جامعة قاصدي مرباح – ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

التخصص: القانون الجنائي و العلوم الجنائية

جريمة الابتزاز الالكتروني

إعداد الطلبة :

ـ بن سليمان محمد الطاهر

ـ رسيوي رشيدة

ـ دراجي عزالدين

تحت إشراف: الاستاذ

ـ لقمـــان بامـــــون

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
قريشي محمد	أستاذ التعليم العالي	رئيسًا
بامون لقمان	أستاذ مساعد قسم "أ"	مشرفًا
طيبي الطيب	أستاذ مساعد قسم "ب"	مناقشًا

السنة الجامعية : 2024/2023

جامعة قاصدي مرباح – ورقلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال المتطلبات لنيل شهادة الماستر أكاديمي

الميدان: الحقوق والعلوم السياسية

التخصص: القانون الجنائي و العلوم الجنائية

جريمة الابتزاز الالكتروني

إعداد الطلبة :

ـ بن سليمان محمد الطاهر

ـ رسيوي رشيدة

ـ دراجي عزالدين

تحت إشراف: الاستاذ

ـ لقمـــان بامـــــون

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الصفة
قريشي محمد	أستاذ التعليم العالي	رئيسًا
بامون لقمان	أستاذ مساعد قسم "أ"	مشرفًا
طيبي الطيب	أستاذ مساعد قسم "ب"	مناقشًا

السنة الجامعية : 2024/2023

شكر و تقدير

الحمد لله والصلاة والسلام على سيدنا و حبيبنا محمد المصطفى رسول الله ،

نحمد الله حمدا كثيرا و نشكره شكرا جزيلا على توفيقه واعانته لنا على إتمام عملنا المتواضع هذا .

و نتقدم بالشكر و الامتنان المليئان بالتقدير والاحترام الى كل اساتذتنا الكرام الذين درسونا ولم يبخلوا علينا بكل ما لديهم من معلومات ووصايا و فوائد ، و نخص بالذكر استاذنا الفاضل الذي اشرف على مذكرة تخرجنا هذه الدكتور الفاضل لقمان بامون، ومن خلالة الى الأساتذة الكرام المقبلين على مناقشة مذكرتنا هذه .

والى كل القائمين على إدارة جامعة قاصدي مرباح بورقلة وبالخصوص كلية الحقوق والعلوم السياسية فكلهم مشكورون على ما يبذلونه من خدمات جليلة ووفيرة والتي يقصدون من خلالها حسن تعليم الطلبة والعمل على راحتهم .

اهداء

•الى روح ابي الغالي وأخي العزيز حسينعلى قلبي ادعوا الله ان يغفر لهما ويرحمهما

•الى اعز الناس واقربهم الى قلبي والدتي العزيزة متمنيا لها وافر الصحة والعافية .

•الى من ساندتني وخطت معي خطواتي ويسرت لي الصعاب الى زوجتي العزيزة التي تحملت الكثير بوقوفها الى جانبي ولولا تشجيعها المستمر لي لما كنت استطيع استكمال عملي هذا .

•الى كل افراد عائلتي الكريمة واخص زهرتي وفلذتي كبدي ابنتي دلوعتي العزيزة آلاء الرحمان وابني الكتكوت محمد الأخضر الذي أشتم فيه دوما رائحة والدي رحمه الله والذي اسميته باسمه.

•الى اساتذتي الافاضل الذين لم يبخلوا عليا بالنصيحة والتوجيه والإرشاد وأخص منهم استاذي المحترم الذي قبل الاشراف على عملنا المتواضع هذا الدكتور الفاضل **بامون لقمان** .

•الى كل هؤلاء وغيرهم من الزملاء و لمن ساعدني ولو بكلمة طيبة ، اهديهم هذا العمل المتواضع ، سائلا الله العلي القدير أن ينفعنا به ويجازينا عنه ويمدنا بتوفيقه .

الطالب : محمد الطاهر بن سليمان

إهداء

الى روح من لديهم فضل عليا وهم سبب وجودي في هذه الحياة ، والديا رحمهما الله واسكنهم جنات الفردوس الاعلى

الى كل افراد اسرتي الكريمة واخص بالذكر اختي العزيزة ليلى التي سخرت كل ما تملك من أجل مساعدتي

الى جميع الأصدقاء والزملاء

الى كافة أساتذة وعمال كلية الحقوق والعلوم السياسية بجامعة قاصدي مرباح بورقلة

الى كل من ساعدني في انجاز هدا العمل المتواضع .

الطالبة : رسيوي رشيدة

إهداء

إلى من شجعني على المثابرة طوال عمري، إلى الرجل الأبرز في حياتي

(والدي العزيز)

إلى من بـــها أعلو، وعليها أرتكز، إلى القـلب المعطاء

(والدتي الحبيبة)

إلى من بذلوا جهدًا في مساعدتي وكانوا خيرَ سندٍ

(اخي و اخواتي)

إلى أسرتي إلى أصدقائي وزملائي

و اخص بالذكر بكاري سليم و شتوح عبد اللطيف

و إلى كل من ساهم ولو بحرف في حياتي الدراسية.....

إلى كل هؤلاء: أهدي هذا العمل، الذي أسال الله تعالى أن يتقبله خالصًا...

الطالب : دراجي عزالدين

قائمة المختصرات

ج. ر. ج. ج : الجريدة الرسمية للجمهورية الجزائرية

ق ا ج ج : قانون الإجراءات الجزائية الجزائري

ق. ع. ج : قانون العقوبات الجزائري.

ص : صفحة

مقدمة

مع التطور السريع والهائل في التكنولوجيا الاتصال أدى إلى إنتاج وسائل حديثة في التواصل الاجتماعي، وإحداث تغيرات جذرية مست حياة الناس في كل محلاتها، والجريمة ليست باستثناء، فقد تأقلمت هي الأخرى مع كل هذه التغيرات التقنية والمعلوماتية فانتقلت الجريمة من الفضاء المادي إلى الفضاء الافتراضي وأخذت أشكالا وأنماطا جديدة في التنفيذ مما أضفى عليها مسمى الجرائم المستحدثة ومن بينها جريمة الابتزاز الالكتروني.

وهذه الجرائم إما تقع على الكمبيوتر أو بواسطته حيث يصبح أداة طيعة في يد الجناة يستخدمونها لتحقيق مآربهم الإجرامية مستغلين بذلك تلك التقنيات المستحدثة والتي أصبحت فيما بعد محلا لتلك الجرائم أو وسيلة لارتكابها، فأصبح الوسط الذي ترتكب فيه الجريمة الإلكترونية ومضات كهربائية أو مغناطيسية ورموز وشفرات ولم يعد مسرح الجريمة إلا مسرحا افتراضيا وكذلك طرق التحقيق، والإثبات فيها كما ان للدليل الرقمي أسس وقواعد مختلفة في التعامل معه بسبب خطورة هاته الجريمة وتوافر أركانها.

ونظرا الى الآثار المترتبة على انتشار جريمة الإبتزاز الإلكتروني في المجتمع، وكونها من المستجدات الطارئة عليه فأن للبحث أهمية من الناحيتين العلمية والعملية.

وتتمثل أهمية هذا البحث في اهتمامه بظاهرة جديدة وهي الابتزاز الإلكتروني، التي بدأت في الظهور والانتشار، وارتبطت بتكنولوجيا الشبكة العنكبوتية، مما أسفر عن تميزها بمجموعة من الخصائص جعلتها تختلف عمن سواها من الجرائم، مما يستتبع ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية، لذلك كان لزاماً علينا مراجعة تقييم النصوص القانونية التي لها علاقة بتجريم الابتزاز الإلكتروني، وما تقدمه هذه النصوص من دعم في مجال مكافحة الابتزاز الإلكتروني والتصدي له من أجل القضاء عليه أو الحد منه.

فمن الناحية العلمية ، لفت انتباه الباحثين لدراسة الموضوع وتسليط الضوء على مختلف جوانبه كذلك لفت انتباه المشرع الى إعادة النظر وضبط النصوص القانونية لمكافحة هذه الجريمة ، أما من الناحية العلمية تبرز أهمية البحث في معرفة مدى كفاية النصوص الجنائية في بعض التشريعات العربية الواردة في قوانين العقوبات إلى الحد من ارتكاب هذه الجريمة وردع مرتكبيها .

أما عن أسباب اختيار الموضوع فهي ذاتية ، تتمثل في الرغبة في دراسته كونه يتناول ظاهرة تؤرق المجتمع وتهدد استقراره ، وموضوعية نظرا لكون الجريمة موضوع الدراسة تفشت وتنامت في المجتمع مما يستدعي دراستها باعتبار المجتمعات العربية معروفة بالعادات ، والأعراف الاجتماعية التي تتحفظ على كل ما يتعرض للسمعة والشرف خصوصا أن هذه الجريمة أغلب ضحاياها فتيات.

وقد ارتكزت الدراسة على المنهج الوصفي لوصف الجريمة، من خلال تعريفها، وآثارها وسائل ارتكابها ونظرا لتزايد نسبة ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرا لخصوصية هذه الجريمة، ووسائل وطرق تنفيذها، أدى إلى انعكاس هذه الخصوصية على مضمون الأنظمة والقوانين، حتى تتماشى مع طبيعة هذه الجريمة ومعطياتها وآثارها، وبناءا عليه كانت الحاجة ملحة لوضع هذا الموضوع موضع دراسة وتحليل وينبني ذلك على الإجابة على إشكالية الدراسة المتمثلة في:

إلى أي مدى وفق المشرع الجزائري كغيره من التشريعات الدولية في معالجة جريمة الابتزاز الالكتروني؟

لمعالجة هذه الإشكالية ارتكزت الدراسة على المنهج الوصفي لوصف الجريمة، من خلال تعريفها، وآثارها وسائل ارتكابها.

ولدراسة هذا الموضوع ارتأينا تقسيم البحث إلى فصلين، الأول بعنوان الإطار الموضوعي الجريمة الابتزاز الإلكتروني وقد تناولنا في المبحث الأول ماهية جريمة الابتزاز الإلكتروني أما المبحث الثاني: تجريم جريمة الابتزاز الالكتروني، أما الفصل الثاني فقد كان بعنوان الإطار الإجرائي لجريمة الابتزاز الالكتروني الذي

يحتوي على مبحثين المبحث الأول تناول إجراءات التحقيق في جريمة الابتزاز الإلكتروني والصعوبات التي تواجه المحقق ، أما المبحث الثاني فتناولنا فيه الإثبات في جريمة الابتزاز الإلكتروني، وفي الأخير انتهينا الى خاتمة للموضوع توضح النتائج والمقترحات التي تم التوصل إليها.

الفصل الأول :

الإطار الموضوعي لجريمة الابتـــزاز الإلكتـــروني

تمهيد :

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

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

وقد ارتأينا الى تقسم الفصل الى مبحثين تناولنا في المبحث الأول ماهية جريمة الابتزاز الالكتروني وفي المبحث الثاني تجريم جريمة الابتزاز الالكتروني.

المبحث الأول: ماهية جريمة الابتزاز الالكتروني.

يعتبر الزمن الحاضر زمنا سريع التطور خاصة في المجال الإلكتروني ، و رغم محاسن هذا المجال وفائدته الى معظم أفراد المجتمع ، الا أنه أفرز صورا من الافعال غير المقبولة اجتماعيا و أصبحت مصدرا لكثير من الأضرار الاجتماعية و انعكست سلبا على العلاقات الإنسانية ، بل و أصبحت تؤثر تأثيرا مباشرا وملموسا على الحقوق و الحريات الشخصية التي تتصل بالفرد و على رأسها حرمة الحياة الخاصة وتبرز جريمة الإبتزاز الإلكتروني كإحدى الجرائم المستحدثة التي ظهرت مؤخرا ، و التي أثرت على عدد كبير من أفراد المجتمع خاصة النساء منهم .

وهذا الأمر يستدعي دراسة مفهوم هذه الجريمة بتعريفها وأنواعها ومختلف أساليبها والتطرق الى الآثار المترتبة عنها،وهذا ما سنتطرق إليه من خلال هذا المبحث.

المطلب الأول: مفهوم الابتزاز الالكتروني

يعتبر الابتزاز الإلكتروني هو نتاج الاستخدام السلبي للثورة التكنولوجية التي لحقت العالم حديثا وهي من الآثار غير المرغوب فيها لهذا التقدم العلمي المذهل الذي جعل المجرم يختبئ خلف شاشة ما ، و يمارس عملا إجراميا بالاعتداء على مصلحة يحميها القانون للضحية، حيث تتم الجريمة عن طريق الجاني بالضغط على المجني عليه بتهديده تارة و الوعيد تارة أخرى و ذلك بنشر معلومات أو صور أو تسجيلات لا يرغب المجني عليه في إظهارها ، فالابتزاز الإلكتروني هو أسلوب من أساليب الضغط و الإكراه على المجني عليه يمارسه الجاني لتحقيق مقاصده الإجرامية و ذلك للوصول لهدفه الذي قد يكون هدفا ماديا أو معنويا.

ومن خلال هذا المطلب سيتم التطرق الى مفهوم الابتزاز الالكتروني حيث يحتوي على فرعين الفرع الأول يتناول تعريف الإبتزاز الالكتروني أما الفرع الثاني يتناول أنواع الابتزاز الالكتروني.

الفرع الأول: تعريف الابتزاز

سنتطرق في هذا الفرع لتعريف جريمة الابتزاز الإلكتروني انطلاقا من التعريف اللغوي، مرورا بالتعريف الاصطلاحي والفقهي على النحو التالي:

أولا: التعريف اللغوي للابتزاز

مصدر: ابتز

معناه من غلب سلب، ويزه بزه بزا: غلبه وعصبه، وبز الشيء انتزعه، ومنه ابتز جارية: إذا جردها من ثيابها والبز أخذ الشيء بحفاء وقهر[1]

ثانيا: التعريف الاصطلاحي للابتزاز

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

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

---

[1] محمد بن مكرم بن منظور، لسان العرب، دار الصادر، بيروت 2010، مج 5 ص 312

وقد عرف على أنه أحد أشكال التلاعب القوية يقوم خلالها المبتز الذي تربطه علاقة أو صلة بالضحية بتهديده بطريقة مباشرة أو غير مباشرة بالعقاب إذا لم يحصل على ما يرغب عندما يستخدم المقربون الخوف، والإلزام، والشعور بالذنب للتلاعب بك[1].

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

ثالثا: التعريف الفقهي لجريمة الابتزاز الإلكتروني

يرى جانب من الفقهاء أن الابتزاز هو " القيام بتهديد شخص بفضح أمره ما لم يستجب المهدد إلى تنفيذ طلبات الجاني وغالباً ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف، أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي يتم ابتزازه.

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

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

وقدعرف جانب من الفقه الابتزاز التقليدي بأنه " الضغط الذي يباشره شخص على إرادة شخص آخر لحمله على ارتكاب جريمة معينة.

---

[1] محمدشاكرعبدالله: "قياسالابتزازالعاطفيلدىطلبةالمرحلةالإعداديةبناءوتطبيق)»،مجلةأبحاثالبصرةللعلومالإنسانية، العراقي،المجلد 44،العدد 2، 2019،ص 162

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

كما تم تعريف الابتزاز بأنه ما يمارسه المجرم المبتز من تهديد وسلوك للمجني عليه بعد حصوله على معلومات تخص المجني عليه كالتسجيلات الصوتية، أو الصور الشخصية بهدف تحقيق رغباته التي يسعى إليها سواءً أكانت مادية أو معنوية. [1]

الفرع الثاني: أنواع الابتزاز الالكتروني

تبدأ العلاقة بين طرفي الإبتزاز عن طريق الثقة الوهمية المتبادلة والأساليب الملتوية والمخادعة والوعود الكاذبة ثم تتطور حتى يكون باستطاعة المبتز الحصول على بعض أسرار ضحيته ويحتفظ بهاومن ثم تبدأ عمليه المساومة والابتزاز.

تتعدد أسباب ودوافع الإبتزاز بحسب شخصية الهدف ومدى قابليته للدخول في هذه الدائرة ولكن في أغلب الأحوال هو الخلل السلوكي لدى الطرفين، المبتز أو الضحية.[2]

تعتبر المرأة الضحية الأبرز في هذه الجريمة و في الغالب كما أن تهاون الأسرة في الرقابة على أبنائها وإعطائهم الحرية دون ضوابط صحيحة، كما يؤدي الفقر والحرمان بالكثير من الأفراد في مختلف المجتمعات في القيام بممارسات تصل في كثير من الأحيان الى حد الانحراف وارتكاب الجرائم ، كما أن استخدام الوسائل التقنية والاتصالات بشكل سلبي مثل البريد الإلكتروني العشوائي والإيميلات المجهولة و المواقع

---

[1] حمزة بن عقون السلوك الإجرامي للمحرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012

[2] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منتوري قسنطينة 2012 – 2013

الإلكترونية العامة والخاصة و مواقع التعارف بين الجنسين ، و مواقع الألعاب و المنتديات الإلكترونية و مواقع الدردشة و الإعلانات المضللة في المواقع الإلكترونية فهي من أكبر الوسائل التي يتم استخدامها لأغراض الإبتزاز .

أما من حيث أساليب الابتزاز التي يمارسها المبتز على الضحية فيعتمد على أسلوب التهديد سواء كان التهديد بالتشهير، أو التهديد بإبلاغ ذوي الضحية الأمر الذي يجعل الضحية يقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته في تحقيق غاياته.

ويمثل الاستخدام السلبي للشبكة العنكبوتية عاملا مهما في انتشار جرائم الإبتزاز الذي يستغلها المبتز وتعد جرائم ابتزاز النساء من أكثر انواع الإبتزاز انتشارا وشهرة، حيث أن جرائم الابتزاز الإلكتروني للنساء تعتبر النموذج المثالي للجريمة لا سيما إذا كان المبتز رجلا وضحية الجريمة امرأة.

هذا لا يمنع من أن جريمة الإبتزاز الإلكتروني من الجرائم ذات الصور المتشعبة حيث أن هذه الصور تنوع تارة بالنظر الى الهدف المرتقب من الجريمة، أو المنفعة التي تعود على المبتز.

أولا: الإبتزاز الالكتروني بالنظر لشخص الضحية

وفيه يقسم جرائم الإبتزاز الإلكتروني تبعا لشخصية المجني عليه المحتمل كضحية للجريمة وذلك

على النحو التالي:

أ. الشخصيات الاعتبارية:

قد تكون الفئة المستهدفة من الإبتزاز الإلكتروني هي أشخاص اعتبارية كالحكومات، و الشركات و المؤسسات، و ذلك عن طريق الحصول على معلومات سرية خاصة بها ثم يقوم المبتز بالتهديد بالإفصاح عنها، و افشاؤها، و نشرها للخرين، فتبدأ الجريمة بمتطفل، أو دخيل على مواقع مهمة أو بالسطو على

الموقع الإلكتروني للشخص الاعتباري، و خاصة و أن المجرم لديه يقين من ملاءة الضحية المالية، و بأنه لن يعاني من كونه معسر.

ب. الأحداث:

تختلف التشريعات في تعريفها للأحداث، و ذلك يرجع الى اختلاف تحديد سن التمييز، و سن الرشد بسبب العوامل الثقافية الخاصة بكل مجتمع وتفرده وتكثر جرائم الإبتزاز الإلكتروني للأحداث و ذلك بالضغط على الحدث بتهديده بنشر صور أو تسجيل مرئي أو محادثات على مواقع الدردشة، أوأية مادة عن واقعة من شأنها تحقير المجني عليه عند أهله، و المجتمع.

وتستهدف هذه الفئة من أجل مطامع جنسية، أو تسريب معلومات عن الأهل فيستغل المجرم جهل الطفل في التصرف ويمارس جريمة الابتزاز الالكتروني بعد التسلل الى عقل الطفل الحدث. [1]

لأن الاحداثهم أكثر الفئات اتصالا بالتكنولوجيا ووسائل التواصل الاجتماعي وأكثر ولعا بها حيث باتت تشكل حيزا كبيرا من يومهم مما يسهل انزلاقهم في الجريمة.

ج. النساء:

يعتبر ابتزاز النساء هو النموذج المثالي الأكثر شهرة وانتشارا خاصة إذا كان المبتز رجلا والضحية امرأة، ويرجع ذلك أنه غالبا ما يكون تهديد المبتز للمرأة يعتمد على صور، أو محادثات خادشة بالحياء أو عرضا مرئيا لعلاقة غير شرعية جمعت بين المبتز وضحيته، أو شخص أخر وقد يكون المبتز قد خطط لجريمته مسبقا، أو قد تزرع الفكرة في رأسه بعد ان وطد أواصر العلاقة مع ضحيته، وقد تكون الضحية امرأة ومن فئة الأحداث والتي غالبا ما تتجاوب مع الإبتزاز خوفا من العار اذا لم ترضخ الطلبات المبتز.

---

[1] سمية مزغيش جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2013-2014

د. الرجال:

قد يقع الرجل ضحية مجني عليه في جريمة الإبتزاز الإلكتروني للعديد من الأسباب فقد يكون ميسور الحال وعرضة للابتزاز من طرف بعض النساء محترفات ببيع الهوى على المواقع الإلكترونية فتهدده بإذاعة صور، أو مقاطع فيلمية تهدد مركزه، أو بسبب أسرار في مجال عمله، أو عائلته، أو معلومات بنشرها قد تمس في شرفه وسمعته ومركزه في المجتمع وبما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره .

ثانيا: بالنظر الى الهدف المرجو من المجني عليه

نتحدث في هذه الجزئية عن الهدف المرجو من عملية الابتزاز، والذي يتفرع الى هدف مادي (مالي)، هدف نفعي، هدف انتقامي، هدف غير اخلاقي (جنسي).

أ. هدف مادي (مالي):

من أهم و أكثر الأهداف التي يرجو المبتز تحقيقها من ارتكابه جريمة الإبتزاز الإلكتروني هي تحقيق منفعة مالية أو عينية ذات قيمة من المجني عليه فقد حقق هذا النوع من الإبتزاز بقيام الجاني بتهديد المجني عليه من أجل تسليم أموال أو أشياء أخرى ذات طابع مالي، سواء بطريقة مباشرة أو غير مباشرة، فيتحقق إبتزاز المال بالطريق المباشر بطلب المبتز من المجني عليه تحويل مبالغ مالية بشكل مستمر، أو لغيره ، أما ابتزاز المال بالطريق غير المباشر فيتحقق عن طريق طلب المبتز من المجني عليه تسديد مبالغ مالية

اقترضها من أحد البنوك أو قيامه بدفع أقساط مالية عند الغير و تسديد ديون مستحقة لمصلحة المبتز و يسعى كل منهم لتحقيق أهدافه الخاصة[1] .

ب. هدف نفعي:

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

ج. هدف انتقامي:

ويكون نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[2].

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

د. هدف غير أخلاقي (جنسي):

---

[1] سعيداني نعيم آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية ، تخصص علوم جنائية ، جامعة الحاج لخضر، 2013 .

[2] صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، مذكرة لنيل شهادة الماجيستير في القانون ، كلية الحقوق و العلوم السياسية ، مدرسة الدكتوراه القانون الأساسي و العلوم السياسية جامعة مولود معمري ، تيزي وزو ص 42.

ينقسم الإبتزاز الجنسي الى قسمين :

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

أما الإبتزاز الجنسي الإلكتروني فيتحقق عن طريق وسائل الاتصال الإلكترونية والأنترنت ، والمبتز في هذا النوع يعتبر مجرما خفيا يسعى للحصول على معلومات[1] تخص الضحية

المطلب الثاني: وسائل الابتزاز الالكتروني وآثاره

إن جريمة الابتزاز هي جريمة قديمة نوعا ما لكنها تطورت لتصبح من أكثر الجرائم خطورة خاصة بعدما اتخذت منحى أكثر خطورة بسبب الثورة التكنولوجية و المعلوماتية حيث استغل البعض هذه التكنولوجيا للإعتداء على خصوصية الآخرين وتهديدهم بما يحقرهم في المجتمع.

حيث يتسلل المجرم إلى تلك الخصوصية ضاربا بعرض الحائط كل الخطوط الحمراء فيقوم باستغلال ما وصل اليه للضغط و التهديد للضحية ، لهذا يرتكب المجرم هذه الجريمة بعد الحصول على ما يمكنه من إبتزاز ضحيته ، فالإبتزاز الإلكتروني هو كل استخدام سيئ صادر من مجرم" متمرس لوسائل الإتصال التكنولوجية الحديثة لتهديد الضحية بنشر صور أو مقاطع فيلمية ، أو محادثات ، أو معلومات سرية تخص الضحية عبر الوسائل الإلكترونية خاصة وسائل التواصل الإجتماعي ، مقابل دفع مبالغ مالية أو استغلال الضحيةللقيام بأعمال مشروعة، أو غير مشروعة لصالح المبتز.

---

[1] رصاع فتيحة الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان 2011-2012، ص 36

لهذا فالابتزاز الإلكتروني يعد أي طريقة تستخدم بواسطة وسائل الإتصال التكنولوجية الحديثة حيث تستدرج الضحية عبر مواقع التواصل الاجتماعي وبعض تطبيقات الهواتف الذكية لإغرائهم بالظهور في أوضاع غير لائقة وتصويرهم دون علمهم،وتهديدهم بنشر الصور والمقاطع وتهديدهم ماليا وللقيام بما يسبب خطرا على الضحية و كما يتنوع المجرمون بالإعتماد على عدة معايير مثل الخبرة، أو علاقتهم بالضحية، أو من حيث المعرفة التقنية، أو من حيث كونهم أفراد، أو ينتمون إلى عصابات منظمة.

هذا ما سيتم التطرق اليه فالفرع الأول يتناول وسائل الابتزاز الالكتروني و الفرع الثاني الآثار المترتبة عن هذه الجريمة.

الفرع الأول: وسائل الابتزاز الالكتروني

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

ومن أشهر مواقع التواصل الإجتماعي استخداما لتصيد الضحايا هي:

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

أولا: الحاسب الآلي

الحاسب الآلي [1](الكمبيوتر): هو جهاز الكتروني قادر على استقبال معطيات المعلومات التي نرغب في إدخالها وتخزينها وكذا تخزين المعلومات الخاصة بالبرامج التطبيقية، للقيام بمعالجة هذه الأخيرة بسرعة فائقة يستحيل على الإنسان القيام بها وذلك بعد أن يدخل عليه لإنشاء معلومات مسبقة وبرامج متخصصة.

ثانيا: برامج الحاسب الآلي.

---

[1] بن زيطة عبد الهادي حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر و التوزيع، الجزائر، 2007، ط01

ورد تعريف البرامج الحاسب الآلي في نظام مكافحة الجرائم المعلوماتية السعودي بأنه: (مجموعة من الأوامر والبيانات التي تتضمن توجيهات وتطبيقات حين تشغيلها في الحاسب الآلي أو شبكات الحاسب الآلي، تقوم بأداء الوظيفة المطلوبة.

ثالثا: الأنترنت

من الطبيعي أن تخلق الأنترنت أنماطا إجرامية مستجدة أو تأثر بالآلية التي ترتكب فيها جرائم الحاسب الآلي ذاتها بعد أن تحقق تشبيك الحواسيب معا في نطاق شبكات محلية، وإقليمية، وعالمية، وقد ساد مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود و فواصل في نطاقه بين وسائل الحاسوب و وسائل الاتصال (الشبكات).

وتعتمد الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت على المعلومة بشكل رئيسي ، هذا الذي أدي الى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم [1]

أ- البريد الإلكتروني.

عرف جانب من الفقه البريد الإلكتروني بأنه طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات، ويعرف جانب آخر من الفقه بأنه مستودع لحفظ الأوراق والمستندات الخاصة في صندوق البريد الخاص بالمستخدم شرط تأمين هذا الصندوق بعدم الدخول إليه وذلك بطرق التامين المعروفة ومنها التشفير وكلمة المرور وغيرها من تقنيات الحماية الفنية.

---

[1] صغير يوسف،مرجع سابق،ص 08

و من خلال التعريف السابق يتضح أن القوانين التي عرفت البريد الالكتروني لم تختلف في مضمون هذا الأخير، إنما الإختلاف بالصياغة فقط أما التشريعات العربية لا تزال بعيدة كل البعد عن معالجة التطور الحاصل في مجال التقنية بدليل أن كل القوانين العربية لم تعرف البريد الالكتروني[1]

ب-مواقع التواصل الاجتماعي

بتم عند محاولة شخص الولوج الى الفيسبوك، أو تويتر أو انستغرام أو واتساب، وغيرها من مواقع التواصل الاجتماعي حيث تعتمد في المقام الأول على النظام المعلوماتي عبر شبكة الأنترنت أو أي وسيلة إلكترونية أخرى حيث يعمل على هذا النظام العديد من الأشخاص، أو الوسطاء ودون هؤلاء لا يمكن لمواقع التواصل أن تعمل ومن هنا تشار إليهم أصابع الاتهام عند حصول جريمة في هذا العالم الافتراضي[2]

رابعا: الهاتف النقال

يعتبر الهاتف النقال وسيلة اتصال لاسلكية تعمل من خلال شبكة من أبراج البث المباشر على تغطية مساحات معينة وتترابط فيما بينها بواسطة خطوط ثابته وأقمار صناعية وهو ما يعرف بشبكة التغطية ومع تطور أجهزة الهاتف الخلوي أصبحت الأجهزة أكثر من مجرد وسيلة للاتصال الصوتي حيث أصبحت تستخدم كأجهزة كمبيوتر وتصفح الأنترنت، وللأجهزة الحديثة نفس خصائص ودقة وضوح الكاميرا الرقمية.

---

[1] عدي جابر هادي ، الحماية الجزائية للبريد الالكتروني ، دراسة مقارنة ، بحث مقدم بمجلة رسالة الحقوق ، السنة الثانية ، العدد الثالث ، كلية القانون جامعة القادسية 2010 – ص 156

[2] بوقرين عبد الحليم ، المسؤولية الجنائية عن الاستخدام غير المشروع المواقع التواصل الاجتماعي ، دراسة مقارنة بحث مقدم في مجلة جامعة الشارقة ، دورية علمية محكمة المجلد 16 ، العدد 01 ، يونيو 2016، ص 373

أما برامج الهاتف النقال مجموعة من التعليمات التي تسمح بمعاينتها على دعامة مقروءة من قبل الآلة لبيان أو أداء أو إنجاز وظيفة مهمة أو نتيجة معينة صادرة عن آلة قادرة على مناقشة المعلومات[1].

تكون هذه المعلومات محلا لجريمة الإبتزاز الإلكتروني وذلك عندما يقوم المجرم الإلكتروني باستخدام الأنترنت في برامج التواصل الاجتماعي أو المعلومات الموجودة بالهاتف الموجه للتجسس على الآخرين وانتهاك حرمة حياتهم الخاصة أو عن طريق الاستخدام غير المشروع الملحقات الهاتف الذكي : الكاميرا أو البلوتوث أو آلات التسجيل.

الفرع الثاني: آثار الابتزاز الالكتروني

إن لجريمة الإبتزاز الإلكتروني آثار خطيرة ومتنوعة و المتمثلة في الآثار الاجتماعية،النفسية و الأمنية .

أولا: الآثار الاجتماعية

إن ظاهرة الإبتزاز الإلكتروني تشكل خطرا جديا على المجتمع والعائلة حيث أن أغلب ضحاياها نساء ، حيث سببت هذه الظاهرة انفصالهم عن أزواجهم كما ان أغلب الفتيات اللائي تعرضن للإبتزاز يتخوفن من تقديم شكوى في المحاكم خوفا من المشاكل الناجمة كان يحجم الناس من التقدم للزواج منهن خاصة المحيط القريب منهن لمعرفة هذا المحيط بقضاياهن. فقد ترفض الفتاة نفسها الزواج خوفا من أن يعرف الزوج تاريخها السابق ، وقد يؤدي الإبتزاز إلى هدم بيت الزوجية بالطلاق فهو أثر مباشر للابتزاز .[2]

---

[1]التوجي محمد الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي ، كلية الحقوق و العلوم السياسية جامعة احمد دراية ، ادرار 2019 ، ص 03 .

[2]محمد بن عبد المحسن بن شلهوب ، جريمة الإبتزاز الالكتروني ، دراسة مقارنة ، بحث تكميلي لنيل درجة الماجيستير في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية ، شعبة الأنظمة ، جامعة الإمام محمد بن سعود الإسلامية . 2011

وقد يتم اغتصاب الفتاة بالانصياع الى رغبة المجرم، وقد ينتج عن ذلك حمل الفتاة وقد يترتب عن ذلك قيامها بالإجهاض أو قتل الطفل غير الشرعي ، وقد تقوم الفتاة بالتخلص من الطفل بإيداعه للملاجئ أو الشارع ويصبح من أولاد الشوارع والمنحرفين فيكون مصيره إما السجن أو القتل.

ثانيا: الآثار النفسية

نتيجة التزايد المقلق لظاهرة الإبتزاز الإلكتروني أصبح هناك من يعاني بصمت وذلك خوفا من التشهير والفضيحة وتبعاتها.

فالضحية قد يكون عرضها للإبتزاز الالكتروني في أي وقت ومن قبل مجموعة من الأشخاص ومما يزيد من الأثر النفسي.

ومما يزيد من الآثار النفسية على الضحية عدم قدرة هذه الأخيرة على طلب المساعدة بسبب الإحراج أوالجهل بأساليب الوقاية أو أن هناك من يستطيع تقديم يد العون له والتخفيف عليه.

ومن أبرز العلامات الدالة على تعرض الشخص للإبتزاز الالكتروني هو التغيير بسلوك هذا الأخير على الشبكات الإلكترونية ممثلا بقله نشاطه أو انعدامه خوفا من التعرف الى المزيد من المعتدين.

كما قد يتحول الضحية في جريمة الإبتزاز الإلكتروني الجنسي من ضحية الى مجرم جنسي آخر ومجرم عادي نتيجة لما حدث له او رد فعل ما أصابه.

ثالثا: الآثار الأمنية

يهدد الإبتزاز الأمن في المجتمع حيث يؤدي إلى تفشي الفساد وانهيار القيم والأخلاق في المجتمع فلا يأمن الفرد على عرضه وشرفه، كما أن جريمة الإبتزاز اذا كان الغرض منها مالي سيؤدي ذلك الى زيادة جرائم النصب والسرقة خاصة إذا كان الضحية معسر ولا يملك ما يقدمه للمبتز لقاء صمته.

كما قد يؤدي الى جرائم القتل حيث يقوم المبتز بقتل ضحيته بعد ارتكاب الفاحشة وتصويره لها، فاذا ما تم تداول صور الجريمة يقوم أهل الضحية بقتل المبتز المعتدي انتقاما منه خاصة في بعض المجتمعات التي لا ترى غسل العار إلا بسفك الدم[1].

المبحث الثاني: تجريم الابتزاز الإلكتروني

قد تستهدف الجريمة الإلكترونية الجاني الأخلاقي خاصة في المجتمعات العربية التي تعتز بمبادئها وقيمها الفاضلة، فهذه الجريمة تقضي على حياة الأفراد، فمعظم القوانين العربية وضعت حد لهذه الجريمة وسنت لها أركان وقوانين رادعة لها، كما وضعت حلول مقترحة لتجنب الأضرار المتوقعة من الإبتزاز الإلكتروني، وللحد من الوقوع ضحية الإبتزاز الإلكتروني، وهذا ما سنتطرق إليه في هذا المبحث تجريم الإبتزاز الإلكتروني من خلال دراسة مطلبيه المطلب الأول الذي يتناول أركان جريمة الإبتزاز الإلكتروني، والمطلب الثاني الذي يتناول عقوبة جريمة الإبتزاز الإلكتروني .

المطلب الأول: أركان جريمة الإبتزاز الإلكتروني

الإبتزاز الإلكتروني الذي يتم عبر الوسائل الإلكترونية هو نوع من أنواع تهديد شخص والضغط عليه، بهدف ابتزازه وجبره على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، وتقضي وجود جريمة الإبتزاز شخصين، أحدهما جاني والآخر مجني عليه، ورغم حداثة عهدها في علم الإجرام إلا أنها في الأساس جريمة كسائر الجرائم الأخرى.

ولقيام جريمة الإبتزاز الإلكتروني، ينبغي توفر أركان متعلقة بالجريمة نفسها، كي تصبح جريمة يعاقب عليها القانون وفق الأنظمة المجرمة لها، والمتمثلة في الركن الشرعي، الذي هو عبارة عن وجود نص قانوني يحدد

---

[1] محمد بن عبد المحسن بن شلهوب، المرجع السابق، ص 58

الفعل المجرم والجزاء الجنائي الذي بوجوده، ينقل الفعل من دائرة الإباحة إلى دائرة التجريم. أما الركن المادي فهو كل ما يدخل في كيان جريمة الإبتزاز الإلكتروني، وتكون له طبيعة مادية ملموسة سواء كان فعلا أو امتناعاً، والركن المعنوي فهو داخلي كامن في نفسية الجاني، ومن هذا المنطلق يمكن تقسيم هذا

المطلب إلى ثلاث فروع، كما يلي:

الفرع الأول: الركن الشرعي لجريمة الابتزاز الإلكتروني

هو نص التجريم والعقاب فهو النص الذي نستند إليه لتجريم فعل معين والعقاب عليه ويكون ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة لا جريمة ولا جزاء ولا عقوبة مرتكب الفعل الإجرامي ومن هنا ظهرت القاعدة "لا جريمة ولا جزاء ولا عقوبة إلا بنص".[1]

ومن بين التشريعات العربية التي عنيت بتجريم الأفعال المادية المكونة لجريمة الإبتزاز الإلكتروني واتجهت إلى إصدار قوانين خاصة لضمان جريمة الإبتزاز الإلكتروني بكافة صورها لتجريم والعقاب ووضع ركن شرعي لهذه الجريمة من بينها :

أولا: الركن الشرعي في التشريع الجزائري

في الجزائر قد أولى المشرع أهمية بالغة للخصوصية الشخصية للأفراد، واعتبر الإعتداء عليها جريمة تصيب مركز المجني عليه، حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه جريمة الإبتزاز الإلكتروني في المجتمع الجزائري، الذي طالما اعتز بمبادئه وقيمه الفاضلة، فمثل هذه الجريمة كفيلة بهدم حياة المجنى عليه، وتفقد عائلته كرامتها و انتمائها للمجتمع.

---

[1] برحال أمال ، جريمة الابتزاز عبر الوسائط الإلكترونية ، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر ، كلية الحقوق والعلوم السياسية جامعة العربي التبسي ، تبسة 2020 ، ص34.

ولقد تطرق المشرع لتلك الحماية لحرمة الحياة الخاصة في الدستور في نص المادة 39 التي تنص : " لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه يحميها القانون وسرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة" .[1]

المشرع الجزائري على غرار باقي التشريعات، تبنى الشمولية في تجريمه للأفعال التي يكون مسرحها الكتروني، وذلك من خلال القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[2]

وهو ما يستشف من نص المادة 02 منه التي جرمت كل الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيات الإعلام والاتصال، فتكون جريمة الابتزاز الإلكتروني بذلك من ضمنها واستنادا إلى عمومية النص الذي يحيلنا بدوره إلى القواعد التقليدية المطبقة على جريمة التهديد في صورتها الكلاسيكية.[3]

وما الإبتزاز الإلكتروني إلا صورة مستجدة للتهديد والابتزاز التقليدي المنصوص عليه في المادة 371 من قانون العقوبات الجزائري .[4]

الفرع الثاني : الركن المادي لجريمة الإبتزاز الإلكتروني

---

[1]أنظر المادة 39 من دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 7 ديسمبر 1996، الجريدةالرسمية رقم 76 المؤرخ في 8 ديسمبر 1996، المعدل

[2]قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430هـ الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها الجريدة الرسمية العدد 47، الصادر بتاريخ 25شعبان عام 1430هـ، الموافق 16 غشت سنة 2009.

[3]أكرم ديب نورة بن بوعبد الله، دور الدليل الرقمي الجنائي في إثبات جريمة الإبتزاز الإلكتروني، مجلة الحقوقوالعلوم الإنسانية جامعة باتنة | كلية الحقوق والعلوم السياسية الجزائر، المجلد 16، العدد 01، 31/03/2023 ، 406.

[4]قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم156-66المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات الجريدةالرسمية، العدد 87، الصادرة بتاريخ 04 ذي الحجة عام 1427هـ الموافق 24 ديسمبر سنة 2006.

يعتر الركن المادي للجريمة، السلوك الذي يظهر إلى حيز الوجود، فهو يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة الإبتزاز الإلكتروني في أركانها عن جريمة الإبتزاز التقليدي، فهي تتطلب سلوك إجرامي يصدر من الجاني سواء بالقول أو الكتابة أو أي فعل آخر يتمثل القيام بالتهديد بنشر البيانات أو الصور أو مقاطع فيديو للضحية.

وقد عرف المشرع العراقي في قانون العقوبات العراقي الركن المادي بأنه: "سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون".[1]

بمعنى وجوب أن يكون هناك فعل أو امتناع عن فعل يمكن إثباته، فلا يعتد بما يدور فينفس البشرية كون ذلك خارج نطاق التجريم بحكم القانون.[2]

وبالتالي فعناصر الركن المادي للجريمة ثلاثة الفعل أو النشاط الإجرامي، والنتيجة والعلاقة السببية بينهما.

فتتطلب سلوك إجرامي يتم عبر وسائل التواص الاجتماعي أو الحاسب الآلي ويعتبر تهديداً كل قول أو كتابة أو رموز أو صور أو شعارات من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد، ولا يهم إن كان الجاني ينوي تنفيذ الأمر المهدد به أم لا، فقط يشترط أن يكون جديا وليس بمجرد هزل .[3]

ترتب على ذلك قيام المسؤولية الجزائية للجاني بتوافر الركن المادي للجريمة، حتى وإن لم تتحقق النتيجة الإجرامية المتمثلة بتنفيذ الجاني لوعيده ونشر وعرض تلك المعلومات والصور والمقاطع المرئية وجعلها معلنة ومتاحة للجمهور.[4]

---

[1]عراب مريم ، جريمة التهديد والإبتزاز الإلكتروني ، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة وهران 2 أحمد بن أحمد، المجلد 7 ، العدد 1 ، 28/06/2021 ، ص1208.

[2]يوسف خليل يوسف الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير الجامعة الإسلامية، غزة، 2013 ، ص50.

[3]عراب مريم ، مرجع سبق ذكره ، ص1208.

[4]أكرم ديب نورة بن بوعبد الله، المرجع السابق ، ص312 ،

فالركن المادي لجريمة الإبتزاز الإلكتروني إذن، يقوم على ثلاثة عناصر النشاط الإجرامي يأتيه الجاني ونتيجة إجرامية سواء تحققت أو لم تتحقق واقتصرت على التهديد فقط، إضافة إلى العلاقة السببية بتنفيذ الجاني لتهديده بالنشر والعلانية لتلك المعلومات التي تتعلق بالشخص المجني عليه على المنصات الإلكترونية ووسائل التواصل الاجتماعي .

أولا: السلوك الإجرامي للابتزاز الإلكتروني

الفعل محل التجريم هو واقعة مادية ظهرت للعالم الخارجي، حيث يتحذ بالقيام بفعل التهديد بنشر بيانات أو صور أو مقاطع فيديو للضحية، والقانون لا يميز ولا يهمه منأين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنه عثر عليها في جهاز الضحية المسروق أو المعثور عليه أو المباع.[1]

ولا يشترط أن يتم التهديد بطريقة معينة، فيمكن أن يتم عن طريق غرف الدردشة (الشات)أو عن طريق البريد الإلكتروني أو التسجيل الصوتي، كما لا يهم بأن كان الإبتزاز المصلحة المبتز المشروعة أو غير المشروعة، فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد الإرغام المجني عليه للقيام بذلك الفعل.

ثانيا : النتيجة الإجرامية لجريمة الإبتزاز الإلكتروني

النتيجة الإجرامية هي الأثر المترتب على السلوك الذي يقصد القانون بالعقاب، فهي الحقيقة المادية إلى كيان ملموس في العالم الخارجي أو أنها الحقيقة القانونية.[2]

وتقع النتيجة الجرمية في جريمة الإبتزاز الإلكتروني لمجرد قيام المبتز بتهديد الضحية بإفشاء سر من أسرارها التي تعتبره أمراً لا يجب الاطلاع عليه أمام الملأ وكان تهديدا بأمر غير مشروع.

---

[1] شاكر سعاد بعيوي، جريمة الإبتزاز الإلكتروني دراسة مقارنة مقال منشور بمجلة ميسان للدراسات القانونية المقارنة كلية القانون، جامعة ميسان العراق، نوفمبر 2019، ص 129

[2] آمال برحال، المرجع السابق، ص 45.

ويسبب الخوف والهلع والتأثير على إرادة نفسية بأن يلقي في نفسها قلقا من قيام المبتز بتنفيذ تهديده.[1]

فإذا قام الجاني بالتهديد بمجرد ترهيب الضحية أو طلب منفعة أو أن يحمل المجني عليه على أداء عمل أو الامتناع عن عمل فهنا تقع النتيجة، سواء فعل المجني عليه ما طلب منه أو لم يفعل.

ثالثا : العلاقة السببية لجريمة الإبتزاز الإلكتروني

تعرف العلاقة السببية بأنها الصلة بين السلوك الذي يعترف به القانون سببا، والأثر الذي يعترف به القانون نتيجة، وتعد العنصر الثالث من عناصر الركن المادي للجريمة فهي الصلة التي تربط ما بين السلوك الإجرامي والنتيجة الجرمية.[2]

ولقيام الركن المادي لابد أن تحدث النتيجة الجرمية بسبب فعل الجاني، أي لو لا حصول الفعل لم تحث تلك النتيجة الإجرامية.

حيث تقوم علاقة سببية بين الإبتزاز والتسليم في حال كان الباعث للجاني هو الخصول على المال، إذ يلزم أن يكون تسليم المال نتيجة ما أحدثه في نفس المجني عليه من الخوف فإن لم يحدث التهديد هذا الأثر، وجرى تسليم المال لاعتبارات أخرى انقطعت علاقة السببية.

أما إذا كان الإبتزاز للقيام بعمل أو الامتناع عن أداء عمل فإن النتيجة هنا وقوع الضرر وهو الخوف في نفس المجني عليه، وتكون علاقة سببية بينه وبين الإبتزاز، هو أن يكون الإبتزاز سببا في امتهان كرامة المعتدي عليه واحتقاره وتعريضه لبعض أهله والناس وبامتناع المجني عليه عن أداء عمل ليس على سبيل

---

[1] رامي أحمد غالبي، جريمة الإبتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق ، مقال منشور في مجلة ثقافتنا الأمنية الإصدار الثاني، وزارة الداخلية العراقية مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد 2019 ، ص41.

[2] محمد بن عبد المحسن بن شلهوب ، المرجع السابق ، ص91.

الخوف من الجاني، وإنما لرغبته في الإلتزام بالقانون، فهنا لا تقع جريمة الإبتزاز وذلك لانتقاء علاقة السببية في الجريمة.[1]

الفرع الثالث : الركن المعنوي لجريمة الإبتزاز الإلكتروني

تتطلب جريمة الابتزاز الإلكتروني لقيامها ركناً معنوياً إلى جاب الركن المادي والشرعي لها، فهي تعد من الجرائم العمدية تأخذ صورة القصد الجنائي الذي يقوم بتوافر عنصري العلم والإرادة.[2]

أي لابد أن يعلم الجاني بنتيجة السلوك الذي اقترفه وأن ينصب علمه على أن ما يقوم بهمن حصوله على الصور الفاضحة وبيانات سرية لأحد الأشخاص وتهديده بها مقابل الحصول على منفعة جريمة يعاقب عليها القانون.

أما العنصر الثاني المتمثل في الإرادة المنصرفة إلى السلوك الإجرامي وتوقع النتيجة الإجرامية في الوقت نفسه.[3]

ويقصد بالركن المعنوي إدراك الجاني وقت اقترافه للفعل المادي المكون للجريمة أن قوله أو كتابته من شأن أي من هما أن يسبب انزعاج الضحية، وهو تهديد مصحوب بطلب أو تكليف بالقيام بأمر ما، والركن المعنوي مسلك ذهني ونفسي للجاني، يوفر معلومات قيام المسؤولية مع اعتبار حق الدولة في العقاب.3

ومن هنا يمكن القول بأن الركن المعنوي هو إرادة الجرمية ولا تخرج الإرادة الإجرامية عنصورتين أساسيتين وهما :

---

[1]محمد عبد المحسن بن شلهوب، المرجع السابق، ص 92.

[2]أكرم ديب نورة بن بوعبد الله ، المرجع السابق، ص 407.

[3]سيف مجيد العاني، مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الإجتماعي (دراسة مقارنة)، دونطبعة دروب المعرفة للنشر والتوزيع الإسكندرية، مصر، لسنة 2022، ص 117.

1. القصد الجنائي وبه تكون الجريمة عمدية.
2. الخطأ غير العمدي وبه تكون الجريمة غير عمدية.

- فالقصد الجنائي هو تعمد إتيان الفعل المجرم أو تركه مع العلم أن القانون يجرم تركه.
- فالقصد الجنائي لدى المبتز أن تكون إرادته وعلمه قد إتجه إلى تهديد الضحية بالمعلومات.

والصور التي يملكها، وهو ما يتمثل إعتداء على حرمة الحياة الخاصة .

أولا: القصد العام

ينهض القصد العام في جريمة الإبتزاز الإلكتروني على عنصرين هما:

أ.العلم:

وهي من عناصر الجريمة والعلم بموضوع الجريمة أنه يعلم المبتز أن ما يقوم به وما يتصل به من وقائع، ويجب أن يعلم أن ما يقوم به من الحصول على صور فاضحةلأحد الأشخاص وتهديده بها، مقابل منفعة جريمة يعاقب عليها القانون.

وبالتالي يتحقق العلم كما يجب أن يكون الجاني عالماً بماهية الفعل أو امتناع المجرم كماأن فعله يلحق ضرراً بالمجني عليه.

ب. الإرادة:

هو الإرادة في تحقيق النتيجة غير مشروعة نحو المساس بحق، أو مصلحة يحميها القانون، ومن ثم ينبغي أن تتجه إرادة المبتز إلى تحقيق النتيجة المتمثلة في ابتزاز المجنيعليه .

وتنقسم الإرادة إلى قسمين إرادة الفعل، وإرادة النتيجة، فلكي تقوم المسؤولية يجب إثبات أنإرادة الفعل اتجهت إلى القيام بهذا الفعل وذلك دون أن تقع الإرادة في عيب من عيوب الإرادة كأن يكون مختار ومدركاً، أنه

يحصل على صور سرية وخاصة بالضحية فإن كان مكرها فلا يوجد قصد جنائي ولا تقوم المسؤولية الجزائية للفعل على المكره.[1]

أما إرادة النتيجة فلا بد أن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية بالحصول على المنفعة المادية أو النفعية أو اللاأخلاقية، فالباعث لا عبرة له في الجريمة، فيستوي في الإبتزاز الإلكتروني أن يكون الباعث شريفا كانتقامه من المجني عليه أو لتحقيق مصلحة ما.

ثانيا: القصد الخاص

بما أن جريمة الإبتزاز الإلكتروني من الجرائم التي تحتاج إلى معرفة خاصة وعالية بتكنولوجيا المعلومات من أجل تنفيذها فلا يمكن تصور حصولها من دون قصد، فهي من الجرائم العمدية التي يكتفي فيها بالقصد العام، ولا يشترط أن يكون القصد خاص.

المطلب الثاني: عقوبة جريمة الابتزاز الالكتروني

تعد العقوبة من أهم الأثار التي تترتب على تجريم السلوك المعتدي، إذا نظم المشرع كل فعل أو ترك مخالفين لنصوصه الموضوعية وجعل مقابل هذا الفعل أو الترك المجرمين عقوبة، هذه العقوبة لضمان تحقيق الردع الخاص للمجرم وتحقيق الردع العام للمجتمع ككل، فللعقوبة وجهين العلاجي والوقائي بكل صوره وتعدياته فوضعت لها عقوبات تتناسب مع الجريمة فتنوعت بين عقوبات أصلية وعقوبات تكميلية .

الفرع الاول: العقوبات الاصلية والعقوبات التكميلية

أولا: العقوبات الاصلية

---

[1] محمد عبد المحسن بن شلهوب، المرجع السابق، ص 107.

ولقد حددالمشرع الجزائري في المواد 303 مكرر و303 مكرر 1، 303 مكرر 2. العقوبات الخاصة بهذه الجنحة وهي كالاتي:

المادة 303 مكرر.[1]

المادة 303 مكرر 1.[2]

م 303 مكرر 2 .[3]

ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة .

ثانيا: العقوبات التكميلية

العقوبة التكميلية هي تلك العقوبة التي تصيب الجاني بناءا على الحكم بالعقوبة الأصلية وهي تختلف عن العقوبة التبعية التي تصيب الجاني بناءا على الحكم بالعقوبة الأصلية دون الحاجة الىإصدار حكم تبعي فهو مرتبط ارتباطا مباشرا ووثيقا بالعقوبة الأصلية.

ففي جريمة الابتزاز الإلكتروني نصت المادة 13 من نظام مكافحة جرائم المعلوماتية على أنه يجوز الحكم بمصادرة الأجهزة أو البرامج، أو الوسائل المستخدمة في أي من الجرائم المنصوص عليها في هذا النظام. أو

---

[1] أنظر المادة 303 مكرر من ق ع ج.

[2] أنظر المادة 303 مكرر 1 من ق ع ج.

[3] أنظر المادة 303 مكرر 2 من ق ع ج.

الأموال المحصلة منها كما يكون الحكم بإغلاق الموقع الإلكتروني أو مكان تقديم الخدمة إغلاقا نهائيا أو مؤقتا، متى كان مصدرا لارتكاب هذه الجرائم وكانت الجريمة قد ارتكبت بعلم مالكه.

المصادرة هي الأيلولة النهائية للمال للدولة والفرق بين المصادرة والغرامة أن هذه الأخيرة هي عقوبة مالية نقدية وعقوبة أصلية أما المصادرة فهي عقوبة عينية تكميلية، وترد على أشياء حيازتها مشروعة وأن تكون حيازة الأشياء المصادرة مشروعة وذلك بأن تكون بينها وبين الجريمة صلة معينة.

هذه الصلة قد حددتها المادة 13 نظام مكافحة الجرائم المعلوماتية السعودي بقولها (الأجهزة والبرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام.

وبالتالي لا يجوز نظاما أن تحكم بمصادرة أشياء لا صلة لها بالجريمة، أو لم تكن قد تحصلت منها، أو من شأنها أن تستعمل فيها، وأن تكون هذه الأشياء قد تم ضبطها فعلا عند إصدار الحكم بالمصادرة فإذا لم تكن الاشياء محل المصادرة مضبوطة بالفعل وقت الحكم بمصادرتها فلا يجوز للقاضي أن يحكم بمصادرتها.

المصادرة تكون على أشياء حيازتها في الأصل مشروعة ولكنها استخدمت، أو كانت وسيلة لارتكاب جريمة فهي مشروعة في الأصل وقد استخدمت في عمل غير مشروع لجريمة الابتزاز الإلكتروني.

وللقاضي سلطة تقديرية في توقيع المصادرة من عدمه شريطة أن ترتبط بالعقوبة الأصلية على المبتز

وهي الحبس، أو الغرامة أو إحداهما. [1]

وإذا لم تكن الأشياء تم استخدامها في الجريمة ليست ملكا للجاني فلا يحكم القاضي بمصادرتها وذلك كما نصت عليه م 13 بقولها ((مع عدم الاخلال بحقوق الغير حسن النية ...)).[1]

---

[1]محمد بن عبد المحسن بن شلهوب، المرجع السابق، ص 134.

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

والمادة 18 من قانون العقوبات حيث يجوز للمحكمة أن تحكم على المحكوم عليه بالجرائم المنصوص عليها في المادة 303 مكرر و المادة 303 مكرر 1 ، وذلك بمنعه من ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة 9 مكرر 1 ق ع ج ، لمدة لا تتجاوز خمس سنوات كما يجوز لها أن تنشر حكم الإدانة طبقا للكيفيات المبينة في المادة 18 ق ع ج ، التي تنص على أن للمحكمة عند الحكم بالإدانة أن تأمر في الحالات التي يحددها القانون بنشر الحكم بأكمله أو مستخرج منه في جريدة أو أكثر أو بتعليقه في الأماكن التي يبينها وذلك كله على نفقة المحكوم عليه على أن لا تتجاوز مصاريف النشر المبلغ الذي يحدده الحكم بالإدانة بهذا الغرض وأن لا تتجاوز مده التعليق شهرا واحدا.[3]

الفرع الثاني: الظروف المشددة للعقاب والمعفية للعقاب الجريمة الابتزاز الالكتروني.

أولا: الظروف المشددة للعقاب لجريمة الإبتزاز الإلكتروني

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

---

[1] أنظر المادة 13 نظام مكافحة الجرائم المعلوماتية.

[2] أنظر المادة 9 مكرر 1 ق ع ج " يتمثل الحرمان من ممارسة الحقوق الوطنية و المدنية و العائلية في:

- العزل أو الإقصاء من جميع الوظائف والمناصب العمومية التي لها علاقة بالجريمة .
- .الحرمان من حق الانتخاب أو الترشح أو حمل أي وسام .
- .عدم الأهلية لأن يكون مساعدا محلفا او خبيرا أو شاهدا على اي عقد او شاهدا أما القضاء الا على سبيل الاستدلال.
- .الحرمان من الحق في حمل الأسلحة و في التدريس و في إدارة مدرسة أو الخدمة في مؤسسة التعليم بوصفه أستاذا أو مدرسا أو مراقب.
- .عدم الأهلية ليكون وصيا أو فيما.

[3] أنظر المادة 18 ق ع ج.

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

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

ثانيا: الظروف المعفية من العقاب لجريمة الإبتزاز عبر الوسائل الإلكترونية

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

أولا: عقوبة الشروع في جريمة الابتزاز الإلكتروني

---

[1] آمال برحال ، المرجع السابق ، ص .

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

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

ولذا نصت المادة 303 مكرر.[1] على ان الشروع في جريمة الابتزاز الإلكتروني يتحقق بالتهديد بإفشاء معلومات أو صور أو مقاطع فيلمية أو أي بيانات خاصة للمجني عليه، حتى وإن تراجع المبتز عن إكمال جريمته لسبب خارجي طالما أن التهديد بنشر الأسرار قد صدر منه ووقع في نفس المجني عليه موضع التأثير والرهبة التي جعلته يعتقد ان المبتز سينفذ تهديده لا محالة، وهو الهدف الذي تحقق بألقاء الرعب في قلب المجني عليه. والشروع في الجريمة هنا يتحقق طالما كان الركن المادي فيها قد شرع في تنفيذه وتوافر القصد الجنائي.[2]

ثانيا: عقوبة الاشتراك في جريمة الابتزاز عبر الوسائل الإلكترونية:

الاشتراك في الجريمة يتم عن طريق أحد صور المساهمة كالاتفاق مع الفاعل الأصلي أو مساعدة المبتز بأي صورة من صور المساعدة حتى يصل إلى النتيجة الإجرامية المستهدفة.

يعاقب نظام مكافحة جرائم المعلوماتية على الاشتراك في جريمة الابتزاز في حال كانت الوسيلة المستخدمة هي من وسائل التقنية والعقاب هنا يشمل الفاعل الأصلي للجريمة وكذلك الشريك بالتسبب.

---

[1] أنظر المادة 303 مكرر، م 303 مكرر 1 ق ع ج.

[2] عبد الرحمن توفيق أحمد، المرجع السابق، ص 150.

بالنسبة للمشرع الجزائري وفي هذه الحالة تطبيق القواعد العامة في المساهمة الجنائية المواد: (41،44،42،45)[1]

ملخص الفصل الأول:

تناول الفصل الأول من الدراسة الإطار الموضوعي لجريمة الابتزاز الإلكتروني كصورة من صور الجريمة الإلكترونية، فتم من خلال هذا الفصل التطرق الى لماهية الابتزاز الإلكتروني لغويا واصطلاحا وفقهيا كما تم التطرق إلى أنواع الابتزاز الإلكتروني بالنظر لشخص الضحية والهدف المرجو من المجني عليه ثم تعرضنا الى وسائل الابتزاز الإلكتروني للحاسب الآلي ، برامجه الانترنت والهاتف النقال ، ثم تجريم ظاهرة الابتزاز الإلكتروني من خلال التعرض الى أركان الجريمة (الشرعي،المادي، والمعنوي). وفي الأخير العقوبات المقررة لجريمة الابتزاز الإلكتروني (الأصلية و التكميلية وعقوبة الشروع والاشتراك).

[1] أنظر المواد، 41-42-44-45 ق ع ج

الفصل الثــاني:

الإطار الإجـرائي لجريمة الابتـزاز الالكتروني

الفصل الثاني : الإطار الإجرائي لجريمة الابتزاز الالكتروني

تمهيد:

بالرغم من خصوصية الجريمة الإلكترونية ، ومنها جريمة الابتزاز الإلكتروني إلا أنها ما تزال تشكل سلوكاً محظورا جرمه المشرع الوضعي، فمن ناحية الإجراءات أو الآليات القانونية لمكافحة هذه الجريمة، ومن خلال القيام بإجراءات التحقيق والإثبات في هذه الجريمة، فكل إجراءات البحث والتحقيق تكون هدفها هو الوصول إلى الحقيقة القانونية التي تحتاج لدليل تأكد معه نسبة التهمة المتهم بها، ولكي تكتمل خصوصية هذه الجريمة، لا بد من القول بأن الدليل في الجريمة الإلكترونية وبالأخص في جريمة الابتزاز الإلكتروني هو دليل يرتبط بالحاسوب وأجهزة الهواتف الذكية وملحقاتها والبرامج والتصنيفات التكنولوجية، فهو عبارة عن رمز و شيفرات وأجهزة وعناوين الكترونية ، كما يخضع الإثبات في المسائل الجنائية لقواعد تحكم المسائل الجنائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة الجريمة .

من خلال هذا الموقف ارتأينا أن تكون نقطة الانطلاق من عنوان هذا الفصل "الإطار الإجرائي لجريمة الابتزاز الإلكتروني من خلال التطرق إلى تقسيمه إلى مبحثين ،المبحث الأول تناول إجراءات التحقيق في جريمة الابتزاز الإلكتروني والصعوبات التي تواجه المحقق ، أما المبحث الثاني فتناولنا فيه الإثبات في جريمة الابتزاز الإلكتروني.

المبحث الأول: إجراءات التحقيق في جريمة الابتزاز الإلكتروني والصعوبات التي تواجه المحقق:

بالرغم من قيام الكثير من الدول بسن تشريعات جديدة لمواجهة الجريمة المعلوماتية، إلا أنها لم تتوصل إلى تدارك كل ما يحيط بالجريمة من الجانب الإجرائي، ونظرا للتطور الحاصل لتقنية المعلومات والانتشار الواسع لشبكة الانترنت مما يتطلب استخدام اساليب متطورة في مجال التحقيق ويتطلب وجود خبراء مختصين وتمتع قاضي التحقيق بالخبرة الكافية[1].

و على هذا الأساس ارتأينا أن نقسم هذا المبحث إلى مطلبين ، الأول يتناول إجراءات التحقيق العامة والخاصة في جريمة الابتزاز الإلكتروني والثاني تناولنا فيه الصعوبات التي تواجه المحقق أو جهات التحقيق.

المطلب الأول: إجراءات التحقيق العامة و الخاصة في جريمة الابتزاز الإلكتروني :

تتشابه إجراءات التحقيق في الجرائم الإلكترونية مع إجراءات التحقيق في الجرائم التقليدية ، بأن كلاهما يتطلب المعاينة والتفتيش والاستجواب وجمع الأدلة وفحصها والمحافظة عليها من العبث بها او ضياعها.

والمقصود بالتحقيق هو مجموع الإجراءات التي يقوم بها المحقق وتؤدي لكشف الجريمة ومعرفة مرتكبها تمهيداً لتقديمه إلى المحاكمة كي ينال عقابه، وقد تكون هذه الإجراءات كالتفتيش أو فنية كالبصمات أو برمجية لتحديد كيفية الدخول إلى المعطيات المخزنة في الحاسوب. [2]

وقد نصت المادة 40 الفقرة الأولى من قانون الإجراءات الجزائية الجزائري المعدل بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 والمرسوم التنفيذي رقم 06-348 المؤرخ في 05/10/ 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق على أن اختصاص قاضي التحقيق المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

[1] اريز سالم الحقبا ، مهارت البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتواره، جامعة نايف للعلوم الأمنية.

[2] جمال ابراهيم الحيدري ، الجرائم الالكترونية وسبل معالجتها ، مكتبة السنهوري ، ط1 ، العراق 2012، ص 83

الفرع الأول: إجراءات التحقيق العامة في جريمة الابتزاز الإلكتروني :

يمكن تقسيم هذه الإجراءات العامة إلى ثلاثة مراحل وهي مرحلة الخبرة الفنية و تدريب الكوادر ومرحلة الانتقال و معاينة مسرح الجريمة المعلوماتية وفي الأخير مرحلة التفتيش.

أولا: الخبرة الفنية وتدريب الكوادر:

إن الخبرة هي إجراء أما تدريب الكوادر فهو آلية من آليات مكافحة الجريمة الإلكترونية ، فيخضع تدريب الكوادر إلى دورات تدريب لتبادل الخبرات على المستوى الإقليمي و الدولي كآلية من آليات التعاون، فالكوادر قد يستعينون بالخبراء و بعد تدريبهم في مجال المعلوماتية يصبحون خبراء في عملهم.

أ:**الخبرة الفنية** : تعتبر الخبرة وسيلة لتحديد التفسير الفني و التقني بالاستعانة بالمعلومات العلمية ، فهي مستقلة عن الدليل القولي أو المادي و إنما هي تقييم لهذا الدليل. [1]

و قد تُعتمد الخبرة من أجل كشف الجريمة المعلوماتية بشرط أن تتماشى مع خصوصية الجريمة الإلكترونية .

و على الخبير أن يتمتع بمؤهلات عالية و مقدرة فنية في تركيب الكمبيوتر و شبكة الانترنت و التعامل مع الجريمة التي خلفتها التقنية الحديثة، وكيفية عزل نظام المعلوماتية و الحفاظ على الأدلة دون تلف.

والمشرع الجزائري أجاز للمحقق الاستعانة بالخبرة ، وبإمكانه طلب خبير في أي وقت الى أن ينتهي التحقيق وهو أمر وجوبي في مجال الجرائم المعلوماتية التي تتطلب خبرة فنية بحتة لا يكشف غموضها إلا

[1] رابحي عزيزة ، الأسرار المعلوماتية وحمايتها الجزائية ، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص ، جامعة أبوبكر بلقايد ، تلمسان 2018، ص 271.

المتخصصون. وذلك ما نصت عليه المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

والجدير بالذكر ان المشرع الجزائري قرر الحماية اللازمة للخبير إذا ما سببت له المعلومات التي أفاد بها للقضاء أي خطر حول حياته، أو سلامته الجسدية، أو سلامة أفراد عائلته ، أو أقاربه، أو مصالحه الأساسية، وذلك بموجب الأمر 02/15 المعدل والمتمم لقانون الإجراءات الجزائية بموجب المواد 65 مكرر الى 65 مكرر 28.

ب:تدريب الكوادر:طبيعة الجرائم الواقعة على الأسرار المعلوماتية تقتضي معرفة بنظم المعلوماتية و كيفية تشغيلها من قبل مستخدميها، ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري و التحقيق في مجال الجرائم المعلوماتية .

ففي الجزائر و على مستوى جهاز الشرطة أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة و مخبرين جهويين في كل من قسنطينة و وهران، أما على مستوى الدرك الوطنيللأدلة الجنائية وعلم الإجرام أنشأت قسم الإعلام و الإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.[2]

كما تسعى الأجهزة الأمنية المعنية بالتحقيق في استقطاب المتخصصين والكفاءات في المجال المعلوماتي لضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم.

---

[1] المادة 05 من القانون09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها التي تنص على انه: (يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها).

[2] رابحي‌عزيزة، المرجع‌السابق، ص 273.

وبالنسبة للتعاون الدولي يظهر من خلال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول وأجهزة العدالة لديها، فمثلا يتم إرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات الدولية بهدف الاطلاع على أحدث الأنظمة المقارنة من خلال عقد ندوات و مؤتمرات وورشات عمل جماعية متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو الإقليمي.

حيث نسلط الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال مناقشة أبعادها وأخطارهاووسائل الوقاية منها بأساليب ووسائل تفوق تلك التي يستعملها مرتكبوها، فالتعاون الدولي في مجال تدريبالكوادر العاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي والإقليمي يستهدف توحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة،من خلالتبادل الخبرة.[1]

ثانيا: الانتقال ومعاينة مسرح الجريمة المعلوماتية :

فالانتقال هو ذهاب ضابط الشرطة القضائية ، أو المحقق الجنائي الى مكان ارتكاب الجريمة، حيث توجد آثارها وأدلتها.

أما المعاينة في جريمة الابتزاز الإلكتروني يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، و تشمل الرسائل المرسلة منه أو التي يستقبلها و كافة الاتصالات التي تمت من خلال الكمبيوتر أو الانترنت، و المعاينة جوازية للمحقق، شأنها شأن سائر إجراءات التحقيق فهي متروكة لتقدير القاضي الجنائي، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في الجريمة التقليدية و ذلك لسببين:

[1] رابحيعزيزة ، المرجعالسابق، ص 274.

1 ـ الجرائم التي تقع على نظم المعلومات قلما يترتب على ارتكابها آثار مادية .

- 2 ـ قد يتردد على مسرح الجريمة عدد كبير من الأشخاص خلال الفترة الزمنية التي تتوسط ارتكاب الجريمة واكتشافها مما يغير أو يتلف الآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة. [1]

وحتى تكون المعاينة لها فائدة في كشف الحقيقة فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات و الأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب الآلي و ملحقاته ، و يراعي تسجيل وقت، و تاريخ و مكان التقاط كل صورة .
- ملاحظة الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية خاصة السجلات الإلكترونية التي تتزودبها شبكات المعلومات لمعرفة موقع الاتصال و نوع الجهاز الذي تم عن طريقه الولوج الى النظام و موقع الاتصال أو الدخول معه في حوار.
- ملاحظة وإثبات حالة التوصيلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة و التحليل حين عرض الأمر على القضاء.

- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة. التحفظ على محتويات سلة المهملات من الأوراق الملقاة، أو الممزقة و أدوات الكربون المستعملة و الشرائط، و الأقراص الممغنطة، و غير السليمة أو المحطمة و فحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

[1] صغير يوسف ، المرجعالسابق، ص86.

- التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد من بصمات، و يلاحظ أن الآثار المعلوماتية، و الرقمية المستخلصة من اجهزة الكمبيوتر من الممكن أن تكون ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة و البريد الإلكتروني،الفيديو الرقمي، الصوت الرقمي،غرف الدردشة،المحادثات،الملفات المخزنة في الكمبيوتر،الصور المرئية.
- و لفهم المعاينة لابد من التعرف على المقصود من مسرح الجريمة في الجريمة الإلكترونية وعموما لم تهتم معظم التشريعات الجنائية المعاصرة بتعريف مسرح الجريمة أو وضع معايير ثابتة لتحديد نطاقه المكاني، فمعظم التشريعات تعبر مسرح الجريمة بمحل الواقعة و يتفق معظم الفقهاء على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها .[1]

ويرجع عدم الاهتمام التشريعي بتعريف مسرح الجريمة إلى اعتبارين:

1- معظم القوانين الجنائية لا ترتب آثار قانونية بالبطلان على تجاوز الحدود المكانية بما هو معروف بمصطلح مسرح الجريمة عند إجراء معاينة تاركا للمحقق السلطة تقديريه .

2 ـ لا تقوم بشأن تحديد المجال الميداني لمسرح الجريمة ضاربة بين أطراف الدعوى العمومية ، فلا يجوز لأي طرف من أطراف الدعوى العمومية أن يعترض على إجراء معاينة لمسرح الجريمة ،أوطريقة أو أسلوب تنفيذها، أو مجالها الميداني فهي إجراء يستهدف التعرف على أبعاد الجريمة ، وأركانها، و ظروفها ، و كشف الحقيقة بشأنها و ليست إجراء موجه ضد شخص معين تمس بحرمة حياته الخاصة حتى ينسب له حق الطعن فيه بالبطلان.

[1] هشام فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلاتالحديثة ، أسيوط مصر،1994 ، ص59.

ومسرح الجريمة في جريمة الابتزاز الإلكتروني هو مسرح سيبراني يقع داخل بيئة الحاسوب، أو ما في حكمه، و يكون في البيانات الرقمية التي تتواجد و تنقل داخل بيئة الحاسوب و شبكاته و في ذاكرته و في الأقراص الصلبة الموجودة بداخله، و التعامل مع الأدلة الموجودة في هذا المسرح لا يتم إلا على يد خبير متخصص في التعامل مع هذا النوع من الأدلة الرقمية.[1]

ثالثا: التفتيش :

يقصد بالتفتيش في قانون الإجراءات الجزائية هو البحث عن شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها، وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة.

وقد أحاط القانون التفتيش بضمانات، فمحل التفتيش إما أن يكون مسكنا أو شخصا، وقد يكون متعلقا بالمتهم أو بغيره وهو في كل أحواله جائز مع الاختلاف في بعض الشروط.

والتساؤل المطروح كيف نكون بصدد تفتيش عن حيثيات جريمة الابتزاز الإلكتروني و مدى قابلية مكوناتو شبكات الحاسب الآلي للتفتيش وللإجابة على هدا التساؤل يجب التطرق لما يلي :

أ: مدى خضوع المكونات المادية للحاسب الآلي للتفتيش :

ويخضع تفتيش المكونات المادية للحاسب الآلي بحثا عن شيء ما يتصل بجريمة من جرائم الانترنتالى إجراءات قانونية خاصة بالتفتيش، كما أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه و هل هو مكان عام أم خاص.

و للمكان أهمية كبيرة فإذا كانت في مسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يكون فيها تفتيش مسكنه و بنفس الضمانات و الإجراءات المقررة قانونا مع مراعاة التمييز بين

[1] صغيريوسف ، المرجعالسابق، ص 76.

ما اذا كانت مكونات الحاسب الآلي المراد تفتيشها منعزلة عن غيرها من الحواسيب الأخرى أومتصلة بحاسب آلي آخر أو بنهاية طرفية في مكان آخر كمسكن غير المتهم.

فلو وجد شخص يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها في مكان ما من الأماكن العامة سواء كانت عامة بطبيعتها كالطرق العامة أو الميادين أو الشوارع أو عامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها التفتيش للأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.[1]

فالتفتيش على المكونات المادية لنظام المعلوماتية لا إشكال فيه، حيث نصت المادة 44 من قانون الإجراءات الجزائية الجزائري،أن التفتيش يكون على الأشياء و هي كلمة تنصرف على الأرجح على المكونات المادية، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها و إمكانية إتلافها.

و الجدير بالذكر فإذا كانت المكونات المادية للحاسب الآلي موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات المقدرة قانونا، فالقانون الجزائري في نص المادة 64 من ق إ ج ج[2]قيدت ممارسة هذا الإجراء بالشروط التالية:

1ـ الحصول على إذن تفتيش من وكيل الجمهورية ، واستظهار هذه المذكرة قبل بدء العملية و تتضمن مذكرة التفتيش البيانات التالية : وصف الجريمة محل البحث و التحري، عنوان الأماكن التي سيتم تفتيشها ،عدم ذكر هذه البيانات يؤدي الى بطلان إجراء التفتيش.

[1] صغيريوسف، المرجعالسابق، ص77.

[2] أنظر: المادة 64 ق.إ.ج.ج

2ـ أن يجري التفتيش بحضور صاحب المسكن، و إن تعذر وجب تعيين ممثل له و إن تعذر الأمر كذلك يقوم ضابط الشرطة القضائية بتعيين شاهدين لا علاقة لهما.

3ـ أن يجري التفتيش بعد الساعة الخامسة 05صباحا، و قبل الساعة 08 مساءا غير أنه يجوز التفتيش في أي وقت إذا طلب صاحب المسكن ذلك و إذا سمعت نداءات من داخل المسكن ، كما يجوز تفتيش الفنادق ، و المحلات ، و النوادي ، و المقاهي، و أماكن المشاهدة العامة (المسرح، السينما) و كل مكان مفتوح للجمهور في أي ساعة ليلا و نهارا.

هذا وقد استثنى عن القاعدة العامة في المادة 64 السالفة الذكر في فقرتها الثالثة ، تطبيق هذه الضمانات على بعض الجرائم ، محيلا ذلك الى المادة 47 في الفقرة 3 حيث أجازت أن يتم التفتيش و المعاينة في المساكن كل ساعة ليلا و نهارا ، و دون التقيد لشرط حضور صاحب المسكن أو ممثليه إذا تعلق الأمر بالجرائم التالية : "...الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات. [1]

ب: مدى خضوع مكونات الحاسب الآلي المعنوية للتفتيش:

ذهب جانب من الفقه الى جواز تفتيشها ولابد من ضبط البيانات الإلكترونية بمختلف أشكالها المحسوسة و غير المحسوسة ، أما جانب آخر من الفقه فيرى عدم انطباق المفهوم المادي على بيانات الحاسب الآلي غير المرئية أو غير الملموسة، لذا فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن يفتش الحاسب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي .[2]

أما المشرع الجزائري فإنه استجاب للرأي القائل بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة و على هذا الأساس أجاز تفتيش المعطيات و لكن بموجب نص جديد و هو المادة 05 من القانون 04/09

[1] رابحي عزيزة ، المرجع السابق، ص280.
[2] صغير يوسف ، المرجع السابق ، ص78.

المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، حيث سمح لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 04 من هذا القانون ، و من بين هذه الحالات توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام ،أو الدفاع الوطني، أو مؤسسات الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها و كذلك المعطيات المخزنة فيها و كذا منظومة تخزين معلوماتية.[1]

ج: مدى خضوع شبكات الحاسب الآلي للتفتيش

عقدت طبيعة التكنولوجيا الرقمية التحدي أمام أعمال التفتيش فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة و بعيدة تماما عن الموقع المادي للتفتيش، و إن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها ، و قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو بلد آخر مما يزيد من تعقيد الإجراءات المتعلقة بالجريمة خاصة العابرة للحدود و يزيد من أهمية تبادل المساعدة القانونية.[2]

وفي هذه الأيام يتم التمييز بين ثلاث احتمالات:

الاحتمال الأول:اتصال حاسب المتهم بحواسيب اخرى أو نهاية طرفية موجودة في مكان آخر داخل الدولة فهناك من الدول من وجدت حلا للإشكالية المتعلقة بمدى جواز امتداد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم أو المشتبه فيه أم على جهازه فقط.

بالنسبة للمشرع الجزائري حيث نصت المادة 5 في الفقرة (أ) إذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من

[1] رابحي عزيزة ، المرجع السابق، ص292.
[2] صغير يوسف ، المرجع السابق، ص79.

المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.[1]

الاحتمال الثاني: إيصال حاسب المتهم بحواسيب أخرى أو نهاية طرفية موجودة في مكان آخر خارج الدولةفطبقا لهذا الاحتمال يمكن أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكة الاتصال البعيدة بهدف عرقلة سلطات الادعاء في جمع الأدلة.

وقد أجاز المشرع الجزائري تفتيش الأنظمة و لو كانت خارج إقليم الدولة و ذلك بموجب المادة 3/5 من القانون 90-04 حيث أجاز النص الحصول على المعطيات المبحوث عنها و المخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني، و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى و ذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.[2] و حسب المادة2/16 من نفس القانون: من واجب سلطات التحقيق الجزائرية أن تقدم جميع التسهيلات لمراقبة الاتصالات و تفتيش المنظومات المعلوماتية الموجودة على التراب الوطني متى طلب منها ذلك مع مراعاة مبدأ المعاملة بالمثل ، و الاتفاقيات الدولية.[3]

وأورد المشرع الجزائري ضمن المادة 18 من نفس القانوناستثناءات على طلب المساعدة القضائية وهي الحالة التي يمكن أن تؤدي الى المساس بالسيادة الوطنية، أو النظام العام كما اشترط المشرع الجزائري قبول المساعدة القضائية بضرورة الالتزام بالمحافظة على سرية المعلومات المبلغة وبشرط عدم استعمالها في غير الأغراض التي أدت الى تجميعها.

---

[1] رابحي عزيزة ، المرجع السابق، ص282.

[2] أنظر المادة5. ق09/04 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام وبالاتصال ومكافحتها.

[3] أنظر المادة 16.ق09/ 04من القانون نفسه.

الاحتمال الثالث: التنصت والمراقبة الالكترونية لشبكات الحاسب الآلي، فالتنصت والأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة 04 الفقرة ج من القانون 04/09 أجاز النص استثناءات المراقبة الالكترونية للوصول الى الحقيقة واشترط ان تكون هي الحل الوحيد للوصول الى الحقيقة.[1]

أما عن السلطة المختصة بالتفتيش فيختص قاضي التحقيق أصلا بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الإجراءات الملائمة بصددها، فالنيابة العامة توجه الاتهاموقاضي التحقيق يباشر إجراءات التحقيق.

و قد نصت المادتين 81 و 82 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد فيه أشياء يفيد اكتشافها في إظهار الحقيقة و لقد أجازت المادة 83 من قانون الإجراءات الجزائية لقاضي التحقيق القيام بنفسه بالتفتيش في أي مكان آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها و كل شيء آخر يفيد في كشف الحقيقة ،كما منحته المادة 48 من قانون الإجراءات الجزائية حق إنابة أحد ضباط الشرطة القضائية للقيام بهذا التفتيش بنفسه ، و طبقا للشروط التي نصت عليها المواد 138 الى 142 من قانونالإجراءات الجزائية حيث ان قاضي التحقيق سلطته مقيدة بمنح الإنابة بشرط استحالة قيامه بالإجراء بنفسه نظرا لخطورة السلطات التي يمتلكها قاضي التحقيق و منها التفتيش.

أما ضابط الشرطة القضائية فإنه من الممكن أن يقوم بعملية التفتيش حيث يتم بمعرفة ضباط الشرطة القضائية في الجرائم المتلبس بها و لقد نصت المادة 15 من قانون الإجراءات الجزائية على أعضاء

[1] أنظر المادة4 .ق 04/09 .

الضبطية القضائية الذين لهم صفة ضباط الشرطة القضائية، إذ نص القانون على ضرورة إجراء التفتيش من طرف ضابط يساعده أعوان ولكن يتم الإجراء بحضوره و تحت إشرافه و إلا وقع باطلا .[1]

الفرع الثاني: إجراءات التحقيق الخاصة في جريمة الابتزاز الإلكتروني :

استحدث التشريع الجزائري على غرار التشريعات الحديثة إجراءات خاصة نظرا لسرعة ارتكاب الجريمة الالكترونية و سهولة محو آثارها مما جعل أمر اكتشافها صعب للغاية من أجل ضبطها قبل تفاقم خطرها، و يمكن تقسيم هذه الإجراءات الخاصة الى نوعين :[2]

الإجراء الأول :مراقبة الاتصالات الإلكترونية

الإجراءالثاني :حفظ المعطيات المتعلقة بحركة السير.

أولا: مراقبة الاتصالات الإلكترونية:

من أهم مصادر التحري مراقبة الاتصالات الإلكترونية سواء في الجرائم التقليدية أو المستحدثة كجرائم الانترنت وهي ما يعرف بالمراقبة الإلكترونية، و قد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية في اعتراض المراسلات و تسجيل الأصوات والتقاط الصور .

وقد اختلف المشرع الجزائري في إعطاء مصطلح واحد للمراقبة الإلكترونية فأحيانا يقر بمصطلح المراقبة الإلكترونية كما قررها في القانون 04/09 أحيانا بمصطلح أساليب التحري الخاصة إلا أنها نفس الإجراءات تختلف في التسمية وفي القانون الذي أقرها.

[1] رابحي عزيزة ، المرجع السابق، ص282.

[2] بوشعير الحسن و حداد شعيب ، جريمة الابتزاز الالكتروني . دراسة مقارنة . مذكرة مقدمة لاستكمال متطلبات لنيل شهادة ماستر مهني في القانون العام ،كلية الحقوق و العلوم السياسية ، جامعة محمد البشير الإبراهيمي ، برج بوعريريج ، 2023، ص 91.

ومن أجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 وفق قانون 22/06 الذي حصر وجوبية اللجوء إلى مثل هذا الإجراء على الجرائم الستة الخطيرة ومن بينها الجريمة المعلوماتية .[1]

وتتمثل هذه الاساليب في :

ـ اعتراض المراسلات

ـ التقاط الصور

ـ تسجيل الاصوات

أ- اعتراض المراسلات:

يقصد بالمراسلات هي جميع الخطابات والرسائل والطرود والبرقيات، والمشرع الجزائري في المادة (65 مكرر5من (ق إ ج ج) حصر مفهوم المراسلات في تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية فقط، وبالتالي استبعد المراسلات العادية.

ب- تسجيل الأصوات:

تسجيل الأصوات يقصد به مراقبة الأحاديث، وتسجيلها و كل الاتصالات التي تتم عن طريق سلكي، أو لا سلكي أي أن عمليات المراقبة تشمل كل أدوات الاتصال سواء سلكية، أو لا سلكية،و تتمثل في وضع تقنية دون موافقة المعنيين من أجل التقاط، و تثبيت،و بث و تسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص.[2]

ج- التقاط الصور:

[1] قانون رقم 06-22 مؤرخ في29ذيالقعدة1427الموافق ل20ديسمبر2006يعدل ويتمم قانون الاجراءات الجزائية.

[2] أنظر المادة65 مكرر5 والمادة 38مكرر10 ق.إ.ج.ج تعديل2006 .

هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، وتتسم هذه الإجراءات بالسرية التامة لأن بها مساس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.

ثانيا:حفظ المعطيات المتعلقة بحركة السير

المعطيات المتعلقة بحركة السير هي تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة باعتبارها جزء من حلقة الاتصال بحيث توضح مصدر الاتصال و الوجهة المرسلة إليها و الطريق الذي سيسلكه ووقت و حجم الاتصال و نوع الخدمة.[1]

وقد قرر المشرع الجزائري على غرار التشريعات الحديثة إلزام مقدمي الخدمات حفظ المعطيات المتعلقة بحركة السير لضمان الوصول الى آثار الجريمة مهما كانت.

المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الابتزاز الإلكتروني:

يعتبر التحقيق في جرائم الابتزاز الإلكتروني أمر ليس بالهين بسبب الصعوبات التي تواجه المحقق أمام جريمة ما زالت غامضة، حتى انعدم التمكن من السيطرة على مجريات التحقيق قد يؤدي إلى فقدان الثقة في المجتمع وزيادة نسبة الجريمة.[2]

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

---

[1] أنظر المادة 12 فقرة "هـ" قانون09 /04.

[2] أنظر المادة 15 من ميثاق الأمم المتحدة سنة 1948.

الفرع الأول: صعوبات اكتشاف جريمة الابتزاز الالكتروني:

يعترض اكتشاف الجريمة الالكترونية عدة صعوبات وذلك راجع الى عدة اعتبارات منها ما هو متعلق بحق الإنسان في الخصوصية ومنها متعلق بفقدان الآثار المادية للجريمة ، ومنها ما هو راجع لتكتم الضحية، ومنها ما هو راجع لنقص الخبرة لدى سلطات التحقيق.

أولا: حق الانسان في الخصوصية:

كثير من التشريعات في الدول جرمت التعدي على حياة الإنسان الخاصة باستخدام شبكة الانترنت، وقد نص عليها ميثاق الأمم المتحدة سنة 1948م، ومنها المادة 15 " لا يعرض أي شخص لتدخل تعسفي في حياته الخاصة، أو أسرته، أو مسكنه، أو رسائله أو شن حملات على شرفه وسمعته، ولكل شخص الحق في طلب حماية القانون له من هذه التدخلات أو تلك الحملات."[1]

ثانيا: فقدان الآثار المادية للجريمة:

تضل الجريمة المرتكبة عبر الانترنت مجهولة ما لم يبلغ عنها للجهات المعنية بالاستدلالات ، أو التحقيق الجنائي، فهي جرائم غير تقليدية لا تخلف آثار مادية حيث تضع الوسيلة التي ترتكب بها الجريمة ضمن قالب غير تقليدي نظرا إلى أن ارتكابها يتم عن طريق نقل معلومات على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي، وشبكة الاتصالات بصورة آلية كما تنساب الكهرباء عبر الأسلاك. و يكفي الضغط على زر في لوحة الاستخدام لزوال ملفات أو حتى قواعد بيانات أو أنظمة بأكملها ، فتأتي من هنا مشكلة ضبط هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل إلا انها تتطلب خبرة عالية ، و إمكانيات قد لا تتواجد عادة لدى مصالح الشرطة القضائية المكلفة بالبحث ، و حتى حال حجز المعطيات

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

الرقمية، فإن البيانات التي تحصل عليها لا تتضمن آثار أو بصمات يمكن الاستدلال من خلالها على صاحبها بل تحتاج للوصول الى هذا الهدف إلى عمليات بحث و تحري أخرى للحصول على نسق من القرائن المادية الأخرى التي يمكن أن تعزز دلالتها و قيمتها في الإثبات. [1]

ثالثا: فرض الجناة لتدابير أمنية

يعمد المجرمون الى إزالة آثار الجريمة عن طريق التلاعب بقواعد البيانات في جهاز الكمبيوتر، و البرامج دون ترك أثر، ولا سيما أن التخزين الإلكتروني غير مرئي,و البيانات بلغة رقمية لا تفهمها إلا الآلة ، و هذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة إلكترونيا لأن هؤلاء المجرمين الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة هم فئة الأذكياء حيث يضربون سياجا أمنيا على افعالهم غير المشروعة قبل ارتكابها كي لا يقعوا تحت طائلة العقاب، كما يقوم المجرمون عبر الانترنت بإخفاء هويتهم أو انتحال شخصيات أخرى حتى لا يمكن التعرف عليهم حال اكتشاف الجريمة ، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته ، كما يقوم المجرمون بانتحال الشخصية عبر البريد الإلكتروني و هي من أكثر الطرق استعمالا من طرف المجرمون[2].

رابعا: التكتم عليها من قبل المجني عليه:

غالبا ما يلجأ الضحية في هذه الجريمة الى التكتم وعدم الإبلاغ عن الجريمة التي راح ضحيتها من أجل إخفاء أساليب ارتكابها للحيلولة دون تقليد الآخرين للجناة ، كذلك للتستر على معلومات لا يجب الإبلاغ عنها خاصة إذا كانت الضحية شركات التأمين أو البنوك.

خامسا: نقص خبرة سلطات الاستدلال:

---

[1] صغير يوسف ، المرجع السابق ، ص117.

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

مازالت جهات التحقيق تعاني من قلة الخبرة الفنية وقلة التدريب على التعامل مع الأدلة الرقمية، وكيفية البحث عنها، وكيفية الحصول على هذا الدليل، كما أن خبرة التحقيق مع مجرم ذكي له طبيعة خاصة، سيما وانهذا المجرم يراوغ ويحاول التهرب من جرمه، ربما بإغراق المحقق في تفاصيل لا يعلمها جيدا، حيث ان المحقق الجنائي في جرائم الابتزاز الإلكتروني يجب أن يكون له تكوين تقني ، فيجب ان يجمع بين مهارة استخدام التقنية الحديثة وكذلك مهارة تقييم الجريمة الإلكترونية ومدى الخطورة الاجرامية لمرتكبها، وكذا مهارة التعرف على المكونات المادية للأجهزة وعلى ملحقاتها من طابعات وماسحات ضوئية وكاميرات، وذلك للتأكد من ارتباطها بالجهاز الأصلي من عدمه، وتقييم الوسائط الخاصة بتخزين الأدلة الرقمية لتحديد مدى ارتباطها بالإنترنت وما إذا كانت جزء من أدوات الجريمة من عدمه[1] .

فقد تكون شخصية المحقق تميل الى التهيب من استخدام الكمبيوتر و التهيب من استخدام الإنترنت ، و عدم الخبرة الكافية و عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية ، وهي كلها صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم ، كذلك عدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية و كذا قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية .[2]

كذلك أجهزة العدالة المقاومة لهذه الجرائم المرتبطة بالتقنية يبدأ بالتكوين والتشكيل عقب ظهور هذه الجرائم و هو أمر يستغرق الوقت فعدم توازي سرعة تقدم التقنية ذاتها و الحركة التشريعية، أو الثقافة القانونية أو الأمنية،حيث لا تسيران بذات المعدل مما يعكس سلبا على إجراءات الاستدلالات، و التحقيقات في الدعوى الجنائية مما يستدعي ضرورة تأهيل سلطات الأمن و جهات التحقيق و الادعاء و الحكم في شأن هذه الجرائم.

[1] عماد جواد موسى ، المرجع السابق ، ص 245

[2] خالد عياد الحلبي، المرجع السابق، ص224

الفرع الثاني: صعوبات متعلقة بالجانب القضائي:

يفترض الطابع الخاص لهذا النوع من الجرائم تعاون أكثر من دولة لكن هذا القصور مقارنة بتفاقموتطور هذه الجريمة يشكل فارق شاسع بين الجريمة،وبطء الإجراءات.

وقد نجم عن هذه الإشكالية أيضا صعوبات تتمثل في القانون الواجب التطبيق، و المحكمة المختصة (تنازع الاختصاص) حيث ترى كل دولة أن لها الحق في ملاحقة، و متابعة مرتكب هذه الجريمة لعدة اعتبارات:

أولا: قصور التعاون القضائي الدولي في مكافحة جريمة الابتزاز الإلكتروني:

يعتبر التعاون الدولي في مجال مكافحة الجريمة الإلكترونية عموما و جريمة الابتزاز الإلكتروني من أصعب المواضيع المطروحة على هذا المستوى بسبب الاختلافات القائمة في الممارسات بين الدول و التشريعات، و كذلك سبب العدد المحدود نسبيا من المعاهدات و الاتفاقيات المتاحة للدول بشأن التعاون الدولي الذي يعد مطلبا تسعى لتحقيقه كل دولة ، إلا أنه له معوقات تقف دون تحقيقه .

ثانيا: عدم وجود نموذج موحد للنشاط الإجرامي:

نظرا لاختلاف المفاهيم الخاصة بالجريمة واختلاف التقاليد والأعراف القانونية الدولية فإن ذلك يضعف منظومة القانون الدولي في مجال ضبط تلك الجرائم، و يسهل إفلات الجناة من المسائلة الجنائية و ذلك بسبب عدم توفر تعريف موحد للجريمة فتكون مجرمة في تشريع و مباحة في تشريع آخر.[1]

فالطبيعة الدولية لهذه الجريمة تثير إشكالية تحديد القانون الواجب التطبيق هل هو قانون الدولة التي ارتكب فيها الفعل أم قانون الدولة التي ظهرت فيها الآثار الضارة .

[1] صغيريوسف، المرجعالسابق، ص133.

كذلك تعارض القوانين من الناحية الموضوعية والإجرائية يتطلب العمل على توحيد التشريعات المتعلقة بمكافحة هذا النوع من الجرائم إضافة الى إبرام اتفاقيات في هذا المجال.[1]

ثالثا: تنوع واختلاف النظم القانونية الإجرائية:

إن اختلاف النظم القانونية الإجرائية والتحقيق والمحاكمة قد تثبت فاعليتها في دولة ما وقد تكون عديمة الفائدة في دولة اخرى وقد لا يسمح بإجرائها كما هو الشأن بالنسبة للمراقبة الإلكترونية وتسليمالمراقب،وغيرها من الإجراءات.

رابعا:عدم وجود قنوات اتصال

إن عدم الاتصال بين الدول لجمع الأدلة والمعلومات يعيق التعاون الدولي في مجال مكافحة الجريمة، فعدم التعاون والتنسيق بين الدول فيما يخص الإجراءات وجمعالاستدلالاتوالتحقيق،وأن الحصول على دليل في هذه الجريمة قد يكون خارج نطاق الدولة هو أمر غاية في الصعوبة.[2]

خامسا: تنازع الاختصاص

من المعلوم أن الشبكة العنكبوتية لا تستأثر بها دولة معينة ويتسنى لمستخدميها ولوجها من أي مكان في العالم من خلال جهاز حاسب آلي يكون متصلا بها، فهي بطبيعتها لا تحدها حدود وهي خارجة عن أي رقابة أو سيطرة من أية جهة وبالتالي عدم خضوعها لأي سلطة قانون جنائي معين، وعملا بمبدأ إقليمية القوانين فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها على إقليمها بصرف النظر عن جنسية مرتكب الجريمة .

[1] رابحيعزيزة ، المرجعالسابق، ص329.
[2] صغير يوسف ، المرجع السابق ، ص135

ولما كانت الجريمة الإلكترونية ذات طبيعة خاصة وتتميز بخصوصيات متعددة، منها أنها جريمة عابرة للحدود خلافا للجرائم التقليدية، الأمر الذي يجعلها في كثير من الأحيان تستعصي الخضوع للقوالب التي تحكم مسألة الاختصاص المكاني، إلا أن الاتجاه الغالب اليوم لحل مشكلة الاختصاص القضائي في العالم الافتِّراضي، هو تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي الدولي في الجرائم التقليدية، وعلى رأسها مبدأ إقليمية القوانين ،أي تطبيق القانون الجزائي على جميع الجرائم التي ترتكب في إقليم الدولة أيا كانت جنسية مرتكب الجريمة.

أما فيما يخص موقف المشرع الجزائري من مسألة الاختصاص القضائي المحلي، فقد حدد المشرع الجزائري معايير الاختصاص المحلي للجرائم المعلوماتية في قانون الإجراءات الجزائية في المواد 37،329،40، ونجد بأنه تخطى مشكلة امتداد التفتيش خارج الإقليم الوطني بموجب ما رسمه القانون.

لكن مشكلة الاختصاص القضائي وملائمة القانون الواجب التطبيق تظل قائمة في مجال الجرائم المعلوماتية ، حتى وان بادر المشرع الجزائري بتعديل قانون الإجراءات الجزائرية بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، حيث عدل المادة329 من قانون الإجراءات الجزائية وذلك بجواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة...." وقد جاء عقب ذلك المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ليجسد فعليا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات....."[1]

[1] مريم اعراب، مقال بعنوان جريمة التهديد والابتزاز الالكتروني ، مجلة الدراسات القانونية المقارنة ، العدد 7 ، كلية الحقوق والعلوم السياسية جامعة وهران 1 محمد بن احمد ، تاريخ النشر 2021/11/22 ، الجزائر

ينجم عن اختلاف التشريعات والنظم القانونية تنازع في الاختصاص بين الدول فقد يحدث أن ترتكب هذه الجريمة في إقليم دولة من طرف أجنبي فهنا تكون هذه الجريمة خاضعة للاختصاص الإقليمي للدولة الأولى طبقا لمبدأ الإقليمية وتخضع للاختصاص للدولة الثانية على أساس مبدأ الاختصاص الشخصي وقد تهدد أمن وسلامة دولة أخرى فتدخل في اختصاصها استنادا لمبدأ العينية .

سادسا: التجريم المزدوج :

يجد شرط التسليم المزدوج أساسه في أن الدولة المطالبة بتسليم ومتابعة من نسب إليه السلوك الإجرامي أو تنفيذ العقوبة عليه لابد أن يكون السلوك مجرما في تشريعها و إلا فلا يتصور وجود دعوى عمومية أو ملاحقة جزائية أو تنفيذ عقوبة جزائية و منه لا يمكن مطالبة الدولة المطلوب إليها التسليم إيقاع عقوبة على ارتكاب سلوك هو في الأساس غير مجرم وفقا لقانونها و ذلك راجع لعدم وجود معاهدات ثنائية للتعاون في هذا المجال.[1]

سابعا:صعوبات الإنابة القضائية الدولية:

وبموجبها يعهد للسلطات القضائية المطلوب منها اتخاذ إجراء القيام بالتحقيق لمصلحة السلطة القضائية المختصة في الدولة الطالبة مع احترام حقوق و حريات الإنسان المعترف بها عالميا و مقابل ذلك تتعهد الدولة الطالبة للمساعدة بالمعاملة بالمثل واحترام النتائج القانونية المتوصل إليها من طرفالدولة المطلوب منها المساعدة القانونية ، وتتسم أعمال الإنابة القضائية بالبطء والتعقيد مما يتعارض مع سرعة الجريمة.

[1] آمال برحال ، المرجع السابق ، ص84 .

المبحث الثاني: الإثبات في جريمة الابتزاز الإلكتروني:

الإثبات هو كل ما يؤدي إلى كشف الحقيقة أما في معناه القانوني هو كل ما يؤدي إلى كشف الحقيقة وإقامة الدليل على وجود قاعدة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون، ويعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ،ويزداد صعوبة في الجريمة الإلكترونية بصفة عامة، لأن اكتشاف الجريمة الإلكترونية بصفة عامة وجريمة الابتزاز الإلكتروني ليس بالسهل، بل وحتى عند اكتشاف الجريمة و الإبلاغ عنها يتبقى عبء الإثبات به الكثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية، لأنها تقع في إطار غير ملموس، لأن أركانها تقوم بين بيئة حاسب آلي أو جهاز الكتروني تقني واستخدام الانترنت وسيلة أخرى، مما يزيد من الصعوبات التي تواجه رجال الضبط الجنائي والقضائي لأن العمل في هذه البيئة تكون فيها البيانات والمعلومات عبارة عن نبضات إلكترونية، ترسل عبر نظام الكتروني.[1]

كما أن وسائل الإثبات التقليدية لا تفلح دائما في إثبات مثل هذا النوع من الجرائم نظرا لاختلافها بطبيعتها الخاصة عن الجريمة التقليدية ولاختلاف العناصر المادية التي تقوم عليها الجريمة الإلكترونية.

كان من الضروري تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام الإلكتروني، وأصبح متطلبا من أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي خاصة مسألة حجية الدليل الإلكتروني.[2]

---

[1] ثنيان ناصر الثنيان ،**إثبات الجريمة الإلكترونية؛ دارسة تأصيلية تطبيقية**، رسالة ماجستير، جامعة نايف للعلوم الأمنية، كلية الد ارسات العليا، السعودية ،2012. ص 214

[2] فيصل بن زحاف ، **مقال قانوني بعنوان الحماية الجنائية للحكومة الإلكتروني، مجلة القانون المجتمع والسلطة**، العدد رقم 032014، ص82.

وبالتالي يمكن تقسيم هذا المبحث الى مطلبين، الأول يتناول ماهية الدليل الجنائي الرقمي في جريمة الابتزاز الإلكتروني، والثاني يتناول صعوبات الإثبات في جريمة الابتزاز الإلكتروني.

المطلب الأول: ماهية الدليل الجنائي الرقمي:

للتعرض الى ماهية الدليل الجنائي الرقمي لابد من توضيح مفهومه وذلك من خلال تعريفه وتبيان خصائصه، كذلك شروط صحة الدليل الرقمي، ومصادر الحصول عليه لذا سيتم تخصيص الفرع الأول لمفهوم الدليل الجنائي الرقمي أما الفرع الثاني سيتم التطرق فيه الى شروط صحة الدليل الرقمي ومصادر الحصول عليه.

الفرع الأول: مفهوم الدليل الجنائي الرقمي:

يشمل مفهوم الدليل الرقمي على عدة عناصر لابد من ذكرها ، و حتى يتضح هذا المفهوم سنتناول تعريف الدليل الرقمي ثم خصائصه.

أولا: تعريف الدليل الرقمي:

هناك عدة تعريفات للدليل الرقمي، تباينت بين التوسع والتضيق نذكر منها:

_ هو" أية بيانات مخزنة أو منقولة بواسطة الحاسوب؛ تدعم أية نظرية حول كيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة .

ويعرف كذلك على أنه "الدليل المأخوذ من أجهزة الكمبيوتر، و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تحميلها .[1]

[1] ممدوح عبدالحميد بن عبدالمطلب ، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية ، مصر، 2003 ، ص22 .

وتحليله يتم باستخدام برامج تطبيقات و تكنولوجيات ، و هو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة، أو الصور، أو الأصوات ،أو الأشكال و الرسوم ، و ذلك من أجل اعتماده أمام أجهزة التحقيق .[1]

و قد عرفه البعض الأخر على أنه مجموعة من البيانات أو المعلومات التي تمكن من أن تثبت أن جريمة ما وقعت أو وجود صلة بين الجريمة و الجاني أو علاقة بين الجريمة و المجني عليه.[2]

فالدليل الرقمي هو الدليل المشتق من أو بواسطة البرمجية والمعلوماتية وأجهزة ومعدات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية و فنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة ، أو رسومات، أو صور، أو أصوات ، لإثبات وقوع الجريمة ، أو لتقرير البراءة أو الإدانة.[3]

ويحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي كوسيلة لإثبات الابتزاز الإلكتروني ، فيتطلب إجراء خطوات جمع الأدلة.

ثانيا: خصائص الدليل الرقمي:

الدليل الرقمي الجنائي له عدة خصائص تميزه عن غيره من الأدلة الجنائية التقليدية، و هذا ما سيتم توضيحه من خلال العناصر الأتية:

---

[1] ممدوح عبد الحميد بن عبدالمطلب ، المرجع السابق ، ص77.

[2] محمدالأمينالبشري ، التحقيقفيالجرائمالمستحدثة ، جامعة نايف العربية للعلوم الامنية ، السعودية ، ط1 ،2004 ، ص 234.

[3] ثنيان ناصر آلثنيان، المرجع السابق ، ص74.

أ:دليل علمي: فهو يتميز بالطبيعة الفنية، حيث يتكون من البيانات والمعلومات ذات صفة الكترونية غير ملموسة، ولا تدرك بالحواس العادية.[1]

ب:دليل قابل للنسخ

تحتاج التكنولوجيا المعلوماتية في استخراج نسخ من الأدلة الرقمية الى محقق جنائي وفني متخصص لديه المهارة الفنية والتقنية الكافية لاستخلاص وجمع الأدلة الرقمية لأن الفصل في دعاوي الجرائم الإلكترونية بصفة عامة وجريمة الابتزاز الإلكتروني بصفة خاصة يتوقف على الرأي الفني الذي يثبت أو ينفي قيام الجريمة من قبل المشتبه به. [2]

ج: إمكانية استرجاع الأدلة الرقمية:

وتعتبر من أهم الخصائص التي تميز الأدلة الالكترونية الرقمية مقارنة بالدليل التقليدي بحيث أن الأدلة الالكترونية الرقمية يمكن استرجاعها بعد محوها و إصلاحها بعد إتلافها ، مما يؤدي الى صعوبة التخلص منها ، فهناك الكثير من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن و العدالة طالما وصل الى علم رجال البحث و التحقيق الجنائي بوقوع الجريمة، و الأكثر من ذلك فان محاولة الجاني محو الدليل الإلكتروني بذاتها تسجل عليه كدليل، و أن قيامه بذلك يتم تسجيله في ذاكرة الآلة و هو ما يمكن استخراج نسخ منه لها نفس الحجية و القوة الثبوتية، الأمر الذي لا يتوافر في أنواع الأدلة التقليدية الأخرى مما يشكل ضمانة فعالة ضد الفقد و التلف.

د: الدليل الجنائي الرقمي متنوع و متطور:

---

[1] آمال برحال ، المرجع السابق ، ص 89 .

[2] ثنيان ناصرآل ثنيان ، المرجعالسابق، ص 24.

إن الدليل الرقمي يشمل جميع البيانات الرقمية التي يمكن تداولها رقميا، سواء كانت هذه الأدلة متعلقة بالحاسب الآلي أو غيرها من الأجهزة، أو شبكة الأنترنت، أو شبكات الاتصال السلكية أو اللاسلكية، و منه فالآثار الرقمية المستخلصة متنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة، فتصبح أدلة براءة أو إدانة، و من بينها صفحات المواقع الالكترونية ، الصور، الفيديوهات الرقمية ، والملفات المخزنة في الحاسب الآلي الشخصي أو المعلومات المتعلقة بمستخدم شبكة الأنترنت و غيرها.

فهذا التنوع يدل على اتساع قاعدة الدليل الجنائي الرقمي الذي يمكن أن يكون دليل براءة أو إدانة.[1]

أما خاصية التطور فهي ناتجة عن تزايد استعمال تقنية المعلومات الرقمية، لتلبية احتياجات المستخدمين الأمر الذي أدى الى ظهور أنواع جديدة من الأدلة.

الفرع الثاني: شروط صحة الدليل الرقمي ومصادر الحصول عليه

أولا: شروط صحة الدليل الرقمي:

هناك شروط في الدليل الرقمي لقبوله كأساس تقوم عليه الحقيقة في الدعاوى الجنائية وهذه الشروط تتمثل في النقاط التالية: لابد أن يكون الدليل الرقمي غير قابل للشك، يجب الحصول على هذا الدليل بصورة مشروعة، كما يجب أن يكون الدليل قابلا للمناقشة، وهذا ما سنستعرضه في الآتي:

: يجب أن يكون الدليل الرقمي غير قابل للشك:

الدليل الرقمي لابد أن يكون يقيني، ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي الى يقين، حيث يصل إليه القاضي بعد عرض الأدلة الرقمية، فمن خلال ما يعرض عليه من

[1] رابحي عزيزة، المرجع السابق، ص270.

مخرجات الكترونية، وما ينطبع في ذهنه من تصورات و احتمالات بالنسبة لها، سيحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية الى شخص معين من عدمه.[1]

ب: يجب أن يكون الدليل الرقمي متحصل عليه بصورة مشروعة: ينبغي على القاضي أن يستقي قناعته في الحكم من خلال أدلة مشروعة ، أما الأدلة التي جاءت ناتجة عن إجراءات غير قانونية ، فلا يجوز الاعتماد عليها، كما يجب استبعاد كل دليل معيب حتى وان استندت في إصدارها الى أدلة أخرى مشروعة إلى جانب الدليل الباطل والمعيب.

وعليه فالمشروعية هي التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام فهي تهدف الى تقرير ضمانة أساسية لحماية الحقوق و الحريات الشخصية ضد تعسف السلطة و التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي و تحقيق حماية مماثلة للفرد.[2]

ج: يجب أن يكون الدليل الرقمي قابلا للمناقشة:

فلا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة اليه في معرض المرافعات والتي حصلت المناقشة فيها وجاهيا علنيا حضوريا من قبل أطراف الدعوى.[3]

فالأدلة المتحصلة من جرائم الحاسب الآلي والانترنت ، ستكون محلا للمناقشة عند الأخذ بها كوسيلة اثبات أمام المحكمة فيجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي،لكن بصفة مباشرة أمام القاضي الجزائي.[4]

ثانيا: مصادر الحصول على الدليل الرقمي:

---

[1] ممدوح عبد الحميد بن عبد المطلب، المرجع السابق، ص 125

[2] رابحي عزيزة، المرجع السابق، ص 255

[3] أنظر المادة 212 ق.إ.ج. ج المعدل و المتمم.

[4] رابحيعزيزة ، المرجعنفسه ، ص296.

يستوجب أن تعتمد جهات التحري و التحقيق على مصادر لتحصيل الدليل الرقمي من بين المصادر التي يسمح بها القانون، و المتمثلة في: إجراء الإرشاد الجنائي و إجراء الوضع تحت المراقبة الالكترونية و تعاون مقدمي خدمات الانترنت مع السلطات القضائية.

أ:إجراء الإرشاد الجنائي:

الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها للولوج للعالم الافتراضي وبالأخص عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستعملين صفات وهمية من أجل الكشف عن هذه الجرائم وكشف المجرمين.

فهذا الإجراء لا يتطلب جهد مادي كبير، حيث يقوم به ضباط الشرطة القضائية أو يكلف غيره من ذوي الاختصاص وهذا بعد الحصول على إذن رسمي للقيام بمهام البحث والتحري عن الجرائم وضبط مرتكبيها.

وقد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت اسم التسرب من خلال نصوص المواد 65 مكرر 05 الى غاية المادة 65 مكرر 18ق.إ.ج. ج بعد الحصول على اذن مسبب من وكيل الجمهورية أو قاضي التحقيق تحت رقابة وكيل الجمهورية لمدة 04 أشهر قابلة للتجديد.[1]

ب:إجراء الوضع تحت المراقبة الالكترونية:

وهي من أهم مصادر البحث و التحري سواء في الجرائم التقليدية أو المستحدثة، و يقصد بها مراقبة شبكة الجرائم المعلوماتية (Cyber surveillance) ، و تسمى بالمراقبة الالكترونية ، فهي العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع البيانات و المعلومات عن المشتبه فيه من أجل تحقيق غرض أمني أو أي غرض آخر و هي مرتبطة بالزمن. وقد أجاز المشرع الجزائري المراقبة الالكترونية في الجرائم

[1]أنظر المواد 65 مكرر 05 الى غاية المادة 65 مكرر 18من ق إج المعدل و المتمم.

المعلوماتية عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الاتصال السلكية و اللاسلكية ، كما أجاز كل الترتيبات التقنية لها دون علم المعنيين و لا موافقتهم، بغية الحصول على تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة ، وذلك بإذن من وكيل الجمهورية. [1]

ج:تعاون مقدمي خدمات الانترنت مع السلطات القضائية

يقصد بمزود الخدمة كل شخص يقدم خدمة الى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بعقد من العقود، وقد عرف المشرع الجزائري مقدم الخدمة بموجب المادة 02 في القانون 04/09 بأنه:

أي كيان عام أو خاص له القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات ، أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.[2]

ونظرا لضلوع الشبكة المعلوماتية في أغلب جرائم العالم الافتراضي، فإن المشرع الجزائري قد فرض على مقدمي خدمات الانترنت مجموعة من الالتزامات من أجل مساعدة السلطات القضائية في أعمال التحقيق وذلك من خلال القانون رقم 09/04 في فصله الرابع تحت عنوان "التزامات مقدمي الخدمات " ومن بين الالتزامات الواردة نجد: الالتزام بمساعدة السلطات والالتزام بحفظ المعطيات المتعلقة بحركة السير.

المطلب الثاني: صعوبات الإثبات في جريمة الابتزاز الإلكتروني

نظرا لكون هذه الجريمة تتم في الخفاء ومن يرتكبها يتصف بمعرفة التقنية والذكاء، وبالرغم من الجهود المبذولة لمكافحة الجريمة الالكترونية وجريمة الابتزاز الإلكتروني بوجه خاص، إلا أنه هناك بعض المعوقات

[1] آمال برحال ، المرجع السابق ، ص 93.
[2] أنظر المادة 2 من القانون09 -04

والصعوبات التي تواجه السلطات المختصة في الإثبات بالدليل الرقمي وذلك لعدة أسباب أهمها: معوقات مرتبطة بالدليل ذاته وكذا معوقات مرتبطة بصعوبة التعاون الدولي.

الفرع الأول: المعوقات المرتبطة بالدليل ذاته:

1/ سهولة محو الدليل :

حرص الجاني الإلكتروني في جرائم الابتزاز الإلكتروني على محو أي آثار للابتزاز بعد القيام بتهديد المجني عليه مما يصعب الوصول إلى الدليل، وفي بعض الأحيان يكون مستحيلا.[1]

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

تختلف جريمة الابتزازاز الإلكتروني عن جرائم التقليدية لأنها تحدث في عالم الكتروني افتراضي تحكمه الرموز والبيانات ويخلو من العنف الظاهر والآثار المادية كالجريمة التقليدية مما يصعب عمل الوصول لدليل مادي كبصمات الأصبع أو نقاط الدم مما يجعل الوصول للجاني معترض بالعقبات.[2]

3/ عرقلة الوصول للدليل :

قد يضع الجاني عقبات فنية لمنع كشف جريمته من خلال أدلتها وذلك بتشفير الملفات الرقمية قصد حجب المعلومات عن التداول ومنع الوصول الى مصدر الإرسال.

4/ صعوبات متعلقة بنقص الخبرة :

نقص الخبرة لبعض العاملين في جهات التحقيق ومن رجال الضبط القضائي ورجال النيابة العامة فيما يخص مهارة استخدام أجهزة الحاسب الآلي وملحقاتها ومهارات الاستجواب للمجرم

[1] نهلا عبد القادر المومني، المرجع السابق، ص54.

[2] غنية باطلي، الجريمة الالكترونية دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، ط1 ،الجزائر ، 2016،ص45.

الالكتروني في جرائم الابتزاز الإلكتروني مما يؤثر على عملية التحقيق برمتها من حيث ضبط الأدلة

وحمايتها والحفاظ عليها حتى لا يتم إتلافها وضياعها، مثل إتلاف القرص الصلب والأقراص الممغنطة أو أوعية المعلومات التي تخزن فيها البيانات.وهي من بين الصعوبات التي تواجه عملية الحصول على دليل رقمي في جريمة الابتزاز الالكتروني، لذا من الضروري جدا الاهتمام وتطوير وتأهيل العنصر البشري من محققين ورجال الضبط القضائي لمواكبة مثل هذا النوع من الجرائم و يتطلب أيضا متابعة العنصر البشري للأمور التقنية و كل مستجد على الساحة .[1]

5/ صعوبات متعلقة في إحجام المجني عليه على الإبلاغ :

ان خوف المجني عليه من الإبلاغ كي لا يفتضح أمره سبب رئيسي في تشكيل الصعوبة التي تواجه رجال الضبط القضائي والمحققين في هذا النوع من الجرائم، وبالتالي فإن هذا الأحجام يساعد على اختفاء الدليل الرقمي الذي يدل على الجاني ويكون هذا سبب في تكوين عقبة تقف كحجر عثرة في طريق الإثبات عن طريق الدليل الرقمي.

الفرع الثاني: صعوبة التعاون الدولي

حيث أن اختلاف تشريعات الدول في تجريم أفعال الابتزاز الإلكتروني بصفة عامة مختلفة من دولة لأخرى، وهذا مما يزيد العراقيل في ملاحقة الجناة، ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية إلا أن هناك عوائق تحول دون تحقيق ذلك، ومن هذه العوائق:

1/: عدم وجود نموذج موحد للنشاط الإجرامي واختلاف النظم القانونية الإجرائية :

[1] آمال برحال ، المرجع السابق ، ص 95.

حيث أنه لا يوجد اتفاق مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات، زيادة على الاختلاف في تجريم الابتزاز الإلكتروني من دولة لأخرى، مما يجعل ملاحقة الجاني تمر بعقبات وعراقيل فما تراه دولة مباح لا يعاقب عليه القانون تراه دولة أخرى فعل مجرم. ويظهر هذا الاختلاف في طرق التحقيق والتحري والمحاكمة التي تثبت فائدتها في دولة ما بينما تكون عديمة الفائدة في دولة أخرى أو لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية وغيرها، حتى إن تم الحصول عليه في اختصاص قضائي وبشكل مشروع. .[1]

2/: مشكلة الاختصاص في جريمة الابتزاز الالكتروني:

ما يعرقل الوصول إلى الجريمة الإلكترونية هو عيب الإختصاص في المستوى المحلي والدولي بسبب تداخل وترابط شبكة المعلومات فقد يكون مكان نشأة الجريمة في دولة والجاني في دولة ثانية والمجني عليه في دولة ثالثة والدليل الرقمي يتبع نظام دولة أخرى في مكانما، ومن هنا تنشأ مشكلة البحث على الدليل الرقمي على شبكة الإنترنت، مما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول.

حيث ينعقد الاختصاص القضائي المكاني أو المحلي للمحاكم الجزائية من خلال القاعدة الثلاثية،حيث يرجع الإختصاص إما لمحكمة ارتكاب الجريمة، أو محكمة إلقاء القبض على المجرم،أو أحد مشاركيه أو محكمة موطن إقامة المجرم، فالإختصاص هو مباشرة المحكمة ولايتها القضائية في نظر الدعوى في الحدود التي رسمها القانون. [2]

[1] بوشعير الحسن و حداد شعيب ، المرجع نفسه ص 100.

[2] وائل سليم عبد الله شاطر ،نفس المرجع، ص 444.

فتطبيق القواعد التقليدية التي تحدد معايير الاختصاص لا يتلاءم مع طبيعة الجريمة الإلكترونية العابرة للحدود ، حيث يصعب تحديد مكان وقوع الفعل المجرم في هذه الجرائم، لأن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة تتطلب تجاوز المعايير التقليدية التي لا تتلاءم مع تحديد محل وقوع الجريمة في العالم الافتراضي، لأن هذه الجرائم لا تعترف بالحدود الجغرافية و السياسية للدول و لا سيادتها ، فهي جرائم عابرة للحدود تتم في فضاء الكتروني معقد عبارة عن شبكة اتصالات لامتناهية غير مجسدة ، و غير مرئية متاحة لأي شخص في العالم ، و غير تابعة لأي سلطة حكومية.

فقواعد الاختصاص القضائي المنصوص عليها في قانون الإجراءات الجزائية صيغت كي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني ولا يمكن إعمالها بشأن الجريمة الإلكترونية.

وهذا ما يجعل التعاون الدولي لضمان الفعالية بمحاربة هذه الجرائم حتمية لا ينبغي غض الطرف عنها، فلابد من توحيد التشريعات أو على الأقل تقليص الفوارق بينها لتعزيز هذه الآليات كي لا يفلت المجرمون من المتابعة الجزائية.[1]

وهو ما قام به المشرع الجزائري عندما عالج مشكلة امتداد التفتيش خارج الدولة الجزائرية بموجب ما أرساه القانون 09-04، أيضا عندما توصل الى حل إشكالات الاختصاص بالنسبة لبعض الجرائم و منها الجرائم الخاصة بالأنظمة المعلوماتية حيث تم تمديد الاختصاص ليشمل اختصاص محاكم أخرى عن طريق التنظيم، مثلما هو الأمر بالنسبة للمشرع الجزائري حينما عدل نص المادة 329 من قانون الإجراءات الجزائية و أيضا تم تمديد الاختصاص الإقليمي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق ليتجسد فعليا موجب المرسوم التنفيذي رقم 06-348 المؤرخ في 05/10/2006 المتضمن تمديد الاختصاص

[1] صغير يوسف، المرجع السابق، ص133.

المحلي لبعض وكلاء الجمهورية ، و قضاة التحقيق الذي أنشأ الجهات القضائية ذات الاختصاص الموسع أو (الأقطاب القضائية).

وقد عدل هذا الأخير بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 حيث تم تعديل هذا الاختصاص الموسع.

3/: الصعوبات الخاصة بالمساعدات القضائية الدولية وتدريب الكوادر:

تتعدد الصعوبات الخاصة بالمساعدات القضائية الدولية وتدريب الكوادر وتشمل ما يلي:

أ:الصعوبات الخاصة بالمساعدات القضائية الدولية:

تعتبرالانابة الدولية من أهم صور المساعدات القضائية الدولية في المجال الجنائي التي تتم عن طريق الطرق الدبلوماسية التي تتسم بالبطء مما لا يتناسب مع طبيعة جرائم الانترنت التي تتسم بالسرعة.

ب:الصعوبات الخاصة بالتعاون الدولي في مجال التدريب:

تتمثل هذه الصعوبات في الفوارق الفردية بين المتدربين و تأثيرها في عملية اكتساب المهارات بطريقة متكافئة لدى المتدربين ، وتأثيرها في عملية اكتساب المهارات المطلوبة سيما في مجال التكنولوجيا الرقمية. [1]

ملخص الفصل الثاني:

تم التطرق في هذا الفصل للإطار الإجرائي لجريمة الابتزاز الالكتروني و ذلك من خلال تسليط الضوء على إجراءات التحقيق العامة والخاصة وكذا الإشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية التحقيق من خلال التطرق إلى صعوبات اكتشاف الجريمة والصعوبات المتعلقة بالجانب القضائي وإشكالية القانون الواجب التطبيق و المحكمة المختصة بالجريمة و كذا الإجراءات المرتبطة بالإثبات في الجريمة موضوع الدراسة والتي تعرضنا فيها إلى خصوصية هذه الإجراءات كما تعرضنا لأهم وسائل الإثبات التي

[1] رابحي عزيزة، المرجع السابق، ص319

تخص هذه الجريمة و هو الدليل الرقمي وذلك من خلال التطرق إلى مفهومه وشروط صحته وكذا صعوبات الإثبات المرتبطة بالدليل الرقمي في حد ذاته و كذا صعوبات التعاون الدولي والمتمثلة في صعوبات عدم وجود نموذج دولي موحد للنشاط الإجرامي مما يخلق مشكلة في الاختصاص القضائي و الصعوبات المتعلقة بالمساعدات القضائية وتدريب الكوادر .

خاتمة

جريمة الابتزاز هي إحدى صور الجريمة الإلكترونية وهي من الجرائم المستحدثة غير التقليدية، ويطلق عليها في علم الجريمة الجرائم الناعمة التي تخلو من العنف، وجريمة الابتزاز الالكتروني تنشأ في عالم افتراضي مليء بالرموز والشيفرات ويزداد التحدي حين نجد العقبات والصعوبات التي تواجه أجهزة التحقيق في التعامل مع الدليل الرقمي.

وبعد التطور السريع للتكنولوجيا الرقمية أصبحت تشكل هوسا لدى مستخدمي التكنولوجيا الحديثة، وأمام هذه الثورة حاولت الدول تطوير تشريعاتها لتواكب هذا النوع من الجرائم المستحدثة، ثم تنبهت لضرورة إفراد نصوص تشريعية خاصة بهذه الجريمة الالكترونية.

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

النتائـج:

1.لم يتفق الفقهاء عل تعريف جامع لجريمة الابتزاز الالكتروني

2.إن أساس ارتكاب الجريمة هو استخدام التكنولوجيا الحديثة المتمثلة في شبكة الانترنت ومواقع التواصل الاجتماعي وهو الواقع الافتراضي لمسرح الجريمة.

3.لجريمة الابتزاز الإلكتروني وسائل وطرق مختلفة في ارتكابها تختلف عن الابتزاز التقليدي ، كالهواتف النقالة المزودة بآلة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، وذلك بالتقاط الصور أو نشر أخبار أو تسجيلات صوتية، أو مرئية تتصل بها و لو كانت صحيحة.

4.سهولة ارتكابها من قبل الجاني كونها لا تتطلب جهد عضلي او الانتقال الى مكان الحادث.

5.تتحقق جريمة الابتزاز باستخدام الجاني سلوكا واحدا أو متعددا ، إذ لا عبرة بالطريقة التي لجأ اليها الجاني لتهديد المجني عليه، فقد تتم عن طريق البريد الإلكتروني أو غرف المحادثة ، أو المنتديات أو أي طريقة أخرى تهدف لحمل المجني عليه على إحداث نتيجة معينة تتمثل في القيام بفعل أو الامتناع عنه.

6.جريمة الابتزاز إلكتروني قد تتسبب في جرائم بعدها، كالزنا أو القتل أو جريمة عنف أو سرقة.

7.جريمة الإبتزاز الإلكتروني جريمة عابرة للحدود، فقد يكون المبتز في دولة و الضحية في دولة أخرى.

8.جريمة الإبتزاز الإلكتروني لها خصوصية في التحقيق و تستلزم فريق عمل من المختصين أو المؤهلين لاستيعاب التطورات الحديثة في التحقيق مع مجرم ذكي له صفات تختلف عن صفات المجرم التقليدي.

9.الدليل الرقمي أهم أدلة الاثبات في جريمة الإبتزاز الإلكتروني إلا أن التعامل معه يحتاج إلى خبرات معينة و أجهزة متخصصة و فريق عمل متكامل الخبرة.

10.وجود فجوة تشريعية بين تشريعات العالم في تجريم الإبتزاز الإلكتروني مما سهل التهرب من المتابعة و العقاب خاصة الدول التي لم تفرد نصوص خاصة تجرم هذا السلوك على غرار المشرع الجزائري والعراقي.

المقترحات:

•ان التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانونية خاصة فيما يتعلق بجريمة الابتزاز الالكتروني.

•إصدار قانون خاص يجرم الإبتزاز الإلكتروني في الدول التي لا يوجد في تشريعها نص ليكون الردع بشقيه العام والخاص ذا فاعلية أكبر.

•لابد من تعاون كل مؤسسات التعليم و التعليم العالي، و دور العبادة لإقامة دراسات وندوات حول مخاطر هذه الجريمة الدخيلة على المجتمعات العربية و الإسلامية .

•أن يعين أخصائيين نفسانيين واجتماعيين تكون مهمتهم التواصل مع كل من تعرض الإبتزاز مهما كان جنس وسن الضحية.

•عقد دورات مكثفة لتدريب وتأهيل العاملين بجهات التحقيق والجهات القضائية، بكل أساليب التحقيق الحديثة، والتعامل مع الدليل الرقمي حتى لا تفلت الجرائم من بين يدي رجال التحقيق بسبب قلة الخبرة في التعامل مع الدليل الرقمي.

•زيادة التعاون الدولي، وذلك بوضع آلية موحدة تجرم الإبتزاز الالكتروني كي لا يفلت المجرم من العقاب نتيجة تساهل بعض الأنظمة وتشدد أخرى.

قائمة المراجع

Les références

قائمة المصادر و المراجع :

المصادر :

دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 7 ديسمبر 1996، الجريدة الرسمية رقم 76 المؤرخ في 8 ديسمبر 1996، المعدل

المراجع :

القوانين:

- قانون رقم 06-22 مؤرخ في 29 ذي القعدة 1427 الموافق لـ 20 ديسمبر 2006 يعدل ويتمم قانون الإجراءات الجزائية.
- قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427هـ الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 156-66 المؤرخ في 18 صفر عام 1386، الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات الجريدة الرسمية، العدد 87، الصادرة بتاريخ 04 ذي الحجة عام 1427هـ الموافق 24 ديسمبر سنة 2006.
- القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الكتب:

- بن زيطة عبد الهادي. حماية برامج الحاسوب في التشريع الجزائري. دار الخلدونية للنشر والتوزيع، ط1.
- جمال ابراهيم الحيدري. الجرائم الالكترونية وسبل معالجتها. مكتبة السنهوري، ط1، العراق، 2012.
- خالد عياد الحلبي. إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت. ط1، دار الثقافة للنشر والتوزيع، دبي، 2011.

- غنية باطلي. الجريمة الإلكترونية دراسة مقارنة. الدار الجزائرية للنشر والتوزيع، ط1، الجزائر، 2016.
- عبد الرحمن توفيق أحمد. شرح قانون العقوبات، القسم العام وفق أحدث التعديلات. ط3، دار الثقافة والنشر والتوزيع، عمان، 2012.
- ممدوح عبد الحميد بن عبد المطلب. البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت. دار الكتب القانونية، مصر، 2006.
- محمد بن مكرم بن منظور. لسان العرب. دار الصادر، بيروت، 2010، مجلد5.
- هشام فريد رستم. الجوانب الإجرائية للجرائم المعلوماتية. مكتبة الآلات الحديثة، أسيوط، مصر، 1994، الجزائر، 2007، ط 01.

الاطروحات والمذكرات الجامعية:

أطروحات دكتوراه:

- اريز سالم الحقبا ، مهارت البحث والتحقيق في الجرائم المعلوماتية. رسالة دكتوراه، جامعة نايف للعلوم الأمنية ، السعودية .
- رابحي عزيزة. الأسرار المعلوماتية وحمايتها الجزائية. أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2018.
- التوجي محمد. الحماية الجنائية من الجرائم المرتكبة بواسطة الهاتف النقال. رسالة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2019.

رسائل الماجستير و الماستر:

- رصاع فتيحة الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد تلمسان 2011-2012،
- ثنيان ناصر الثنيان. إثبات الجريمة الإلكترونية؛ دراسة تأصيلية تطبيقية. رسالة ماجستير، جامعة نايف للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.
- حمزة بن عقون. السلوك الإجرامي للمحرم المعلوماتي. بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012.
- دردور نسيم. جرائم المعلوماتية على ضوء القانون الجزائري والمقارن. مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منتوري قسنطينة، 2012 – 2013.
- سعيداني نعيم. آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، 2013 .
- صغير يوسف. الجريمة المرتكبة عبر الانترنت. مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه القانون الأساسي والعلوم السياسية، جامعة مولود معمري، تيزي وزو.
- يوسف خليل يوسف. الجرائم الإلكترونية في التشريع الفلسطيني. رسالة ماجستير، الجامعة الإسلامية، غزة، 2013.
- محمد بن عبد المحسن بن شلهوب. جريمة الإبتزاز الإلكتروني دراسة مقارنة. بحث تكميلي لنيل درجة الماجستير في السياسة الشرعية، المعهد العالي للقضاء، قسم السياسة الشرعية، شعبة الأنظمة، جامعة الإمام محمد بن سعود الإسلامية، 2011.

- برحال أمال. جريمة الابتزاز عبر الوسائط الإلكترونية. مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2020.
- سمية مزغيش. جرائم المساس بالأنظمة المعلوماتية. مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2013-2014.

مقالات :

- بوقرين عبد الحليم. المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي. دراسة مقارنة، بحث مقدم في مجلة جامعة الشارقة، دورية علمية محكمة، المجلد 16، العدد 01، يونيو 2016.

* مريم اعراب. جريمة التهديد والابتزاز الالكتروني. مجلة الدراسات القانونية المقارنة، العدد 7، كلية الحقوق والعلوم السياسية، جامعة وهران 1 محمد بن أحمد، تاريخ النشر 2021/11/22، الجزائر.

- رامي أحمد غالبي. جريمة الإبتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق. مقال منشور في مجلة ثقافتنا الأمنية، الإصدار الثاني، وزارة الداخلية العراقية، مديرية العلاقات والإعلام، دار الكتب والوثائق، بغداد، 2019.
- شاكر سعاد بعيوي. جريمة الإبتزاز الإلكتروني دراسة مقارنة. مقال منشور بمجلة ميسان للدراسات القانونية.
- عدي جابر هادي. الحماية الجزائية للبريد الالكتروني، دراسة مقارنة. بحث مقدم بمجلة رسالة الحقوق، السنة الثانية، العدد الثالث، كلية القانون، جامعة القادسية، 2010.
- فيصل بن زحاف. الحماية الجنائية للحكومة الإلكتروني. مجلة القانون المجتمع والسلطة، العدد رقم03، 2014.

- عماد جواد موسى. التحقيق والصعوبات التي تواجه جريمة الابتزاز الالكتروني. مجلة كلية المعارف الجامعة، كلية التربية للعلوم الإنسانية، جامعة الأنبار، الرمادي، العراق.
- محمد شاكر عبد الله. "قياس الابتزاز العاطفي لدى طلبة المرحلة الإعدادية بناء وتطبيق"، محلة أبحاث البصرة للعلوم الإنسانية، المقارنة كلية القانون، جامعة ميسان، العراق، نوفمبر 2019.
- أكرم ديب نورة بن بوعبد الله. دور الدليل الرقمي الجنائي في إثبات جريمة الابتزاز الإلكتروني. مجلة الحقوق والعلوم الإنسانية، جامعة باتنة | كلية الحقوق والعلوم السياسية الجزائر، المجلد 16، العدد 01، 31/03/2023.
- محمد الامين البشري ، التحقيق في الجرائم المستحدثة ،جامعة نايف العربية للعلوم الامنية ، السعودية ، ط1 ، 2004 .

فهرس المحتويات

ملخص

قمنار بتقسيم مذكرتنا هذه إلى فصلين تناولنا في الفصل الأول الإطار الموضوعي لجريمة الابتزاز الالكتروني حيث تم التطرق فيه إلى ماهية جريمة الإبتزاز الإلكتروني و أنواعها وكذا ظاهرة تجريم الإبتزاز الإلكتروني من خلال أركان الجريمة و العقوبات المقررة لمرتكبي هذه الجريمة، و ثم تطرقنا للفصل الثاني الذي تناولنا فيه إجراءات التحقيق و الصعوبات و العوائق أثناء اجراء التحقيق و كذا تناولنا لأهم وسائل الاثبات التي تخص هذه الجريمة و الصعوبات التي تحول دون الوصول إلى الاثبات.

الكلمات المفتاحية: جريمة الابتزاز الالكتروني–الدليل الرقمي – صعوبات التعاون الدولي في جريمة الابتزاز–ظاهرة تجريم جريمة الابتزاز الالكتروني–الاطار الموضوعي لجريمة الابتزاز–الاطار الاجرائي لجريمة الابتزاز.

Résumé

Nous avons divisé cette note en deux chapitres, dans le premier chapitre, nous avons traité du cadre objectif du crime d'extorsion électronique, dans lequel il a été discuté de ce qu'est le crime d'extorsion électronique et de ses types, ainsi que du phénomène de criminalisation de l'extorsion électronique à travers les éléments du crime et les peines prescrites pour les auteurs de ce crime, puis nous avons abordé le deuxième chapitre, dans lequel nous avons traité des procédures d'enquête, des difficultés et des obstacles au cours de l'enquête, ainsi que des moyens de preuve les plus importants liés à ce crime et des difficultés empêchant l'accès aux preuves.

Mots clés: crime d'extorsion électronique-preuves numériques-difficultés de la coopération internationale dans le crime d'extorsion-le phénomène de criminalisation du crime d'extorsion électronique-le cadre objectif du crime d'extorsion-le cadre procédural du crime d'extorsion.

Summary

We have divided this note into two chapters, in the first chapter we dealt with the objective framework of the crime of electronic extortion, in which it was discussed what the crime of electronic extortion is and its types, as well as the phenomenon of criminalizing electronic extortion through the elements of the crime and the penalties prescribed for the perpetrators of this crime, and then we touched on the second chapter, in which we dealt with the investigation procedures, difficulties and obstacles during the investigation, as well as we dealt with the most important means of proof related to this crime and the difficulties preventing access to evidence.

Keywords: crime of electronic extortion-digital evidence-difficulties of international cooperation in the crime of extortion-the phenomenon of criminalization of the crime of electronic extortion-the objective framework of the crime of extortion-the procedural framework of the crime of extortion.