض والمراقبة ليشمل كل المراسلات السلكية واللاسلكية[256]. وحذا حذوه المشرع الجزائري بموجب قانون الإجراءات الجزائية 06-22[257] فاستحدث الفصل الرابع تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المواد 65 مكرر 5 إلى 65 مكرر 10 وعززه بقانون 09-04.

---

[252] عزيزة رابحي، مرجع سابق، ص297.

[253] نفس المرجع، ص298.

[254] مريم عراب، مرجع سابق، ص1224.

[255] جمال براهيمي، مرجع سابق، ص86.

[256] نفس المرجع، ص88.

[257] المؤرخ في 29ذي القعدة1427 الموافق ل 20 ديسمبر 2006 يعدل ويتمم الأمررقم66-155 المؤرخ في 18 صقر 1386 الموافق ل 8 جوان1966 والمتضمن قانون الإجراءات الجزائية.

لم يعرف المشرع الجزائري المراقبة الإلكترونية وعرفها الفقهاء بأنها: "إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد، بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها، ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض.[258]"

1. اعتراض المراسلات:

قد تضطر السلطة القضائية ممثلة في وكيل الجمهورية عن طريق ضابط الشرطة القضائية لاستعمال كاميرا خفية أو أجهزة تصنت لكن يجب أن تكون في إطار احترام الشرعية الإجرائية حفاظا على كرامة حياة الإنسان[259] .

ولتحقيق التوازن بين ضرورة التحقيق واحترام الحياة الخاصة لا بد من شروط:

الحصول على إذن من السلطة القضائية المختصة (م65 مكرر 5 ق.إ.ج)، وتسبيب اللجوء إلى اعتراض أو مراقبة المراسلات (م4 من قانون 09-04)، وتحديد الجرائم محل الإعتراض والمراقبة (م65 مكرر 5 وم4/أ.ب.ج.د من قانون 09-04 وسرية الإجراءات وكتمان السر المهني م4/45 ق.إ.ج. والمواد 5 فقرة أخير و7 و8 من القانون 09-04)[260].

2. تسجيل الأصوات والتقاط الصور:

يكون أسلوب تسجيل الأصوات والتقاط الصور دون موافقة المعنيين، وهذا من أجل التقاط وتثبيت وبث تسجيل الكلام المتفوه به من قبل شخص أو عدة أشخاص وكذلك التقاط صور لهم في أماكن عامة أو خاصة[261]. المادة 65 مكرر 5 من ق.إ.ج.

[258] مريم عراب، مرجع سابق، ص1225.

[259] سارة محمد حنش، مرجع سابق، ص65.

[260] جمال براهيمي، مرجع سابق، ص94 وما بعدها.

[261] مريم عراب، مرجع سابق، ص1226.

3) الحفظ والإفشاء العاجلان للمعطيات الإلكترونية:

يستطيع الجاني إزالة الدليل التقني عن بعد باستعمال التقنية، لهذا ألزم المشرع الجزائري حفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية، مسايرا بذلك ما تضمنته قرارات الجمعية العامة للأمم المتحدة رقم63/55 المؤرخة في 2001، وتعد اتفاقية بودابست 2001 من أول النصوص التي اعتمدت مساعدة مقدمي الخدمات للسلطة القضائية، وهو ما أكده المشرع الجزائري في المادة 10 من قانون 09-04[262]، مثل حفظ البيانات والمعلومات وإفشاء أي معلومة مهمة لرجال الضبطية القضائية، وفي حال عدم التزامهم تترتب عليهم المسؤولية الجزائية[263] .

الفرع الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني والحلول المقترحة:

أولا :الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني:

يتسم التحقيق في جرائم الإبتزاز الإلكتروني بالصعوبة التي من شأنها عرقلة الوصول إلى الكشف عن الجريمة وإثباتها، بل قد تؤدي إلى نتائج سلبية تنعكس على المحقق بفقدان الثقة في نفسه، وفي أدائه وعلى المجتمع، بفقدان الثقة في أجهزة الأمن، وعلى المجرم نفسه بالغرور والتفاخر بمعرفته وخبرته التي تفوق خبرة المحققين، فيبعث الثقة في نفسه ويرفع من عزيمته في ارتكاب المزيد من الجرائم التي قد تكون أكثر ضررا من ذي قبل[264].

[262] نفس المرجع، ص1227.

[263] عبد القادر فلاح، نادية عبد المالك، مرجع سابق، ص1699.

[264] جمال براهيمي، مرجع سابق، ص184.

ومن أهم الصعوبات:

❖ الطبيعة الخاصة للجريمة:

بما أن الجريمة مستحدثة، وغير محسوسة، وتنشأ في الفضاء الإفتراضي، فالطابع العابر للحدود من أكثر الصعوبات التي تواجه التحقيق، لما يثيره من تنازع الإختصاص حسب مبدأ الإقليمية أو الشخصية أو العينية[265]. ولتفادي التنازع جاءت إتفاقية الأمم المتحدة بحل هذا الإشكال[266]، وحذت حذوها إتفاقية أوربا في مادتها 12. ونجد أن المشرع الجزائري نص في المادة 15 من القانون 09-04 على إشكالية الإختصاص وهي نفسها المادة 588 من ق.إ.ج[267]، إضافة إلى مشكلة احترام مبدأ سيادة الدولة[268]والذي يعد من بين أهم الصعوبات التي تعترض التحقيق.

أما الإختصاص داخل الدولة الجزائرية فحلها المشرع بتحديد الإختصاص للمحاكم ووكلاء الجمهورية وقضاة التحقيق في المادة 329 ق.إ.ج. والمرسوم التنفيذي رقم06/348[269] (سبق ذكره).

أضف إلى ذلك صعوبة اكتشاف الجريمة وهذا لغياب الآثار المادية وسهولة محو الدليل، كما أن المجني عليهم يعزفون عن التبليغ، وفي إحصائيات قامت بها الفيدرالية الأمريكية وجدت

---

[265] آمال برحال، مرجع سابق، ص83.

[266] المادة 15 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.

[267] أنظر جمال براهيمي، مرجع سابق، ص190.

[268] اتفاقية بودابست في مادتها 25 حلت مشكلة التدخل في سيادة الدولة وهذا بإقرار المساعدة القضائية للدول الأعضاء في الإتفاقية وأجازت التفتيش عن بعد في مادتها 32. بالمقابل، سمح المشرع الجزائري بالتفتيش عن بعد المادة 3/5 من القانون 09-04)

[269] مريم عراب، مرجع سابق، ص1216.

أن 70% من الجرائم لا تبلغ عنها المؤسسات خاصة التجارية خوفا من فقدان الثقة من العملاء[270].

وبما أن الجاني شخص يتسم بالذكاء فصعوبة تحديد هويته من بين الصعوبات التي تعيق التحقيق ناهيك عن تعذر تحديد العنوان رغم أن لكل حاسب IP خاص به إلا أن الجناة يفرضون تدابير أمنية تعيق الوصول إلى بياناتهم[271]. وبالمقابل نقص خبرة وكفاءة المحققين وقلة التدريب على التعامل مع الأدلة الرقمية وكيفية البحث عنها. فللتكنولوجيا لغة ومفردات يجب تعلمها واستخدامها، كما أن خبرة المحقق في التعامل مع مجرم مطلع على كل تفاصيل التقنية لا يعلمها هذا المحقق، ومراوغة الجاني ومحاولة هروبه من جرمه، وإغراق المحقق في تفاصيل ومتاهات متشعبة، كان على المحقق الجنائي أن يتسلح بتكوين مهاري يجمع بين استخدام التقنية وتقييم الجريمة والجاني، ومهارة التعرف على المكونات المادية والمعنوية للحاسب ومعرفة الأنظمة الأساسية لعمل الشبكات[272].

من بين المعوقات التي تصدم التحقيق وتصعبه حق الإنسان في الخصوصية فقد جرمت معظم التشريعات في العالم التعدي على حياة الإنسان الخاصة باستخدام شبكة الإنترنت، ومنها ميثاق الأمم المتحدة سنة 1948، وكل الإعلانات العالمية لحقوق الإنسان أكدت على مبدأ الخصوصية وسايرتها الدساتير العربية[273] مثل الدستور الجزائري (ارجع للفصل الأول)، وضخامة كم البيانات الواجب التحقيق فيها.

[270] جمال براهيمي، مرجع سابق، ص199.

[271] المرجع نفسه، ص202.

[272] داليا عبد العزيز، مرجع سابق، ص27.

[273] مريم عراب، مرجع سابق، ص1215.

❖ صعوبات ناتجة عن ضعف قوانين مكافحة الجرائم الإلكترونية:

يواجه التحقيق صعوبات ناجمة عن سرعة تطور الجرائم الإلكترونية من جهة، وفي المقابل جمود القوانين الجنائية الموضوعية التقليدية من جهة أخرى. فقصور التشريعات، وعدم كفاية واتساع النصوص العقابية لتشمل الجرائم المستحدثة، ومن بينها جرائم الإبتزاز الإلكتروني، يحول دون التحقيق فيها. كذلك عدم ملاءمة إجراءات التحقيق المألوفة والتقليدية[274].

ويعتبر عدم فعالية التعاون الدولي النابع من تباين التشريعات العقابية للدول وغياب نموذج موحد للنشاط الإجرامي مع صعوبة إجراء المساعدات القضائية الدولية من أكثر الصعوبات التي تواجه التحقيق في الجرائم الإلكترونية العابرة للحدود[275].

ثانيا: الحلول المقترحة لتجاوز الصعوبات في التحقيق:

- تحريك المنظومة التشريعية الوطنية لمواجهة الجريمة، بتطبيق النصوص التقليدية على الجرائم الإلكترونية، حتى لا تترك الحقوق دون حماية. كما يجب ضمان تحيين وتحديث القوانين وفقا لمستجدات الجريمة. (كما رأينا في القواعد المستحدثة والعامة في التحقيق)[276].

أما في المجال الدولي:

- تكثيف التعاون الدولي وتعزيز التعاون القضائي الدولي.

[274] جمال براهيمي، مرجع سابق، ص219 وما بعدها.

[275] نفس المرجع، ص233 وما بعدها.

[276] جمال براهيمي، المرجع السابق، ص243 وما بعدها.

- تبادل الإنابة القضائية، تبادل المعلومات، نقل الإجراءات والتعاون الدولي لتسليم المجرمين، دون أن نغفل عن الحماية الفنية عن طريق البرامج الأمنية، مثل برنامج كشف الاختراق IDS[277].

المطلب الثاني

الإثبات في جريمة الإبتزاز الإلكتروني والصعوبات التي تواجهه

التحقيق والإثبات قرناء لا ينفصلان فالأول يتصل بالوسيلة والآخر بالغاية[278].

تتواجد الأدلة الجنائية في مسرح الجريمة، وفي الجريمة الإلكترونية تتواجد في الوسط الرقمي عموما[279]. وهذا يضاعف الصعوبات التي تواجه رجال الضبط الجنائي والقضائي، ووسائل الإثبات التقليدية لا تجدي نفعا في إثبات هذه الجرائم، فكان من الضروري تطوير وسائل الإثبات تباعا للجريمة الإلكترونية وتطوراتها[280]. وهكذا اتسع نطاق الدليل الإلكتروني وأصبحت الأجهزة الإلكترونية (حواسب، هواتف نقالة ذكية، كاميرات وشبكات الإتصالات الرقمية ...) تشكل مستودعا مهما للمعلومات والبيانات التي تظهر وتكشف الحقيقة، فما طبيعة الدليل الرقمي وما هي حجيته أمام القاضي الجنائي[281].

---

[277] نفس المرجع ص267 وما بعدها.

[278] أحمد لطفي السيد مرعي، مرجع سابق، ص34.

[279] أكرم ديب، نورة بن بو عبد الله، دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني، مجلة الحقوق والعلوم الإنسانية، الجزائر، المجلد16، العدد01، سنة2023، ص40.

[280] الحسن بوالشعير، شعيب حداد، مرجع سابق، ص95.

[281] أحمد لطفي السيد مرعي، مرجع سابق، ص34.

الفرع الأول: الإثبات في جريمة الإبتزاز الإلكتروني:

يقصد بالإثبات: "إقامة الحجة والدليل والبرهان، ولكنه لا يصل إلى درجة اليقين الذي لا يقبل الشك. فللدليل عدة استخدامات كأن يكون وسيلة لإثبات واقعة، أو وسيلة للدفاع إذا كان لصالح المتهم. ولإظهار حقيقة فعل مرتكب يدعي به المدعي وينكره المتهم.[282]"

أولا: الطبيعة القانونية للدليل الرقمي:

يعتبر الدليل الجنائي الرقمي الدليل المأخوذ من أجهزة الكومبيوتر في شكل مجالات مغناطيسية أو نبضات كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة[283].

I. تعريف الدليل الرقمي: تعتبر المنظمة الدولية لأدلة الحاسوب IOCE المرجع الأساسي لتعريف الدليل الرقمي سنة 2000: "المعلومات المخزنة والمتنقلة بشكل ثنائي والتي يمكن الإعتماد عليها أمام المحكمة". وعرفته مجموعة العمل العلمية للأدلة الرقمية SWEGDE "مجموعة المعلومات القيمة التي تخزن أو ترسل في شكل رقمي .[284]"

"مجموعة من البيانات أو المعلومات التي تتمكن من أن تثبت بأن جريمة ما وقعت أو وجود صلة بين الجريمة والجاني أو وجود علاقة بين الجريمة والمجني عليه."

وتعريف البيانات الرقمية: "مجموعة الأرقام التي تمثل المعلومات كافة بما فيها الصوت والصورة والنصوص المكتوبة.[285]"

---

[282] داليا عبد العزيز، مرجع سابق، من ص27 إلى ص 76.

[283] وائل سليم عبد الله شاطر، مرجع سابق، ص441.

[284] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص401.

[285] داليا عبد العزيز، مرجع سابق، من ص27إ لى ص 76.

لم يعرف المشرع الجزائري الدليل الإلكتروني سواء في قانون 09-04 أو في المرسوم 261/15 المتعلق بتنظيم الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال[286]. تنبه المشرع المصري وعرفه في المادة الأولى من القانون 175 لسنة 2018[287]. يعود السبب في تسميته بالدليل الرقمي لأن كل البيانات داخل العالم الإفتراضي (صور، تسجيل، نص ...) تأخذ شكل أرقام، ومن ثم تحويلها عند عرضها إلى صورة أو تسجيل أو نص[288].

II. مميزات الدليل الرقمي:

يعتقد البعض أن الأدلة الجنائية الإلكترونية هي مرحلة متقدمة من الأدلة التقليدية المادية ولكن الحقيقة عكس ذلك، وتظهر من خصائصها المرتبطة أساسا بطبيعة البيئة التي تتواجد فيها[289]:

- الدليل الرقمي دليل علمي: يتشكل من معطيات إلكترونية غير ملموسة يتم استخلاصها من طبيعة تقنية المعلومات[290].
- الدليل الرقمي دليل تقني: مستوحى من البيئة التقنية والمتمثلة في مختلف الأجهزة التكنولوجية (حواسب-هواتف-شبكات-خوادم-مضيفات ...) ولا يمكن تواجده خارج هذا الإطار[291].
- دليل قابل للنسخ :على خلاف الأدلة التقليدية التي لا تتوافر فيها هذه الخاصية فإن الدليل الرقمي يمكن استخراج نسخ منه مطابقة للأصل ولها نفس القيمة العلمية، لذا فهو محمي

[286] عبد القادر فلاح، نادية آيت عبد المالك، مرجع سابق، ص1700.

[287] أحمد لطفي السيد مرعي، مرجع سابق، ص36.

[288] مريم عراب، مرجع سابق، ص1222.

[289] جمال براهيمي، مرجع سابق، ص124

[290] عبد القادر فلاح، نادية آيت عبد المالك، مرجع سابق، ص1700.

[291] جمال براهيمي، مرجع سابق، ص125.

تقنيا من أي استخدام غير مشروع لمحتواه بغرض محاولة الطمس أو الإخفاء أو الإتلاف[292].

- صعوبة التخلص منه وهي أهم ميزة يتمتع بها هذا الدليل الإلكتروني عن غيره من الأدلة المادية (قتل الشهود–مسح البصمات ...) إذ يمكن استرجاع الدليل الرقمي بعد محوه وإصلاحه بعد إتلافه وإظهاره بعد إخفائه باستخدام برمجيات مثل Recovery. كما أن الجاني إذا حاول التخلص من الملفات في الحاسوب يتم تسجيله وتخزينه في ذاكرة الجهاز ويمكن استخلاصه لاحقا كدليل إثبات ضد الجاني[293].
- الرقمية الثنائية للدليل الرقمي: يتكون من تعداد غير محدود لأرقام ثنائية موحدة من الصفر والواحد، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة البث، وتختلف من حيث الحجم والموضوع، فكمية الرقمية الثنائية في ملف معين تختلف عن الحجم في ملف آخر[294].
- الدليل الرقمي متطور ومتنوع: تبعا للمصدر المستمد منه. فالتطور خاصية تلقائية نظرا لارتباطه بطبيعة حركة الإتصال عبر الإنترنت، وأما التنوع فقد يكون في عدة أشكال (بيانات مقروءة – أفلام رقمية ...)[295].

ثانيا: القيمة القانونية للدليل الرقمي الجنائي في الإثبات:

يعتبر الإثبات الجزائي العصب الرئيسي للحكم الجزائي الذي يقضي به القاضي إما ببراءة المتهم أو إدانته[296].

---

[292] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص403.

[293] جمال براهيمي، مرجع سابق، ص126.

[294] سمير عالية، مرجع سابق ،ص431.

[295] عزيزة رابحي، مرجع سابق، ص267.

[296] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص409.

كما تخضع مسألة قبول الدليل الرقمي إلى نوع النظام القانوني المتبنى من طرف الدولة. فمنها من يأخذ بنظام الأدلة القانونية ومنها من يأخذ بنظام الإثبات الحر[297] مثل المشرع الفرنسي والمشرع الجزائري في المادة 212 ق.إ.ج والمادة 06 من القانون 09-04[298].

I. شروط قبول الدليل الرقمي أمام القضاء:

يقبل الدليل عموما وفقا لمعايير قانونية وقضائية يقرر القاضي وفقها قبول الدليل أو رفضه، والدليل الإلكتروني باعتباره واحد من الأدلة فإن العمل به مرهون بتوفر جملة من الشروط منها:[299]

1- مشروعية الدليل الرقمي:

يجب أن يكون الدليل الرقمي مشروعا، أي أن جمع الأدلة الرقمية يجب أن يكون ضمن الإطار العام المحدد في الدستور وإلا يكون باطلا بطلانا مطلقا لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به وللمحكمة أن تقضي به من تلقاء نفسها[300]، مثل الضغط أو إكراه المشتبه فيه دون مسوغ قانوني.[301]

2- مبدأ يقينية الدليل الرقمي (غير قابل للشك):

---

[297] بن فردية، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي والعلوم الإجرامية، كلية الحقوق، جامعة الجزائر، سنة 2015، ص384 وما بعدها.

[298] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص409.

[299] خالد ضو، حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي آفلو-الأغواط، العدد الثامن سنة 2022، ص206.

[300] مبارك بن الطيبي، محمد حموني، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، الجزائر، المجلد 05 العدد 02 سنة 2019، ص27.

[301] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص410.

لا مجال لدحض قرينة البراءة أو الإدانة إلا عندما يصل اقتناع القاضي إلى حد الجزم باليقين[302]، فتبنى اليقينية التي تقود القاضي للبينة القانونية والحقيقة وفق الخبرة الإلكترونية للتأكد من عدم العبث به والتغيير فيه[303]، فمجرد الشك يفسر لصالح المتهم في المسائل الجنائية[304].

3-استساغة الدليل عقلا: القاضي حر في اقتناعه بالدليل وله أن يؤسس حكمه عليه بالإدانة أو البراءة ولا يخضع لرقابة قضائية، المهم تسبيب حكمه تسبيبا كافيا يقبله العقل والمنطق[305].

4- إمكانية مناقشة الدليل الرقمي:

لا يمكن للقاضي أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى، فكل دليل رقمي يجب أت يعرض في الجلسة بصفة مباشرة أمام القاضي للمناقشة، وله الحرية والاجتهاد في الحكم بعد استشارة الخبراء وارتياح ضميره[306]. والمناقشة ضمانة هامة من ضمانات المحاكمة العادلة طبقا للمادة 2/212 ق.إ.ج[307].

II. حجية الدليل الرقمي في جريمة الإبتزاز الإلكتروني

[302] سامية بلجراف، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، الجزائر، المجلد 07، العدد01، سنة 2021، ص686.

[303] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص411.

[304] خالد ضو، مرجع سابق، ص207.

[305] عزيزة رابحي، مرجع سابق، ص270.

[306] مبارك بن الطيبي، محمد رحموني، مرجع سابق، ص28.

[307] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص410.

يقصد بحجية الدليل الرقمي ما يتمتع به من القوة الإستدلالية في كشف الحقيقة وصدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه[308]. (الحصول على الدليل وتقديمه للقضاء لا يعني الإدانة وإنما تخضع لسلطة القاضي).

من الممكن عدم إدراك القاضي للحقائق المتعلقة بالدليل الإلكتروني لعدم كفاءته التقنية، فضلا عن تمتع الدليل بقيمة إثباتية تصل إلى حد اليقين مع الطبيعة الفنية للدليل الإلكتروني، والتي يمكن العبث بمضمونه بسهولة على نحو يحرف الحقيقة دون إدراك لذلك من غير الخبراء. فكيف تكون سلطة القاضي الجزائي مع هذه الصعوبات في قبول أو رفض هذا الدليل؟[309].

يتمتع الدليل الإلكتروني بحجية قوية في الإثبات بحكم طبيعته العلمية ويحتل مرتبة أفضل دليل، هذا رأي الفريق الأول الذي رأى بحجية الدليل الإلكتروني المطلقة.

أما الفريق الثاني فرأى أن إعطاء الدليل الإلكتروني قوة ثبوتية مطلقة رجوع إلى نظام الإثبات المقيد وهي قرائن يستخلص منها الدليل[310].

حسم المشرع الجزائري موقفه في نصي المادتين 212 و307 من قانون الإجراءات الجزائية. خاصة أن قانون 09-04 وقانون الإجراءات الجزائية لم يتضمنا القواعد الخاصة بالدليل الإلكتروني[311]، أي منحا القاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لقناعته الذاتية واستلهام عقيدته من أي وسيلة أو دليل يطمئن إليه ضميره[312].

الفرع الثاني: الصعوبات التي يثيرها الدليل الرقمي في الإثبات والحلول المقترحة :

أولا: الصعوبات التي يثيرها الدليل الرقمي في الإثبات:

---

[308] جمال براهيمي، مرجع سابق، ص150.

[309] نفس المرجع، ص151.

[310] نفس المرجع، ص161 وما بعدها.

[311] مبارك بن الطيبي، محمد رحموني، مرجع سابق، ص28

[312] جمال براهيمي، نفس المرجع، ص167-168.

تنبع الصعوبات التي يثيرها الدليل الرقمي في جرائم الإبتزاز الإلكتروني من أن هذا النوع من الجرائم يحدث في الخفاء، والجاني ملم بالمعرفة التقنية ومتصف بالذكاء، وبالرغم من الجهود المبذولة لمكافحة هذه الجرائم إلا أن هناك صعوبات تواجه رجال السلطة في الإثبات بالدليل الرقمي منها ما هو مرتبط بالدليل نفسه، ومنها متعلق بنقص الخبرة، ومنها ما هو متعلق بإحجام المجني عليه وأخرى بصعوبة التعاون الدولي[313]:

I. صعوبات متعلقة بالدليل ذاته:

- سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره:

انعكس ارتباط الجريمة الإلكترونية عموما وجريمة الإبتزاز الإلكتروني خصوصا بالبيئة التقنية على طبيعة الدليل المترتب عنها، كون البيانات والمعلومات عبارة عن نبضات إلكترونية يمكن استقبالها، أو إشعاعات كهرومغناطيسية يمكن إلتقاطها، تمكن الجاني من فرض تدابير أمنية، كمنع اكتشافه وبالتالي صعوبة الحصول على دليل ضده[314]. فيستعمل المجرم عدة أساليب لإخفاء آثار جريمته من محو أو تعديل أو تدمير.

- عرقلة الوصول إلى الدليل: وضع العقبات الفنية من قبل الجناة كتشفير الملفات الرقمية لمنع الكشف عن جريمتهم[315].
- صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي:

يستخدم مجرمو الجرائم الإلكترونية برامج إخفاء الهوية أو استعمال الهوية المستعارة مثل برنامج TOR الذي يحضر الوصول وحركة المرور وإخفاء عنوان بروتوكول

[313] وائل سليم عبد الله شاطر، مرجع سابق، ص442.

[314] بن شهرة الشول، هانية بوشارب، مرجع سابق، ص71.

[315] وائل سليم عبد الله شاطر، مرجع سابق، ص443.

الأنترنت، فيتيح مشاركة المعلومات دون الكشف عن أنشطة الجناة مما يصعب عمل المحققين[316].

- الطبيعة غير المرئية للدليل الإلكتروني: فهو موجود في عالم افتراضي يصعب قراءته واستيعابه بوسائل غير تقنية، أو استخراجه في شكل ملموس يتطلب خبرة عالية، لا تتوفر عادة لدى مصالح الشرطة القضائية المكلفة[317].

II. صعوبات متعلقة بنقص الخبرة وكفاءة سلطات الإستدلال: قد يؤدي عدم إلمام المحقق بمعارف التقنية، أو عدم الاهتمام بمستجداتها، أو جهله باللغة العلمية الرقمية إلى تدمير الدليل وإتلافه، ما يستدعي تدريب الكوادر لكن قد يكون هذا فوق الميزانية المرصودة لهذا الغرض[318].

III. صعوبات متعلقة في إحجام المجني عليه عن الإبلاغ:

يرجع السبب في ذلك إلى خوف المجني عليه من الإبلاغ كي لا يفتضح أمره، فالجريمة ارتكبت أساسا لخوف المجني عليه من انكشاف أسراره وهذا الإحجام يساعد على اختفاء الدليل الرقمي[319].

IV. صعوبة التعاون الدولي:

تختلف التشريعات الدولية في تجريم الإبتزاز الإلكتروني من دولة لأخرى مما صعب ملاحقة الجناة، ورغم المناداة بضرورة التعاون الدولي في مكافحة هذه الجريمة، إلا أن هناك صعوبات تعتريها منها مثلا عدم وجود نموذج واحد متفق عليه يتعلق بالنشاط الإجرامي فضلا عن عدم وجود تنسيق دولي للإجراءات الجنائية في شأن هذه الجريمة، إضافة إلى ذلك عدم

[316] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص414.

[317] بن شهرة الشول، هانية بوشارب، مرجع سابق، ص69.

[318] جمال براهيمي، مرجع سابق ص209 وما بعدها.

[319] داليا عبد العزيز، مرجع سابق، ص27 إلى ص 76.

وجود معاهدات دولية ثنائية وما يعرقل الوصول إليها عيب الإختصاص على المستوى المحلي والدولي[320].

ثانيا: حلول الإشكالات التي يثيرها الدليل الرقمي في الإثبات:

على الرغم من الصعوبات التي أثيرت في الإثبات والمتعلقة بالدليل الإلكتروني إلا أن هذا لا ينفي وجود تقنيات وأدوات فنية تتلاءم وطبيعة الدليل الرقمي في جريمة الإبتزاز لا سيما مع النمو الرقمي في مجال التكنولوجيا[321]:

- الإهتمام أكثر بالتأهيل التقني والفني لجهات التحقيق في مجال التعامل مع الأدلة الإلكترونية وإمدادهم بأفضل وسائل التقنية الحديثة[322].
- تسخير التكنولوجيا الحديثة في استخلاص الدليل الإلكتروني وتطويعها، وتطوير برامج مضادة لاقتفاء أثر الجناة والوصول إليهم، وإدراج الذكاء الإصطناعي مع الإستعانة بالخبراء[323].

[320] وائل سليم عبد الله شاطر، مرجع سابق، ص443 و444.

[321] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص414.

[322] بن شهرة الشول، هانية بوشارب، مرجع سابق، ص76.

[323] أكرم ديب، نورة بن بو عبد الله، مرجع سابق، ص414.

المبحث الثاني

صعوبات تحديد القانون الواجب التطبيق والمحكمة المختصة في جريمة الإبتزاز الإلكتروني والعقوبات المترتبة

تتمثل أهم الإشكالات المطروحة في الجرائم الإلكترونية عامة وجرائم الإبتزاز الإلكتروني خاصة أساسا في إشكالية الإختصاص القضائي والقانون الواجب التطبيق[324] على المستويين المحلي والدولي. فكيف عالج المشرع الجزائري تحديد قواعد الإختصاص على المستويين؟ ثم كيف تكون عقوبة الإبتزاز الإلكتروني؟ للإجابة على هذا السؤال أقسم المبحث إلى مطلبين: المطلب الأول الإختصاص القضائي والمطلب الثاني العقوبات المترتبة على جريمة الإبتزاز الإلكتروني.

[324] سارة محمد حنش، مرجع سابق، ص70.

المطلب الأول: الإختصاص القضائي.

يعنى بالاختصاص القضائي مباشرة سلطة المتابعة والتحقيق والحكم في الجريمة.

الفرع الأول: الإختصاص القضائي الدولي:

الغالب لحل مشكلة الإختصاص القضائي في الجريمة الإلكترونية هو تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الإختصاص الجزائي الدولي في الجرائم التقليدية، وعلى رأسها إقليمية القوانين، أي تطبيق القانون الجزائري على الجرائم المرتكبة في إقليم الدولة أيا كانت جنسية الجاني[325].

ولأن الجرائم المستحدثة باتت أكثر انتشارا، فإن مبدأ الإقليمية لم يعد يتسع لها، فلجأت إلى مبدأ العينية وهو تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة والمرتكبة خارج إقليمها مهما تكن جنسية مرتكبها [326] (م15 من قانون 09-04) ومبدأ الشخصية وهو ملاحقة الجاني بالقانون الذي يحمل جنسية الدولة حتى وإن كان الجاني أجنبيا وهذا حماية لرعايا الدولة[327].

الفرع الثاني: الإختصاص القضائي الداخلي:

يتحدد الإختصاص بمحل وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه فيهم أو المكان الذي تم في دائرته القبض على هؤلاء ولو حصل القبض لسبب آخر[328].ولما كانت جرائم الإبتزاز الإلكتروني لا تعرف إقليما محددا تفطن المشرع الجزائري ومد الإختصاص

---

[325] مريم عراب، الإختصاص القضائي في الجرائم المعلوماتية، مجلة القانون والعلوم السياسية، الجزائر، المجلد7 العدد3 سنة 2015، ص276.

[326] بجاد عبد الرؤوف بوديسة، مرجع سابق، ص80.

[327] مريم عراب، مرجع سابق، ص279.

[328] المادة 37 من قانون الإجراءات الجزائية الجزائرية.

لوكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية[329] (الفصل الأول) واختصاص المحاكم. المادة 329 تمديد الإختصاص لدائرة محاكم أخرى (مرسوم تنفيذي348/06) أي أن الإختصاص القضائي يتحدد حسب ضرورة التحقيق وفي جرائم معينة (م5 من القانون 09-04) وبالتالي الإختصاص القضائي الداخلي لا يثير أي مشاكل ما دام المشرع تدخل لحله.

[329] المواد 40 -37 – 1/16 من ق.إ.ج.

المطلب الثاني

العقوبات المترتبة على جريمة الإبتزاز الإلكتروني

لضمان تحقيق الردع الخاص للمجرم والردع العام للمجتمع ككل، نظم المشرع لكل فعل أو ترك مخالفين لنصوصه الموضوعة عقوبة. وتعد العقوبات من أهم الآثار التي تترتب على تجريم السلوك المعتدي. فللعقوبة وجه علاجي وآخر عقابي، وتختلف الأنظمة والقوانين المجرمة في كل دولة باختلاف السياسة الجنائية التي يتخذها المشرع بين التشديد والتخفيف[330]. وهناك العقوبات الأصلية والعقوبات التكميلية.

الفرع الأول: العقوبات الأصلية[331]:

لكل جريمة جزاء وتتفاوت العقوبة بحسب فاعلها وبحسب كونه شخصا طبيعيا أو معنويا[332].

نلاحظ بالاطلاع على نص المادة 303 مكرر و المادة 303مكرر1 أن المشرع عدد السلوك المادي المكون للجريمة (سبق ذكره في الركن المادي لجريمة الإبتزاز الإلكتروني) وأقر العقوبة التالية:

أولا: عقوبات الشخص الطبيعي:

1- العقوبة السالبة للحرية: وهي الحبس من 6 أشهر إلى 3 سنوات، مما يجعل أمر تقدير العقوبة للسلطة التقديرية للقاضي[333].

---

[330] داليا عبد العزيز، مرجع سابق، من ص27إلى ص 76.

[331] ارجع إلى المادة 5 مكرر من قانون الإجراءات الجزائية الجزائرية.

[332] خديجة روابح، فادية قلي، الحماية القانونية لحرمة المحادثات الشخصية، مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة 8 ماي 1945، قالمة، سنة 2022-2023، ص55.

[333] نورة هارون، وهيبة برازة، حق الفرد على صورته بين مقتضيات الحق في حرمة الحياة الخاصة وضرورات الكشف عن الجريمة، حوليات جامعة الجزائر1، المجلد35، العدد3، 2021 ص316.

2-العقوبة المالية: أرفق المشرع بالعقوبة السالبة للحرية عقوبة مالية نص عليها بموجب (المادة 303 مكرر) وهي من 50.000 دج إلى 300.000 دج مما يجعل إعمال السلطة التقديرية للقاضي ممكنا بين الحدين الأدنى والأقصى[334].

كما عاقب بالشروع في الجريمة بنفس العقوبات التي قررها للجريمة التامة على أن يضع صفح الضحية حدا للمتابعة[335].

العقوبات المستحدثة: استحدث المشرع الجزائري المادة 26 في القانون رقم24-06 المؤرخ في 19 شوال عام 1445 الموافق ل28 ابريل سنة 2024 المعدل والمتمم للأمر رقم66-156 المؤرخ في 18 صفر عام1386 الموافق ل8يونيو سنة 1966 والمتضمن قانون العقوبات، الصادر في ج .ر عدد30،الصادرة في 21شوال عام1445 هـ ،الموافق ل30ابريل سنة 2024م،(م333 مكرر4)والتي نصت على عقوبة:

حبس من سنة إلى خمس سنوات وبغرامة مالية من 100.000دج إلى500.000دج كل من نشر أو أذاع أو هدد بأي طريقة كانت صورا أو فيديوهات أو رسائل إلكترونية أو أي معلومات خاصة لأي شخص كان قد التقطها أو تحصل عليها دون إذنه أو رضاه.

حبس من ثلاث سنوات إلى سبع سنوات كل من استعمل صورا إلكترونية للغير أو قام بتحويرها أو نقلها أو نسخها أو نشرها قصد الإضرار به ، وتضاعف العقوبة إذا مورست ضغوطات على الضحية . نلاحظ هنا أن المشرع قد شدد في العقوبة سواء السالبة للحرية أو العقوبة المالية. ويزيد في التشديد بالحبس من خمس إلى عشر سنوات وبغرامة من500.000دج إلى1.000.000دج اذا تعلق الأمر بنشر صور خادشة أو التهديد بالنشر من الخاطب أو المخطوبة أو من الزوج أو الزوجة أثناء قيام الرابطة أو بعد انتهائها وذلك طبقا ل (م333 مكرر5). وتضاعف العقوبة إذا استعملت بتكنولوجيا الإعلام والإتصال (م 333 مكرر 6)

[334] نورة هارون، وهيبة برازة، المرجع السابق ونفس الصفحة.

[335] أنظر المادة 303 مكرر ق.إ.ج.

ثانيا: عقوبات الشخص المعنوي

أقر الإتجاه الحديث في التشريعات العقابية مسؤولية الشخص المعنوي عن الجرائم التي يرتكبها ممثلوه ولصالحه[336]. وخطا المشرع الجزائري نفس الخطوة في تحميل الشخص المعنوي الخاضع للقانون الخاص المسؤولية الجزائية عن مخالفات ممثليه الشرعيين أو أجهزته المرتكبة لحسابه[337].حسب المادة 303 مكرر3: أن الشخص المعنوي يكون مسؤولا جزائيا عن الجرائم المحددة قانونا وتطبق عليه عقوبة الغرامة وفقا للمادة 18 مكرر2.فالعقوبة الأصلية في هذه الحالة (الغرامة) والتي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي (م18 مكرر) أي من 300.000 دج إلى 1.500.000 دج. وإزاء عدم نص القانون على عقوبة الغرامة بالنسبة للأشخاص الطبيعيين سواء في الجنايات أو الجنح، وقامت المسؤولية الجزائية للشخص المعنوي طبقا لأحكام المادة 51 مكرر، فإن الحد الأقصى للغرامة للشخص المعنوي يكون كالآتي:

- 2.000.000دج عندما تكون الجناية معاقبا عليها بالإعدام أو بالسجن المؤبد،
- 1.000.000دج عندما تكون الجناية معاقبا عليها بالسجن المؤقت،
- 500.000 دج بالنسبة للجنحة وهذا طبقا للمادة18مكرر2.

[336] زوليخة رواحنة، نادية رواحنة، جريمة انتهاك حرمة المكالمات أو الأحاديث الخاصة أو السرية في قانون العقوبات الجزائري، مجلة الفكر،الجزائر، المجلد17، العدد02 2022، ص324.

[337] المادة 07 من الأمر 03-01 المؤرخ في 19 فيفري 2003 المعدلة للمادة 05 من الإمر 96-22 المؤرخ في 9 جويلية 1996 الذي يتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة الأموال من وإلى الخارج، ج.ر. عدد43 صادرة في 10 جويلية 1996 معدل ومتمم. والمادة 65 مكرر من القانون 14/04 المؤرخ في 10 نوفمبر والمتضمن قانون الإجراءات الجزائية.

✔ يذكر أنه من شروط قيام المسؤولية للشخص المعنوي[338]:

- أن يكون الشخص المعنوي خاضعا للقانون الخاص.
- اقتراف الجريمة من قبل أجهزة الشخص المعنوي أو ممثليه الشرعيين[339].

الفرع الثاني: العقوبات التكميلية:

تعرف العقوبة التكميلية بأنها العقوبة التي تصيب الجاني بناء على الحكم بالعقوبة الأصلية بشرط أن يحكم القاضي بالعقوبة الأصلية، وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناء على الحكم بالعقوبة الأصلية دون الحاجة إلى إصدار حكم تبعي فهو مرتبط ارتباطا مباشرا بالعقوبة الأصلية[340].

وفي جريمة الإبتزاز الإلكتروني يفرق أيضا بين الشخص الطبيعي والمعنوي.

أولا: عقوبات الشخص الطبيعي: تنقسم العقوبات التكميلية إلى وجوبية وجوازية[341].

1. العقوبات التكميلية الوجوبية: تتمثل في الحكم بمصادرة الأشياء المستعملة لارتكاب الجريمة (م303 مكرر2)[342] والتي أحالت للمادة 9 مكرر1 والمادة 18، فالحكم بالمصادرة وجوبي. وحسب (م333 مكرر7) المستحدثة في قانون 24-06 سابق الذكر يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجرائم المنصوص عليها في م 333 مكرر4 وم333 مكرر5 وم 333 مكرر6 والأموال المتحصلة منها

[338] ناجية الشيخ، الإقرار بالمسؤولية الجزائية للشخص المعنوي في جرائم الصرف، منصة المجلات العلمية الجزائرية، الجزائر، المجلد02، العدد1، سنة 2011، ص27.

[339] المادة 51 مكرر من قانون العقوبات الجزائري.

[340] داليا عبد العزيز، مرجع سابق، من ص27إلى ص 76.

[341] نورة هارون، وهيبة برازة، مرجع سابق، ص316.

[342] نفس المرجع ونفس الصفحة.

وإغلاق الموقع أو الحساب الإلكتروني المستعمل لارتكاب الجريمة، وغلق المحل الذي ارتكبت فيه الجريمة إذا كان المالك يعلم بها.

الملاحظ أن المشرع الجزائري قد وسع في الأشياء المصادرة عن ذي قبل وشدد في العقوبة، وهذا لردع الجناة والحد من تفشي الإبتزاز والمساهمة في ارتكابه.

2. العقوبات التكميلية الجوازية: (المادة303 مكرر2) تتمثل في منع المحكوم عليه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر1 من ق.ع. لمدة لا تتجاوز 5 سنوات. كما يجوز للمحكمة أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 من قانون العقوبات[343]. في حالة الحكم بعقوبة جنائية، يجب على القاضي أن يأمر بالحرمان من حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 لمدة أقصاها عشر (10) سنوات، تسري من يوم انقضاء العقوبة الأصلية أو الإفراج عن المحكوم عليه.

ثانيا: العقوبات التكميلية المقررة للشخص المعنوي:

ذكرت المادة 303 مكرر 03 في فقرتها الأخيرة "يتعرض أيضا لواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 18 مكرر والتي تنص على:

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر وتعليق حكم الإدانة.

[343] نورة هارون، وهيبة برازة، المرجع السابق، ص316.

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.[344]

[344] تناول المشرع الفرنسي جريمة الإبتزاز الإلكتروني في المادة 312 في الفقرات من 1 الى 12 من قانون العقوبات إذ فرق بين الإبتزاز بالإيذاء المادي والذي أقر له عقوبة السجن سبع سنوات وغرامة مالية 100,000 يورو، والتهديد بالإيذاء المعنوي بالسجن خمس سنوات وغرامة مالية قدرت ب 75,000 يورو وعلى خلاف المشرع الجزائري أفرد فقرات المادة 312(2 3 4 5 6 7 11) بالعقوبة المشددة بالسجن لعشر سنوات وغرامة 150,000 يورو كما أورد إعفاء وتخفيضا في العقوبات في الفقرة 6-1 من المادة 312 قانون العقوبات الفرنسي، ولكن تدارك المشرع الجزائري الامر واستحدث مواد شددت في العقوبة وهذا في المواد333 مكرر4 م 333 مكرر5 وم333 مكرر6 في القانون رقم24-06 المؤرخ في 19 شوال1445 الموافق ل28 افريل 2024 المعدل والمتمم للأمر رقم66-156 المؤرخ في 18 صفر1386 الموافق ل8 يونيو1966 والمتضمن قانون العقوبات الصادر في ج ر العدد30الصادرة في 21 شوال 1445 الموافق ل30 اقريل2024، و نص القانون الفرنسي على المصادرة كعقوبة تبعية المادة 312 / 13 -4 والحرمان من بعض الحقوق والمزايا كعقوبة تكميلية المادة 312/ 13 -2 قانون العقوبات الفرنسي.

وبالمقارنة نص المشرع المصري على عقوبة الإبتزاز الإلكتروني في المادة 25 من القانون رقم 175 لسنة 2018 بالحبس بمدةلا تقل عن ستة أشهر وبغرامة لا تقل عن 50,000 جنيه ولا تتجاوز 100,000 جنيه. وشدد العقوبة الى الحبس بين سنتين على الأقل وخمس سنوات على الأكثر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين إذا كانت الجريمة اقترفت لربطها بمحتوى منافي للآداب العامة أو لإظهار المجني عليه بطريقة من شأنها المساس باعتباره أو شرفه "المادة 26 من قانون مكافحة جرائم تقنية المعلومات المصري. كما عاقب بالسجن المشدد إذا اقترفت الجريمة ضد الآمن القومي للبلاد أو إضرارا للنظام العام المادة 34 من نفس القانون كما شدد العقوبة إذا كان المجني عليه طفلا وخففها إذاكان هو الجاني طبقا لقانون الطفل.

واكد على العقوبة التكميلية حتى جعلها وجوبية وهي مصادرة الأجهزة المستخدمة في جريمة الإبتزاز الإلكتروني.

وعاقب في الشروع في جريمة الإبتزاز الإلكتروني بخلاف المشرع الجزائري بنصف الحد الأقصى للعقوبة المقررة للجريمة التامة وأكد على قيام المسؤولية الجزائية للشخص الإعتباري متى ارتكبت باسمه ولحسابه.

خلاصة الفصل الثاني

تناول الفصل الثاني في المبحث الأول التحقيق والإثبات في جريمة الإبتزاز الإلكتروني والصعوبات التي تتصدى لهما حيث تطرقت لإجراءات التحقيق العامة والمستحدثة موضحة الصعوبات التي تواجه الهيآت المختصة في هذه الجرائم، كما ذكرت بعض الحلول المقترحة. وكذا الإثبات حيث أخذ الدليل الرقمي حقه في التعريف به وبمميزاته وشروط قبوله مع تبيان حجيته، مع ذكر الصعوبات في استعماله وبعض الحلول الممكنة.

وعالج في المبحث الثاني صعوبات الاختصاص القضائي والقانون المطبق والعقوبات المترتبة على جريمة الإبتزاز الإلكتروني.

خاتمة

في ختام هذا البحث المتعلق بالآليات القانونية لحماية الأشخاص من الإبتزاز الإلكتروني، يمكن القول أن التطور العلمي ودخول التقنية الإلكترونية والشبكة العالمية قرب المسافات البعيدة، مما أدى الى تدخلها في مختلف نواحي الحياة، وأصبح يستعملها مختلف الفئات العمرية وهذا أدى إلى تمادي المجرمين على الاعتداء على حرية الحياة الخاصة، فهذه الجريمة مستحدثة وعابرة للحدود تهدف إلى إلحاق الضرر بالغير وبأمواله وهي في تطور مستمر، تطور الوسائل المرتكبة بها الجريمة الغامضة أو كما تعرف بالجريمة الناعمة. ويتميز مرتكبها بشدة الإحترافية، وهي تشكل أكبر تهديد للأمن والاستقرار، لذا وجب اعتماد العديد من الإجراءات والتدابير التي إن لم تحد منها ساهمت في خفض وقوعها. وبعد الإنتهاء من البحث الذي عرضنا من خلاله:

إبراز المنظمات والمجموعات التي لعبت دورا في مكافحة جريمة الإبتزاز الإلكتروني ووصلت لوضع آليات تعاون دولي تمخض في تشريعات عالمية أو اتفاقيات دولية ومنها منظمة الأمم المتحدة، الشرطة الدولية، واتفاقية بودابست. كذلك اللجنة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا) والجامعة العربية.

ثم انتقلنا لمواجهة الإبتزاز الإلكتروني في التشريع الجزائري حيث أعطى المشرع الجزائري حماية لحرية الأشخاص وحياتهم الخاصة في دستور 1996، وسن مجموعة من النصوص القانونية التي تخص الجرائم المعلوماتية عامة سنة2004 بصدور القانون 04/ 15المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم156/66 المتضمن قانون العقوبات، ولما انتشرت الجرائم الإلكترونية خصه بتعديل سنة2006. وأدرج جرائم المعالجة الآلية للمعطيات ضمن قانون 04/09.بعدها دلفنا إلى الموضوع للتعريف بالجريمة وصورها وطرق ارتكابها وكذا مدى خطورتها، واكتشفنا أن المشرع الجزائري لم يتطرق لتعريف جريمة التهديد الإلكتروني كما عرفها المشرع الفرنسي والمصري والإماراتي والسعودي، وعرفها الفقه أنها "كل قول أو كتابة من شأنه إلقاء الرعب والخوف

في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخدشة للشرف وقد يحمله التهديد تحت تأثير ذلك الخوف إلى استجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب "

وبما انها نتاج تقنية المعلومات فقد اكتسبت لونا وطابعا خاصا يختلف عن الجرائم التقليدية ومن بين خصائصها سهولة وسرعة التنفيذ، صعوبة اكتشافها، عابرة للحدود، جرائم دون عنف، ذكاء وحرفية الجاني، سهولة إتلاف الأدلة من طرف الجناة، قلة الإبلاغ عن الجريمة. ثم عددنا صور الإبتزاز الإلكتروني بحسب الضحية المستهدفة (شخصية اعتبارية، أحداث، رجال، نساء) أو الهدف المرجو من الإبتزاز (مادي، جنسي، نفعي) او بحسب وسائل ارتكابها (صور، مقاطع صوتية أو مرئية، تهديد إلكتروني). ترتكب الجريمة بعده طرق إما باستعمال الحاسب الآلي وملحقاته وبرامجه (الدخول غير المصرح به إلى النظام، الإستيلاء على البيانات المخزنة، واستعماله كبيئة للجريمة كجعله مخزن للمواد الإباحية والبرامج المقرصنة. أو بالأنترنت (الهاتف النقال وبرامجه، خدمة الدردشة، البريد الإلكتروني)

ومن بين الأساليب لكيفية حصول المبتز على المعلومات (أسلوب الولوج غير المشروع إلى المعلومات، أسلوب السرقة المعلوماتية، خيانة الأمانة، الدخول إلى شبكة الأنترنت وتقديم المساعدة الفنية. إنشاء المواقع مثل مواقع الزواج، تقديم خدمة البريد الإلكتروني. إنشاء المتجر الإفتراضي، بيع البرامج وتأجيرها واستعمالها. عقود خدمات الهواتف النقال..). وتقوم جريمة الإبتزاز على أركان أساسية بدونها لا يمكن أن تكون لا جريمة ولا عقوبة. فيجب توفر الركن المادي والمكون من السلوك والنتيجة والعلاقة السببية، كما يجب توافر الإرادة الحرة الواعية والمتمثلة في الركن المعنوي، و الركن الشرعي وهو نص التجريم والعقاب، تضمنه المشرع الجزائري في المواد من 296 إلى 303 من قانون العقوبات ويذكر أن مواد التهديد التقليدي (من 284 إلى 287) والتي جاءت عامة تدخل ضمنها جريمة الإبتزاز الإلكتروني طبقا لإحالة المادة 2 من القانون رقم04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إليها. واستحدث في القانون 24-06 الصادر في30 أفريل2024 مواد 333 مكرر 4 و333مكرر5 و333 مكرر6 و333 مكرر7 حيث نص على عقوبات مشددة .

. ثم الهيآت والأشخاص المكلفين بحماية ضحايا الجريمة والمتمثلة في الشرطة، الدرك الوطني، مقدمي الخدمات، المعهد الوطني للأدلة الجنائية على الإجرام والهيئة الوطنية للوقاية من جرائم الإعلام والإتصال ومكافحتها.

اعتمد المشرع الجزائري على النصوص الجزائية التقليدية في التحقيق (الإنتقال للمعاينة، التفتيش، الضبط في مجال الجريمة الإلكترونية، الخبرة التقنية، تدريب الكوادر، سماع شهادة الشهود، الإستجواب). واستحدث إجراءات تحقيق خاصة لتسع هذه الجريمة بموجب قانون الإجراءات الجزائية الجديد 06-22 والقانون 09-04(التسرب الإلكتروني، إعتراض المراسلات والمراقبة الإلكترونية المتمثلة في تسجيل الأصوات التقاط الصورو الحفظ والإفشاء العاجلان للمعطيات الإلكترونية)

الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني هي تنازع الإختصاص كونها عابرة للحدود و مشكلة احترام مبدأ سيادة الدولة، صعوبة اكتشاف الجريمة وهذا لغياب الآثار المادية وسهولة محو الدليل، كما أن المجني عليهم يعزفون عن التبليغ، صعوبة تحديد هوية الجاني وتعذر تحديد العنوان، فرض الجناة لتدابير أمنية تعيق الوصول إلى بياناتهم. نقص خبرة وكفاءة المحققين، حق الإنسان في الخصوصية، ضخامة كم البيانات الواجب التحقيق فيها. سرعة تطور الجرائم الإلكترونية، جمود القوانين الجنائية الموضوعية التقليدية، عدم ملاءمة إجراءات التحقيق المألوفة والتقليدية. عدم فعالية التعاون الدولي، تباين التشريعات العقابية للدول وغياب نموذج موحد للنشاط الإجرامي مع صعوبة إجراء المساعدات القضائية الدولية. ثم عرجنا إلى الإثبات أين يتواجد الدليل الجنائي في مسرح الجريمة، في الوسط الرقمي وهذا يضاعف الصعوبات التي تواجه رجال الضبط الجنائي والقضائي، ومن مميزات الدليل الرقمي أنه (علمي، تقني، دليل قابل للنسخ، صعوبة التخلص منه، الرقمية الثنائية للدليل الرقمي، الدليل الرقمي متطور ومتنوع).

ومن شروط العمل بالدليل الرقمي :(أن يكون مشروعا ، غير قابل للشك، استساغته عقلا، إمكانية مناقشته).يتمتع الدليل الإلكتروني بحجية قوية في الإثبات لكن يخضع لسلطة القاضي التقديرية وهنا حسم المشرع الجزائري موقفه في نصي المادتين 212 و307 من قانون الإجراءات الجزائية. قد يثير الدليل الرقمي صعوبات في الإثبات (سهولة محو آثار الدليل الإلكتروني أو تعديله أو تدميره، عرقلة الوصول إلى الدليل، صعوبة الكشف عن هوية الجاني من خلال الدليل الرقمي، الطبيعة غير المرئية للدليل الإلكتروني، نقص الخبرة وكفاءة سلطات الاستدلال ، إحجام المجني عليه عن الإبلاغ وصعوبة التعاون الدولي).وتطرقنا لصعوبات الإختصاص القضائي والقانون المطبق ، فالغالب ولحل مشكلة الإختصاص القضائي تدخل المشرع الجزائري ليزيح المشكل بتطبيق إقليمية القوانين ولأن الجرائم المستحدثة باتت أكثر انتشارا فإن هذا المبدأ لم يعد يتسع لها، فلجأت إلى مبدأ العينية و الشخصية، أما الإختصاص القضائي الداخلي فلا يثير أي مشاكل ذلك ان المشرع مد الإختصاص لوكيل الجمهورية وقاضي التحقيق وضباط الشرطة القضائية واختصاص المحاكم لدائرة محاكم أخرى وفق المادة 329 ق.إ.ج ومرسوم تنفيذي348/06. ولضمان تحقيق الردع الخاص للمجرم والردع العام للمجتمع ككل، نظم المشرع العقوبات الأصلية والعقوبات التكميلية: العقوبة السالبة للحرية والعقوبة المالية للشخص الطبيعي وهي عقوبات أصلية. كما عاقب بالشروع في الجريمة بنفس العقوبات التي قررها للجريمة التامة على أن يضع صفح الضحية حدا للمتابعة. والعقوبة الأصلية للشخص المعنوي هي الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. أما العقوبات التكميلية فهي وفقا للمواد9 مكرر1 و18ق.إ.ج.

توصلنا إلى النتائج التالية.

النتائج:

1. جريمة الإبتزاز الإلكتروني جريمة متطورة جدا من ناحية طرق ووسائل ارتكابها مقارنة بآليات التصدي لها المعروفة إما بالجمود أو عدم المواكبة، ذلك أن الدول اتجهت لمواجهة هذه الجريمة إما بتعديل النصوص التقليدية وتحديثها، أو تشريع قوانين خاصة بها ورغم هذا لاتزال عاجزة عن التصدي لها ومواجهتها.
2. من بين نتائج جريمة الإبتزاز الإلكتروني حدوث جرائم بعدها كالسرقة والانتحار والزنا والقتل.
3. جريمة الابتزاز الإلكتروني جريمة صعبة الاكتشاف تتميز بالصعوبة في التحقيق والإثبات فهي تحتاج إلى فريق عمل من الخبراء والمختصين.
4. المجرم في الإبتزاز الإلكتروني ذكي يختلف عن المجرم التقليدي ويصعب تحديد هويته.
5. لم تتعمق أغلب التشريعات والقوانين في الدليل الرقمي ومن بينها المشرع الجزائري رغم أنه يعتبر المساهم الأول في مواجهة الجريمة الإلكترونية ومن أهم أدلة الإثبات في لكنه يحتاج إلى أجهزة متطورة وخبراء للتعامل معه.
6. واجهت الجزائر على غرار بقية دول العالم الجريمة الإلكترونية بتعديل قانون العقوبات بإضافة القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات والمستحدثة بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر2004، وبما أن الإبتزاز الإلكتروني صورة من صور الجريمة الإلكترونية فيندرج تحت هذا القسم في بعض الأحكام. كما يدخل ضمن هذه المواد من 296 إلى 303 مكرر3 في الفصل الأول من الباب الثاني تحت عنوان "الجنايات والجنح ضد الإفراد "كما تعالجه مواد التهديد التقليدي من المادة 284 إلى المادة 287.وأضاف المواد 333 مكرر4 وم333 مكرر5 و333 مكرر6 و333 مكرر 7 ضمن قانون 24-06 المؤرخ في

30 أفريل 2024.كما استحدث المشرع الجزائري قانون 09-04 المؤرخ في 5 أوت2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ليكمل التعديل الذي أجراه في قانون العقوبات وقانون الإجراءات الجزائية.

7. وازن المشرع الجزائري بين حق المجتمع في عقاب المتهم من خلال تشريع إجراءات استثنائية، وبين الحق في عدم انتهاك حرمة الحياة الخاصة بموجب المواد سابقة الذكر.
8. الهيآت والأشخاص المخولة لحماية الأشخاص من هذه الجريمة في القانون الجزائري مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها التابعة للدرك الوطني، والمعهد الوطني للبحث في علم التحقيق الجنائي. والقسم الخاص بالخبرة الرقمية التابع لنيابة الشرطة العلمية والتقنية بمديرية الشرطة القضائية المتواجد على مستوى المديرة العامة للأمن الوطني وتمتد مصالحها إلى بعض الولايات. والمخابر الجهوية الجنائية والتي تضم عدة أقسام متخصصة بما فيها قسم الأدلة الإلكترونية والرقمية. والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

وللفصل في هذه النتائج اقترح ما يلي:

المقترحات:

1) التنسيق المستمر بين الجهات القضائية والأمنية والتقنية لمسايرة ما يستجد في هذا المجال.
2) ضرورة النص صراحة على الأدلة الإلكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة. إضافة إلى النص على وسائل التأكد من سلامة الدليل الإلكتروني التي تعتبر شرطا لقبوله.
3) ضرورة استحداث نصوص قانونية إجرائية ملائمة.
4) نشر الوعي داخل المجتمع بأخطار جريمة الابتزاز الإلكتروني.
5) إتصال المجني عليه مباشرة بالسلطة المختصة.
6) عدم مسح المحتوى محل الابتزاز حتى ولو كان حميميا ومحرجا، وتسليمه للجهات الأمنية لاتخاذه دليلا ضد المبتز.
7) تعديل وترشيد القوانين لتتلاءم مع جريمة الابتزاز الإلكتروني، لتفادي القصور التشريعي وسد الثغرات القانونية التي يستغلها الجناة
8) دعوة الدول العربية إلى إنشاء منظمة شرطة عربية لمكافحة الجرائم الإلكترونية.
9) إدخال مادة أخلاقيات استخدام الأنترنت ضمن المناهج التعليمية.
10) تطويع وتطوير قواعد القانون الدولي والإتفاقيات الدولية الخاصة بتسليم المجرمين وتفعيلها في كل دولة.
11) تدريب القضاة وأعضاء النيابة العامة ومأموري الضبط القضائي وتعلمهم لقيمة الدليل الرقمي وكيفية استخلاصه ومعرفتهم كيفية التحقيق واثبات الجريمة الإلكترونية

12) تشديد عقوبة الجرائم الإلكترونية أكثر، مع التخفيف أو الإعفاء من العقوبة لكل جاني عدل عن جرمه قبل التبليغ عنه.
13) عدم الاستهانة بالتبليغ من طرف الهيآت الرسمية حتى يشجع الجناة على الإستمرار في جرائمهم وخوف الضحايا من انتقام المبتزين عند عدم تلقي الحماية من الدولة.
14) فتح المجال لانضمام محترفي المعلوماتية إلى جهات البحث والتحري والتحقيق.
15) التأكيد على ضرورة عقد اتفاقيات دولية جادة وحث الانضمام إليها.
16) دعم التشريعات الجنائية الوطنية على مكافحة هذه الجرائم بتقديم المساعدة الفنية والتقنية لها.
17) حجب المواقع والتطبيقات التي من شأنها أن تزيد من تفشي الجريمة.
18) توعية الآباء بعدم السماح لأبنائهم اقتناء أجهزة ذكية إلا بعد تسليحهم وتثقيفهم تقنيا وعلميا ودينيا.

قائمة المصادر والمراجع

I. المصادر:

1. الدستور: التعديل الدستوري الجزائري الصادر بتاريخ07 ديسمبر1996ج.ر76 الصادرة في 08ديسمبر1996 المعدل بمقتضى:

- بالقانون رقم 02-03، مؤرخ في 10 أفريل سنة 2002، المتضمن التعديل الدستوري، ج.ر.عدد 25، صادر في 14 أفريل 2002،
- بالقانون رقم 08-19، مؤرخ في 15 نوفمبر سنة 2008، يتضمن التعديل الدستوري، ج.ر. عدد 63، صادر في 16 نوفمبر سنة 2008،
- بالقانون رقم 16-01، مؤرخ في 06 مارس سنة 2016، يتضمن التعديل الدستوري، ج.ر. عدد 14، صادر في 07 مارس سنة 2016،

2. النصوص القانونية:

- القانون رقم 04-14 المؤرخ في 27 رمضان1425 الموافق ل 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155المتضمن قانون الإجراءات الجزائية، ج.ر 2004/71.
- القانون 04-15المؤرخ في 27 رمضان1425 الموافق ل 10نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، ج. ر 2004/71.
- قانون06-22 المؤرخ في 29ذي القعدة1427 الموافق ل 20 ديسمبر 2006 يعدل ويتمم الأمررقم66-155 المؤرخ في 18 صقر 1386 الموافق ل 8 جوان1966 والمتضمن قانون الإجراءات الجزائية. ج.ر عدد84 الصادرة في 2006/12/24.
- قانون رقم 06-23. مؤرخ في 29 ذي القعدة 1427 الموافق ل 20 ديسمبر 2006. يعدل ويتمم الإمر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق

ل 8 جوان 1966 والمتضمن قانون العقوبات. ج.ر العدد84، الصادر في 4 ذي الحجة 1427هـ الموافق ل 24 ديسمبر 2006.

- القانون04/09 المؤرخ في 14 شعبان1430 الموافق ل 05 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الصادر في ج.ر عدد 47، المؤرخ في 16 أوت 2009.
- القانون رقم24-06 المؤرخ في 19 شوال عام 1445 الموافق ل28 ابريل سنة 2024 المعدل والمتمم للأمر رقم66-156 المؤرخ في 18 صفر عام1386 الموافق ل8يونيو سنة 1966 والمتضمن قانون العقوبات، الصادر في ج ر عدد30،الصادرة في 21شوال عام1445 هـ ،الموافق ل30ابريل سنة 2024م.
- الأمر رقم 69-73 المؤرخ في 16 سبتمبر 1969) من قانون الإجراءات الجزائية المعدل بموجب القانون رقم 14-04 المؤرخ في 10نوفمبر 2004 المعدل والمتمم للامر 66-155 المتضمن قانون الاجراءات الجزائية ج.ر عدد71 بتاريخ 10 نوفمبر 2004.
- الأمر 03-01 المؤرخ في 19 فيفري 2003 المعدلة للمادة 05 من الأمر 96-22 المؤرخ في 9 جويلية 1996 الذي يتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة الأموال من وإلى الخارج، ج.ر. عدد43 صادرة في 10 جويلية 1996 معدل ومتمم.
- المرسوم التنفيذي رقم06-348 المؤرخ في12 رمضان 1427 الموافق ل 2006/10/05 والمتضمن تمديد الإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.ج.ر 2006/63.

II. المراجع:

1. الكتب المتخصصة:

1) جاسم محمد جندل، الجرائم الإلكترونية، ط1، دار المعتز للنشر والتوزيع، عمان (الأردن) سنة 2022.
2) حسين عبد الكريم يونس خليل يونس الجندي، الإبتزاز الإلكتروني والجرائم الإلكترونية، ط1، دار كفاءة المعرفة عمان (الأردن) 2021.
3) سمير عالية، الجرائم الإلكترونية ،في القانون الجديد رقم 2018/81 والمقارن، (حرية التواصل الإلكتروني والقواعد العقابية والإجرامية)، الطبعة الأولى منشورات الحلبي الحقوقية بيروت، لبنان، سنة 2020.
4) يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، مخبر أتر الإجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، الطبعة الأولى مطبعة الرمال، الوادي (الجزائر)سنة 2019.

2. الرسائل والأطروحات

➢ أطروحات الدكتوراه:

1) جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، سنة 2018.
2) عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبوبكر بلقايد، تلمسان، سنة 2017-2018.

3) محمد بن فردية، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي والعلوم الإجرامية، كلية الحقوق، جامعة الجزائر، سنة 2015.

➢ رسائل الماجستير

1) عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون جنائي، جامعة وهران، الجزائر، سنة 2012-2013.

2) سارة حنش، المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، (دراسة مقارنة) رسالة للحصول على ماجستير في القانون العام، كلية الحقوق، قسم القانون العام، جامعة الشرق الأوسط، الأردن، سنة 2020.

3. المقالات العلمية

1) أحمد لطفي السيد مرعي، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني، (دراسة مقارنة) كلية الحقوق، قسم القانون الجنائي، جامعة المنصورة، مصر، المجلد الثامن عدد يونيو 2022.

2) أكرم ديب، نورة بن بو عبد الله، دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني، مجلة الحقوق والعلوم الإنسانية، الجزائر، المجلد16، العدد01، سنة2023.

3) باقر غازي حنون، حسن حماد حميد، جريمة الإبتزاز الإلكتروني (دراسة مقارنة)، مجلة دراسات البصرة، جامعة البصرة مركز دراسات البصرة والخليج العربي، العراق، المجلد 16 العدد42، ديسمبر 2021..

4) حسين عباس حميد، جريمة الإبتزاز الإلكتروني، مجلة القانون للدراسات والبحوث القانونية، جامعة ذي قار كلية القانون، العراق، المجلد 23، العدد22 سنة 2021.

5) خالد ضو، حجية الدليل الإلكتروني وشروط قبوله في الإثبات الجنائي، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي آفلو–الأغواط، العدد الثامن سنة 2022.
6) داليا عبد العزيز، المسؤولية الجنائية عن جريمة الإبتزاز الإلكتروني في النظام السعودي، دراسة مقارنة، مجلة جيل للأبحاث القانونية المعمقة، مركز جيل البحث العلمي بالجزائر / فرع لبنان، المجلد 03، العدد25، سنة 31 ماي 2018،
7) زوليخة رواحنة، نادية رواحنة، جريمة انتهاك حرمة المكالمات أو الأحاديث الخاصة أو السرية في قانون العقوبات الجزائري، مجلة الفكر،الجزائر، المجلد17، العدد02 2022.
8) زينب محمود حسين، المواجهة الجنائية للإبتزاز الإلكتروني، مجلة كلية القانون للعلوم القانونية والسياسية، قسم القانون، جامعة كركوك كلية القانون والعلوم السياسية، العراق، المجلد 10، العدد 37 سنة 2021.
9) سامية بلجراف، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، الجزائر، المجلد 07، العدد01، سنة 2021.
10) سبخاوي خديجة، جريمة الإبتزاز الإلكتروني دراسة ميدانية على عينة من طلبة جامعة البليدة 2، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور بالجلفة . الجزائر المجلد09، العدد01، السنة مارس 2024.
11) سعيد زيوش، ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها ،قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الإجتماعية،الجزائر، المجلد 11، العدد 01، سنة جانفي2017.
12) بن شهرة الشول، هانية بوشارب، صعوبة عملية استخلاص الدليل الإلكتروني، مجلة الدراسات القانونية والسياسية، الجزائر، المجلد09، العدد 01 جانفي 2023
13) الطاهر ياكر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والإتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، الجزائر، المجلد 4، العدد 4، سلة 2022.

14) عبد العزيز بن حمين، الإبتزاز ودور الرئاسة العامة لهيئة الإمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الإبتزاز: المفهوم، الأسباب والعلاج، مكتبة الملك فهد الوطنية، الرياض 1432هـ

15) عبد القادر زرقين – مصطفى قزران، الآليات الدولية لمكافحة الجريمة الإلكترونية، مجلة صوت القانون، المجلد الثامن العدد2، الجزائر، سنة2002، ص1223.

16) عبد القادر فلاح، نادية أيت عبد المالك، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري. مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر، المجلد 04، العدد 02، السنة 2019.

17) عبد الله شيباني، وداد بن سالم، النظام القانوني لمقدمي خدمة الإنترنت في ظل القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مجلة الإجتهاد للدراسات القانونية والاقتصادية، الجزائر، المجلد13، العدد01 سنة 2024.

18) عماد جواد مرسي، التحقيق والصعوبات التي تواجه جريمة الإبتزاز الإلكتروني، مجلة كلية المعارف الجامعة، الأنبار، العراق، المجلد33، العدد4 سنة 2022..

19) الغديان سليمان بن عبد الرزاق، خطاطبة يحيى بن مبارك وآخرون، صور جرائم الإبتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية كلية الملك فهد الأمنية – مركز البحوث والدراسات، السعودية، المجلد27، العدد69، 2018/01/31.

20)فاطمة الزهراء قرينح، كمال راشد، حماية الطفل من جريمة التهديد الإلكتروني بين التشريعين الدولي والجزائري، مجلة القانون والمجتمع، الجزائر، المجلد09، العدد 02، سنة2021.

21) فاطمة العرفي، الحماية القانونية للحق في الخصوصية للأطفال من جريمة التشهير عبر مواقع التواصل الإجتماعي في القانون الجزائري، مجلة الإجتهاد القضائي، مخبر الإجتهاد القضائي على حركة التشريع، بسكرة، الجزائر، المجلد12، العدد 02، أكتوبر 2020.

22) ليندة شرابشة – السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية الإتجاهات الدولية في مكافحة الجريمة الإلكترونية، منصة المجلات العلمية الجزائرية، الجزائر، المجلد 01، العدد01، سنة 2009.

23) مبارك بن الطيبي، محمد حموني، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية، مجلة القانون والعلوم السياسية، الجزائر، المجلد 05 العدد 02 سنة 2019.

24) محمد بن حيدة، مكانة الحق في الحياة الخاصة في ظل التعديل الدستوري 01/16، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، الجزائر، لمجلد الأول، العدد 10، جوان2018.

25) محمد سعيد عبد العاطي محمد، محمد أحمد المنشاوي محمد، دور القانون الجنائي في حماية الطفل من الإبتزاز الإلكتروني (دراسة مقارنة)، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون، قرع جامعة الأزهر، دمنهور، محافظة البحيرة، المجلد 33، العدد 36، سنة2021.

26) محمد موسى جابر، المواجهة الجنائية للابتزاز الإلكتروني، مجلة الجامعة العراقية، العراق، المجلد2، العدد49، د.س.ن.

27)محمود محمد صفاء الدين علي شرشر – الجهود الدولية والتشريعية لمكافحة جرائم الإنترنت، مجلة البحوث القانونية والإقتصادية، المنوفية، المجلد 54 العدد 03، سنة 2021.

28) مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، الجزائر، المجلد12 العدد2019،02م.

29) مريم عراب، الإختصاص القضائي في الجرائم المعلوماتية، مجلة القانون والعلوم السياسية،الجزائر، المجلد7 العدد3 سنة 2015.

30) مريم عراب، جريمة التهديد الإلكتروني، مجلة الدراسات القانونية، الجزائر، المجلد07، العدد01، سنة2021.

31) مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، دراسة مقارنة، مجلة علوم الشريعة والقانون، الأردن، المجلد45، العدد4، سنة 2018.

32) مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة والاقتصاد، الجزائر المجلد السابع، العدد01، سنة 2018

33) ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الإبتزاز الإلكتروني، المجلة العربية للدراسات الأمنية الرياض، السعودية، المجلد33، العدد80، سنة2017.

34) منصور عبد السلام عبد الحميد حسان، جريمة الإبتزاز الإلكتروني، دراسة مقارنة بين القانون المصري والفرنسي والإماراتي والنظام السعودي، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، المجلد17، العدد5، اوت2023.

35) ناجية الشيخ، الإقرار بالمسؤولية الجزائية للشخص المعنوي في جرائم الصرف، منصة المجلات العلمية الجزائرية، الجزائر، المجلد02، العدد1، سنة 2011.

36) نورة هارون، وهيبة برازة، حق الفرد على صورته بين مقتضيات الحق في حرمة الحياة الخاصة وضرورات الكشف عن الجريمة، حوليات جامعة الجزائر1، المجلد35، العدد3، 2021.

37) هند علي حنون، وسائل حماية الأسرة من الابتزاز الإلكتروني، مجلة العلوم الإنسانية والإجتماعية، مجلة جامعة دهوك العراق، المجلد، 26 العدد1، سنة 2023.

38) وائل سليم عبد الله شاطر، الإطار القانوني لجريمة الإبتزاز الإلكتروني في الألعاب الإلكترونية، دراسة مقارنة وفق النظام السعودي والقانون الكويتي، المجلة العربية للنشر العلمي، جدة، المملكة العربية السعودية، العدد 16، 2شباط2020.

39) يوسف علي حسن الداودي، حكم الإبتزاز الإلكتروني دراسة مقارنة بين الشريعة والقانون، سنة 2022.

4. المؤتمرات والندوات

- ابتسام كريم وآخرون، انتشار ظاهرة الإبتزاز الإلكتروني في المجتمع العراقي، استطلاع آراء عينة من المجتمع العراقي حول التعامل مع هذه الظاهرة، شبكة المؤتمرات العرب، مركز التطور الإستراتيجي الأكاديمي، جامعة دهوك العراق، 11 و12 فيفري 2019.

5. المحاضرات الجامعية

- علي ابراهيم بن دراج، محاضرات في الجرائم المعلوماتية، مقدمة للسنة الثانية ماستر تخصص جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، المركز الجامعي آفلو، الأغواط، لعام2020 /2021.

6. المواقع الإلكترونية :

1. موقع الألوكة نت عبر الرابط التالي:

عبد الباقي دعماش، ثراء الفكر وفكر الثراء (alukah.net) تاريخ الإطلاع يوم2024/07/02 على الساعة 16:30.

2. موقع محاماة نت عبر الرابط التالي:

القانون الجزائري (mohamah.net) 2024 تاريخ الإطلاع 01 فيفري 2024، الساعة 16:00.

3. موقع بصمة أمان عبر الرابط:

https://www.secprint.sa/blackmail-number-algeria/، تاريخ الإطلاع 01 ماي 2024 الساعة:02:45.

4. موقع النجاح عبر الرابط،

(annajah.net)، تاريخ الإطلاع 2024/05/01، الساعة 09:52

5. موقع إستشارات قانونية مجانية، محاماة نت عبرا الرابط:

www.mohamat.net/law/.

6. موقع إستشارات قانونية أون لاين عبر الرابط:

legal-advice.online)) 2024 و303

تاريخ الإطلاع2024//05/01.الساعة09:20 .

7. هيئة التحرير ،كيفية مكافحة الإبتزاز ،منصة معك عبر الرابط
معك (- m3k.net) .

8. هيئة التحرير، أبرز 8 طرق الوقاية من الابتزاز الالكتروني في السعودية ، موقع محامي الرياض، عبر الرابط https://yalawyer.sa

فهرس المحتويات

ملخص البحث تعرض هذه الدراسة الآليات القانونية لحماية الأشخاص من الإبتزاز الإلكتروني، وقد تناولت في البداية الهيآت الدولية التي عنيت بدور هام لا يستهان به في مواجهة هذه الجريمة المستحدثة، ومنها منظمة الأمم المتحدة، والشرطة الدولية واتفاقية بودابست، والتي كانت حجر الأساس في بداية المواجهة الدولية. كما تطرق البحث للهيآت الإقليمية واللجان، كاللجنة الاقتصادية والإجتماعية لغرب آسيا وجامعة الدول العربية. ثم عرجت الدراسة إلى النظام القانوني للإبتزاز الإلكتروني في التشريع الجزائري، فتناولت مفهوم الجريمة ومدى خطورتها، صورها وطرق ارتكابها وأهم دوافعها، وآثارها ووسائل ارتكابها، إضافة إلى أركانها وأسبابها ومراحلها، ثم الهيآت والأشخاص المكلفة بمتابعة الجريمة، حتى دلفت إلى الإجراءات القانونية في حماية الأشخاص منها بالتطرق للتحقيق والإثبات والصعوبات التي تعتريهما، دون أن تغفل الدراسة عن الدليل الرقمي ومميزاته وحجيته وختمت بالصعوبات في الإختصاص القضائي والعقوبات المترتبة..

الكلمات المفتاحية: الإبتزاز، الحاسب الآلي، الجريمة الإلكترونية، التهديد، الآليات القانونية.

Title: Legal Mechanisms for Protecting Individuals Fromm Electronic Extortion

Abstract: This study examines the legal mechanisms for protecting individuals from electronic extortion. It begins by discussing the international bodies that have played a significant role in confronting this emerging crime, including the United Nations, Interpol, and the Budapest Convention, which served as the cornerstone of the international response. The research then addresses regional bodies and committees such as the Economic and Social Commission for Western Asia and the League of Arab States. Subsequently, the study delves into the legal system of electronic extortion in Algerian legislation, covering the concept of the crime, its severity, its forms, methods of commission, primary motives, effects, means of commission, its elements, causes, and stages. It then discusses the bodies and persons responsible for investigating the crime, leading to the legal procedures for protecting individuals from it, addressing investigation, evidence, and the difficulties that hinder them. The study does not overlook digital evidence, its characteristics, and its probative value, concluding with the difficulties in judicial jurisdiction and the applicable penalties.

Keywords: -Extortion –Computer-electronic Crime-threat- legal mechanisms.