جامعة 20 أوت 1955 – سكيكدة

كلية الحقوق والعلوم السياسية

قسم الحقوق

الإبتزاز الإلكتروني

مذكرة مكملة لنيل شهادة الماستر تخصص: (قانون جنائي)

إعداد الطالبين:

- غليلة الحسين
- معاوي عبد الناصر

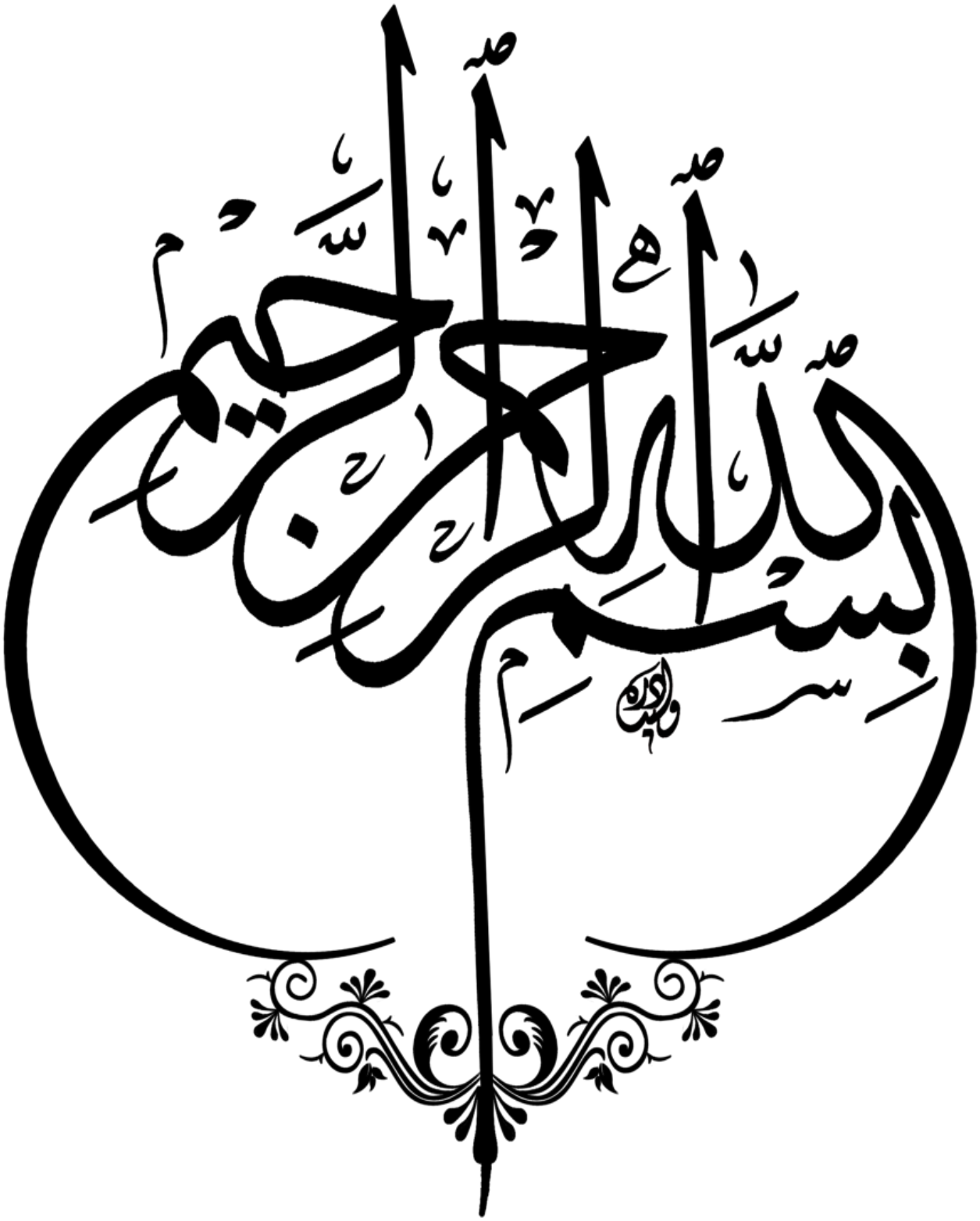
إشراف الأستاذ:

- د.منصف فيلالي

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
د.بوصيدة فيصل	أستاذ محاضر	رئيسا
د.منصف فيلالي	أستاذ محاضر	مشرفا ومقررا
د.شعلال نوال	أستاذة محاضر	مناقشا

دورة جوان 2024


بسم الله الرحمن الرحيم

شكر وتقدير

نشكر الله عز وجل الذي أنار لنا دربنا وفتح لنا أبواب العلم وأمدنا بالصبر والإرادة،

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين وآله وصحبه إلى يوم الدين.

وبعد نحمد الله ونشكره الذي بفضله أنجزنا هذا العمل،

كما نتقدم بالشكر والامتنان للأستاذ الفاضل " **منصف فيلالي** " على توجيهاته القيمة ودعمها لنا.

كما نتوجه بالشكر الجزيل إلى كل أساتذتنا وأعضاء لجنة المناقشة وعميدة الكلية وكل أساتذة كلية الحقوق والعلوم السياسية بجامعة 20 أوت 1955–سكيكدة–

إهداء

اهدي ثمرة جهدي وعملي المتواضع

إلى من كانا السبب الأوّل والحافز الكبير لوصولي لما أنا عليه الأن

إلى من أفنيا عمرهما في سبيل رؤيتي في موقف مشرف كهذا الموقف

إلى أمي وأبي

أطال الله في أعمارهم وحفظهما من كل سوء

وإلى كلّ شخص ساعدني من قريب أو بعيد في إنجاز مذكرة تخرجي

إلى أخواتي وسندي في الحياة وإلى أصدقائي

وإلى كل الزملاء الذين رافقوني طيلة مشواري الدراسي

الحسين

إهداء

شكرا لكل من ساندني طيلة مسيرتي الدراسية

أهذي ثمرة عملي إلى روح والدي رحمه الله وأسكنه الله الفردوس الأعلى

وإلى أمي الغالية حفظها الله

إلى إخوتي حفظهم الله

وإلى كل عائلة " **معاوي** " وإلى جميع أحبتي.

عبد الناصر

قائمة المختصرات باللغة العربية

الرمز	المعنى
ق.إ.ج.ج	قانون إجراءات جزائية الجزائرية
ق.إ.م.إ	قانون الاجراءات المدنية و الإدارية
ص	صفحة
ج	جزء
ق.ع	قانون العقوبات
ق.م	قانون المدني
ع	عدد
ص ص	من الصفحة إلى الصفحة
ق.ج	قانون جنائي
م	مادة
ط	طبعة
ب.س.ن	بدون سنة النشر
د.ط	دون طبعة

مقدمـــــــــــة

يعرف العالم تطور هائل في المجال العلمي والتقني بسبب ظهور الأنترنت ، و من أهم أوجه إنتفاضتها التقدم المذهل في مجال الحواسيب الآلية و ملحقاتها و البرامج التي تلحق بها حيث أصبح الإعتماد على هذه التكنولوجيا جليا في كل الجهات الرسمية و غير الرسمية . فأصبحت الدول يقاس تقدمها على مدى قدرتها على امتلاك و التعامل مع التكنولوجيا الحديثة لكن هذه النعمة صاحبها الاستخدام غير القانوني لهذه التكنولوجيا، فأصبحت تستخدم كمعول هدم لا بناء في أيدي الخارجين عن القانون، ذوو الصفات الخاصة، صاحبو الإجرام الناعم الذي لا يراق فيه نقطة دماء ، و بذلك أسهمت في ظهور نوع جديد من الجرائم التي تتصف في الغالب بخطورتها و بسهولة ارتكابها لا سيما أنها جرائم عابرة للحدود و هي ما يطلق عليها الجرائم الإلكترونية.

لعل هذه الجرائم تقع بواسطة الكمبيوتر حيث يصبح أداة طاغية في يد الجناة يستخدمونها لتحقيق مآربهم الإجرامية مستغلين بذلك تلك التقنيات المستحدثة و التي أصبحت فيما بعد محلا لتلك الجرائم أو وسيلة لارتكابها، فأصبح الوسط الذي ترتكب فيه الجريمة الإلكترونية ومضات كهربائية أو مغناطيسية و رموز و شفرات و لم يعد مسرح الجريمة إلا مسرحا افتراضيا.

إن بعض مجرمي الأنترنت التقليديين قد عزفوا عن جريمة سرقة بطاقات الائتمان ،و معلومات التعريف الشخصية و اتجهوا الى أسلوب أسهل ألا و هو الإبتزاز الإلكتروني، حيث يستخدمون التهديدات التي تحتوي على صور شخصية و أفلام رقمية للضحية للمطالبة بأموال بدلا من سرقتها.

حيث أصبحت جريمة الإبتزاز الإلكتروني ظاهرة تخترق المجتمع و تهدد دعائمه، و تضرب في مقتل أهم أهداف أي مجتمع متحضر في تحقيق الأمن لأفراده، ولعل جوهر تجريم الإبتزاز الإلكتروني هو التهديد ، و التعدي على حقوق الافراد في الخصوصية ، و استغلالهم على غير وجه حق، و الضغط الذي يمارس على الضحية بكشف أسرار من شأنها أن تضره، مما يضطره للإنصياع والإذعان لرغبة الجاني و تحقيق مطالبه تحت الإكراه أو الخوف من الفضيحة، و هو ما دعى المشرعين في العديد من الدول الى سن قوانين تجرم السلوك الإجرامي الذي يتمثل في جريمة الإبتزاز الإلكتروني واهتم شراح القانون

بتفسيره، و شرحه، و بيان أركان الجريمة التي تقوم عليها ، و كذلك طرق التحقيق، والإثبات فيها كما ان للدليل الرقمي أسس وقواعد مختلفة في التعامل معه بسبب خطورة هذه الجريمة.

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

فمن الناحية العلمية، لفت انتباه الباحثين لدراسة الموضوع و تسليط الضوء على مختلف جوانبه، كذلك لفت انتباه المشرع الى إعادة النظر و ضبط النصوص القانونية لمكافحة هذه الجريمة، أما من الناحية العلمية تبرز أهمية البحث في معرفة مدى كفاية النصوص الجنائية في التشريع الجزائري الواردة في قوانين العقوبات إلى الحد من ارتكاب هذه الجريمة و ردع مرتكبيها للتقليل من آثارها و زيادة الوعي لدى مستخدمي الأجهزة الحديثة بمخاطر هذه الجريمة و ضرورة توخي الحيطة والحذر في استخدامها.

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 معروفة بالعادات، والأعراف الإجتماعية التي تتحفظ على كل ما يتعرض للسمعة والشرف خصوصا أن هذه الجريمة أغلب ضحاياها فتيات.

تهدف هذه الدراسة الى التعرف الى النقاط التالية:

-التعرف على الابتزاز الالكتروني وجريمته.

-التعرف على طرق ارتكابها والتعرف على دوافع ارتكابها.

-دراسة أركان الجريمة في التشريع الجزائري.

-التعرف على كيفية التحقيق و الإثبات في جريمة الإبتزاز الإلكتروني ،و التعرف على الدليل الرقمي و علاقته بهذه الجريمة.

-التعرف على الصعوبات التي تواجه السلطات في التحقيق على هذه الجرائم ،و إثباتها و التعرف على العقوبات المقررة لهذه الجريمة في التشريع الجزائري .

ونظرا لتزايد نسبة ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرا لخصوصية هذه الجريمة ، ووسائل وطرق تنفيذها، أدى إلى إنعكاس 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 ويتبين ذلك على الإجابة على إشكالية الدراسة المتمثلة في: ماموقف المشرع الجزائري من جريمة الإبتزاز الإلكتروني عبر الوسائل الإلكترونية ؟

لمعالجة هذه الإشكالية إرتكزت الدراسة على المنهج الوصفي لوصف الجريمة من خلال تعريفها ، وآثارها وسائل ارتكابها ، و المنهج التحليلي معتمدين على تحليل نصوص كل من قانون العقوبات الجزائري وكذلك بعض التشريعات العربية و بيان موقفها من جريمة الإبتزاز الإلكتروني .

و لدراسة هذا الموضوع ارتأينا تقسيم البحث إلى فصلين ، الأول بعنوان ماهية الإبتزاز الإلكتروني و قد تناولنا في المبحث الأول منه مفهوم الإبتزاز الإلكتروني أما المبحث الثاني

بعنوان تجريم الإبتزاز الإلكتروني ،أما الفصل الثاني فقد كان بعنوان : الإطار الإجرائي لجريمة الإبتزاز عبر الوسائل الإلكترونية الذي يحتوي على مبحثين الأول بعنوان إجراءات التحقيق في جريمة الإبتزاز الإلكتروني وجهاته ، أما المبحث الثاني فتناول الإثبات في جريمة الإبتزاز الإلكتروني و في الأخير انتهينا الى توضيح النتائج و المقترحات التي تم التوصل إليها في خاتمة الموضوع.

الفصل الأول :
ماهية الابتزاز الالكتروني

الفصل الأول: ماهية الابتزاز الالكتروني

من المُسلَّم به أَنَّ لكلّ عصرٍ مُشكلاته ورؤيتَهُ التي تنبثق من طبيعة العصر والتي ترتبط ارتباطا كبيرًا بالتغيرات المتنوعة والصراعات التي تنتج عنها، وعليه فإنَّ أخطر المشاكل التي تتعرض لها المجتمعات كافة ظهور الجرائم الإلكترونية وخصوصًا جريمة الابتزاز الإلكتروني، حيث تعد جرائم الابتزاز الالكتروني من الجرائم المستحدثة، إذ أنه وبظهور مجتمع الانترنت الجديد الذي قد فرض نفسه علي كل المجتمعات الحديثة، أصبحت أجهزة الحاسب الآلي التي تستخدم الإنترنت هي مسرح لارتكاب جرائم الابتزاز الالكتروني، فلا يمكن ارتكابها في مكان آخر وهو ما يميزها عن جرائم الابتزاز التقليدية.

ومن منطلق أنَّ القانون هو صمام الأمان للشعوب أصبح واجبًا على التشريعات أن تُعالج هذه الظاهرة المستحدثة وتُسهم في الحدّ منها، ولإعطاء فكرة عامة عن الابتزاز الالكتروني في هذا الفصل، ارتأينا تقسيمه إلى مبحثين كالآتي:

المبحث الأول: مفهوم الابتزاز الالكتروني.

المبحث الثاني : تجريم الإبتزاز الإلكتروني.

المبحث الأول :مفهوم الإبتزاز الالكتروني.

لقد استعمل العلماء لفظ الابتزاز في كتاباتهم قديمًا وحديثًا، ولم يكن هذا المصطلح يختلف في معناه القديم عن معناه المعاصر، فجميعها تهدف إلى مفهوم واحد[1]، ألا وهو الحصول على الأموال أو معلومات سرية، من أجل استغلالها لأغراض مالية أو القيام بأعمال غير مشروعة، وذلك تحت تهديد إفشاء سر مشين صحيح كان أو كاذب.

والجميع منا معرضاً إلى الابتزاز الإلكتروني، حيث لم يسلم منه الرجل والمرأة والصغير والكبير والفرد الواحد والمؤسسات الكبرى، فهناك شركات ومؤسسات أعمال تبتز إلكترونيا لإجبارها على شيء معين عادة ما يخص أمور العمل، لكن الأكثر تعرضا له هم الأفراد على وجه الخصوص والفتيات بالأكثر.

ومن خلال هذا المبحث سنقوم بتقسيم المبحث إلى مطلبين، وهما على النحو التالي:

-المطلب الأول :تعريف الابتزاز الالكتروني و مدى خطورته.

- المطلب الثاني: أنواع الابتزاز الالكتروني و خصائصه.

[1]- محمد بن جرير الطبري، التبصير في معالم الدين، تحقيق: علي بن عبد العزيز بن علي الشبل، دار العاصمة السعودية، ط 1، 1996، ص157 .

المطلب الأول : تعريف الابتزاز الالكتروني ومدى خطورته.

على الرغم من حداثة مصطلح الابتزاز الإلكتروني، إلا أننا نستطيع القول بأن مضمون هذا المصطلح وجد من قبل في القانون الجنائي، ويعدّ تعريف ظاهرة التهديد والابتزاز الإلكتروني في فهم الشروحات والأساليب والأفعال التّي يتعامل بها المجرمون في تعاطيهم مع الضحايا والتأثير وإلحاق الأضرار بشخصياتهم مادّيا، اجتماعيا، نفسيا ومعنويا.

ضمن هذا السياق، سيأتي مطلبنا في تعريف جريمة التهديد والابتزاز الإلكتروني ومدى خطورته حيث سنوضح هدا المطلب في فرعين متتاليين (فرع أول بعنوان تعرف التهديد والابتزاز الالكتروني) و(الثاني بعنوان مدى خطورة الابتزاز الالكتروني).

الفرع الأول : تعريف الابتزاز الإلكتروني.

يعدّ مفهوم ظاهرة التهديد و الإبتزاز الإلكتروني في فهم الشروحات والأساليب والأفعال التّي يتعامل بها المجرمون في تعاطيهم مع الضحايا والتأثير وإلحاق الأضرار بشخصياتهم مادّيا، اجتماعيا، نفسيا ومعنويا.

ضمن هذا النحو، تأتي ديباجتنا في تعريف التهديد والإبتزاز الإلكتروني وفق التتابع المنهجي التّالي:

أولا : لغة.

ابتز يبتز ابتزز ابتزازاً، فهو مبتز، والمفعول مبتز ابتز المال من الناس، سلبهم إياه، نزعه منهم بجفاء وقهر ،التهديد في اللّغة العربية هو الوعيد والتخويف، فيقال فلان هدّد فلانا، أي هددّه أو خوّفه بالعقوبة أو محاولة تحقيق المهدّد مكاسب مادية أو معنوية أو جنسية من وراء ابتزازاته أو تهديداته بالإكراه [1].

[1]– نورة بنت عبد الله بن محمد المطلق، ابتزاز الفتيات أحكامه وعقوبته في الفقه الإسلامي، كلية الشريعة، جامعة الإمام محمد بن سعود الإسلامية، السعودية ،بدون ذكر سنة الطبعة، ص ص 4–5.

و الإبتزاز في اللّغة مصدره الفعل بَزّ ومعناه الغلبة والغصب، بَزّهُ يَبزّهُ بزّا، والبزّ: النزعُ والسلبْ[1].

ليشتق أيضا مفهوم الإبتزاز من الجدر ابتزّ، يبتزّ، ابتزازا، أي أنّ الإبتزاز التّهديدي لغة هنا يتأتّى في شكل انتزاع المال من شخص عن طريق التّهديد التعسّفي أو بكشف عمل إجراميّ أو معلومة ضارّة بالسّمعة أو هو الحصول على المال أو المنافع من شخص تحت التَّهديد بفضح بعض أسراره أو غير ذلك[2].

ثانيا: إصطلاحا.

يعرف اصطلاحا بأنه استخدام التهديد بالإيذاء الجسدي أو النفسي، أو الإضرار بالسمعة والمكافحة الإجتماعية بتلقيف الفضائح وإلصاق التهم، ونشر أسرار مما يجبر

الشخص (المبتز) على الدفع مكرها لمن يمارس الإبتزاز عليه [3].

الحصول على معلومات سرية أو صور شخصية أو مواد فلمية تخص الضحية، واستغلالها لأغراض مادية أو القيام بأعمال غير مشروعة وهو الحصول على المال أو المنافع من شخص وابتزازه بواسطة التهديد بفضح بعض أسرار التي يمتلكها[4].

---

[1]– أبو الفضل جمال الدين محمد بن مكرم ابن المنظور، معجم لسان العرب، دار صابر، لبنان، مج 02، باب حرف الباء.

[2]_ معجم المعاني الجامع، في شرح مفهوم لفظة ابتزّ، تمّ تصفّحه من موقع المعاني، من على الرابط https://www.almaany.com/fa/dict/ar-fa/، بتاريخ 2024/04/18 على الساعة 02:51.

[3] - سليمان بن عبد الرزاق الغديان، يحيى بن مبارك خطاطبة، عزالدين بن عبد الله النعيمي، صور جرائم الإبتزاز الإلكتروني ودوافعها وآثارها المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين، مجلة البحوث الأمنية، دار المنظومة الرواد في قواعد المعلومات العربية، مجلد 27، العدد 69،مصر، يناير 2018 ص166.

[4] -محمد بن المحسن بن شلهوب ، جريمة الإبتزاز الإلكتروني ، دراسة مقارنة، بحث تكميلي لنيل درجة الماجيستير في السياسة الشرعية ، المعهد العالي للقضاء، قسم السياسة الشرعية ، شعبة الانظمة ، جامعة الامام محمد بن سعود الاسلامية، السعودية ، 2011، ص 59.

ثالثا: الفقهي

تعددت تعريفات الفقه للابتزاز ، فقد عرفه بعض الفقه على أنه الضغط الذي يباشر شخص على إرادة شخص آخر بجملة على ارتكاب جريمة معينة.

وقد عرفه البعض الآخر على أنه فعل يقوم به شخص بتهديد شخص آخر بأي طريقة ولا يهم نوع عبارات التهديد مادام من شأنها التأثير في نفس المجني عليه بتخويفه، أو ازعاجه من خطر لم يتحقق بعد قد يلحق على المجني عليه، أو نفسه، أو أي شخص آخر له صلة بالمجني عليه وقد عرف على أنه القيام بتهديد شخص بفضح أمره ما لم يستجيب المهدد إلى تنفيذ طلبات الجاني وغالبا ما تهدف تلك الطلبات إلى أمور غير مشروعة تمس الشرف، أو الكرامة، أو تتعلق بحرمة الحياة الخاصة للشخص المهدد الذي تم ابتزازه.[1]

وفي تعريف آخر فقد عرف الإبتزاز الإلكتروني بأنه الحصول على وثائق، وصور، ومعلومات عن الضحية من خلال وسائل الكترونية أو التهديد بالتشهير بمعلومات ووثائق خاصة عن طريق استخدام الوسائل الإلكترونية لتحقيق أهداف يسعى لها المبتز[2]

من خلال التعاريف السابقة للإبتزاز نجد أنها لا تخرج على اعتبار الإبتزاز وسيلة ضغط أو تهديد يمارسه المبتز على إرادة المجني عليه بهدف الوصول إلى تحقيق مراده لأن الإبتزاز مرتبط بالتهديد فدون هذا الأخير لا يتحقق الإبتزاز كما نستطيع القول أن الإبتزاز الإلكتروني يمثل سلوك غير مشروع أو غير أخلاقي ويعد من الجرائم التي تقع عن طريق الشبكة المعلوماتية[3].

[1] - ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الإبتزاز، مقال منشور على الشبكة الإلكترونية، المجلة العربية للدراسات الأمنية، المجلد 33، العدد 70، الرياض، السعودية ، 2017، ص 199.

[2]- نفس المرجع ، نفس ص.

[3]- الشحات ابراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية و القوانين الوضعية، بحث فقهي مقارن، ط1، دار الفكر الجامعي، الاسكندرية، مصر،2012 ، ص 80.

رابعا–الإبتزاز الإلكتروني بالنسبة للمشرع الجزائر.

يعد الإبتزاز الإلكتروني في القانون الجنائي الجزائري نوعاً من أنواع جريمة السرقة، فهو محوره التهديد بنشر المعلومات الخاصة التي يكون المبتز سرقها من الضحية.

فانتهاك جريمة الإبتزاز الإلكتروني لمفهوم الخصوصية في نطاق الرقمنة، فالحق في الخصوصية من الحقوق الدستورية الأساسية الملازمة واللصيقة للشخص الطبيعي بصفته الإنسانية كأصل عام[1].

ولو أن القانون الجزائري لا يحدد هذا المفهوم ومحدداته مما ينبئ عن تعقده وتشعب مراميه، بحيث يصبح الشخص معرضا للإنتهاك متى تم تسجيل محتوى متعلق به في العالم الرقمي، مما يجعله غير قابل للمحو[2].

فالابتزاز بشكل عام تعرف بأنه: سلوك يتضمن مساومة الشخص للحصول على مكاسب

مادية أو معنوية أو جنسية أو لمجرد الإنتقام عن طريق وسائل الإكراه والقسر بتهديده بإفشاء أسرار ممكن أن تسيء له أو تلحق الضرر به، وهو أنواع منه الإبتزاز الإلكتروني الذي يعني التهديد والمساومة التي تقع بواسطة آلية إلكترونية، أو هو الحصول على معلومات سرية إلكترونية تتعلق بالمجني عليه لا يرغب وصولها للآخرين والتهديد بإفشاء السر أو نشر المعلومات إن لم تتحقق مطالبه وتنفذ، مما يؤثر على إرادة ونفسية المجني عليه، فيستجيب لرغبات الجاني[3].

فالابتزاز في مضمونه طلب خدمة من شخص مع العلم المسبق بعدم قدرته المطلقة على قيامه بها، فهو إذا في معناه الدقيق استخدام المبتز سواء أكان شخصا أم تنظيما أسلوب من

---

[1]- فاطمة العرفي، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون الجزائري، مجلة صوت القانون المجلد الثامن، العدد خاص ،02، 2022، ص 494.

[2]- نفس المرجع ،ص 495.

[3]- نجاء المطيري، سامي مرزوق ،المسؤولية الجنائية عن الإبتزاز الإلكتروني في النظام السعودي دراسة مقارنة، رسالة مقدمة استكمال لمتطلبات الحصول على درجة الماجستير في الشريعة والقانون :إشراف عبد الفتاح باباه، الرياض، أكاديمية نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، بدون ذكر السنة الجامعية ، ص 13.

أساليب الضغط المادي أو المعنوي لدفع الضحية لنهج سلوك معين يجلب المنفعة للجهة المبتزة ، متبعا أسلوب التهديد بالتشهير بالضحية على أوسع نطاق، حتى يجعل الضحية تقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته وتحقيق رغباته الجنسية أو المادية، مما يعني أن محل الإبتزاز خدمة تقترن الفعل المؤذي بالرضا، لذا لابد من توافر القصد الجنائي من خلال اتجاه نية المبتز لاستعمال التهديد والمساومة من أجل الحصول على الخدمة مع العلم المسبق بعدم القدرة على الدفع [1].

من هذا المنطلق يمكن اعتبار ابتزاز الأشخاص ضمن هذا المفهوم الذي ذكرته المواد 284 و286 و371 من قانون العقوبات الجزائري، ولو أنه كان من الأفضل ذكرها في نصوص قانونية واضحة تأخذ بعين الاعتبار المستجدات التكنولوجية التي أصبحت جزء منها.[2]

وأيضا نظرا لانتشارها وخطورتها على اعتبار أن هذا النوع من المواد المسيئة أصبحت تنتج ثم تروج عبر الوسائط الرقمية، أو تنتج بشكل مباشر أمام جمهور يشاهدها، حيث يتم استغلال قوة الهوية المجهولة للجناة للإساءة للأشخاص، مثل تظاهر المتصيد بأنه صديق حتى يكتسب ثقة الشخص ومن ثم يطلب منه رقم هاتفه بغرض التواصل معه في العالم الحقيقي، لاستغلاله فعليا أو الإكتفاء بالتسجيل أو التصوير أو الدردشة ذات الطابع الإباحي ومن ثم ابتزازه فإن رفض قام بالتشهير به.[3]

الفرع الثاني: مدى خطورة الابتزاز الالكتروني

تكمن خطورة الإبتزاز الإلكتروني بعد الانتشار اللّامتناهي للسيبرنية والتدفّق المعلوماتي في عصر العولمة، خاصّة ما يسمى بشبكات التواصل الاجتماعي عبر شبكة الأنترنيت وتماشي أنواع الدردشات بين عموم الأفراد من الناس كبارا أو صغارا، بالتّالي الكلّ

[1]- رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه، المجلة العربية للدراسات الأمنية، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 33 ، العدد 70 ، 2017، ص ص،193-220.

[2]- فاطمة العرفي، المرجع السابق، ص 496.

[3]- - نفس المرجع، نفس ص.

يضع معلوماته شخصية، من صور ومقاطع فيديو وتسجيلات وبيانات ومعلومات خاصة بهم[1].

من ثمّة، فالجميع عرضة للمتطفّلين أو الهاكرز أو محترفي الأنترنيت ذوي السلوكيات الذميمة والأمراض النفسية الذّين يتلذّذون بفضح خصوصية الأفراد عبر الوسائل الإتصالية الإلكترًونية لأغراض ما أو لأخرى.

نتيجة لذلك، يقع الضحايا في شباك المبتزّين، خاصة الضعفاء منهم، كالنساء والأطفال والفئات الهشّة، لتكمن خطورة الابتزاز الإلكتروني هنا في جعل هؤلاء الضحايا يقبلون[2]:

- ✓ على الإنتحار أو محاولة الإنتحار أو قتل أنفسهم.
- ✓ على القتل أو محاولة القتل من قبل عائلاتهم.
- ✓ ناهيك، على استغلالهم للقيام بأعمال غير مشروعة كالتطرّف، الدعارة، السرقة والتزوير...إلخ.
- ✓ زيادة عن احتمالية التصاقهم بحالات الرعب الشديد وما ينجم على إثره من أزمات صحّية أو أمراض نفسية دائمة.
- ✓ الخوف منهم الإبلاغ الأجهزة الأمنية بسبب الفضيحة أو مواجهة ذويهم بحيثيات التهديد والإبتزاز الإلكتروني، خاصّة وأنّ أغلب التهديدات والإبتزازات يغلب عليها طابع الإحراج والخدش بالشرف أو الكرامة.[3]
- ✓ بالإضافة إلى اتّخاد العزلة الإجتماعية قهرا، نتيجة الخوف من الوصف الاجتماعي، خاصّة بتلك الأمور الملتصقة بحالات الشرف أو المزالق الجنسية.
- ✓ كما وأنّ مشكلات وخطورة الإبتزاز الإلكتروني تعدّ من الطابوهات المسكوت عنها في المجتمع الجزائري.

---

[1]- عراب مريم، جريمة التهديد والإبتزاز الإلكتروني، مجلة الدراسات القانونية المقارنة، مج 07، ع 01، 2021، ص 1207.

[2]– عراب مريم، المرجع السابق، ص1208

[3]– ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق ، ص10 .

هذا ونظرا لضبابية الأرقام المعلن عنها، بالرغم من وجود القوانين والتشريعات في هذا الصدد مع وجود الإرادة السياسية أو التنظيمية أو القانونية لمجابهة هذه الجريمة المستحدثة ونشر إلزامية الحماية القانونية للضحايا والتعامل مع المهدّدين والجناة بيد من حديد وتحت طائل القانون الجزائي.

المطلب الثاني : أنواع الإبتزاز الإلكتروني و خصائصه.

تبعا لما سلف، يحمل الإبتزاز الإلكتروني ضمن طيّاتها مجموعة كبيرة من الديباجات والنصوص التّي تتحدّث عن أبرز أنواع وخصائص الإبتزاز الإلكتروني وعليه تقتضي الضرورة البحثية في هذا المطلب تقسيمه إلى فرعين أساسين: ليرتبط الفرع الأوّل بأنواع الإبتزاز الإلكتروني، أمّا الفرع الثّاني فيتعلّق بالخصائص المرتبطة بالابتزاز الإلكتروني.

الفرع الأوّل: أنواع الإبتزاز الإلكتروني.

يُقسّم الإبتزاز الإلكتروني إلى تقسيمات متعددة، وفقا لمعايير عدة، بالتّالي نتطرّق لذكرها بحسب تقسيم الباحثين المتمثل في التقسيم الأوّل من حيث المجني عليه، والتقسيم الثّاني من حيث الهدف المقصود.

أولا- التهديد والإبتزاز الإلكتروني من حيث المجني عليه.

ينقسم التهديد والإبتزاز الإلكتروني من حيث المجني عليه إلى أربعة أنواع، نذكرها تباعا كما يلي:

أ- تهديد وابتزاز النساء.

يعتبر تهديد وابتزاز النساء هو النموذج المثالي الأكثر شهرة وانتشارا بين ثنائية الضحايا المجني عنهم والمبتزّين الجناة، خاصة إذا كان المبتز والجاني رجلا والضحية امرأة ليرجع ذلك الإنتشار، أنّ غالبا ما يكون تهديد المبتزين للنساء يعتمد على صور الكاشفة أو محادثات خادشة بالحياء أو عرضا مرئيا لعلاقة غير شرعية جمعت بين المبتز وضحيّته، أو بينها وبين شخص أخر، كما وقد يكون المبتز خطط لجريمته مسبقا أو قد تزرع الفكرة في رأسه بعد أن وطدّ أواصر العلاقة مع ضحيته، كما وقد تكون الضحية المرأة من فئة

الأحداث التّي غالبا ما تتجاوب مع الابتزاز والتهديد الالكتروني خوفا من الفضيحة اذا لم ترضخ الى طلبات المبتز عموما[1].

ب-تهديد وابتزاز الأحداث.

تختلف التشريعات في تعريفها للأحداث ويرجع ذلك الاختلاف إلى تحديد سنّ التمييز وسنّ الرشد بسبب العوامل الثقافية الخاصة بكل مجتمع.

لتكثر جرائم التهديد والابتزاز الإلكتروني الخاصّة بفئة الأحداث من الجنسين وتأتي أرقامها في المرتبة الثانية بعد جرائم التهديد والابتزاز الإلكتروني الخاصّة بالنساء، حيث يتمّ ذلك بالضغط على الحدث بتهديده إمّا بنشر صوره الخاصّة أو بالتسجيلات المرئي أو المحادثات على مواقع الدردشة أو أيّة مادة عن واقعة من شأنها تحقير المجني عليه عند أهله أو المجتمع الصغير الذّي يقطن به[2].

لتستهدف هذه الفئة غالبا من أجل مطامع جنسية أو تسريب معلومات عن الأهل فيستغل المجرم جهل الأطفال وسذاجتهم في التصرّف، ليمارس عليهم جريمة التهديد الالكتروني بعد التسلّل الى أفكارهم ومعنوياتهم، ولأنّ الأحداث هم الفئات الأكثر اتصالا بالتكنولوجيا ووسائل التواصل الإجتماعي والأكثر وللعب بها، حيث باتت تشكل أشواطا كبيرة من يومياتهم ممّا يسهل انزلاقهم في الجريمة أو جرّهم للسرقة أو الإستغلال الجنسي[3].

ج- تهديد وابتزاز الرجال

قد يقع الرجال ضحية المجني عليهم في جريمة التهديد الإبتزاز الإلكتروني للعديد من الأسباب والعوامل نذكر منها ما يلي:

---

[1]- الحسين عبد العزيز بن حمين بن أحمد، الإبتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة والإبتزاز: المفهوم، الاسباب، العلاج، جامعة الملك سعود، السعودية ، 2011، ص61.

[2]- خالد حسن أحمد، جرائم الانترنت بين القرصنة الالكترونية وجرائم الإبتزاز الالكتروني، دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2018، ص 138.

[3]- ممدوح رشيد مشرف العنزي، المرجع السابق، ص 200.

- ✓ فقد يكون بعض الرجال المجني عليهم ميسوري الحال، من ثمّة تجدهم أكثر عرضة للإبتزاز من طرف بعض النساء محترفات بيع الهوى على المواقع الإلكترونية فيهددون بإذاعة صورهم الماجنة أو مقاطع فيلمية تهدد مراكزهم.
- ✓ أو بسبب نشر أسرارهم في مجال عملهم أو ما يخصّ عائلاتهم أو نشر معلومات قد تمسّ شرفهم أو سمعتهم أو مراكزهم الإجتماعية[1].

د-تهديد وابتزاز الأشخاص المعنوية.

يعرف الشخص المعنوي بأنّه تكتّل من الأشخاص أو الأموال أو الهيئات تحظى باعتراف القانون بالشخصية والكيان المستقل[2].

كما وقد تكون الفئة المستهدفة من التهديد والإبتزاز الإلكتروني من أشخاص اعتبارية كالحكومات أو الشركات أو المؤسسات وذلك عن محاولة أو الشروع في الحصول على معلومات سرية خاصة بها ثم يقوم المبتز بالتهديد بالإفصاح عنها أو إفشاؤها واستمالة الضحايا لأغراض مادّية أو لوجستيكية أو أمنية أو معلوماتية تتعلّق بهذه الشخصية الإعتبارية...إلخ.[3]

ثانيا- التهديد والإبتزاز الإلكتروني من حيث الهدف المقصود.

ينقسم التهديد والإبتزاز الإلكتروني من حيث الهدف المقصود إلى أربعة أنواع، نذكرها تباعا كما يلي:

أ- التهديد والإبتزاز بهدف مادّي.

يعدّ التهديد والإبتزاز بهدف مادّي من أهمّ وأكثر الأهداف التّي يرجو المبتز تحقيقها من ارتكابه جريمة التهديد والإبتزاز الإلكتروني وهي تحقيق منفعة مالية أو عينية ذات قيمة من المجني عليه.

---

[1]- خالد حسن أحمد، المرجع السابق، ص 138.

[2]- حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الإجتماعي، دار النهضة العربية، مصر،2018 ، ص 423.

[3]- خالد حسن أحمد، المرجع السابق، ص 136.

فقد حقّق هذا النوع من الجرائم الإلكتروني بقيام الجاني بتهديد المجني عليه من أجل تسليم أموال أو أشياء أخرى ذات طابع مالي، سواء بطريقة مباشرة أو غير مباشرة. فيتحقق الإبتزاز أو التهديد بالطريق المباشر بطلب المبتز من المجني عليه تحويل مبالغ مالية بشكل مباشر أو لغيره، مقابل ألاّ يقوم الجاني بتنفيذ تهديده.[1]

أمّا الطريق غير المباشرة، فتتحقق عن طريق طلب المبتز من المجني عليه تسديد مبالغ مالية ما أو قيامه بدفع أقساط مالية عند الغير وتسديد ديون مستحقة لمصلحة المبتز[2].

ب- التهديد والإبتزاز بهدف جنسي.

- ✓ يتحقّق هذا النوع من التهديد والإبتزاز حينما يكون المقابل الذّي يطلبه المبتزّ ممارسة الفعل الجنسي أو مقدّماته، لينقسم بدوره التهديد والإبتزاز بهدف جنسي إلى قسمين:
- ✓ القسم الأول: يرتبط التهديد والإبتزاز الجنسي الإلكتروني الإفتراضي والذّي يتمّ عن بعد عن طريق الوسائط الإتصالية المرئية.
- ✓ القسم الثاني، يرتبط التهديد والإبتزاز الجنسي الإلكتروني الواقعي أي المراد هنا استمالة الضحيّة لممارسة الجنس على أرض الواقع.[3]

ج-التهديد والإبتزاز بهدف نفعي.

يتحقق ذلك بقيام المبتز بتهديد الضحية بإذاعة أسراره أو نشرها للعلن وذلك إذا لم يتمّ تلبية طلباته المنفعية على سبيل المصالح التّالية:

- ✓ المنفعة المرجوة من الإبتزاز الإلكتروني كالأعمال غير المشروعة كتنفيذ سرقة لصالح المبتز.
- ✓ القيام بترويج المخدرات أو الممنوعات أو التهريب...إلخ.
- ✓ التوسّط لدى شخص لإتمام عمل، إيجاد وظيفة، سكن...إلخ.

---

[1]- خالد حسن أحمد، المرجع السابق، ص 138.

[2]- نورة بنت عبد الله بن محمد المطلق، مرجع سابق ، ص ص 4-5.

[3]- القاضي علي الزيدي، جريمة الإبتزاز الالكتروني، دراسة مقارنة، ط1 ، مكتبة القانون المقارن، بغداد،2019، ص ص 25- 26.

✓ كما وقد يكون التهديد لغرض القيام بأمور التطّرف والإرهاب.[1]

د- التهديد والإبتزاز بهدف انتقامي.

يؤدّي الجانب النفسي دورا كبيرا في عملية التهديد والإبتزاز الإلكتروني، ذلك باعتبار المجني عليه يعيش صراعا داخليا، نتيجة أنّ الجاني سيقوم بتنفيذ تهديداته ضدّه في أيّ وقت شاء، ما يدفعه إلى تلبيه طلبات الجاني تجنّبا للفضيحة والحفاظ على السمعة.

حيث يستمتع الجاني بأذية المجني عليه واستماعه لتوسّلاته وما يزيد الأمر سوءا أن يقوم الجاني بتصوير المجني عليه، فيطلب منه ذكر أي بيانات تتعلّق به، كما يكون الدافع لدى الجاني هو الإنتقام من المجني عليه عن طريق إلحاق الأذى به وتشويه سمعته بنشر صوره عن طريق شبكة الانترنت[2].

الفرع الثاني: خصائص الإبتزاز الإلكتروني.

لكل ظاهرة إجرامية جديدة أو كل نمط أو سلوك إجرامي حديث خصائص وسمات تميزه عن غيره[3].

لذلك لابد أن يكون للمجرم المعلوماتي صفات أو خصائص قد لا تتوافر في المجرم الإعتيادي لأن ظاهرة الإجرام المعلوماتي والجريمة الإلكترونية بصفة عامة و الإبتزاز لإلكتروني بصفة خاصة هي أنماط إجرامية مستحدثة[4].

ويمكن القول بأن اختراع الحاسوب وظهور الشبكات المعلوماتية فيما بعد كشبكة

الأنترنت، وشيوع وسائل التواصل الاجتماعي أدت إلى تكوين مجرمين يتمتعون بمواصفات ومؤهلات وشخصيات معينة.[5] فالمجرم الإلكتروني يرتكب جرائمه في أوساط البيئة الحاسوبية

---

[1]- خالد حسن أحمد، المرجع السابق، 139.

[2]- ممدوح رشيد مشرف الرشيد العنزي، المرجع السابق، ص 202.

[3]محمود أحمد عبانية، جرائم الحاسوب وأبعاد الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ،2009،ص4.

[4] محمد علي العريان، الجرائم المعلوماتية: انعكاسات دورة المعلومات على قانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، 2004،ص 60.

[5]مدحت رمضان، جرائم الإعتداء على الأشخاص والأنترنت، دار النهضة العربية، القاهرة، 2000،ص11.

والشبكات الإنترنت، ويتمتع بقدر من الذكاء والاحتراف في عمله، كذلك قد يكون هادئ الطباع ولا يميل لاستعمال العنف والقوة وعادة ما يكون المجرم المعلوماتي إنسان اجتماعي بطبعه.

وفيما يأتي نتناول الخصائص العامة للابتزاز الإلكتروني والسمات التي يتمتع بيها الجاني الذي يقوم بالإبتزاز الإلكتروني على نحو ما يأتي:

أولا-الخصائص العامة للابتزاز الإلكتروني.

يحتاج الإبتزاز الإلكتروني إلى استخدام تقنية من البرمجيات الحديثة في عالم الإتصال ما بين الأفراد باستخدام الوسائل الإلكترونية الحديثة وشبكة الأنترنت، ولهذا فإن هذه الظاهرة تتمتع بخصائص متعددة تتمثل فيما يلي:

أ-الابتزاز الإلكتروني عابر للحدود.

إذا كانت السرقة أو الإحتيال أو الضرب أو غيرها من الجرائم التقليدية الأخرى تتم داخل إقليم الدولة، فإن الإبتزاز الإلكتروني عابر للحدود، فهو لا يحترم الحدود السياسية ومن الممكن ارتكابه عن بعد، مما قد يجعل العالم بأسره مسرحاً جرمياً لمرتكبها، فيمكن أن يكون الجاني في قارة والمجني عليه في قارة أخرى.[1]

فهذه الخاصية تصنع على الإبتزاز الإلكتروني الصبغة العالمية، حيث يمكن أن يكون الجاني في الإبتزاز الإلكتروني موجوداً في الصين ويكون المجني عليه في العراق، وهو ما يتطلب وجود تعاون دولي في مكافحة هذه الجرائم حول العالم.[2]

[1] محمد على سالم، حسون عبيد، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، مجلد 14، العدد 2، العراق، 2007، ص92 .

[2] عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات-شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط 1، دار وائل للنشر والتوزيع، عمان، الأردن، 2017، ص- ص، 78-79.

بالنسبة للمشرع الجزائري تنص المادة الثالثة 03 قانون العقوبات على ما يلي: يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية"، بمفهوم المخالفة فإن قانون العقوبات الجزائري لا يسري على الجرائم التي تُرتكب في خارج الإقليم الجزائري.[1]

أكد تقنين العقوبات الجزائري مبدأ السريان الإقليمي بنص صريح هو ينص الفقرة الأولى من المادة الثالثة منه، فطبقا لهذا النص فإن تقنين العقوبات الجزائري يسري على كل الجرائم التي ترتكب في الجزائر بغض النظر عن جنسية مرتكبها جزائريا كان أو أجنبيا، وبصرف النظر عن جنسية المجني عليه وبصرف النظر أيضا عن طبيعة الجريمة، وبمفهوم المخالفة فإن هذا التقنين لا يسري على ما يرتكب من جرائم خارج الإقليم الجزائري.[2]

ب-الإبتزاز الإلكتروني يمس بحرية الأشخاص.

يتميز الإبتزاز الإلكتروني بكونه من الظواهر الإجرامية التي تمس حرية الأشخاص وحرمتهم، فهي تشبه جرائم السب و القذف أو التشهير وافشاء الأسرارالشخصية والاعتداء على الحياة الخاصة حيث يقوم الجاني في كثير من الأحوال بالاعتداء على الحياة الشخصية للأفراد، سواء كانوا أشخاص طبيعيين أو أشخاص معنوية عن طريق إعتداء ملف يحتوي على معلومات أو بيانات شخصية دون علم هذا الشخص[3].

ومن ثم يقوم بتهديد بنشر تلك المعلومات الشخصية، مما يمثل إعتداء على الحرية الشخصية والحق في الخصوصية الذي يمثل أهم الحقوق الدستورية[4].

ج-الإبتزاز الإلكتروني يتم بواسطة الوسائل الإلكترونية الحديثة.

يتم الإبتزاز الإلكتروني عن طريق استخدام الوسائل الإلكترونية الحديثة مما يستلزم لارتكابها وجود أحد الأجهزة الإلكترونية الحديثة كالكمبيوتر أو الهاتف المحمول أو غيرها

---

[1] أنظر الفقرة الأولى من المادة 3من قانون العقوبات الجزائري.

[2]أنظر، المادة 3من ق. ع .ج.

[3]زهراء عادل سلبي، جريمة الإبتزاز الإلكتروني –دراسة مقارنة–، ط ،1دار الأكاديميون للنشر والتوزيع، عمان–الأردن، 2020م، ص60.

[4]زهراء عادل سلبي، المرجع نفسه، ص61.

من الأجهزة الإلكترونية الأخرى.

والدخول إلى أحد برامج التواصل الإلكتروني عبر شبكة الأنترنت من أجل التواصل مع المجني عليه والحصول على الصور أو المقاطع أو البيانات أو المعلومات الشخصية التي يستخدمها المبتز في الإبتزاز، لذلك فإن الجاني يكون بحاجة إلى أدوات تقنية إلكترونية حديثة من أجل القيام بهذه الجريمة، بالإضافة إلى معرفة الجاني لكيفية استخدام تلك الوسائل الإلكترونية التي تتم الجريمة من خلالها[1].

د-ظاهرة جرمية بالغة الخطورة.

ظاهرة الإبتزاز الإلكتروني ظاهرة بالغة الخطورة على المجتمع، وهذا يظهر من خلال الخسائر المادية التي تنتج عن هذه الظاهرة كما يصعب معرفة حجم الخسائر المادية الحقيقية التي ترتبت على هذه الظاهرة نتيجة أن الكثير من المنظمات أو الشركات التي تتعرض للإبتزاز الإلكتروني لا تقوم بإبلاغ الجهات المختصة نتيجة خشية التعرض لإساءة السمعة أو التأثير على الوضع المالي لهذه الشركات والمؤسسات وأسهمها في سوق الأوراق المالية[2] .

وبالنسبة للأفراد الطبيعيين تظهر خطورة الإبتزاز الإلكتروني من خلال ما يمسه من شرف الإنسان وسمعته والمساس بحياته الخاصة، علاوة على أنهذه الظاهرة قد تمس الدول في أمنها القومي مما يظهر خطورتها وبالتالي ضرورة مكافحتها من كافة الدول.[3]

لذلك نرى أن المشرع الإماراتي قد نص في المادة 46 من قانون مكافحة جرائم تقنية المعلومات رقم 5لسنة 2012م على أنه:"...كما يعد ظرف مشدداً ارتكاب أي جريمة

[1] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري –دراسة مقارنة–، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2019ص – ص37–38.

[2] زهراء عادل سلبي، المرجع السابق، ص54.

[3] علي حسن الطوالبة، الجرائم الإلكترونية، مطبعة جامعة العلوم التطبيقية، البحرين ،2008ص60.

منصوص عليها في هذا المرسوم بقانون لحساب أو مصلحة دولة أجنبية أو أي جماعة ارهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة."[1]

هـ-صعوبة إثبات الإبتزاز الإلكتروني.

لما كان الإبتزاز الإلكتروني يتم من خلال الوسائل الإلكترونية الحديثة بحيث يقوم الجاني بابتزاز المجني عليه وتهديده عبر هذه الوسائل الإلكترونية فإنه يتعذر إثباته، نظرا أن عملية الإبتزاز تتم من خلال الوسائل الإلكترونية وهو ما يمكن الجاني من محو أثار فعلته وتدمير كافة الأدلة في وقت قياسي.[2]

كما أن المجني عليه قد يحجم عن التبليغ عن وقوع الجريمة، بالإضافة إلى أن وجود الجاني في دولة أخرى يصعب عملية الإثبات ومن ثم التحقيق أو المعاقبة.[3].

و-الإبتزاز الإلكتروني من الجرائم الناعمة.

يعد الإبتزاز الإلكتروني أحد أنواع الجرائم الناعمة التي لا تتطلب عنها فالجاني في تلك الجرائم لا يستخدم العنف كما هو الحال في جرائم السرقة أو جرائم الضرب والقتل وغيرها من الجرائم التي يعتمد فيها الجاني على استخدام العنف في تنفيذها، بل تتم هذه الجريمة عبر الوسائل الإلكترونية دون استخدام أي وجه من أوجه العنف، مع المجني عليه...[4] وهذا ما يراه الباحث أيضا بالنسبة للإبتزاز الإلكتروني فهي من ضمن الجرائم الناعمة التي لا تحتاج أي عنف من قبل الجاني تجاه الشخص المجني عليه[5].

---

[1] المادة 46من قانون مكافحة جرائم تقنية المعلومات الإماراتي، رقم 5لسنة 2012.

[2] رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية،" مركز جيل البحث العلمي، طرابلس 25-24مارس2017م، ص102.

[3] – رحيمة نمديلي، المرجع نفسه ،ص103.

[4] ذياب موسى البدانية، الجرائم الإلكترونية المفهوم والأسباب، ورقة علمية مقدمة خلال الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من 9 ،4/2014-2م، عمان- الأردن، ، 2014 ص 20.

[5] محمد علي سالم، حسون عبيد، المرجع السابق، ص 92.

ز-الإبتزاز الإلكتروني من جرائم الأموال.

ويتحقق ذلك عندما يهدف الجاني الحصول على منافع نقدية أو غيرها، من خلال حصول الجاني على بيانات أو معلومات تجارية ومالية أو براءات اختراع أو غيرها من المعلومات والبيانات التي يترتب على نشرها حدوث خسائر مالية للمجني عليه، مما يجعل محل الإعتداء في تلك الصورة هي الأموال وليس الأشخاص.[1]

ثانيا-سمات الجاني في الإبتزاز الإلكتروني.

يتميز المجرم في الإبتزاز الإلكتروني ببعض السمات التي تموه عن المجرمين الآخرين في الجرائم التقليدية وهذه السمات والخصائص تتمثل فيما يلي:

أ-المبتز إنسان إجتماعي بطبعه مسؤول عن أفعاله يجب أن يكون المبتز مسؤولا عن أفعاله الجرمية من الناحية القانونية الجزائية[2]. ولكي يكون الإنسان مسؤولا جزائيا، يشترط في إرادته أن تكون حرة ومختارة.[3]

وينبغي أن تكون موجهة بصورة مخالفة للقانون وهذه الإرادة تسمى بالإرادة الجرمية فهو إنسان إجتماعي بطبعه ولا تظهر عليه أي علامات الإجرام، يستطيع التحدث واستدراج الضحية من أجل ابتزازها، وتختلف دوافع اللهو أو الكبرياء أو الحصول على منفعة مالية من وراء الجريمة.[4]

ب-المهارة في مجال تكنولوجيا المعلومات.

يتمتع الجاني عادة في جرائم الإبتزاز الإلكتروني بالمهارة في استخدام وسائل الإتصال الإلكترونية الحديثة والإنترنت والمعلومات، بحيث يستطيع الجاني في بعض الأحيان الدخول إلى البيانات الشخصية والصور والفديوهات الخاصة بالمجني عليه عبر استخدام برامج

[1]-زهراء عادل سلبي، المرجع السابق، ص 62.

[2]-علي حسين الخلف، سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت 1982، ص 328.

[3]-أحمد فتحي سرور، الوسيط في قانون العقوبات -القسم العام-، الجزء 1،دار النهضة العربية، القاهرة ، 1981م،ص 456.

[4] - ا أحمد فتحي سرور،المرجع نفسه، ص77.

المعلومات والإنترنت ثم ابتزاز المجني عليه، لهذا فإن الجاني يتميز دائما في تلك الجرائم بالمهارة في استخدام تلك الوسائل التي تمكنه من ارتكاب الجريمة ومحو آثارها وأدلتها.[1]

ج-المبتز في الإبتزاز الإلكتروني يتمتع بالذكاء.

توجد العديد من الدراسات العضوية التي قام بها المختصون بدراسة الظاهرة الإجرامية[2] للوقوف على أهم العوامل التي تؤدي بالإنسان إلى ارتكاب الجريمة، توصلوا من خلالها إلى نتائج عدة أهمها أنهم قاموا بتقسيم المجرمين إلى أنواع ، وكل نوع يتصف بصفات معينة.

ومما لاشك فيه أن المجرم المعلوماتي يختلف عن المجرم الإعتيادي، فالقيام بارتكاب جريمة معلوماتية يتطلب على الأقل درجة من الدقة والذكاء لكي يتعامل مع جهاز الحاسوب ويختلق الشبكات المعلوماتية ويقوم بوضع فيروسات من شأنها اختراق برامج الحاسوب.[3]

وعليه، يمتاز مرتكبو هذه الجرائم في أغلب الأحيان بالذكاء،... أي أنهم ليسوا كالمجرمين التقليديين، لذا يرغبون في إثبات الذات، وتجربة ما يتمتعون به من قدرة علمية وتسخير ما لديهم من قدرات مالية وتقنية من أجل التفوق على النظم الإلكترونية واختراقها.[4]

وبالتالي يتمتع المجرم في جرائم الابتزاز الإلكتروني بقدر كافي من الذكاء الذي يمكنه من استدراج ضحيته والحصول على الثقة الوهمية والتحايل عليها بفكرة الحب والحنان والعاطفة والأسباب الملتوية المخادعة التي تمكن من استدراج الضحية ثم الحصول على الصور أو مقاطع شخصية فاضحة لها أو بيانات أو غير ذلك مما قد يسيء للفتاة عند نشره ويهددها بالنشر مالم تقوم بدفع أموال أو أن يطلب منها أعمال جنسية غير مشروعة، وكل ذلك يستلزم أن يكون هذا المجرم على قدر معقول من الذكاء[5].

---

[1]-عبد الإله محمد النوايسة، المرجع السابق، ص 85.

[2]-محمد شلال العاني، علي حسن طوالبة ، علم الإجرام والعقاب، ط ،1دار المسيرة، عمان، 1998م، ص57.

[3]-محمد علي العريان، المرجع السابق، ص 62.

[4]-آمال قارة، الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة الجزائر،2002 ، ص27.

[5]-عبد العزيز بن حمين، الإبتزاز ودور الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر في مكافحته، مركز باحثات لدراسات المرأة، بحوث ندوة الإبتزاز المفهوم، الأسباب، العلاج، فهرسة مكتبة الملك فهد الوطنية الرياض،1432هـ، ص58.

المبحث الثاني : تجريم الإبتزاز الإلكتروني.

إن معظم القوانين العربية و الدولية تعاقب على جنحة الابتزاز وكونها من الجرائم الخطيرة التي تلحق الكثير من الضرر للشخص في سمعته ونفسيته وحياته الخاصة لذا فان الكثير من القوانين تنظر الى جريمة الإبتزاز كجريمة مصنفة ضمن الجرائم الخطيرة، والتي تحدثت معظم القوانين عنها بصراحة وعالجت أغلب وقائعها وفرضت عقوبات على المجرم تصل إلى الحبس لسنوات وغرامات مالية ، حيث تتعامل معها على الأغلب الأجهزة الشرطية في الدول بكل سرية وبكل دقة وحرفية على أيدي أناس مدربين سواء خبراء في عالم التقنيات أو خبراء في القبض على المجرم المتخفي.

ولقد أولت معظم القوانين أهمية و مكانة بالغة للخصوصية الشخصية للأفراد أن لا يمسها خدش يطيح بها على المستوى الذي يتمتع به صاحبها ونتج عن ذلك بان تدخل القانون وفرض حمايته الجزائية على هذه المكانة الأدبية واعتبر الإعتداء عليها جريمة تصيب مركز المجني عليه حيث أن الجانب الأخلاقي هو أخطر ما قد تستهدفه الجريمة الإلكترونية وخاصة في المجتمعات العربية التي طالما اعتزت بمبادئها وقيمها الفاضلة فجريمة من هذا النوع كفيلة بأن تقضي على حياة الفرد، أو تفقد عائلته كرامتها وحتى انتمائها للمجتمع ، فالكثير منها ألصقت بها وصمة عار إذا ما تم نشر تلك الصور والبيانات الشخصية والتي لا يوافق على عرض هذه عموم الناس، ولقد تناولنا في هذا المبحث تجريم الإبتزاز الإلكتروني من خلال مطلبين أولهما هو أركان جريمة الإبتزاز الإلكتروني ،و الثاني يتناول الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني.

المطلب الأول : أركان جريمة الإبتزاز الإلكتروني.

يعتبر التهديد والإبتزاز الإلكتروني أسلوب من أساليب الضغط، يلجأ إليه المبتز للضغط على الضحية أو اجباره على الإذعان لمطالبه، مستغلا بذلك عدة طرق منها التهديد بالمساس بحرمة حياة الضحية الخاصة أو التشهير به، من ثمّة تتكوّن جريمة التهديد والإبتزاز الإلكتروني من عدّة أركان وسنوضح هذه الأركان في ثلاث فرع على النحو التالي:

الفرع الأول: الركن المادّي لجريمة الإبتزاز الإلكتروني.

يعتبر الركن المادّي للجريمة السلوك الذّي يظهر حيز وجود الجريمة، فهو يبرزها ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة التهديد الإلكتًروني في أركانها عن جريمة التهديد التقليدي، فهي تتطلب سلوك إجرامي يصدر من الجاني سواء بالقول أو الكتابة أو أي فعل أخر يتمثل في القيام بفعل التهديد بنشر البيانات أو الصور أو مقاطع فيديو للضحية، ولا يهم من أين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنّه عثر عليها في جهاز الضحية المسروق أو المعثور عليه، كما لا يشترط أن يتمّ التهديد بطريقة معينة، فيمكن أن يتمّ عن طريق الدردشة أو عن طريق البريد الإلكترًوني أو بتسجيل صوتي، كما لا يهم إن كان الإبتزاز لمصلحة المبتزّ المشروعة أو غير المشروعة، فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد لإرغام المجني عليه للقيام بذلك الفعل[1].

بالتّالي نجد ثلاثة عناصر الركن المادّي للجريمة تتمثّل في:

1. الفعل أو النشاط الإجرامي ومحاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه أو بالتهديد.[2]
2. الضرر والنتيجة المتحصّل عليها جرّاء هذا السلوك الإجرامي.
3. العلاقة السببية بينهما، أي المادّية أو النفعية أو الجنسية أو الإنتقامية.

[1]– مريم عراب، المرجع السابق، ص 1208.

[2]– تامر محمد صالح، الابتزاز الالكتروني: دراسة تحليلية مقارنة، بحث منشور في مجلة كلية الحقوق البحوث القانونية والاقتصادية، ع1، جامعة الإسكندرية، مصر،2018، ص 58.

فهي تتطلب سلوكا إجراميا، يتمّ عبر وسائل التواصل الإجتماعي أو الحاسب الآلي ويعتبر تهديدا كل قول أو كتابة أو رموز أو صور أو شعارات من شأنه إلقاء الرعب في قلب الشخص المهدّد أو المجني عليه، ولا يهم إن كانف الجاني ينوي تنفيذ الأمر التهديد أم لا، فقط يشترط أن يكون جديا وليس مجرد هزل.

الفرع الثاني : الركن المعنوي لجريمة الإبتزاز الإلكتروني

المسؤولية لا تقرر لمجرد وقوع الفعل المادي للجريمة فلا بدّ من دور الإرادة في الجريمة، أو ما يسمى بالقصد الجنائي الذي يتخذ صورتين القصد الجنائي العام والقصد الجنائي الخاص.

أي لابد ن يعلم الجاني بنتيجة السلوك الذّي يرتكبه والوقائع التّي تتصل بها والتّي تعدّ من عناصر الجريمة والعلم بموضوع الجريدة، فيجب أن ينصب علمه على أن ما يقوم به من الحصول على صور فاضحة لأحد الأشخاص وتهديده بهذه الصور مقابل الحصول على منفعة، تعدّ جريمة يعاقب عليها القانون، هنا يتحقق العلم وتكتمل أركان الجريمة.[1]

كما ينبغي أن يعلم أنّ فعل التهديد و الإبتزاز الإلكتروني يلحق ضررا بالمجني عليه، فلا عبرة في قيام القصد ان انصرفت الإرادة إلى هذه النتيجة إذ يكفي توقعها.

ولكي تقوم المسؤولية الجنائية يجب اثبات أنّ إرادة الفاعل اتجهت إلى القيام بهذا الفعل، وذلك دون أن تقع إرادته في عيب من عيوب الإرادة، كأن يكون مدركا وأنّه يحصل على معلومات وصور سرية خاصّة بالضحية من مستودع أسرار الأخير، فإن كان مكرها فلا يوجد قصد جنائي، ولا تقوم مسؤولية الفاعل المكره، كما أنّه لابد أن يتحقق القسم الثاني من الإرادة وهو إرادة النتيجة فلا بدّ أن تتجه إرادة الجاني إلى تحقق النتيجة الاجرامية من فعله بالحصول على المنفعة المادية أو المعنوية أو غير الأخلاقية، ويجب أن يكون التهديد جدّي بدرجة كافية للتأثير في نفسية المجني عليه.

الفرع الثالث: الركن الشرعي لجريمة الإبتزاز الإلكتروني

الركن الشرعي في الجريمة هو نص التجريم أو التحريم والعقاب، فهو النص الذي نستند اليه لتجريم فعل والعقاب عليه، وأن يكون هذا النص ساريا من حيث الزمان والمكان والأشخاص

[1]– مريم عراب، المرجع السابق، 1209.

على مرتكبي الفعل الإجرامي، ومن هذا ظهرت القاعدة القانونية الأشهر وهي: " لا جريمة ولا عقوبة بغير نص" وهو ما يعرف بمبدأ الشرعية الجنائية.

إن النتيجة الحتمية لمبدأ الشرعية الجنائية تتمثل في انحصار مصادر التجريم والعقاب في فكرة التشريع لأنه لا جريمة ولا عقوبة إلا بنص خاص، وهذا يعتبر ضمانا للمجرم بحيث لا توقع عليه أي عقوبة غير تلك المنصوص عليها، وبالتالي وأما التزايد المستمر للجرائم المعلوماتية، باشرت معظم الدول أليات قانونية تمثّلت في المواجهة التشريعية للإجرام على الصعيد الوطني، وذلك بمساهمة كل دولة بتشريعها الداخلي بإيجاد النصوص القانونية الكفيلة بمكافحة الجريمة وقمعها والردع لمرتكبيها، وذلك بحسب قدراتها وظروفها ومصالحها، فالبعض سارع لمواجهة الجريمة بسنّ تشريع مستقل والبعض الأخر اكتفى بتطبيق النصوص التقليدية.

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لمواجهة الجريمة المعلوماتية، خاصة مع ظهور شبكة الأنترنت التي ساهمت بشكل خطير في تفشي هذه الجريمة، فقامت الدولة بتبني نصوص عقابية خاصة بالجريدة المعلوماتية وقد ترددت في اختيار التقنية التشريعية المناسبة، فمنها من قام بإدماج نصوص خاصّة بالإجرام المعلوماتي في قانون العقوبات التقليدي ومنها من وضع قانون جنائي مستقل للمعلوماتية.

فالركن الشرعي في الجرائم المعلوماتية هو نص التجريم الواجب التطبيق على الفعل والعقوبة المقررة له، ومعظم الدول التّي تستعمل تكنولوجيا الإعلام والاتصال سنت تشريع جنائي تجرّم السلوك الذّي يرتكبه المجرم باستخدام وسائل تكنولوجيا الإعلام والاتصال والذّي يضر بمصلحة الأشخاص.

وبالرجوع للقانون الجزائري فنجد أنّ جريمة التهديد الإلكترونية بصفة عامة فلم تنل حضّها في قانون العقوبات، وبالرجوع للقواعد التقليدية الخاصة بجريدة التهديد وفق المواد من 284 إلى 287 من قانون العقوبات الجزائري، فقد عاقبت المادة 284 كل من هدّد بارتكاب جرائم القتل أو السجن أو أي اعتداء أخر على الأشخاص ممّا يعاقب عليها بالإعدام أو السجن المؤبد وكان ذلك بمحرر موقّع أو غير موقّع عليه أو بصور أو رموز أو شعارات يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 20.000 إلى 100.000 دج، إذا كان التهديد مصحوبا بأمر بإيداع مبلغ من النقود في مكان معين أو بتنفيذ أي شرط أخر[1].

وقد يكون التهديد كتابة أو شفاهة، فالمادة 287 من قانون العقوبات الجزائري تتضمن في فحواها: " بأنّه يعاقب بالحبس من ثلاث أشهر إلى سنة"، وبغرامة من 20.000 إلى 100.000دج، إذا كان ومصحوبا بأمر أو شرط التهديد بالعنف أو القتل.

المطلب الثاني: الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني

غالبًا ما تنشأ مشكلة الابتزاز الإلكتروني بسبب الممارسات الخاطئة والسلوكيات غير الأخلاقية. وقد يرجع ذلك إلى ضعف الوازع الديني لدى الناس أو الاستخدام الخاطئ لوسائل التواصل الاجتماعي.

الأمر يحتاج فقط للوعي والمعرفة والثقافة الإلكترونية التي تمكنك من عدم الوقوع في فخ أحد المجرمين الذين يتصيدون المجني عليه عن طريق جهلهم ببعض الأمور البسيطة وتكاد تكون بسيطة حيث أنك فقط تحتاج إلى أن تتحقق من بعض أمور وعندما تتأكد من عدم صحتها، يجب عليك فوارً أن تبتعد عن إتخاذ أي إجاراء من قبلك[2] وتنقسم حلول الإبتزاز الإلكتروني إلى حلول تخص أفراد مستخدمين الأنترنت، وحلول تخص الدولة، كذلك ومن بين أهم الحلول التي نرها قد تلعب دوارً مهما في الحد من الوقوع ضحية ابتزاز الكتروني الإهتمام بالجانبين التاليين، الجانب الوقائي الداخلي، والذي سنوضحه في الفرع الأول والجانب الخارجي في الفرع الثاني.

[1]- المشرع الجزائري، المادة 284 والمادة 287 من ق ع ج ، المتضمّن مكافحة الجريمة الإلكترونية المؤرخ 30ديسمبر سنة 2020 المتعلق بالتعديل الدستوري الجديد، الجريدة الرسمية.

[2]– جناجرة بلال، الأنترنت والإبتزاز الإلكتروني، 2019، ص21 .

الفرع الأول: الجانب الوقائي الداخلي.

وهي حلول تقع على مستخدمين الأنترنت فهناك مجموعة من الأسس الواجب اتخاذها من طرف الفرد الذي يستخدم شبكة الأنترنت، سواء في مكان علمه أو في الأماكن العامة أو حتى في بيته، حيث سنبين هذه الأسس كما يلي[1]:

يجب على الأشخاص الذين يستخدمون شبكة الأنترنت في الأماكن العامة والخاصة، أن يكون على قدر كاف من الحيطة والحذر، كأن يحذروا عندما يكتبون إسم المستخدم وكلمة السر لموقع ما[2].

وأن يختاروا كلمة سر قوية لحسابات مواقع التواصل الإجتماعي والبريد الإلكتروني، بحيث يطالبهم الموقع المعين بحفظ كلمة المرور فبمجرد كبسة واحدة على الزر موافق يكون الموقع قد احتفظ بكلمة السر حتى ولو تم مسح بيانات المتصفح في نهاية العمل، لذا يجب أن يكون حفظ كلمات السر للمواقع المسجل فيها في الأجهزة الشخصية الموجودة في البيت فقط[3].

ونشير في هذا الصدد إلى أن كل ما يقوم به الفرد الذي يستخدم جهاز الكمبيوتر المتصل بشبكة الأنترنت، يكون عرضة لمجموعة من الهجمات المقصودة وغير المقصودة، كأن يسجل في موقع لتعليم اختراق المواقع أو البريد الإلكتروني، فيكون هو ضحية أو أنه يقوم بمشاركة ملف من الملفات والتي تكون صورة أو فيديو أو برنامج معين، يحتوي على شفرات مخفية لا تظهر إلا بعد أن يتم النقر على الملف، وبالتالي يصبح جهازه عرضة لكل أنواع الإختراق و الجوسسة الإلكترونية[4].

إن جهاز الحاسوب عبارة عن أداة وليست غاية، حيث أن سرعة معالجة المعطيات ومختلف العمليات التي تدخل في تبويب وتصنيف البيانات بالإعتماد على برامج رئيسية وأخرى ثانوية تساهم في حل الكثير من مشاكلنا اليومية[5].

---

[1]– زيوش سعيد، ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الإجتماعية، العدد 22، جانفي 2017.، ص.84.

[2]زيوش سعيد، المرجع نفسه،ص 84.

[3]سعيد زيوش، المرجع السابق، ص_ص84-85 .

[4]سعيد زيوش، نفس المرجع، ص85 .

[5]المرجع نفسه.

لذا لا يجب أن نغفل عن مدى تعرض هذه البرامج للإصابة بنوع معين من الفيروسات التي قد لا تظهر للعيان في الوهلة الأولى، حتى باستخدام أقوى البرامج التي تكافح الفيروسات التي يتعرض بها الفرد للقرصة أو للإستحواذ في جهازه بما يحتويه من ملفات حتى ولو كانت تلك الملفات محمية بكلمات مرور.

لذا وجب تحصين جهاز الذي تتعامل معه سواء كان حاسب آلي أم هاتف محمول بأحد برامج الحماية من الفيروسات.

لذا يجب على الشخص المستعمل للأنترنت، الإبتعاد عن المواقع المشبوهة، والإبتعاد عن تصفح المواقع الجنسية مثلا، غالبا ما يكون هدفها تتبعك وسرقة معلوماتك وسرقة معلومات المتصفح الخاص بك ناهيك عن زرع برامج التجسس من غير علمك وتعتبر وسيلة إلى إسقاط الكثير من الأشخاص[1].

كما يجب أن لا يسجل الفرد المستخدم للأنترنت في مواقع غريبة ومريبة ، خاصة تلك التي توهمك بتعليم اختراق المواقع أو البريد الإلكتروني، أو توهمه بتحصيل المال عن طريق تبادل الملفات وغيرها من أساليب وطرق الإحتيال الإلكتروني[2]

وفي حالة حدوث خلل في الحاسوب أو الهاتف المحمول لا تقم في تصليحه إلا عند فني موثوق بسبب زرع برامج تجسس وفيروسات تنقل معلومات الجهاز للشخص الآخر[3].

_ابتعد تماما عن الفضول في الأنترنت خاصة إن لم تكن محترف في التعامل مع المواقع الغير موثوقة، كأن تجد رابط في بريدك أو في مواقع التواصل الإجتماعي بعنوان فاضح أو مثير للفضول بشكل غريب ويطلب منك إدخال معلومات خاصة بك كتسجيل الدخول مجدداً للبريد أو الحساب أو حتى أحياناً لا يحتاج الأمر إلى إرسال بياناتك إذ كان منشئ رابط التصيد الإحتيالي محترف فيرسلك إلى رابط يقوم بتحميل ملفات بشكل تلقائي إلى جهازك.

_لا ترسل أي صور شخصية لك لأي شخص كان، حتى لو صديقك أو صديقتك فربما هاتفه أو جهازه يتعرض للسرقة أو الإختراق وتقع أنت الضحية، فضلا على تغير نفوس الأشخاص.

---

[1] بلال جناجرة، المرجع السابق، ص21 .

[2] سعيد زيوش، المرجع السابق، ص 85.

[3] بلال جناجرة، المرجع السابق، ص 22.

لذا تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الأنترنت[1].

_تجنب قبول طلب صداقة من قبل أشخاص غير معروفين، وعدم الردود والتجاوب على أي محادثة ترد من مصدر غير معروف، والرفض التام لطلبات إقامة محادثات الفيديو مع أي شخص، مالم تكن تربطك به صلة وثيقة.

_لا تعط كلمة السر الخاصة ببريدك الإلكتروني أو حساباتك لأي شخص كان، ولا تجعل أحد يستخدم جهازك أو هاتفك خاصة إذا كان من خارج أفراد أسرتك، والقيام بفعل خاصية الغلق لحساباتك على مواقع التواصل الإجتماعي[2].

_الحضور والإستماع للمحاضرات والندوات التي تنبه الناس باستخدام الأمن للأنترنت وخبايا مواقع التواصل الإجتماعي[3]

_زيادة المستوى الثقافي لدى الأفراد ويأتي هنا دور المؤسسات الإجتماعية في توعية الأفراد ونشر حملات توعية ضد مخاطر الإبتزاز الإلكتروني.

_قبل شراء جهاز الكمبيوتر وجب على أفراد الأسرة أن يكونوا على إطلاع تام وواسع بمجال شبكة الأنترنت ومخاطرها وسلبياتها، وبفوائدها وايجابياتها، وأن يكون جهاز الكمبيوتر المتحصل بشبكة الأنترنت الموجودة بالبيت تحت رقابة الأسرة وأن لا يكون في غرفة المراهق والأطفال.

لذا يجب توعيتهم بالإستخدام الصحيح للأنترنت ومتابعة ما يتابعونه ومع من يتحدثون، فالأطفال من أبرز ضحايا الإبتزاز الإلكتروني لذا يجب أن يكون جهاز الكمبيوتر تحت مراقبة الأولياء، كما يجب أن يكون هناك توقيتا مخصصاً لاستعمال الجهاز[4].

كما يجب أن يكون الجهاز أو الأجهزة المتحصلة في البيت تحتوي على برامج لمكافحة الفيروسات، ويجب أن تكون خاضعة لنظام التحيين اليوم)،(La mise à jour) وهذا لإثراء قاعدة البيانات لدى هذه البرامج[5].

---

[1] بلال جناجرة، المرجع نفسه، ص23.

[2] – سعيد زيوش، المرجع السابق، ص 85.

[3] –سعيد زيوش ،المرجع نفسه،ص85.

[4] سعيد زيوش، المرجع السابق، ص.85

[5] رحيمة نمديلي، المرجع السابق ،ص106.

كما يجب على الأجهزة أن يكون بها جدار الحماية مفعل ومنتظم وهذا حتى يتم التعامل مع البرامج الخبيثة والضارة التي يقوم الجهاز بكشفها ومن ثم منعها من التجوال بحرية داحل الجهاز[1].

الفرع الثاني: الجانب الخارجي

ونقصد به " كل الأفعال التي من شأنها أن تؤدي إلى الحماية من التدخلات التي قد يتعرض لها الفرد جراء ولوجه المستمر لشبكة الأنترنت (بما فيها من مواقع، ومنتديات، وبرامج)...، وبالتالي يكون عرضة للعديد من الهجمات الإلكترونية وتكون ضارة وخطيرة أحيانا[2]."

ونشير في هذا الصدد إلى مجموعة من الإجراءات الواجب القيام بها بعدما يتأكد الفرد أن وقع ضحية ابتزاز عبر شبكة الأنترنت حيث سنعرضها كما يلي:

_يجب على الضحية التقرب من أقرب مصلحة أمنية مقر شرطة، مقر الدرك الوطني وتقديم شكوى مؤسسة على وقائع مبينة[3] لذا يجب الإهتمام بتزويد جهاز الشرطة بأحدث الأجهزة التقنية التي تراقب من يفعل فعلا ينتهك الأخلاق عبر الأنترنت، وزيادة الرقابة على مواقع التواصل الإجتماعي، فهي أكثر الأماكن التي ينتشر عليها الإبتزاز الإلكتروني لذا يجب على الدولة وضع رادع قانوني للأشخاص الذين يقومون بالإبتزاز الإلكتروني يمنعهم من هذا الفعل، ومحاسبتهم حسابا عسي اًر على ما يفعلوه[4] ووضع قانون أو لائحة تقنن من استخدام الأطفال الصغار للأنترنت فنجد كثي اًر أطفال في عمر 3سنوات و 4سنوات يستخدمون ألعابا وبرامج قد تكون خطيرة وتعرض أجهزة أهلهم إلى الإختراق ومن ثم الإبتزاز.

_يجب على الضحية عدم التمادي مع المبتز كأن يحاول أن يستعطفه أو يحاول أن يلبي رغباته، نتيجة ما يملكه هذه المبتز من ملفات شخصية (قد تكون صوتية، أو صور، أو فيديو).

---

[1] رحيمة نمديلي، المرجع السابق ،ص106.

[2] سعيد زيوش، المرجع السابق، ص 86.

[3] سعيد زيوش، المرجع السابق، ص 86.

[4] أنظر، أضرار الإبتزاز الإلكتروني، متوفر على الموقع، https://cyberone.com، اطلع عليه بتاريخ 10:30.، الساعة20224مارس28.

_ويجب على الضحية إخبار أفراد الأسرة بما وقع له من مشكل، كي يجد كل المساندة والدعم من طرف أهله[1] ويجب أن لا يخاف أبدا من التحدث إلى أهله وأصدقائه في حال تعرض لأي نوع من الإبتزاز أو الإهانة[2] يجب فصل الأنترنت عن الجهاز أو الأجهزة المتصلة في البيت تحت ما يسمى بالشبكة المحلية ،Le réseau localحيث لا يقوم المبتز بالسطو على الأجهزة الأخرى.

يجب عمل نسخة احتياطية ،Une sauvegardeعن كل البرامج والملفات التي يراها الفرد مهمة، وهذا كي يسهل الوصول إليها فيما بعد، خاصة إذا عمل مسح تام للجهاز والأقراص الصلبة التي تحتوي على المعلومات[3] وبالفعل حكومات بعض الدول نجدها لا تتأخر بتاتاً عن الإستجابة لشكوى في الإبتزاز مقبوضا الإلكتروني، فتقوم بدعم الضحية وتطمئنه، وخلال ساعات معدودة يكون المبتز عليه لينال جزاءه.

ونظرا للإنتشار الكبير الإبتزاز الإلكتروني ، خاصة في السنوات الأخيرة ونتيجة لما يترتب عليه من الآثار لا حصر لها، فجريمة الإبتزاز الإلكتروني جريمة معقدة متلفة الجوانب.

[1] سعيد زيوش، المرجع السابق، ص86.

[2] بلال جناجرة، المرجع السابق، ص22 .

[3] سعيد زيوش، المرجع السابق، ص86.

خلاصة الفصل الأول:

وفي ختام هذا الفصل يمكن القول أن هذا الفصل (الأول،) تناول ماهية الإبتزاز الإلكتروني، من خلال دراسة أحكامه العامة، كصورة من صور الجرائم الإلكترونية، فتم من خلال هذا الفصل إلى التطرق إلى مفهوم الإبتزاز الإلكتروني من خلال تعريفه لغويا واصطلاحا، وشرعيا، وفقهيا، وقانونا أين تم تحديد أنواعه بالنظر لشخص الضحية، والهدف المرجو من المجني عليه، ثم تعرفنا على خصائصه والسمات التي يتميز بها الجاني في جريمة الإبتزاز الإلكتروني، ثم تعرضنا إلى وسائل الإبتزاز الإلكتروني وأشكاله وآثاره المترتبة عليه، من خلال التطرق إلى طرق جريمة الإبتزاز الإلكتروني عبر وسائله الإلكترونية من حاسب آلي وملحقاته، الهاتف النقال وبرامجه، والأنترنت... ثم التطرق إلى أشكال الإبتزاز الإلكتروني من ابتزاز عاطفي الكتروني، ابتزاز الكتروني مادي،... والأسباب التي تؤدي إلى ارتكاب هذه الجريمة من أسباب إجتماعية، وأسباب نفسية، وأسباب تقنية، وأسباب اقتصادية.... ثم تجريم الإبتزاز الإلكتروني من خلال التعرض لدراسة أركانه (الشرعي، المادي، المعنوي وفي الأخير تم معالجة الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني، من خلال دراسة جانبيه الجانب الوقائي الداخلي، والجانب الخارجي.

اَلْفَصْل اَلْثاني: الإطار الإجرائي للإبتزاز الالكتروني

الفصل الثاني: الإطار الإجرائي للإبتزاز الإلكتروني

إن انفجار المعلومات التي شهدناها والتطور السريع والمستمر لهذه التكنولوجيا قد خلق العديد من الأنشطة الإجرامية التي تدق الأجراس الخطرة لتحذير المجتمع من حجم الخطر والخوف من الخسارة التي تسببها. ومن أهم التحديات التي تواجه مكافحة هذه الجريمة عدم كفاية مراسيمها وصعوبة الامتثال القانوني وإجراءات المتابعة.

بالرغم من خصوصية الجريمة الإلكترونية، و منها جريمة الإبتزاز الإلكتروني إلا أنها ما تزال تشكل سلوكا محضورا جرمه المشرع الوضعي، ونص على عقوبته مشددا هذه العقوبة في أحوال معينة و لأسباب نص عليها.

و تمر هذه الجريمة و بعد وقوعها بمراحل مرحلة جمع الإستدلات و التحقيق الجنائي، والذي يهدف إلى اكتشاف الجريمة و مرتكبها أو مرتكبيها ، فكل هذا البحث و التحقيق تكون أهدافه هو الوصول الى الحقيقة القانونية التي تحتاج الى دليل تتأكد معه نسبة التهمة الى المتهم بها، أو نفي الجريمة عنه لكي تكتمل خصوصية هذه الجريمة فلابد من القول بأن الدليل في الجريمة الإلكترونية و بالأخص في جريمة الإبتزاز الإلكتروني و هو دليل غير تقليدي، حيث يرتبط بالحاسوب و أجهزة الهواتف الذكية و ملحقاتها و البرامج و التطبيقات التكنولوجية، ففي جريمة الإبتزاز الإلكتروني الدليل ليس مضروفا فارغا لطلق ناري و ليس خصلة شعر من الضحية بل هو رموز و شيفرات و أجهزة و عناوين الكترونية، وهذه الأدلة التي يجوز أن يقبلها في حالة معينة ويحظر عليه أن يقبل أدلة سواها،و نتناول في هذا الفصل:

المبحث الأول : إجراءات التحقيق في جريمة الإبتزاز الإلكتروني وجهاته.

المبحث الثاني:الإثبات في جريمة الإبتزاز الإلكتروني.

المبحث الأول: إجراءات التحقيق في جريمة الإبتزاز الإلكتروني وجهاته.

الجرائم الإلكترونية بصفة عامة وجريمة الإبتزاز الإلكتروني بصفة خاصة هي في الأصل جريمة محضورة تشكل سلوك إجرامي يجرمه المشرع فجريمة الإبتزاز الإلكتروني مثل غيرها من الجرائم لها عناصرها، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى الجنائية في الجرائم العادية (التقليدية).

كما هو الحال في القصور التشريعي لتحديد كل جريمة معلوماتية على حدى، لإزالة كل غموض يحيط بها، فإن مظاهر الفراغ التشريعي تظهر أيضا في المجال الإجرائي الذي يواجه الطبيعة الخاصة للجريمة المعلوماتية بصفة عامة وجريمة الإبتزاز الإلكتروني بصفة خاصة.

وبالرغم من قيام الكثير من الدول بسن تشريعات جديدة، القائمة لمواجهة الجريمة المعلوماتية، إلا أنها لم تتوصل إلى تدارك كل ما يحيط بالجريمة من الجانب الإجرائي، كذلك بالنسبة للمشرع في الدول العربية لم يتدخل جديا لمواجهة هذا النوع من الجرائم بنصوص إجرائية خاصة، وأمام هذا القصور التشريعي تبرز مسألة صعوبة الأدلة جمع في مجال الجريمة المعلوماتية من جهة، ومن جهة أخرى صعوبة في تطبيق الإجراءات الجنائية التقليدية.

ونظرا لخصوصية جريمة الإبتزاز الإلكتروني فإن هناك صعوبات تثار أثناء التحقيق في هذه الجريمة و سنتعرض لهذه النقاط من خلال مطلبين الأول يتناول إجراءات التحقيق العامة و الخاصة في جريمة الابتزاز الالكتروني و المطلب الثاني يتناول الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الالكتروني .

المطلب الأول: إجراءات التحقيق العامة و الخاصة في جريمة الإبتزاز الإلكتروني.

يوجد نوعان من إجراءات التحقيق وسنبين ذلك خلال الفرعين التاليين:

الفرع الأول :إجراءات التحقيق العامة في جريمة الإبتزاز عبر الإبتزاز الإلكتروني.

تتشابه إجراءات التحقيق في الجريمة الإلكترونية مع إجراءات التحقيق في الجريمة التقليدية

فكلاهما، يحتاج الى المعاينة و التفتيش و الإستجواب و جمع وسائل الإثبات و فحصها المحافظة عليها من العبث بها أو ضياعها[1].

فقد تكون إجراءات التحقيق عملية كالتفتيش أو فنية كمضاهاة البصمات ،أو برمجية لتحديد كيفية الدخول الى المعطيات المخزنة في أجهزة الحاسوب.

أولا: الخبرة الفنية و تدريب الكوادر.

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

أ: الخبرة الفنية.

الخبرة هي وسيلة لتحديد التفسير الفني و التقني، بالإستعانة بالمعلومات العلمية فهي ، مستقلة عن الدليل القولي أو المادي و إنما هي تقييم لهذا الدليل. [2]و قد تعتمد الخيرة من أجل كشف الجريمة المعلوماتية و لابد ان تتماشى هذه الخبرة مع خصوصية الجريمة الإلكترونية.

و قد تعمل بعض البلدان على إعادة تأهيل بعض المجرمين المعلوماتيين من أجل الإستفادة من خبرتهم في الإختراق.

و على الخبير أن يتمتع بمؤهلات عالية ومقدرة فنية في تركيب الكمبيوتر و شبكة الأنترنت و التعامل مع الجريمة التي خلفتها التقنية الحديثة و كيفية عزل النظام المعلوماتي و الحفاض على الأدلة دون تلف [3].

---

[1] – داليا عبد العزيز ، المسؤولية الجنائية عن جريمة الابتزاز الالكتروني في النظام السعودي،دراسة مقارنة،مجلة البحث العلمي،العدد 25.2018 ص.72.

[2] رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبو بكر بلقايد،تلمسان2018 ص 271.

[3] – رابحي عزيزة، المرجع نفسه، ص 271.

المشرع الجزائري أجاز للمحقق الإستعانة بالخبرة ، و منه يطلب خبير في أي وقت إلى أن ينتهي التحقيق و هو أمر وجوبي في مجال الجرائم المعلوماتية التي تتطلب خبرة فنية بحتة لا يكشف غموضها إلا المتخصصون.

و من خلال نص المادة 05 من القانون 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها التي تنص على انه : (... يمكن للسلطات المكلفة بتفتيش المنظومة المعلوماتية التي تتظمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها).

و الجدير 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 اقاربه ، أو مصالحه الأساسية ، وذلك بموجب الأمر 15/02 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 الوطني للأدلة الجنائية وعلم الإجرام قسم الإعلام و الإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية .[1]

كما تسعى الأجهزة الأمنية المعنية بالتحقيق في استقطاب المتخصصين و الكفاءات في المجال المعلوماتي لضمهم إليها ليكونوا ضمن كوادرها و الإستفادة منهم.

و التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول و أجهزة العدالة لديها، فمثلا يتم إرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية و ذلك بالتعاون معى أجهزة النيابة العامة في الدول الأخرى و الهيئات الدولية بهدف الإطلاع على أحدث الأنظمة المقارنة من خلال عقد ندوات و مؤتمرات

[1] رابحى عزيزة ، المرجع السابق، ص 273.

وورشات عمل جماعي متخصصة في مواجهة تلك الجرائم، تعقد على المستوى الدولي أو الإقليمي.

حيث تسلط الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال مناقشة أبعادها، أخطارها و وسائل الوقاية بأساليب ووسائل تفوق تلك التي يستعملها مرتكبوها، فالتعاون الدولي في مجال تدريب الكوادر العاملين في أجهزة العدالة الجزائية و المعنيين بمكافحة الجريمة على المستوى الدولي والإقليمي يستهدف توحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة.

من خلال تبادل الخبرة . [1]

ثانيا : الإنتقال و معاينة مسرح الجريمة المعلوماتية.

فالإنتقال هو ذهاب مأموري الظبط القضائي، أو المحقق الجنائي الى مكان ارتكاب الجريمة حيث توجد آثارها و أدلتها.

أما المعاينة فهي تخص مكان أو شيئ أو شخص له علاقة بالجريمة وإثبات حالته، فالمعاينة تستلزم الإنتقال إلى محل الجريمة ، أو الواقعة، أو إلى أي محل آخر توجد به اشياء أو آثار يرى المحقق أن لها صلة بالجريمة غير أن المحقق قد ينتقل الى غرض آخر غير المعاينة كالتفتيش مثلا، و في جريمة الإبتزاز الإلكتروني يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها و كافة الإتصالات التي تمت من خلال الكمبيوتر أو الأنترنت، و المعاينة جوازية للمحقق ، شأنها شأن سائر إجراءات التحقيق فهي متروكة لتقديره، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في الجريمة التقليدية و ذلك لسببين:

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

– 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] رابحى عزيزة ، المرجع السابق، ص 274.

و كي تكون المعاينة لها فائدة في كشف الحقيقة عنها و عن مرتكبها فإنه ينبغي مراعاة عدة قواعد و ارشادات فنية ابرزها ما يلي:

-تصوير الحاسب و الاجهزة الطرفية المتصلة به و المحتويات و الأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب الآلي و ملحقاته ، و يراعي تسجيل وقت، و تاريخ ومكان التقاط كل صورة .

-ملاحظة الطريقة التي تم بها إعداد النظام و الآثار الإلكترونية خاصة السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الإتصال و نوع الجهاز الذي تم عن طريقه الولوج الى النظام و موقع الإتصال أو الدخول معه في حوار[1]

- تصوير الحاسب و الاجهزة الطرفية المتصلة به و المحتويات 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 و إثبات 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 إختبارات للتأكد من خلو المحيط الخارجي الموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن ان تتسبب في محو البيانات المسجلة[2].

- التحفظ على محتويات سلة المهملات من الأوراق الملقاة ، أو الممزقة و أدوات الكربون المستعملة و الشرائط ، و الأقراص الممغنطة ، و غير السليمة أو المحطمة وفحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

-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

[1] هشام فريد رستم ،الجوانب الإجرائية للجرائم المعلوماتية ملط مكتبة الآلات الحديثة، أسيوطن مصر، 1994 ،ص 59.

[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، الجزائر،2013 ،ص 86.

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.

عموما 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 الفقه على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها.

و يرجع عدم الاهتمام التشريعي بتعريف مسرح الجريمة إلى إعتبارين:

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

لا تقوم بشأن تحديد المجال الميداني لمسرح الجريمة ضاربة بين أطراف الدعوى العمومية.

فلا يجوز لأي طرف من أط ارف الدعوى العمومية أن يعترض على إجراء معاينة لمسرح الجريمة ،أو طريقة ،أو أسلوب تنفيذها، أو مجالها الميداني فهي إجراء يستهدف التعرف على أبعاد الجريمة ، و أركانها، 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].

و مسرح الجريمة في جريمة الإبتزاز 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 التعامل الأدلة و مع الموجودة في هذا المسرح لا يتم إلا على يد خبير متخصص في التعامل مع هذا النوع من الأدلة الرقمية.

ثالثا: التفتيش.

التفتيش في قانون الإجراءات الجزائية هو البحث عن شيئ يتصل بجريمة وقعت، و يفيد في كشف الحقيقة عنها، و عن مرتكبيها, و قد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة.

[1]صغير يوسف، المرجع السابق، ص76.

و قد أحاط القانون التفتيش بضمانات، فمحل التفتيش أما أن يكون مسكنا أو شخصا، و قد يكون متعلقا بالمتهم أو بغيره و هو في كل أحواله جائز مع الإختلاف في بعض الشروط.

التساؤل المطروح كيف نكون بصدد تفتيش عن حيثيات جريمة الإبتزاز الإلكتروني و مدى قابلية مكونات و شبكات الحاسب الآلي للتفتيش.

أ: مدى خضوع المكونات المادية للحاسب الآلي للتفتيش.

تفتيش المكونات المادية للحاسب الآلي بحثا عن شيئ ما يتصل بجريمة من جرائم الأنترنت يفيد في كشف الحقيقة عنها و عن مرتكبيها و تخضع للإجراءات القانونية الخاصة 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 مراعات التمييز بين ما إذا كانت مكوانت الحاسب الآلي المراد تفتيشها منعزلة عن غيرها من الحاسبات الأخرى أو متصلة 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 ، و المطاعم ، و السيارات العامة فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها التفتيش للأشخاص وبنفس الضمانات و القيود المنصوص عليها في هذا المجال . [1]

فالتفتيش على المكونات المادية للنظام المعلوماتي لا إشكال فيه . حيث نصت المادة 44 من قانون الإجراءات الجزائية الجزائري ، ورد فيه بأن التفتيش يكون على الأشياء و هي كلمة للتصرف على الأرجح على المكونات المادية، مع الأخذ بعين الإعتبار 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

[1] صغير يوسف، المرجع السابق، ص 77.

مسكنه و بنفس الضمانات المقدرة قانونا، فالقانون الجزائري في نص المادة 64 من قانون الإجراءات الجزائية الجزائري.[1]

والتي قيدت ممارسة هذا الإجراء بالشروط التالية:

-الحصول على إذن تفتيش من وكيل الجمهورية واستضهار هذه المذكرة قبل بدء العملية و تتضمن مذكرة التفتيش البيانات التالية : وصف الجريمة محل البحث والتحري عنوان الأماكن التي سيتم تفتيشها عدم ذكر هذه البيانات يؤدي إلى بطلان إجراء التفتيش.

-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. [2]

أن يجري التعشيش بعد الساعة الخامسة 05 صباحا ، 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 ونهارا.

هذا و قد 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 ونهارا ، و دون التقيد لشرط حضور صاحب المسكن أو ممثليه إذا تعلق الأمر بالجرائم التالية : .... الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات. [3]

ب مدى خضوع مكونات الحاسب المعنوية للتفتيش.

أثار تفتيش المكونات المنطقية للحاسب الآلي جدلا كبيرا لدى الفقه بشأن جواز تفتيشها. فذهب جانب من الفقه إلى 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

[1] أنظر المادة 64 قانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 45 ق ا ج ج.

[3] رابحي عزيزة ،المرجع السابق ،ص280.

على أن يفتش الحاسب الآلي لابد أن يشمل المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي ، لأن الغاية الجديدة من التفتيش بعد التطور الثاني الذي حدث بسبب ثورة الإتصالات ترتكز على البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي[1].

أما المشرع الجزائري فإنه استجاب للرأي القائل بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة و على هذا الأساس أجاز تقشيش المعطيات و لكن بموجب نص جديد و هو المادة 05 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها ، حيث سمحى للضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 من هذا القانون ، و من بين هذه الحالات توفر معلومات عن احتمال الإعتداء على منظومة معلوماتية على نحو يهدد النظام أو الدفاع الوطني، أو مؤسسات الدولة، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكذا منظومة تخزين معلوماتية .[2]

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. [3]

و في هذه الأيام يتم التمييز بين ثلاثة احتمالات:

الإحتمال الأول : إتصال حاسب المتهم بحاسب 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؟

---

[1]صغير يوسف، المرجع السابق ،ص 78.

[2]رابحي عزيزة، المرجع السابق، ص 282.

[3]صغير يوسف، المرجع السابق، ص 79.

بالنسبة للمشرع الجزائري، حيث نصت المادة 05 في الفقرة (أ) من هذه المادة. إذا كانت هناك أسباب تدعوا للإعتقاد بأن المعطيات المبحوث عنها في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك. [1]

الإحتمال الثاني: ايصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة، فطبقا لهذا الإحتمال يمكن أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكة الإتصال البعيدة بهدف عرقلة سلطات الإدعاء في جمع الأدلة.

وقد أجاز المشرع الجزائري تفتيش الأنظمة و لو كانت خارج إقليم الدولة و ذلك بموجب المادة 5 في فقرتها 03 من القانون 04/09 حيث أجاز النص الحصول على المعطيات المبحوث عنها و المخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني، و التي يمكن الدخول إليها إنطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل. [2]

و حسب م 2/16 من نفس القانون : من واجب سلطات التحقيق الجزائرية أن تقدم جميع التسهيلات المراقبة الإتصالات و تفتيش المنظومات المعلوماتية الموجودة على التراب | متى طلب منها ذلك مع مراعاة مبدأ المعاملة بالمثل ، و الإتفاقيات الدولية. [3]

و حسب المادة 18 من نفس القانون [4]أورد المشرع الجزائري استثناءات على طلب المساعدة القضائية و هي 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 و بشرط عدم استعمالها في غير الأغراض التي أدت إلى تجميعها.

الإحتمال الثالث: التنصت و المراقبة الالكترونية لشبكات الحاسب الآلي ، فالتنصت و الأشكال الأخرى للمراقبة الإلكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف

---

[1] رابحي عزيزة، المرجع السابق ،ص 282.

[2] انظر، المادة 3-5 في 09/04 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكالمتها.

[3] انظر، المادة 16 في 09/04 من القانون نفسه.

[4] أنظر، المادة 18 في 04-09 من القانون نفسه.

معينة في جميع الدول تقريبا مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة 04 الفقرة ج من القانون 09/04 أجاز النص استثناءا المراقبة الالكترونية للوصول الى الحقيقة و اشترط 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، ثم يحضر قاضي التحقيق الذي يتولى مباشرة التحقيق، فالنيابة العامة توجه الإتهام و قاضي 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 و بالتالي أي مسكن آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها و كل شيئ آخر يفيد في 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 قانون الإجراءات الجزائية حيث ان قاضي التحقيق سلطته مقيدة بمنح الإنابة بشرط إستحالة قيامه بالإجراء بنفسه نظرا لخطورة السلطات التي يمتلكها قاضي التحقيق و منها التفتيش.

اما ضابط الشرطة القضائية فإن 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 أعظاء 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 [2].

[1] أنظر، المادة في 09/04 من القانون نفسه.

[2] رابحي عزيزة، المرجع السابق، ص 286.

الفرع الثاني: إجراءات التحقيق الخاصة في جريمة الإبتزاز الإلكتروني.

نظرا لسرعة إرتكاب الجريمة الالكترونية و سهولة محو آثارها ، جعل أمر إكتشافها صعب للغاية، لذا استحدث التشريع الجزائري على غرار التشريعات الحديثة إجراءات خاصة من أجل ضبطها قبل تفاقم خطرها، و يمكن تقسيم هذه الإجراءات الخاصة الى نوعين الإجراء الأول: مراقبة الإتصالات الإلكترونية أما الإجراء الثاني : حفظ المعطيات المتعلقة بحركة السير.

أولا- مراقبة الإتصالات الإلكترونية.

تعتبر المراقبة من أهم مصادر التحري سواءا في الجرائم التقليدية أو المستحدثة كجرائم الأنترنت و هي ما يعرف بالمراقبة الإلكترونية، و قد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية في اعتراض المراسلات ، و تسجيل الأصوات والتقاط الصور.

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

إن أساليب التحري الخاصة تمس حرمة الحياة الخاصة المكفولة دستوريا. [1]

و من أجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 الذي طرأ عليه وفق قانون 06/22 الذي حصر وجوبية اللجوء إلى مثل هذا الإجراء على الجرائم السنة الخطيرة و من بينها الجريمة المعلوماتية . [2]

و تتمثل هذه الاساليب في:

-اعتراض المراسلات.

-التقاط الصور.

تسجيل الاصوات.

[1] المادة 39 من دستور 1996 ، المعدل.

[2] القانون رقم 05-22 مؤرخ في 29 ذي القعدة 1427 الموافق لـ 20 ديسمبر 2006 يعدل و يتمم قانون الاجراءات الجزائية.

أ- اعتراض المراسلات.

المراسلات هي جميع الخطابات و الرسائل والطرود و البرقيات و المشرع الجزائري في المادة 65 مكرر ق إ ج ج حصر مفهوم المراسلات في التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية فقط ، و بالتالي استبعد المراسلات العادية.

ب: تسجيل الأصوات.

يقصد به مراقبة الأحاديث و تسجيلها وكل الإتصالات التي تتم عن طريق سلكي، أو لا سلكي أي أن عمليات المراقبة تشمل كل أدوات الإتصال 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 اشخاص . [1]

ج: إلتقاط الصور.

هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة اشخاص يتواجدون في مكان خاص و تقسم هذه الإجراءات بالسرية التامة لأنها بها مساس بحرمة الحياة الخاصة للاشخاص المكفولة دستوريا.

وقد عرفت الفقرة 03 من قانون 04/09 مراقبة الإتصالات الإلكترونية حيث تشمل الإتصالات السلكية و اللاسلكية و الخلوية كالفاكس و البريد الإلكتروني، و مواقع الدردشة حتى المنتديات، و ساحات الرأي و النقاش التي تسمح بنقل الأفكار و المعلومات. [2]

ثانيا : حفظ المعطيات المتعلقة بحركة السير.

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

أ: تعريف المعطيات المتعلقة بحركة السير.

المعطيات المتعلقة بحركة السير هي تلك المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها تلك الأخيرة باعتبارها جزء من حلقة الإتصال، توضح مصدر الإتصال و الوجهة المرسلة إليها و الطريق الذي سيسلكه ووقت و حجم الإتصال و نوع الخدمة.[3]

---

[1] أنظر، المادة 65 مكرر 650 مكرر 10 ق.ا.ج تعديل 2006.

[2] انظر، المادة 11 في قانون 09/04.

[3] انظر، المادة 12 في قانون 09/04.

أما مقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو مستعمليها . المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها. أما بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفترة أ من هذه المادة و كذا تلك التي تسمح بالتعرف على مصدر الإتصال و تحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداءا من تاريخ التسجيل.

ولا تعرض مقدمو الخدمة الى العقوبات المقدرة في المادة 11 من القانون 09-04 [1]

المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني.

تتميز الجرائم التي ترتكب عبر الأنترنت بكون محلها معلومات أو برامج معالجة آلية عبر الحواسيب أو جرائم تتعلق بالأشخاص عبر عالم إفتراضي غير متناهي و غير محدود مما يعطيها طابع خاص ليس فقط في طريقة إرتكابها ، و بل كذلك في الوسيلة التي ترتكب بها، الأمر الذي ينجم عنه صعوبات إكتشاف الجريمة و التحقيق فيها.

فهي تتنوع بين صعوبات متعلقة بالجريمة و الجهات المتضررة ، وصعوبات متعلقة بالجانب القضائي.

الفرع الأول: صعوبات إكتشاف الجريمة المرتكبة عبر الأنترنت الإبتزاز الإلكتروني.

يعترض إكتشاف الجريمة المرتكبة عبر الأنترنت عدة صعوبات و ذلك راجع إلى عدة اعتبارات منها ما هو متعلق بفقدان الآثار المادية للجريمة ، و منها ماهو راجع للتكتم الضحية و منها ما هو راجع النقص الخيرة لدى سلطات التحقيق.

أولا : فقدان الآثار المادية للجريمة.

تضل الجريمة المرتكبة عبر الأنترنت مجهولة ما لم يبلغ عنها للجهات المعنية بالإستدلالات 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

[1] أنظر المادة 11 في في قانون 09/04.

طريق نقل معلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي ، و شبكة الإتصالات بصورة آلية كما تنساب بالكهرباء عبر الأسلاك. [1]

و يكفي الضغط على زر في لوحة الإستخدام 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 الرقمية، فإن البيانات التي تشمل عليها لا تتضمن آثار أو بصمات يمكن الإستدلال 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. [2]

ثانيا: 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 انفعالهم غير المشروعة قبل إرتكابها كي لا يقعوا تحت طائلة العقاب، كما يقوم المجرمون عبر الأنترنت بإخفاء هويتهم أو انتحال شخصيات أخرى حتى لا يمكن التعرف عليهم حال إكتشاف 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.[3]

[1] صغير يوسف، المرجع السابق، ص 117.

[2] المرجع نفسه ، ص 118.

[3] نفسه، نفس ص.

ثالثا: التكتم عليها من قبل المجني عليه.

غالبا ما يلجأ الضحية في هذه الجريمة إلى التكتم ، وغالبا ما يكون مصرفا أو مؤسسة مالية أو شركة أو مشروعا صناعيا ضخما.[1]

و يعرض المجرمون على عدم الإبلاغ عن الجريمة التي راحت ضحيتها من أجل إخفاء أساليب إرتكابها للحيلولة دون تقليد الآخرين للجناة ، كذلك للتستر على معلومات لا يجب الإبلاغ عنها خاصة إذا كانت الضحية شركات التأمين أو البنوك[2].

رابعا : نقص خبرة سلطات الإستدلال.

قد تكون شخصية المحقق مثل التهيب من إستخدام الكمبيوتر و التهيب من إستخدام الإنترنت ، و عدم الخبرة الكافية و عدم الإهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية ، 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، [3]كذلك أجهزة العدالة المقاومة لهذه الجرائم المرتبطة بالتقنية يبدأ بالتكوين و التشكيل عقب ظهور هذه الجرائم و هو أمر يستغرق الوقت فعدم توازي سرعة تقدم التقنية ذاتها والحركة التشريعية، أو الثقافة القانونية أو الأمنية، حيث لا تسيران بذات المعدل مما يعكس سلبا على إجراءات الإستدلالات، و التحقيقات في الدعوى الجنائية مما يستدعي ضرورة تأهيل سلطات الأمن وجهات التحقيق و الإدعاء و الحكم في شأن هذه الجرائم[4].

[1]– صغير يوسف ، المرجع السابق، ص 120.

[2]صغير يوسف، مرجع نفسه، ص 121.

[3]خالد عباد الطلبي إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت، ط 1 دار الثقافة للنشر والتوزيع، د ب ن 2011، ص 224.

[4]صغير يوسف، مرجع سابق، ص 121.

الفرع الثاني : صعوبات متعلقة بالجانب القضائي.

يفترض الطابع الخاص لهذا النوع من الجرائم تعاون أكثر من دولة. لكن هذا القصور مقارنة بتفاقم و تطور هذه الجريمة يشكل فارق شاسع بين الجريمة ، حيث من الناحية القانونية غير موجودة لأنها من قواعد النظام العام.

و قد 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 ، ومتابعة مرتكب هذه الجريمة لعدة إعتبارات:

أولا : قصور التعاون القضائي الدولي في مكافحة جريمة الإبتزاز الإلكتروني.

يعتبر التعاون الدولي في مجال مكافحة الجريمة الإلكترونية عموما و جريمة الإبتزاز الإلكتروني من أصعب المواضيع المطروحة على هذا المستوى بسبب الإختلافات القائمة في الممارسات بين الدول و التشريعات ، و كذلك سبب العدد المحدود نسبيا من المعاهدات ، و الإتفاقيات المتاحة للدول بشأن التعاون الدولي الذي يعد مطلبا تسعى للتحقيقه كل دولة، إلا أنه له معوقات تقف دون تحقيقه[1].

ثانيا: عدم وجود نموذج موحد للنشاط الإجرامي.

نظرا لاختلاف المفاهيم الخاصة بالجريمة واختلاف التقاليد ، و الأعراف القانونية الدولية فإن ذلك يضعف منظومة القانون الدولي في مجال ضبط تلك الجرائم، مما يسهل إفلات الجناة من المسائلة الجنائية ، و ذلك بسبب عدم توفر تعريف موحد للجريمة فتكون مجرمة في تشريع و في تشريع آخر مباحة .[2]

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] صغير يوسف، المرجع السابق، ص 133.

[2] صغير يوسف، المرجع نفسه، ص 134.

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

ثالثا: تنوع واختلاف النظم القانونية الإجرائية.

إن اختلاف النظم القانونية الإجرائية و التحقيق والمحاكمة قد تثبت فاعليتها في دولة ما و قد تكون عديمة الفائدة في دولة اخرى و قد لا يسمح بإجرائها كما هو الشأن بالنسبة للمراقبة الإلكترونية و التسليم المراقب ، و غيرها من الإجراءات.

رابعا : عدم وجود قنوات إتصال.

إن عدم الإتصال بين الدولة لجمع الأدلة ، و المعلومات يعيق التعاون الدولي في مجال مكافحة الجريمة ، فعدم التعاون والتنسيق بين الدول فيما يخص الأجراءات ، و جمع الإستدلالات و التحقيق خاصة ، و أن الحصول على دليل في هذه الجريمة قد يكون خارج نطاق الدولة هو أمر له غاية في الصعوبة. [2]

خامسا : مشكلة الإختصاص في جريمة الإبتزاز عبر الوسائل الإلكترونية.

ينجم عن اختلاف التشريعات و النظم القانونية تنازع في الإختصاص بين الدول فقد يحدث أن ترتكب هذه الجريمة في إقليم دولة من طرف أجنبي، فهنا تكون هذه الجريمة خاضعة للإختصاص الإقليمي للدولة الأولى، طبقا لمبدأ الإقليمية وتخضع للإختصاص للدولة الثانية على أساس مبدأ الإختصاص الشخصي، و قد تهدد أمن وسلامة دولة اخرى فتدخل في اختصاصها إستنادا لمبدأ العينية. و يرتبط بمشكلات الإختصاص والقانون الواجب التطبيق مشكلات إمتداد انشطة الملاحقة و التحري و الضبط و التفتيش خارج الحدود مما أعاق التعاون الدولي و شنت الجهود في مكافحة هذه الجريمة[3].

[1] رابحي عزيزة ،المرجع السابق ،ص 329.

[2] صغير يوسف، المرجع السابق ، ص 135.

[3] نفس المرجع، ص 136.

سادسا : التجريم المزدوج.

يجد شرط التجريم المزدوج أساسه في أن الدولة طالبته التسليم الذي تهدف به إلى متابعة من نسب إليه السلوك الإجرامي أو تنفيذ العقوبة عليه ، و بالتالي لابد أن يكون السلوك مجرما في تشريعها و إلا فلا يتصور وجود دعوى عمومية، أو ملاحقة جزائية أو تنفيذ عقوبة جزائية.[1]

سابعا : صعوبات الإنابة القضائية الدولية.

إنبثقت الإنابة القضائية الدولية من الواجبات و الإلتزامات التي يفرضها القانون الدولي على الأمم المتحدة و بموجبها 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 طرف الدولة المطلوب منها المساعدة القانونية[2].

الفرع الثاني: الصعوبات التي تواجه المحقق (جهات التحقيق) في جريمة الإبتزاز الإلكتروني.

يعتبر التحقيق في جرائم الإبتزاز الإلكتروني، أمرا ليس بالهين بسبب الصعوبات التي تواجه المحقق أمام جريمة ما زالت غامضة، حتى أن عدم التمكن من السيطرة على مجريات التحقيق، قد يؤدي إلى فقد الثقة في المجتمع، وزيادة نسبة الجريمة.[3] وتتمثل هذه الصعوبات في:

أولا: الحق في الخصوصية.

غالبية الدول جرمت التعدي على حياة الإنسان الخاصة باستخدام شبكة الأنترنت، وقد نص عليها ميثاق الأمم المتحدة سنة 1948م.[4] ومنها المادة 15 منه على أنه " لا يعرض أي شخص لتدخل تعفسي في حياته الخاصة، أو أسرته، أو مسكنه، أو رسائله أو شن حملات

[1] صغير يوسف، المرجع السابق ، ص 137.

[2] صغير يوسف، المرجع نفسه، ص 138.

[3] مريم أعراب، مرجع سابق، ص 1214.

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

على شرفه وسمعته ولكل شخص الحق في طلب حماية القانون له من هذه التدخلات أو تلك الحملات[1].

ثانيا: نقص الخبرة.

نقصد بها هي مهارة تتطلب توفرها لرجال التحقيق للوصول إلى مراحل متقدمة من الخبرة والمعرفة للعمل في مثل هذه الجرائم، ومازالت جهات التحقيق والضبط تعاني من قلة الخبرة الفنية وقلة التدريب على التعامل مع الأدلة الإلكترونية وكيفية البحث والإستدلال وهو بمثابة ثغرة كبيرة في النظام الجنائي[2].

كما أن خبرة التحقيق مع المجرم الذكي له طبيعة خاصة، سيما أنه يحاول الهرب من الجريمة، حيث أن المحقق الجنائي في جرائم الإبتزاز الإلكتروني يجب أن يكون له تكوين تقني، فيجب أن يجمع بين مهارة استخدام التقنية الحديثة، وكذلك مهارة تقييم الجريمة الإلكترونية، ومدى الخطورة الإجرامية لمرتكبها، وكذلك مهارة التعرف على المكونات المادية للأجهزة وعلى ملحقاتها من طابعات ومساحات ضوئية وكاميرات. [3]

ثالثا : تنازع الإختصاص.

هي مشكلة تؤرق عمل جهات الضبط والتحقيق لأن جريمة الإبتزاز الإلكتروني من إحدى مشكلاتها، أي أنها قد تكون عابرة للحدود الإقليمية للدولة، بحيث يكون الجاني من دولة والمجني عليه من دولة أخرى، بحيث يتنازع كل قانون في محل تطبيق العقوبة المقررة في حق الجاني بحسب النظام الذي تتضمنه العقوبة والقانون الواجب التطبيق.[4]

[1] مريم أعراب، مرجع سابق، ص 1214.

[2]- وائل سليم عبد الله شاطر، الإطار القانوني لجريمة الإبتزاز الإلكتروني، في6 الألعاب الإلكترونية دراسة مقارنة وفق النظام السعودي والقانون الكويتي، المجلة العربية لنشر العلمي، تاريخ الإصدار 2 شباط 2020 ، المملكة العربية السعودية، ص 439.

[3]- عراب مريم ، المرجع السابق ، ص 1216.

[4]- نفسه، نفس ص.

المبحث الثاني: الإثبات في جريمة الإبتزاز الإلكتروني.

لإثبات جريمة الإبتزاز الإلكتروني يجب استحداث وسائل حديثة تختلف عن ما يتم اعتماده في الجريمة التقليدية، و هذا راجع الى عجز إجراءات التحقيق التقليدية في مجاراة نسق تطور هذه الجريمة، بالإضافة إلى عجز الأدلة الجنائية المادية في اثبات وقوعها، مما يستلزم اعتماد الأدلة الجنائية الرقمية. و قد تناول هذا المبحث مطلبين، المطلب الأول: ماهية الدليل الجنائي الرقمي ، أما المطلب الثاني: صعوبات الإثبات. وسنوضح ذلك بما يلي:

المطلب الأول: طرق الإثباث في جريمة الإبتزاز الإلكتروني.

كما هو مقرر قانونا فإن جريمة الإبتزاز الإلكتروني تكمن في صعوبة إثباتها، لأنها تتم عن طريق وسائل تقنية معقدة، وتتم في مسرح رقمي، وكل هذا ينعكس على مدى حجية الدليل الرقمي المتحصل عليه من سلسلة إجراءات التحري والإستدلال[1] .

الدليل الرقمي، ويعني مفهومه في إيجاد الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواس وشبكة الأنترنت وهذا الدليل تبنته معظم التشريعات وذلك بتحديد الشروط التي يجب توافرها في الدليل الرقمي حتى يمكن قبوله من قبل القضاء الجزائي.[2]

وبهذا الصدد سنتطرق في هذا المطلب إلى ماهية الدليل الرقمي كفرع أول و أما الفرع الثاني سيتم التطرق فيه الى شروط صحة الدليل الرقمي و مصادر الحصول عليه.

[1]- العرفي فاطمة، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون، مجلة صوت القانون، المجلد 8 ، العدد خاص 2، 2022،ص499.

[2]- مريم عراب المرجع السابق، ص 1222.

الفرع الأول : ماهية الدليل الجنائي الرقمي.

للتعرض الى ماهية الدليل الجنائي الرقمي لابد من توضيح مفهومه و ذلك من خلال تعريفه و تبيان خصائصه، كذلك شروط صحة الدليل الرقمي و مصادر الحصول عليه.

أولا : 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.

1: تعريف الدليل الرقمي.

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

باستخدام برامج تطبيقات و تكنولوجيا، 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 [2].

و قد عرفه البعض الآخر، 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.[3]

فالدليل الرقمي هو الدليل المشتق الأصل عن البراميجية و المعلوماتية و أجهزة و معدات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية و فنية لتقديمها للقضاء بعد

---

[1] ممدوح عبد الحميد بن عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، بدار الكتب القانونية، مصر، 2006، ص 77.

[2] ممدوح عبد الحميد بن عبد المطلب، المرجع نفسه، ص 78.

[3] محمد الأمين البشري، التحقيق في الجرائم المستحدثة بطل، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004،ص234.

تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أصوات ، لاثبات وقوع الجريمة، أو لتقرير البراءة أو الإدانة[1].

و يحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي كوسيلة لإثبات الإبتزاز الإلكتروني، فيتطلب إجراء خطوات جمع الأدلة.

ثانيا : خصائص الدليل الرقمي.

الدليل الرقمي له خصائص تميزه عن غيره من الأدلة الجنائية التقليدية، و هذا يعود للبيئة الافتراضية التي يستخلص منها هذا الدليل، حيث أن هذه البيئة هي بيئة متطورة بطبيعتها و التي تنعكس على هذا الدليل مما أضفت عليه خصائص لا تتوفر في باقي الأدلة الجنائية.

وهذا ما سيتم توضيحه من خلال العناصر الأتية :

أ: دليل علمي غير مرئي.

فهو يتميز بالطبيعة الفنية ، حيث يتكون من بيانات ومعلومات ذات صفة الكترونية غير ملموسة ولا تدرك بالحواس العادية، فتقوم الجهات القضائية بتمريره على البرامج المختصة لمعرفة ما اذا تم العبث بهذا الدليل العلمي الذي يخضع لقاعدة لزوم التجاوب مع الحقيقة كاملة وفق قاعدة (أن القانون مسعاه العدالة، أما العلم فمسعاه الحقيقة) فبحكم الطبيعة الخاصة للدليل الإلكتروني، فإنه لا يجب أن يخرج عما توصل إليه العلم الرقمي وإلا فقد معناه[2].

ب: دليل قابل للنسخ.

حيث تتيح التكنولوجيا المعلوماتية استخراج نسخ من الأدلة الرقمية إلى محقق جنائي، و فني متخصص لديه المهارة الفنية و التقنية لاستخلاص ، و جمع الأدلة الرقمية .

[1]– ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية، دراسة تأصيلية تطبيقية، رسالة ماجيستير ، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا السعودية، 2012، ص 74.

[2]– نفس المرجع، نفس ص.

فالدليل الرقمي يتكون من بيانات و معلومات إلكترونية غير ملموسة. و يتطلب إدراكها الإستعانة بأجهزة و برامج معينة لتقديم معلومات بشكل نصوص مكتوبة، أو صور أو أصوات أو غيرها بترجمة البيانات الرقمية المخزنة على الأجهزة الالكترونية و شبكة الأنترنت لاثبات الواقعة المطلوب اثباتها في الجرائم الالكترونية ، و نسبتها إلى الشخص المشتبه فيه[1].

و قد استدعى واقع التقدم التقني الإستعانة بالخبراء و المختصين.

ويختلف الإعتبار بحجية الدليل الرقمي و اعتبارها حجة في إثبات الدعوى أو نفيها ، باختلاف النظم القانونية فنجد الدول التي تأخذ بمبدأ التقييم الحر لهذه الأدلة الرقمية فيكون لدى القاضي الجنائي الأخذ بجميع الأدلة و المعلومات الكافية بإستبيان الدليل العلمي و الإفتراضي.

يعد تقييم مدى اعتماد المحكمة على تلك الأدلة، و يكون هذا في النظام الأنجلوساكسوني أو ما تأخذ بمبدأ الترافع بحيث يكون لدى الخصم مناقشة الشاهد لفحص و إفادته بالمعلومات الكافية.

ج صعوبة طمس الأدلة الرقمية.

الأدلة الالكترونية (الرقمية) يمكن استرجاعها بعد محوها و إصلاحها بعد إتلافها ، مما يؤدي إلى صعوبة التخلص منها[2]. و هي من أهم الخصائص التي تميزه مقارنة بالدليل التقليدي، فهناك الكثير من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة 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 بواسطة تقنية جمع المعلومات و البيانات المقترفة لإرتكاب لمثل هذه الجرائم، بواسطة تطبيقها بوسائل الإعلام المتطورة.

[1] ثنيان ناصر آل ثنيان، المرجع السابق، ص74.

[2] – نفس المرجع، نفس ص.

وهو ما يمكن استخراج نسخ منه لها نفس الحجية و القوة الثبوتية.

د: الدليل الجنائي الرقمي متنوع ومتطور.

مفهوم 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 ومنه فالآثار الرقمية المستخلصة متنوعة بما تحتويه من معلومات عن وقائع قد تشكل جريمة، فتصبح أدلة براءة أو إدانة، ومن بينها صفحات المواقع الالكترونية، الصور، الفيديوهات الرقمية، والملفات المخزنة في الحاسب الآلي الشخصي أو المعلومات المتعلقة بمستخدم شبكة الأنترنت وغيرها.

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 و مصادر الحصول عليه.

ونبين ذلك من خلال شروطه و مصادر حصوله و فقا للترتيب التالي:

أولا: شروط صحة الدليل الرقمي.

هذه 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، و هذا ما سنستعرضه في الآتي:

[1] رابحي عزيزة، المرجع السابق، ص270.

أ: يجب أن يكون الدليل الرقمي غير قابل للشك.

أي لابد أن يكون يقيني[1]. 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[2]. فمن خلال ما يعرض عليه من مخرجات الكترونية، فما ينطبع في ذهنه من تصورات و

احتمالات بالنسبة لها، سيحدد قوتها الإستدلالية على صدق نسبة الجريمة المعلوماتية الى شخص معين من عدمه[3].

ب: يجب أن يكون الدليل الرقمي متحصل عليه بصورة مشروعة.

فالمشروعية هي التوافق والتقيد بأحكام القانون في إطاره و مضمونه العام فهي تهدف إلى تقرير ضمانة أساسية لحماية الحقوق والحريات 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.

وعليه ينبغي على القاضي أن يستقي قناعته في الحكم من خلال أدلة مشروعة ، أما الأدلة التي جاءت ناتجة عن إجراءات غير قانونية وباطلة، فلا يجوز الإعتماد عليها كما يجب استبعاد كل دليل معيب حتى وإن استندت في إصدارها الى أدلة أخرى مشروعة إلى جانب الدليل الباطل و المعيب[4].

ج :يجب أن يكون الدليل الرقمي قابلا للمناقشة.

لا يعتمد القاضي إلا على الدليل الذي تم مناقشته عند المرافعة ، وجاهيا ، و يشترط أن يكون علنيا حضوريا من قبل أطراف الدعوى[5].

---

[1]– ممدوح عبد الحميد بن عبد المطلب، المرجع السابق، ص125.

[2]– نهلا عبد القادر المومني، مرجع سابق،52.

[3]ممدوح عبد الحميد بن عبد المطلب، المرجع السابق، من 125.

[4]رابحي عزيزة ،المرجع السابق، ص 255.

[5]أنظر، المادة 212 ق إ ج ج المعدل والمتمم.

فالأدلة المتحصلة من جرائم الحاسب الآلي و الأنترنت، ستكون محلا للمناقشة عند الأخذ بها كوسيلة اثبات أمام المحكمة فيجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي بالمواجهة بصفة مباشرة أمام القاضي الجزائي لذا المحكمة الإبتدائية.

فلا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة اليه في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه و تكون علانية[1].

و متى كان للأدلة أصل في ملف الدعوى ولا يمكنه بناء اقتناعه على مادار خارج التحقيقات، أو أدلة لم يطلع عليها الخصوم و لم يتمكنوا من مناقشتها.[2]

ثانيا: مصادر الحصول على الدليل الرقمي.

تعتمد جهات التحري والتحقيق على مصادر لتحصيل الدليل الرقمي من المصادر التي يسمح لها القانون و المتمثلة في اجراء الارشاد الجنائي ، و اجراء الوضع تحت المراقبة الالكترونية، و تعاون مقدمي خدمات الانترنت مع السلطات القضائية[3].

أ: إجراء الإرشاد الجنائي.

الذي يقوم بمقتضاء ضباط الشرطة القضائية بتجنيد أحد عناصرها للولوج للعالم الاقتراضي و بالأخص عبر حلقات النقاش و قاعات الدردشة و الاتصال المباشر، مستعملين صفات وهمية من أجل الكشف عن هذه الجرائم و كشف المجرمين.

فهذا الإجراء لا يتطلب جهد مادي كبير، حيث يقوم به ضباط الشرطة القضائية ، أو يكلف غيره من ذوي الاختصاص، و هذا بعد الحصول على إذن رسمي للقيام بمهام البحث والتحري عن الجرائم و ضبط مرتكبيها[4].

وضح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت اسم التسرب من خلال نصوص المواد 65 مكرر 05 الى غاية المادة 65 مكرر 18 (ق.إ. ج. ج) بعد الحصول

[1] رابحي عزيزة ، مرجع سابق، ص256.

[2] المرجع نفسه، ص 257.

[3] عدي جابر هادي، مرجع سابق،ص158.

[4] نهلا عبد القادر المومني، مرجع سابق،ص57.

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.

و هي من أهم مصادر البحث والتحري سواء في الجرائم التقليدية أو المستحدثة، و يقصد بها مراقبة شبكة الجرائم المعلوماتية (Cyber surveillance) ، و تسمى بذلك بالمراقبة الالكترونية[2].

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 المعلوماتية عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الإتصال السلكية واللاسلكية. كما أجاز كل الترتيبات التقنية لها دون علم المعنيين و لا موافقتهم، بغية الحصول على تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة ، وذلك باذن من وكيل الجمهورية[3].

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 آدائها على طائفة معينة من المتعاملين معه بعقد من العقود، وقد عرف المشرع الجزائري مقدم الخدمة بموجب المادة 02 في القانون 09/04 بأنه:[4]

"...1-أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و / أو نظام للاتصالات.

2- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها..." .

---

[1] أنظر، المادة 65-مكرر، من في ق إج ج المعدل والمتمم.

[2] عزيزة رابحي، مرجع سابق، ص297.

[3] نهلا عبد القادر المومني، مرجع سابق، ص53.

[4] أنظر، المادة 2 من قانون 04/09 المعدل و المتمم.

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

المطلب الثاني : صعوبات الإثبات في جريمة الإبتزاز عبر الوسائل الإلكترونية.

نظرا لكون هذه الجريمة تتم في الخفاء، و من يرتكبها يتصف بمعرفة التقنية و الذكاء، و بالرغم من الجهود المبذولة لمكافحة الجريمة الالكترونية ، و جريمة الإبتزاز الإلكتروني بوجه خاص ، إلا أنه هناك بعض المعوقات و الصعوبات التي تواجه السلطات المختصة في الإثبات بالدليل الرقمي و ذلك العدة أسباب أهمها:

الفرع الأول: معوقات مرتبطة بالدليل ذاته.

أولا: سهولة محو الدليل.

حيث أن الجناة بعد ارتكابهم للجريمة يحرصون على محو أي آثار للتهديد و الإبتزاز مما يجعل الوصول للدليل صعب وفي بعض الأحيان يكون مستحيل[1].

ثانيا : صعوبه الكشف عن هويه الجاني من خلال الدليل الرقمي.

تتم جريمة الإبتزاز الإلكتروني في بيئة افتراضية تحكمها الرموز و البيانات و تخلو من العنف الظاهر و الآثار المادية كالجريمة التقليدية مما يصعب الوصول لدليل مادي، كبصمات الأصبع أو نقاط الدم، مما يجعل الوصول للجاني معترض بالعقبات[2].

[1] نهلا عبد القادر المومني، مرجع سابق، ص54.

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

ثالثا: عرقلة الوصول للدليل.

قد يضع الجاني عقبات فنية لمنع كشف جريمته من خلال أدلتها وذلك بتشفير الملفات الرقمية قصد حجب المعلومات عن التداول و منع الوصول إلى مصدر الارسال[1].

رابعا: صعوبات متعلقة بنقص الخبرة.

من بين الصعوبات التي تواجه عملية الحصول على دليل رقمي في جريمة الابتزاز الالكتروني، نقص الخبرة لدى بعض العاملين في جهات التحقيق و من رجال الضبط القضائي و رجال النيابة العامة .

فيما يخص مهارة استخدام أجهزة الحاسب الآلي وملحقاتها ومهارات الاستجواب للمجرم الالكتروني في جرائم الإبتزاز الإلكتروني، لذا من الضروري جدا الإهتمام وتطوير وتأهيل العنصر البشري من محققين و رجال الضبط القضائي لمواكبة مثل هذا النوع من الجرائم و يتطلب أيضا متابعة العنصر البشري للأمور التقنية و كل مستجد على الساحة[2].

خامسا: صعوبات متعلقة في إحجام المجني عليه على الإبلاغ.

إن عدم الإبلاغ من قبل المجني عليه سبب رئيسي في تكوين الصعوبة التي تواجه السلطات المختصة، وبالتالي فإن هذا الإحجام يساعد على إختفاء الدليل الرقمي ، و بالتالي يكون هذا سبب في تكوين عقبة تقف كحجر عثرة في طريق الاثبات عن طريق الدليل الرقمي فكل ذلك يعود إلى خوف المجني عليه من الإبلاغ كي لا يفتضح أمره ، فهذه الجريمة أرتكبت أساسا بسبب خوف المجني عليه من أن يكتشف أسراره[3] .

[1] غنية باطلي ،المرجع السابق ، ص46.

[2] غنية باطلي، المرجع نفسه، ص ص46-47.

[3] نهلا عبد القادر المومني، مرجع سابق، ص58.

ملخص الفصل الثاني:

يعالج هذا الفصل، الإطار الإجرائي لجريمة الإبتزاز عبر الوسائل الالكترونية، و ذلك بتسليط الضوء على الإجراءات العامة والخاصة، وكذا الإشكالات الإجرائية التي تثيرها هذه الجريمة من ناحية التحقيق من خلال التطرق إلى صعوبات إكتشاف الجريمة والصعوبات المتعلقة بالجانب القضائي، وإشكالية القانون الواجب التطبيق، و كذا الإجراءات المرتبطة بالإثبات في الجريمة موضوع الدراسة، والتي تعرضنا فيها إلى خصوصية هذه الإجراءات، كما تعرضنا لأهم وسائل الإثبات التي تخص هذه الجريمة، و هو الدليل الرقمي، وذلك من خلال التطرق إلى مفهومه، وشروط صحته، وكذا صعوبات الإثبات المرتبطة بالدليل الرقمي في حد ذاته وكذا صعوبات التعاون الدولي، والصعوبات المتعلقة بالمساعدات القضائية، وتدريب الكوادر لذا لجهات المختصة.

خاتمة

خاتمة .

جريمة الإبتزاز الإلكتروني من الجرائم المستحدثة ، و يطلق عليها في علم الجريمة الجرائم الناعمة، التي تخلو من العنف ، و هي احدى صور الجريمة الإلكترونية، فجريمة الإبتزاز الإلكتروني هي الوجه الآخر لجريمة الإبتزاز التقليدية التي تنشأ وترتكب في عالم مادي

و في مسرح جريمة تقليدي حيث يترك فيه الجاني أثر ، أما الابتزاز الالكتروني فيتم في عالم افتراضي مليء بالرموز و الشيفرات و يزداد التحدي حين نجد العقبات و الصعوبات التي تواجه أجهزة التحقيق في التعامل مع الدليل الرقمي.

قد أصبحت هذه الجريمة تشكل هوسا لدى مستخدمي التكنولوجيا الحديثة، بعد التطور السريع للتكنولوجيا الرقمية ، و أمام هذه الثورة حاولت الدول تطوير تشريعاتها لتواكب هذه الجرائم المستحدثة، ثم تنبهت لضرورة إقرار نصوص تشريعية خاصة بهذه الجريمة الالكترونية.

وبعد الإنتهاء من دراسة موضوع البحث جريمة الابتزاز الإلكتروني، التي استعرضنا من خلالها الإطار الموضوعي للجريمة الذي تحدثنا عن ماهية الإبتزاز الالكتروني وتجريمه من خلال القانون 07-18، كما تطرقنا الى الإطار الإجرائي للجريمة موضوع البحث من خلال التطرق الى التحقيق في الجريمة و الإثبات فيها، وأخيرا الى أهم النتائج و المقترحات.

ونلخصها فيما يلي:

أولا: النتائج:

وتتمثل كما يلي بيانها:

1- جريمة الإبتزاز الإلكتروني صورة من صور الجريمة الإلكترونية حيث تتم باستخدام الوسائل التقنية الحديثة.

2-لجريمة الإبتزاز الإلكتروني وسائل وطرق مختلفة في ارتكابها تختلف عن الإبتزاز 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.

3-تتحقق جريمة الإبتزاز الإلكتروني 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 الإمتناع عنه.

4-جريمة الإبتزاز الإلكتروني قد تتسبب في جرائم بعدها كالزنا أو القتل أو جريمة عنف أو سرقة.

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

6- لم تشترط التشريعات العربية و منها الجزائرية أن يبلغ التهديد درجة من الجسامة ، إذ نجد نصوصهم بينت أن كل شخص هذه شخصا آخر، أو ابتزه لحمله على القيام بفعل أو الإمتناع عنه، و لو كان القيام بهذا الفعل أو الإمتناع مشروعا، كما أنه لا عبرة لموضوع

و نوع التهديد، فقد يكون بالقول أو بإنزال ضرر بالمجني عليه عن طريق التشهير به عبر إرسال مجموعة من الرسائل النصية عبر الهاتف النقال لمجموعة من الأشخاص بهدف حمل المجني عليه للقيام بعمل.

7- جريمة الإبتزاز الإلكتروني لها خصوصية في التحقيق و تستلزم فريق عمل من المختصين أو المؤهلين لاستيعاب التطورات الحديثة في التحقيق مع مجرمين.

8- جريمة الإبتزاز الإلكتروني جريمة صعبة الإثبات حيث أنه من السهل محو آثارها

و تحتاج لعمل شاق كي يتم إثباتها.

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.

المقترحات: ونلخصها وفقا لما يلي توضيحه:

1- ضرورة استحداث نصوص قانونية إجرائية تتلائم مع رجال الضبط والتحقيق في المجال الإفتراضي، لأن جريمة الإبتزاز الإلكتروني أكثر تطور مستقبلا، والأجيال القادمة تكون أكثر خبرة.

2-الإتصال فورا بالجهة المختصة لأنها الأقدر للتعامل مع الجاني، مع عدم مسح المحتوى محل الإبتزاز مهما كان جد حميمي وحساس ومحرج، وتسليمه للجهات الأمنية لأنه يشكل دليل إدانة الجاني.

3-ضرورة رفع مستوى التعاون الدولي وتعزيز هذا التعاون في مجال مكافحة هذه الجرائم من خلال الإتفاقيات الدولية، لأن جرائم الإبتزاز الإلكتروني عابرة للحدود.

4-تدريب 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.

5- لابد من ضرورة نشر الوعي داخل المجتمع بأخطار جريمة الإبتزاز الإلكتروني، مع اتخاذ كل الإجراءات الإحترازية للحيلولة دون وقوع الأشخاص ضحايا للإبتزاز الإلكتروني، وتشجيع من يتعرض للإبتزاز بالإبلاغ عن الجريمة، للتخلص منها دون إبلاغ.

6-ضرورة عدم بقاء الضحية لوحده والإسراع بطلب الدعم المادي والمعنوي من شخص موثوق فيه، من أخصائيين نفسانيين واجتماعيين حتى يتم تجاوز المحنة.

قائمة المصادر والمراجع

قائمة المراجع:

-المراجع باللغة العربية :

أولا: -الكتب.

1- أحمد فتحي سرور، الوسيط في قانون العقوبات -القسم العام-، الجزء1، دار النهضة العربية، القاهرة ، 1981م.

2- حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الإجتماعي، دار النهضة العربية، مصر، 2018.

3- خالد حسن أحمد، جرائم الانترنت بين القرصنة الالكترونية وجرائم الإبتزاز الالكتروني دراسة مقارنة، ط1، دار الفكر الجامعي، الإسكندرية، 2018.

4- خالد عباد الطلبي، إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت، ط 1 دار الثقافة للنشر والتوزيع، د. ب. ن، 2011.

5- دالياعبد العزيز، المسؤوليةالجنائيةعنجريمةالابتزاز الالكترونيفيالنظامالسعودي،دراسة مقارنة،مجلة البحث العلمي ،العدد25، 2018.

6- زهراء عادل سلبي، جريمة الإبتزاز الإلكتروني -دراسة مقارنة-، ط ،1دار الأكاديميون للنشر والتوزيع، ..2010.

7- عبد الإله محمد النوايسة، جرائم تكنولوجيا المعلومات-شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمان، الأردن،2017.

8- علي حسن الطوالبة، الجرائم الإلكترونية، مطبعة جامعة العلوم التطبيقية، البحرين ،2008.

9- علي حسين الخلف، سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، مطابع الرسالة، الكويت، 1982.

10- غنية باطلي، الجريمة الالكترونية. دراسة مقارنة، الدار الجزائرية للنشر والتوزيع، دلس الجزائر، .2016.

11- القاضي علي الزيدي، جريمة الإبتزاز الالكتروني، دراسة مقارنة، ط 1، مكتبة القانون المقارن، بغداد،2019.

12- محمد الأمين البشري التحقيق في الجرائم المستحدثة بطل، جامعة نايف العربية للعلوم الأمنية، السعودية، 2004.

13- محمد على سالم، حسون عبيد، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، مجلد ،14العدد2 العراق، 2007.

14- محمد علي العريان، الجرائم المعلوماتية، انعكاسات دورة المعلومات على قانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

15- محمود أحمد عبانية، جرائم الحاسوب وأبعاد الدولية، دار الثقافة للنشر والتوزيع، عمان الأردن، 2009.

16- مدحت رمضان، جرائم الإعتداء على الأشخاص والأنترنت، دار النهضة العربية، القاهرة، 2000.

17- ممدوح عبد الحميد بن عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، بدار الكتب القانونية، مصر، 2006،

18- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

19- نورة بنت عبد الله بن محمد المطلق، ابتزاز الفتيات أحكامه وعقوبته في الفقه الإسلامي، كلية الشريعة، جامعة الإمام محمد بن سعود الإسلامية، السعودية، 2012.

20- هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، ملط مكتبة الآلات الحديثة، أسيوط مصر، 1994.

❖ **ثانيا: الرسائل.**

أ-أطروحات دكتوراه:

1. رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص، جامعة أبو بكر بلقايد،تلمسان،2018.

ب-رسائل الماجيستير.

1. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري -دراسة مقارنة- رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2019.
2. ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة ماجيستير ، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2012.
3. 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، 2013.

❖ **ثالثا:المقالات.**

ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجني عليه من الإبتزاز، مقال منشور على الشبكة الالكترونية، المجلة العربية للدراسات الأمنية، المجلد33 ، العدد79، الرياض،2017 .

❖ **رابعا:المجلات و الدوريات.**

1. الحسين عبد العزيز بن حمين بن أحمد، الإبتزاز ودور الرئاسة العامة لهيئة الامر بالمعروف والنهي عن المنكر في مكافحته، بحث مقدم لندوة الإبتزاز: المفهوم، الاسباب، العلاج، جامعة الملك سعود، 2011.

2. ذياب موسى البدانية، الجرائم الإلكترونية المفهوم والأسباب، ورقة علمية مقدمة خلال الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، خلال الفترة من2 إلى 9 لسنة 2014/، عمان- الأردن، 2014.
3. العرفي فاطمة، حجية الدليل الرقمي في إثبات جريمة الإبتزاز الإلكتروني في القانون، مجلة صوت القانون، المجلد 8 ، العدد خاص 2، 2022،ص499.
4. رحيمة نمديلي، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية،" مركز جيل البحث العلمي، طرابلس، 25-24مارس2017م.

❖ **خامسا:الوثائق المستخرجة من المواقع الإلكترونية.**

1. معجم المعاني الجامع، في شرح مفهوم لفظة ابتزّ، تمّ تصفّحه من موقع المعاني، من على الرابط https://www.almaany.com/fa/dict/ar-fa/، بتاريخ 2024/04/18 على الساعة 02:51.
2. أنظر، أضرار الإبتزاز الإلكتروني، متوفر على الموقع، https://cyberone.com، اطلع عليه بتاريخ 10:30.، الساعة20224مارس28.

ب-النصوص التنظيمية الجزائرية .

- النصوص القانونية.

1. قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.
2. القانون رقم 05-22 مؤرخ في 29 ذي القعدة 1427 الموافق لـ 20 ديسمبر 2006 يعدل و يتمم قانون الاجراءات الجزائية.
3. القانون 04-09 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

4. قانون العقوبات، المتضمّن مكافحة الجريمة الإلكترونية المؤرخ 30 ديسمبر سنة 2020 المتعلق بالتعديل الدستوري الجديد، الجريدة الرسمية العدد 3، 2020.
5. مرسوم المادّة رقم 18-07 المؤرخ يوم 10 جوان 2018 المرتبط بحماية الأشخاص الطبيعيين من الجرائم الإلكترونية أو المتّصلة بتكنولوجيا الإعلام والإتصال.
6. مرسوم المادّة رقم 40 المؤرخة يوم 06 مارس 2016 المرتبطة بانتهاك حرمة الأفراد والإبتزاز والتشهير الإلكتروني.

فهرس المحتويات

فهرس المحتويات

شكر وتقدير .....

الإهداءات .....

مقدمة 1

الفصل الأول: ماهية الابتزاز الالكتروني 5

المبحث الأول :مفهوم الإبتزاز الالكتروني.....6

المطلب الأول : تعريف الابتزاز الالكتروني ومدى خطورته......7

الفرع الأول : تعريف الابتزاز الإلكتروني. 7

أولا : لغة. 7

ثانيا: إصطلاحا......8

ثالثا: الفقهي.....9

رابعا–الإبتزاز الإلكتروني بالنسبة للمشرع الجزائر. 10

الفرع الثاني: مدى خطورة الابتزاز الالكتروني.....11

المطلب الثاني : أنواع الإبتزاز الإلكتروني و خصائصه. 13

الفرع الأوّل: أنواع الإبتزاز الإلكتروني. 13

أولا- التهديد والإبتزاز الإلكتروني من حيث المجني عليه.....13

ثانيا- التهديد والإبتزاز الإلكتروني من حيث الهدف المقصود. 15

الفرع الثاني: خصائص الإبتزاز الإلكتروني.....17

أولا-الخصائص العامة للابتزاز الإلكتروني. 18

ثانيا-سمات الجاني في الإبتزاز الإلكتروني. 22

المبحث الثاني : تجريم الإبتزاز الإلكتروني......24

المطلب الأول : أركان جريمة الإبتزاز الإلكتروني.....25

الفرع الأول: الركن المادّي لجريمة الإبتزاز الإلكتروني.....25

الفرع الثاني : الركن المعنوي لجريمة الإبتزاز الإلكتروني.....26

الفرع الثالث: الركن الشرعي لجريمة الإبتزاز الإلكتروني 26

المطلب الثاني: الحلول المقترحة للحد من الوقوع ضحية الإبتزاز الإلكتروني 28

الفرع الأول: الجانب الوقائي الداخلي. 29

الفرع الثاني: الجانب الخارجي 32
خلاصة الفصل الأول: 34
الفصل الثاني: الإطار الإجرائي للإبتزاز الإلكتروني.....36
المبحث الأول: إجراءات التحقيق في جريمة الإبتزاز الإلكتروني وجهاته. 37
المطلب الأول: إجراءات التحقيق العامة و الخاصة في جريمة الإبتزاز الإلكتروني. 37
الفرع الأول :إجراءات التحقيق العامة في جريمة الإبتزاز عبر الإبتزاز الإلكتروني. 37
أولا: الخبرة الفنية و تدريب الكوادر. 38
ثانيا : الإنتقال و معاينة مسرح الجريمة المعلوماتية.....40
ثالثا: التفتيش.....42
الفرع الثاني: إجراءات التحقيق الخاصة في جريمة الإبتزاز الإلكتروني. 48
ثانيا : حفظ المعطيات المتعلقة بحركة السير.....49
المطلب الثاني: الصعوبات التي تواجه جهات التحقيق في جريمة الإبتزاز الإلكتروني. 50
الفرع الأول: صعوبات إكتشاف الجريمة المرتكبة عبر الأنترنت الإبتزاز الإلكتروني. 50
أولا : فقدان الآثار المادية للجريمة.....50
ثانيا: فرض الجناة لتدابير أمنية.....51
ثالثا: التكتم عليها من قبل المجني عليه. 52
رابعا : نقص خبرة سلطات الإستدلال. 52
الفرع الثاني : صعوبات متعلقة بالجانب القضائي. 53
أولا : قصور التعاون القضائي الدولي في مكافحة جريمة الإبتزاز الإلكتروني. 53
ثانيا: عدم وجود نموذج موحد للنشاط الإجرامي.....53
ثالثا: تنوع واختلاف النظم القانونية الإجرائية.....54
رابعا : عدم وجود قنوات إتصال.....54
خامسا : مشكلة الإختصاص في جريمة الإبتزاز عبر الوسائل الإلكترونية. 54
سادسا : التجريم المزدوج.....55
سابعا : صعوبات الإنابة القضائية الدولية.....55
الفرع الثاني: الصعوبات التي تواجه المحقق (جهات التحقيق) في جريمة الإبتزاز الإلكتروني. 55
أولا: الحق في الخصوصية.....55
ثانيا: نقص الخبرة. 56
ثالثا : تنازع الإختصاص. 56
المبحث الثاني: الإثبات في جريمة الإبتزاز الإلكتروني.....57

المطلب الأول: طرق الإثبات في جريمة الإبتزاز الإلكتروني. 57
الفرع الأول : ماهية الدليل الجنائي الرقمي. 58
أولا : مفهوم الدليل الجنائي الرقمي. 58
ثانيا : خصائص الدليل الرقمي.....59
الفرع الثاني: شروط صحة الدليل الرقمي و مصادر الحصول عليه.....61
أولا: شروط صحة الدليل الرقمي. 61
ثانيا: مصادر الحصول على الدليل الرقمي. 63
الفرع الأول: معوقات مرتبطة بالدليل ذاته.....65
أولا: سهولة محو الدليل.....65
ثانيا : صعوبه الكشف عن هويه الجاني من خلال الدليل الرقمي.....65
ثالثا: عرقلة الوصول للدليل. 66
رابعا: صعوبات متعلقة بنقص الخبرة. 66
خامسا: صعوبات متعلقة في إحجام المجني عليه على الإبلاغ.....66
ملخص الفصل الثاني:.....67
خاتمة 69

قائمة المصادر والمراجع.....72
ملخص. 83

ملخص

ملخص.

تعد الجريمة ظاهرة اجتماعية تُصاحب كافة المجتمعات وتعوقها عن التقدم والتطور، لذا يصفها الغالب من شراح القانون الجنائي بأنها سلوك اجتماعي مُضاد للمجتمع ومخالف للقانون ولثقافة المجتمع، والجريمة على هذا الأساس توجد في كل المجتمعات مع اختلاف ملامحها وأشكالها وأساليب ارتكابها ، وبسبب الظواهر الإجرامية المستحدثة والخطرة تسعى هذه الدراسة إلى محاولة تحديد معالم جريمة الابتزاز الإلكتروني، التي تعتمد على استخدام وسائل الاتصال الحديثة، وشبكات الإنترنت، لما لهذه الظاهرة من خطورة بالغة على الأفراد والمجتمع من خلال انتهاك حق من حقوق الإنسان المهمة، وهو حقه في الحياة الآمنة والهادئة بعيدا عن القلق والرعب، إذ إنها تنعكس سلبا على حياته. ومن الجدير بالذكر أن جريمة الابتزاز الإلكتروني تمر بعدة مراحل تبدأ بحصول المبتز على مادة الابتزاز المتمثلة بالصور أو مقاطع صوت أو فيديو أو معلومات سرية أو بيانات وينتج عنها أن الضحية تمر بحالات صراع داخلية تؤثر على نفسيته نتيجة تهديد وترهيب من قبل المبتز من أجل الحصول على مقابل سواء كان ماديًا أو معنوياً، وبالتالي تكون الضحية رهينة في يد المبتز عند خضوعها وتنفيذها الأوامره خوفًا من الفضيحة، ولا سيما أن للوسائل الإلكترونية دورًا كبيرًا وفعالا في ارتكاب الجرائم الإلكترونية، كونها تمثل أرضا خصبة تساعد على ممارسة الجرائم الإلكترونية عموما وجريمة الابتزاز الإلكتروني خصوصا، إذ إنها غزت جميع نواحي الحياة وسيطرت عليها، بل تحكمت في معظمها، إذ إنها جريمة عالمية جاوزت الحدود الإقليمية بين الدول.

ولعل سبب تحريم الابتزاز الإلكتروني ما يمثله من اعتداء على خصوصية الأفراد وما تشكله من خطورة على المجتمع، إذ إن من أهم طرق الإثبات التي تختص بجريمة الابتزاز الإلكتروني، ألا وهي الدليل الرقمي، إذ إن هناك صعوبات تواجه أجهزة التحقيق وطرق تعاملهم مع الدليل الرقمي من أجل الوصول للحقيقة، لا سيما أن الجرائم الإلكترونية تتم في عالم افتراضي غير ملموس، وبالتالي فإن مسرح الجريمة افتراضي مملوء بالرموز والشفرات، فلا بد من وضع نصوص خاصةٍ تشمل كافة صور السلوك في جريمة الابتزاز الإلكتروني، وتعكس مدى خطورتها وسهولة ارتكابها، فضلا عن صعوبة إثباتها.

Abstract

The crime is a social phenomenon that accompanies all societies and impedes it from progress and development, so most of the criminal law is described as a social behavior that is against society and contrary to the law and the culture of society, and the crime on this basis is found in all societies with different features, forms and methods of committing it, and because of the new and dangerous criminal phenomena seeks to seek This study is to try to define the features of the crime of electronic blackmail, which depends on the use of modern means of communication and Internet networks, because of this phenomenon of great danger to individuals and society by violating an important human rights, which is his right to safe and calm life away from anxiety and terror, It reflects negatively on his life. It is worth noting that the crime of electronic blackmail is going through several stages that begins with the extreme obtaining the blackmail of pictures, audio clips, video, secret information or data, and it results in that the victim is going through internal conflict situations that affect his psyche as a result of threat and intimidation by the blackmailer in order to obtain a fee Whether it is material or moral, and therefore the victim is hostage in the hands of the blackmailer when submitting and carrying out orders for fear of the scandal, especially since electronic means have a big and effective role in committing electronic crimes, as it represents a fertile ground that helps to practice electronic crimes in general and electronic extortion crime in particular, as It invaded and dominated all aspects of life, and even controlled, as it is a global crime that exceeded the regional borders between countries.

Perhaps the reason for the prohibition of electronic extortion is the attack on the privacy of individuals and the danger that it poses to society, as one of the most important methods of proof that concerns the crime of electronic blackmail, which is the digital guide, as there are difficulties facing the investigation agencies and their ways of dealing with the digital guide for the sake Access to the truth, especially since electronic crimes take place in a virtual uninfected world, and therefore the crime scene is virtual filled with symbols and blades, it is necessary to put special texts that include all forms of behavior in the crime of electronic blackmail, and reflects the extent of their risk and ease of committing, as well as the difficulty of proving them.