ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية الحقوق
College of Rights

The role of electronic penal procedures in proving and adapting electronic extortion

Dr. Nawras Rashid Taha
College of Rights, Al-Nahrain University, Baghdad, Iraq
nawras.rasheed@gmail.com

Zahraa Mohammed Rashid
College of Rights, Al-Nahrain University, Baghdad, Iraq

Article info.

Article history:
- Received 9 Aug 2021
- Accepted 15 Aug 2021
- Available online 1 Sept 2022

Keywords:
- Concept.
- Definition.
- Adaptation.
- Procedures.
- Monitoring.
- Prosecution.
- Investigation.

Abstract: Electronic blackmail is an advanced technical method, resulting from the outcome of the interaction between the digital system and the criminal world. Ethical, or carrying out criminal acts in violation of the law, requests differ from one offender to another according to the circumstances and circumstances surrounding each electronic blackmail, and the offender with his requests exposes the personal rights to the abyss of danger, and puts them in the angle of damage in the event that these requests are implemented. Extortion is the cause of every offense committed by the blackmailer, because he is forced to commit it.

© 2022 TUJR, College of Right, Tikrit University

دور الإجراءات الجزائية الإلكترونية في إثبات وتكييف الابتزاز الإلكتروني

د. نورس رشيد طه
كلية الحقوق، جامعة النهرين، بغداد، العراق
nawras.rasheed@gmail.com

الباحثة زهراء محمد رشيد
كلية الحقوق، جامعة النهرين، بغداد، العراق

معلومات البحث :

تواريخ البحث:
- الاستلام : ٩ / آب / ٢٠٢١
- القبول : ١٥ / آب / ٢٠٢١
- النشر المباشر : ١/ ايلول /٢٠٢٢

الكلمات المفتاحية :
- مفهوم.
- التعريف.
- التكييف.
- إجراءات.
- المراقبة.
- الملاحقة.
- التحقيق.

الخلاصة: يعد الابتزاز الإلكتروني أسلوباً تقنياً متطوراً ، ناتجاً عن حصيلة التفاعل ما بين النظام الرقمي وعالم الإجرام ، أعتاد الجناة على إتباع الابتزاز كوسيلة للضغط على إرادة المجنى عليه ، لتنفيذ ما يطلبه الجاني منه ، فقد يطلب الجاني من المجنى عليه دفع أموال أو يطلب منه القيام بأمور غير أخلاقية ، أو القيام بتنفيذ أعمال إجرامية مخالفة للقانون ، تختلف الطلبات من جاني إلى أخر بحسب الظروف والملابسات المحيطة بكل ابتزاز إلكتروني، والجاني بطلباته يعرض الحقوق الشخصية لهاوية الخطر ، ويجعلها في زاوية الضرر في حالة ما إذا تم تنفيذ تلك الطلبات. الابتزاز هو سبب كل مخالفة صادرة عن الشخص المبتز ، لكونه مكرهاً على ارتكابها .

© ٢٠٢٢، كلية الحقوق، جامعة تكريت

المقدمة :

شهد العالم في العقود الأخيرة، ثورة كبيرة في تقنيات المعلومات وفي كافة المجالات، أذ أصبح من الصعوبة بمكان الاستغناء عن خدماتها. وعلى الرغم من الفوائد الكثيرة التي رافقت ظهورها ، إلا إنها اسهمت أيضاً في ظهور جيل جديد من الجرائم التي يقترفها بعض من مستخدمي هذه التكنولوجيا والتي تتسم غالباً بخطورتها وسهولة ارتكابها ، و التي توصف بأنها جريمة عابرة للحدود، أطلق عليها تسمية "الجرائم الالكترونية".

ترتكب هذه الجرائم بإحدى طريقتين : أولهما استخدام الكمبيوتر كأداة لتنفيذها ثانيهماً : أن يكون الكومبيوتر هو محل الجريمة الإلكترونية العابرة للحدود . أذ يستخدم الكومبيوتر كأداة لتنفيذ الابتزاز الإلكتروني ضد المجنى عليه . مثال ذلك قيام الجاني بإرسال رسالة إلكترونية

من خلال الكومبيوتر، تحتوي على طلبات الجاني ومن ضمنها الزام المجنى عليه بتنفيذها و إلا ستكون أسراره معلنة أمام الجميع . وقد يقع الابتزاز على البيانات المحفوظة في الكومبيوتر فتكون تلك البيانات سلاح الجاني يبتز به المجنى عليه ، لإجباره على تنفيذ ما يطلب . وغالباً ما يكون ضحايا الابتزاز الإلكتروني من الفتيات . وهذا يرجع لعدة أسباب منها استخدام المواقع الالكترونية والتخزين فيها وبشكل متزايد يفوق استخدام الرجال لتلك المواقع خصوصاً أذا كانت الفتاة ربة بيت ، وليس لها تحصيل دراسي ، فيكون أمر خدعها سهلاً على الجاني لأنه غالباً ما تكون عاطفتها هي من تقودها للتصرف ، خصوصاً فيما يتعلق بالمواقف الإنسانية يصعب تجاوزها .

أولاً: أهمية البحث:

تبرز أهمية موضوع الإجراءات الجزائية الإلكترونية لإثبات وتكييف الابتزاز الإلكتروني بكونه حديث الساعة ، نظراً للمساحة الكبيرة التي شغلها في العالم العربي ما يجعل هذا الموضوع من الناحية النظرية جديراً بالدراسة ، لإيضاح مفهومه ، لغرض ايجاد التكييف القانوني المناسب له ، لتكون العقوبة المفروضة على الجاني مناسبة للآثار السلبية الناشئة عن سلوكه الإجرامي .

ومن الناحية العملية ، فأن أهمية البحث في الموضوع محل الدراسة تبرز من حيث المحاولة في إتباع الإجراءات التي تساعد على إثباته ، للقبض على مرتكبه وردعه ، وزجر الغير ومنعه من ارتكابه .

ثانيا: إشكالية البحث:

تكمن مشكلة البحث في التساؤلات الآتية :

(١) هل أن النصوص العقابية الموضوعية كافية لتحديد التكييف القانوني المناسب لجريمة الابتزاز الإلكتروني . لمحاكمة فاعلها و الحد من فرص ارتكابها مستقبلاً .

(٢) هل أن الإجراءات الجزائية الشكلية كافية لإثبات الابتزاز الالكتروني بحق مرتكبيه.

ثالثا:منهجية البحث:

سنعتمد في بحث موضوع الإجراءات الجزائية المتخذة لإثبات وتكييف الابتزاز الإلكتروني على المنهج التحليلي للنصوص الموضوعية الواردة في قانون العقوبات العراقي رقم

(١١١) لسنة ١٩٦٩ المعل ، وللنصوص الإجرائية الواردة في قانون أصول المحاكمات الجزائية . مع الاسترشاد بآراء الفقهاء وموقف القضاء الجنائي العراقي .

رابعا: اهداف البحث :

نهدف من خلال بحثنا إلى:-

١- توفير الحماية الجنائية لضحايا الابتزاز .

٢- إلقاء الضوء على ظاهرة خطيرة ، و المحاولة في إيجاد الحلول المناسبة للحد منها.

٣- إيجاد تكييف قانوني مناسب للابتزاز الإلكتروني لزجر الجاني وردع غيره ، ممن تتوافر لديه نية ارتكابه .

٤- إلقاء الضوء على دور الإجراءات الجزائية الإلكترونية في مجابهة الابتزاز الإلكتروني للحد من ارتكابه .

خامسا: هيكلية البحث :

ستكون هيكلية البحث في موضوع دور الإجراءات الجزائية الإلكترونية في إثبات وتكييف الابتزاز الالكتروني " على وفق مبحثين ، سنخصص المبحث الأول للبحث في تعريف الابتزاز الإلكتروني و إجراءات الحد منه ، وسنبين في المبحث الثاني الإجراءات الجزائية الإلكترونية الخاصة بإثباته وكالآتي :-

المبحث الأول

مفهوم الابتزاز الإلكتروني و تكييفه القانوني

يقصد بمفهوم الشيء ، ما يفهمه العقل دون الحواس ، أي بمعنى أن المفهوم هو الفكرة الذهنية الكامنة في ذهن الإنسان عن حقيقة الشيء ، والتي تكون واضحة عندما يتم الكشف عن الشيء وازالة كل ما يتعلق به من غموض ، حتى يكون معناه مفهوماً ، والمفهوم فلسفة لإيضاح حقيقة الشيء ، من غير لبس أو غموض ، والحقيقة تظهر عندما يتم الكشف عن ماهية الشيء ، من خلال طرح الأسئلة بشأنه للاستفهام عنه ، أي بمعنى طلب الاخبار عن حدث أو واقعة وما يحيط بها من ظروف وملابسات ، ليكون بالإمكان مباشرة أو أتخاذ الإجراء المناسب بشأنها . وأن البحث عن مفهوم الابتزاز الإلكتروني والإجراءات الخاصة بإثباته ، يتطلب منا الخوض بالتعريفات الخاصة بالابتزاز ليكون معناه واضحاً ومفهوماً ، ومن

ثم بيان أنواع الإجراءات الجزائية الإلكترونية الخاصة بإثباته ، وهذا ما سنبينه من خلال تقسيم هذا المبحث إلى مطلبين وكالآتي :-

المطلب الأول / التعريف بالابتزاز الإلكتروني

التعريف بالشيء يتطلب البحث عن معناه ، ليكون مفهومه والغرض المقصود منه واضحاً ، و الحصول على معنى الشيء يتضح من خلال إلقاء الضوء على التعريفات المطروحة بشأنه، وكما هو معلوم أن لكل مصطلح تعريفات لغوية ، و اصطلاحية ، وللتعريفات الاصطلاحية أكثر من نوع إلا أننا سنركز على التعريف الاصطلاحي الصادر عن شراح القانون ، لكونه الأهم ، حتى تكون الفكرة في جميع الحيثيات واحدة ومفهومة ، وعليه سنخصص هذا المطلب للبحث في التعريفات الخاصة بالابتزاز الإلكتروني والذي سنقسمه إلى فرعين وكالآتي :-

الفرع الأول / المدلول اللغوي للابتزاز

يرجع أصل كلمة ابتزاز إلى الفعل الثلاثي بزَّ بتشديد الزاي ، بز الشيء يبزه بزاً: بمعنى اغتصبهُ ،والبز هو السلب ، وابتززتُ الشيء: استلبه ، ومن ذلك جاء المثل ،من عزَّ بزَّ معنى ذلك قهر واغتصب([1]) وبزّ ثوبه عنه أي غلبه سلبه([2]).والابتِزاز بكسر التاء اصله ثلاثي من بَزَّ الشيءَ يبُزُّه بَزّاً: والبَزُّ: السلب ، وبزَّ الشيءَ : انتزعه، وبزَّ المال: سَلَبه من الناس بغير الحق أو نزعه منهم بقهر وإذلال والبَزُّ أيضاً: السلاحُ. وبَزَّ ثَوْبَه: جَذَبَهُ إِلَيْه.([3])

وقد عُرف الابتزاز لغةً بأنه :-مفردة مزعجة وتجلب معها قدرٌ كبيرٌ من المشاعر السلبية فهو تجسيد حيٌ لواحد من أحط الخصال التي يمكن أن يتحلى بها الإنسان حين يستغل قوة ما بيده فيما حصل عليه بأساليب غير صحيحة مقابل ضعف انسان آخر سواء كان هذا الضعف مؤقتاً او دائماً ([4]) .

---

١) العلامة أبو الفضل جمال الدين محمد بن مكرم (ابن منظور) – معجم لسان العرب – دار صادر – لبنان- **المجلد الثاني – حرف الباء – مادة (بزز) ، لا يوجد سنة نشر ، ص,١٥٧**

٢) القاموس المحيط للفيروز أبادي ،بيروت – لبنان،ط٨ ، باب الزاي ، فصل الباء،٢٠٠٥،ص,٦٤٧

٣) محمد مرتضى الحسيني الزبيدي ، تاج العروس،ج،٧مط حكومة الكويت– ط٢ – ١٩٩٤ ص,٤٣٦

٤) مستشار أشرف أحمد هلال ، الجرائم المعلوماتية في الاعتداء على الحق في الحياة الخاصة ، دار ال غالب للنشر والتوزيع ، جدة،١٤٣٦هـ، ص ٦٨.

الفرع الثاني / المدلول الاصطلاحي للابتزاز الإلكتروني

أن محاولة الحصول على مكاسب مادية أو معنوية عن طريق الإكراه الموجه ضد الأشخاص الطبيعية والمعنوية عن طريق التهديد بفضح أسرارهم أو خصوصياتهم يضعهم بدائرة من الخوف والقلق النفسي والذي من شأنه أن يدفعهم إلى تنفيذ كل ما يطلبه الجاني من أمور ، مقابل امتناعه عن التشهير بهم و فضح أسرارهم .

فقد عرّف الابتزاز الإلكتروني "بأنه الوعيد بالشر أو زرع الخوف في النفس وذلك بالضغط على إرادة الإنسان من أن ضرر ما سيلقاه أو سيلحق أشخاصا أو أشياء له بها صله، أو هو ذلك الفعل الذي يقوم به شخص بإنذار آخر بخطر يريد إيقاعه بشخصه أو ماله أو بشخص أو مال غيره ويستوي هذا الإنذار سواء كان شفاهية أو كتابة بأي عبارة من شأنها إلقاء الرعب في نفس المجني عليه أو مجرد ازعاجه أو تخويفه من الخطر قد يلحق بنفسه أو مال".([١])

وقد عرف ايضاً بانه "الضغط الذي يباشره شخص ما على إرادة شخص آخر في محاولة لحمله على ارتكاب جريمة ما." ([٢]) وقد ورد تعريف آخر وهو" قيام شخص أو عدة أشخاص بتهديد طرف آخر ذكراً كان أو انثى، بنشر معلومات او أخبار أو صور ، لا يرغب الضحية بنشرها وتكون بقصد التشهير به للتأثير في نفسية الضحية من خلال تهديده وبالنتيجة الحصول على مكاسب معينة من الضحية أو تنازلات ومواقف بما يخدم المبتز"([٣]).

يمكن أن **نعرف** الابتزاز الالكتروني:- " بأنه الاستيلاء على الاشياء المملوكة للغير بطرق إلكترونية، بوساطة جهاز الحاسوب ، مع الاستعانة بالبرامج والشبكات المحملة فيه، لمساواة المجنى عليه و اجباره على الرضوخ لطلبات الجاني وتعليماته غير المشروعة " . أن السبب الدافع للقيام بالابتزاز الالكتروني يختلف من حالة لأخرى ، فقد السبب مادي وقد يكون

---

[١]) أفراح بنت خميس بن عامر اللويهية ،مشكلة الابتزاز الإلكتروني لدى طلبة مرحلة التعليم ما بعد الأساسي ، رسالة مقدمة لنيل شهادة الماجستير في الآداب ، كلية الآداب والعلوم الاجتماعية ،جامعة السلطان قابوس ،سلطنة عمان ،٢٠١٨، ص ٦.

[٢]) أحمد شوقي ، شرح الاحكام العامة لقانون العقوبات ، دار النهضة العربية ، القاهرة ، ٢٠٠٣، ص ٥٥٩.

[٣]) فايز عبد الله الشهري ، دور مؤسسات المجتمع في مواجهة ظاهرة الابتزاز وعلاجه ، الابتزاز الإلكتروني نموذًجا، بحث مقدم لندوة الابتزاز ((المفهوم–الاسباب– العلاج))، مركز باحثات لدراسات المرأة، بالتعاون مع قسم الثقافة الإسلامية، جامعة الملك سعود، ٢٠١٣،ص١٣.

عاطفي ، وهذا ما بينه أحد قضاة التحقيق ، في لقاء أجري له بخصوص الدعاوى المتعلقة بالابتزاز الإلكتروني [١] ، وقد أكد على أن حالات الابتزاز الإلكتروني بتزايد مستمر ، وهذا بدوره يؤدي إلى اضعاف الروابط الاجتماعية عموماً ، والأسرية خصوصاً حتى صار الابتزاز الإلكتروني أحد أخطر الأسباب المؤدية إلى الطلاق [٢] .

المطلب الثاني / التكييف القانوني للابتزاز الالكتروني

ينشأ عن الابتزاز الإلكتروني نوعين من الاعتداء ، الأول يمس حق المجنى عليه في الاحتفاظ بخصوصياته و أسرار حياته ، بعيداً عن فضول الأخرين وتطلعاتهم والثاني اعتداء من شأنه المساس بسلامة جسم المجنى عليه ، مساساً معنوياً يتمثل بالضغط الشديد الموجه ضد إرادته ، ما يجعله بحالة من الخوف والفزع والقلق النفسي في أن تكون خصوصياته عرضة للخطر في أي وقتاً يراه الجاني مناسباً ، ما يؤثر ذلك الأمر سلباً على حقه في السلامة الجسدية .

وعليه فإذا ما أدى الابتزاز الإلكتروني إلى تعطيل أحد أعضاء الجسم أو توقفها مؤقتاً عن أداء وظيفتها بالشكل المطلوب ، فهنا يكون بالإمكان تكييف الابتزاز بأنه جريمة إيذاء ، تطبق بشأنها النصوص المتعلقة بجريمة الإيذاء لا سيما بنص المادة (٤١٣) من قانون العقوبات رقم (١١١) لسنة ١٩٦٩ المعدل ، والتي نصت على " ١- من اعتدى عمدا على اخر بالجرح او بالضرب او بالعنف او بارتكاب اي فعل اخر مخالف للقانون فسبب له اذى او مرضا يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائة دينار او بإحدى هاتين العقوبتين ٢ – وتكون العقوبة الحبس مدة لا تزيد على ثلاث سنوات والغرامة التي لا تزيد على ثلاثمائة دينار او بإحدى هاتين العقوبتين ... ب – اذا نشأ عن الاعتداء اذى او مرض اعجز المجنى عليه عن القيام بأشغاله المعتادة مدة تزيد على عشرين يوما [٣] . هذا من جهة ومن جهة أخرى يمكن للقاضي تكييف الابتزاز الإلكتروني بأنه ظرفاً مشدداً للعقوبة إذا ما كان مقترناً بأحد الحالات الواردة في المادة (٤١٤) من قانون العقوبات العراقي.

---

[١] مقال بعنوان " أغلب ضحايا الابتزاز الالكتروني "فتيات" والجناة غرضهم "الأموال" ، منشور على موقع مجلس القضاء الأعلى https://www.hjc.iq/view.3774/ ، تمت الزيارة بتاريخ ٢٠٢١/٨/٢ .

[٢] المرجع نفسه .

[٣] المادة (٤١٣) من قانون العقوبات العراقي ، الغرامة تعدلت وفي الجنحة ما لا تقل عن ٢٠١٠٠٠ مئتين والف دينار. ولا تزيد عن مليون دينار.

كما يمكن للقاضي تشديد عقوبة الابتزاز الإلكتروني باعتباره ظرفاً قضائياً مشدد لها تصل إلى حد السجن مدة لا تزيد عن سبع سنوات أو الحبس في حالة اقترانه مع جريمة التهديد [١] أو السب او أفشاء الاسرار أو الفعل الفاضح وغيرها بحسب ظروف وملابسات كل جريمة .

المبحث الثاني

إجراءات الإثبات الإلكترونية للابتزاز الإلكتروني

أفرز التطور والتقدم العلمي والتقني في مجال الاتصالات وتكنولوجيا المعلومات وشبكة الإنترنت العنكبوتية (وسائل التواصل الاجتماعي) أنماطاً مستحدثة من الجرائم المعقدة ، التي تتطلب إجراءات تكون من صنفها حتى يكون بالإمكان إثباتها ، و احالة مرتكبها أمام الجهات القضائية المختصة لمحاكمته ، وتحديد العقوبة المناسبة لسلوكه الإجرامي. أي يجب أن تكون إجراءات الإثبات إلكترونية أيضا وتتمثل بالمراقبة الالكترونية و الملاحقة الإلكترونية والتحقيق الإلكتروني ، مع العرض أن إجراءات المراقبة والملاحقة الملاحقة تسبق إجراءات التحقيق الإلكتروني، وفي ضوء ما تقدم سنبحث في إجراءات الإثبات على وفق ثلاثة مطالب وكالآتي :-

المطلب الأول / المراقبة الإلكترونية

يعد نظام المراقبة الإلكترونية نظاماً مستحدثاً بديلاً عن العقوبة السالبة للحرية قصيرة المدة، صار يشغل حيزاً في مجال التطبيق خارج المؤسسة العقابية ، أن لهذا النظام العديد من الإيجابيات منها ، إبعاد المحكوم عليه بالحبس البسيط من الاختلاط بالمجرمين الخطرين ، حتى لا يتأثر بسلوكياتهم وأطباعهم الخطرة ، كما أن المراقبة الإلكترونية تسمح للمحكوم عليه بكسب رزقه ، و البقاء في المنزل مع عائلته وغيرها كما أن من هناك إيجابيات تعود فائدتها

---

[١] وقد اتجهت محكمة جنايات المثنى إلى إدانة المتهم والحكم عليه بموجب المادة (٤٥٢/ أ) بالحبس مدة خمس سنوات ، وذلك لقيامه بتهديد المجنى عليها بنشر الصور الشخصية المتعلقة بها والتي أستولى عليها بطريقة غير مشروعة عن طريق اختراقه لصفحتها الشخصية والعائلية والضغط =عليها ومساومتها بإعطائه ارصدة بطاقات تعبئة ومبالغ مالية ، القرار ذي العدد ٥٠٤ / الهيئة الجزائية / ٢٠١٨ ، والمؤرخ في ٢٠١٨/١٢/٢ ، وقد تم المصادقة على هذا الحكم من قبل التمييز الاتحادية بقرارها ذي العدد ٣٧٥٨/ الهيئة الجزائية / ٢٠١٩ والمؤرخ في ٢٠١٩/٣/١٧ . منشور على الموقع https://www.dorar-aliraq.net/threads/1083279 ، تمت الزيارة بتاريخ ٢٠٢١/٨/٣ .

للمصلحة العامة ، وهي عدم تكفل الدولة بتوفير الطعام والدواء والمستلزمات الأخرى التي يجب عليها توفيرها ، فيما لو كان المحكوم عليه موجوداً داخل السجن ،لتنفيذ العقوبة المحكوم بها عليه، إلا أنه وبالمقابل تعد المراقبة الإلكترونية إجراء في غاية الأهمية يمكن اعتمادها للاستدلال والكشف عن الجريمة الإلكترونية، من خلال مراقبة سلوكيات المجرم بدءً من التجهيز للجريمة ولغاية اتمامها من خلال كاميرات المراقبة المثبتة في الطرق العامة ، أو في المنازل القريبة من مكان الحادث . وفي ضوء ما تقدم سنبين المدلول الاصطلاحي للمراقبة الإلكترونية و آلية تنفيذها ، على شكل فرعين وكالآتي :-

الفرع الأول / المدلول الاصطلاحي للمراقبة الإلكترونية

أطلق على المراقبة الإلكترونية تسميات مختلفة منها الحبس المنزلي ، والوضع تحت نظام المراقبة الإلكترونية باستعمال السوار الإلكتروني ، إلا إنها تدل على نفس المعنى وهو العقوبة الإلكترونية البديلة عن العقوبة التقليدية السالبة للحرية ، على الرغم من أن المراقبة الإلكترونية من شأنها المساس بحرية الجاني ، إلا إنها تقيدها لا تسلبها منه . فقد عرف المركز العربي للبحوث القانونية في القرار رقم ٨٥٢ نظام المراقبة على بأنه : جهاز إلكتروني يثبت في شكل سوار إما في معصم المحكوم أو كاحله ويستعمل كبديل عن عقوبة السجن قصيرة المدة أو كإجراء تحفظي لمراقبة المتهم المفرج عنه"[١] .

وعرف أيضاً بأنه : أحد الأساليب الحديثة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج أسوار السجن – في الوسط الحر – بصورة ما يعبر عنه " بالسجن في البيت " .

كما عرف نظام المراقبة الإلكترونية أو ما يسمى بالسوار الإلكتروني أو الحبس في البيت بأنه " إلزام المحكوم عليه أو المحبوس احتياطيًا بالإقامة في منزله أو محل إقامته، خلال ساعات محددة بحيث تتم متابعة الشخص الخاضع للمراقبة الكترونياً، من خلال وضع أداة إرسال على يد هذا الأخير تشبه الساعة – سوار الكتروني – تسمح لمركز المراقبة من

---

[١] معجم المصطلحات القانونية والقضائية المستخرجة من القوانين العربية والمعتمدة من قبل مجلس وزراء العرب – قوانين تنظيم المؤسسات العقابية – المركز العربي للبحوث القانونية و القضائية، الدورة ٢٦،القرار ٨٥٢ بتاريخ ٢٠ ديسمبر ٢٠١٠،ص ٢٤.

الكمبيوتر المركزي بمعرفة ما إذا كان المحكوم عليه موجود في المكان والزمان المحددين بواسطة الجهة القائمة على التنفيذ " [١] .

وعرفت أيضاً بأنها " أحد البدائل الرضائية للعقوبات السالبة للحرية التي بمقتضاها يتم متابعة الشخص الخاضع لها – من خلال استخدام تقنيات حديثة – من قبل أجهزة أنفاذ القانون خارج السجن في أماكن و أوقات محددة سلفا ومن خلال إخضاعه لمجموعة من الالتزامات والشروط، ويترتب على مخالفة هذه الالتزامات معاقبته بعقوبة سالبة للحرية " [٢] .

نستخلص مما تقدم أن نظام المراقبة الإلكترونية يسمح للمحكوم عليه بممارسة نشاطاته اليومية المعتادة ، إلا أنها ستكون معلنة للسلطات المختصة بتنفيذ العقوبة ، مما يقيد ذلك من حريته ، إلا أنه لا يعدمها ، تتم مراقبته من خلال سوار إلكتروني يربط بيده أو كاحله ، وعلى هذا الأساس أطلق على نظام المراقبة الإلكترونية تسمية " السوار الالكتروني" وهذه التسمية متعمدة من قبل بعض المختصين بعلم العقاب[٣] .

الفرع الثاني / ألية تنفيذ المراقبة الإلكترونية

تُعد المراقبة الإلكترونية أحد الأساليب الحديثة في مجال السياسة الجنائية ، من شأنها التخفيف من شدة العقوبات السالبة للحرية ، من خلال فرض بدائل عنها يتحقق على أساسها المصلحتين العامة والخاصة على حدٍ سواء . فيتم من خلال تلك البدائل تأهيل الجاني من خلال مراقبته وتتبع تصرفاته عن بعد وتنبيهه أن صدرت عنه أي مخالفة للقيود المفروضة عليه بناءً على تلك المراقبة . وبالمقابل تعد المراقبة وسيلة لإثبات الجريمة بحق الجاني وأدانته بها ، في حالة ما إذا لاحظ عضو الضبط القضائي أو المحقق أو القاضي عند إجراء المراقبة الإلكترونية لمحل الحادث الرقمي (الافتراضي) ، أو قاضي التحقيق ، بأن المتهم قد شرع للجريمة أو قام بأي سلوك من شأنه الدخول في محل الجريمة الإلكترونية (الابتزاز الإلكتروني نموذجاً) ، كأن يلاحظ القاضي عن بعد بأن المجرم الإلكتروني قد استخدم الفيروسات كوسيلة

---

[١] صفاء أوتاني، الوضع تحت المراقبة الإلكترونية "السوار الإلكتروني" في السياسة العقابية الفرنسية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج ٢٥، ،ع١ ،٢٠٠٩، ص ١٣١.

[٢] رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون، العدد ٦٣ الصادرة عن كلية القانون جامعة الإمارات العربية المتحدة، السنة ٢٩، يوليو ٢٠١٥، ص ٢٨٥.

[٣] سالم عمر، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج أسوار السجن، الطبعة الأولى، دار النهضة العربية، ٢٠٠٠، القاهرة ، ص ٩.

لتهكير المعلومات المحفوظة في الحساب الشخصي للضحية ، والاستيلاء عليها بصورة غير مشروعة ، فعلى القاضي أو المحقق أو عضو الضبط القضائي ممن كان حاضراً أثناء المراقبة الإلكترونية لسلوكيات المجرم الإلكتروني أو لمحل الحادث الإلكتروني أن يقوم بتسجيل تلك الملاحظات في محضر خاص بالمراقبة الإلكترونية ، يمكن تسميته بمحضر المراقبة الإلكترونية ، أو محضر إجراءات الكشف والاستدلال الإلكتروني . فقد ألزم المشرع العراقي عضو الضبط القضائي بعد أخباره أو أتصال علمه بوقوع جريمة مشهودة ، أن يخبر قاضي التحقيق والادعاء العام بوقوعها ، و بعد الانتقال فوراً إلى محل الحادث ، أن ينظم محضراً يدون فيه جميع الإجراءات المتخذة من قبله قبل وصول القاضي ، كتدوين افادة المجنى عليه وتوجيه الأسئلة للمتهم أن تم القبض عليه متلبساً بجريمته ، وضبط الأسلحة وكل ما استُعمل في ارتكاب الجريمة ومعاينة الآثار المادية للجريمة ، وتثبيت حالة الأشخاص والأماكن وكل ما يفيد في اكتشاف الجريمة ، أو يمكن الحصول منه على إيضاحات بخصوص الجريمة ومرتكبها [١] . كما ألزم المشرع كلاً من القاضي والمحقق عند الكشف عن محل الحادث اتخاذ جميع الإجراءات الواردة في أعلاه ومن ضمنها تنظيم محضر خاص يدون فيه جميع ما أتخذ من إجراءات [٢] .

تدل مفردة "المراقبة" بأنها مرتبطة بالأجهزة الحكومية والأمنية [٣]، إلا أن الواقع يدل على غير ذلك ، لأن هناك العديد من الجهات التي لها سلطة المراقبة كالمراقبة المطبقة من

---

[١] المادة (٤٣) من قانون أصول المحاكمات الجزائية رقم (٢٣) لسنة ١٩٧١ المعدل.

[٢] المادة (٥٢ / ب) من القانون نفسه .

[٣] تقوم شعبة مكافحة الجرائم الإلكترونية التابعة لوكالة الاستخبارات في وزارة الداخلية العراقية الكشف على محلات الحوادث عبر كاميرات المراقبة المربوطة فيها ، كما أنها تقوم بفحص الصور للتأكد من صحتها وبأنها غير مفبركة وتقوم أيضا بفحص وتفريغ أجهزة الموبايل والحاسبات وكافة وسائل الخزن ، واسترجاع المحذوف منها ، كما يقوم هذه الشعبة بمساعدة الخبراء بفتح بعض الموز السرية لبعض الهواتف النقالة والحواسيب وأجهزة التسجيل للكاميرات كما تقوم بالحصول على المعلومات الخاصة ببعض صفحات التواصل الاجتماعي التي تكون محل الاتهام لتزويد الجهات القضائية والتحقيقية بها ، كما تقوم بفحص وتفريغ التسجيلات الصوتية المسجلة عبر الهواتف النقالة ، فضلاً عن قيامها بتنسيق التعاون مع الجهات القضائية للحفاظ على مسرح الجريمة الإلكترونية ، ينظر مجموعة مؤلفين ، الابتزاز الإلكتروني جريمة العصر الحديث ، سلسلة ثقافاتنا الأمنية ، العدد الثاني ، ٢٠١٩ ، ص ١٢٨-١٢٩، منشور على الموقع https://moi.gov.iq/upload/upfile/ar/925.pdf ، تمت الزيارة بتاريخ ٢٠٢١/٨/٣ .

قبل إدارة المواقع الإلكترونية ، والمستخدمين لتلك المواقع عندما يرون منشوراً مخالفاً لذوقهم العقائدي أو الأخلاقي ، فضلاً عن المراقبات المطعمة بصفة التجسس التي تنفذها الجهات الحكومية أو غير الحكومية لتحقيق أغراضها السياسية أو الاقتصادية ، أو الاجتماعية ، أو قد يكون الغرض منها لتقويم سلوكيات أفراد المجتمع أذ يمكن للجهات القائمة بالمراقبة التحكم بالمعلومات التي تكون محلاً للنشر عبر المواقع الإلكترونية ، فيمكنها أن تحجب أي فرد من الاشتراك في الموقع إذا ما وجدت بأنه غير مؤهل أو أن شروط الاشتراك لا تنطبق عليه . كما لها حذف المنشورات المبلغ عن عدم صلاحها ، وغيرها من الأمور المحددة من قبل الجهات المختصة بإدارة تلك المواقع .. أما عن مراقبة وسائل الاتصال وشبكات التواصل الاجتماعي، فتربط بعض الحكومات هذا الأمر بالحفاظ على الأمن القومي من التهديدات، وتعد أشهر الدول في الرقابة على الإنترنت هي كوريا الشمالية، إيران، وفي الدول العربية السعودية وقطر ومصر [١].

ومن المسائل الأساسية التي من شأنها أن تحد من تطبيق المراقبة الإلكترونية هي مسألة أخطار الأفراد الموضوعين تحت الرقابة بالقرار الخاص بإذن المراقبة والأسباب الموجبة لذلك ، ولا يجوز الامتناع عن أخطارهم ، إلا في حالة ما إذا كان الأخطار سيؤدي إلى أفشال الفرض المنشود من المراقبة ، كوجود خطر يهدد حياة الشخص الموضوع تحت المراقبة على أن يتم أخطارهم بعد زوال ذلك الخطر ، يكون الأخطار من واجب الجهات الحكومية المختصة بالمراقبة ، إلا أنه يسمح لمقدمي خدمة الاتصالات أن يخطروا الأشخاص بمراقبة اتصالاتهم طوعاً أو عند الطلب [٢].

المطلب الثاني / الملاحقة الإلكترونية

يعد الابتزاز الإلكتروني من الاعتداءات الأخطر و الأكثر وقعاً في الآونة الأخيرة، خاصة في مجتمعاتنا العربية ، و أنها بتزايد مستمر يتعرض لها الاشخاص الذين لا يملكون ثقافة المعرفة باستخدام تلك المواقع ، فتكون عملية تهكير و اختراق واستهداف المواقع الشخصية لهم سهلة المنال ، وذلك يعود لعدة أسباب منها ضعف كلمة السر الخاصة

---

[١] فاطمة الزهراء عبد الفتاح ، آليات وضوابط مراقبة مواقع التواصل الاجتماعي ، بحث منشور على موقع الانترنت ، https://futureuae.com/ تاريخ زيارة الموقع ٢٠٢١/٦/٩ .

[٢] عبد الفتاح بيومي حجازي ،مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي ط١، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٦ ، ص ٥٧.

بالحساب الشخصي ، أو بسبب ثقته المفرطة وغير المسؤولة بالأصدقاء الافتراضيين الذين يتواصل معهم عبر تلك المواقع ، والقيام بتزويدهم بالصور والأسرار الشخصية العائدة له ، ترك المعلومات الشخصية داخل الموقع الشخصي من دون تشفير وغيرها من الاسباب ، لذا صار لازماً البحث عن الحلول المناسبة للحد من عمليات الاختراق غير المشروعة للحسابات الشخصية ، وذلك يتم عبر تتبع وملاحقة الجاني إلكترونياً ، وعليه سنخصص هذا المطلب للبحث في مدلول الملاحقة الإلكترونية ، وألية تنفيذها ،على وفق فرعين وكالآتي :-

الفرع الأول / مدلول الملاحقة الإلكترونية

يعتبر مصطلحي المضايقة والمطاردة الإلكترونية كلمات مرادفة لمصطلح الملاحقة الإلكترونية ، ويقصد بها عملية الترصد الموجهة صوب المجرم الإلكتروني لرصد تحركاته الإجرامية وإثباتها عليه ، لتكون إدانته بارتكاب الجريمة الإلكترونية صحيحة لاستنادها على إجراءات قانونية ". وعليه فإن إجراء الملاحقة القانونية هو إجراء قانوني صحيح إذا ما أمعنا النظر في المادة الأولى من قانون أصول المحاكمات الجزائية رقم (٢٣) لسنة ١٩٧١ المعدل لوجدنا بأن نص المادة قد نص على إجراء تتبع الجاني أي ملاحقته في الجريمة المشهودة من قبل المجنى عليه أو الجمهور وقت ارتكابها أو بعد ارتكابها ببرهة يسيرة ، أو إذا وجد مرتكبها بعد وقوعها بوقت قريب حاملاً آلات أو أسلحة أو أمتعة أو أوراق أو أشياء أخرى يستدل منها على أنه فاعل أو شريك فيها ، ومن كلمة الأشياء نستنتج بأن الجاني الالكتروني المرتكب لجريمة الابتزاز الإلكتروني ، إذا ما وجد من خلال ملاحقته الإلكترونية بعد ارتكاب جريمته الإلكترونية بأنه حاملاً (حائزاً) في حسابه الإلكتروني بعد ارتكاب جريمته للصور الشخصية أو البيانات والمستندات المتعلقة بأسرار المجنى عليه ، بشكل أوراق أو بشكل بيانات مخزنة بصورة إلكترونية على قرص أو فلاش أو هارد . وعليه فأن اقامة الدورات التدريبية بخصوص التحقيق والضبط الإلكتروني ، وتطويرات الخبرات والمهارات لدى ضباط التحقيق وغيرهم ، يضيف لأليات وإجراءات تتبع الجناة والكشف عن جرائهم ، قدراً من المهارة المعلوماتية التي تمكنهم من إثبات الجريمة الإلكترونية والقبض على مرتكبها متلبساً بها [١] .

---

[١] عبير نجم ،تداعيات الابتزاز الالكتروني على الشباب والاحداث الصغار وسبل المواجهة والعلاج ٢٠١٩، منشور على الموقع https://www.alnahrain.iq/post/448 ، تمت الزيارة بتاريخ ٢٠٢١/٧/٤.

الفرع الثاني / ألية تنفيذ الملاحقة الإلكترونية

إن المواجهة الحقيقة لأي نوع من الجرائم الإلكترونية ، لا سيما الابتزاز الإلكتروني ، تتطلب أجهزة مختصة ، وإجراءات منصوص عليها قانوناً أو بناءً على قانون ، حتى تكون الملاحقة والكشف وإحراز الأدلة وصولاً إلى إثبات الجريمة الإلكترونية ، إجراءات قانونية صحيحة يمكن الاعتماد عليها للوصول إلى النتيجة النهائية بخصوص الواقعة محل الدعوى ، لإقرار العقوبة المناسبة الرادعة بحق مقترف السلوك [١] .

وهنا تجدر الإشارة إلى دور وسائل الإعلام في ملاحقة مرتكبي الجرائم الإلكترونية، بما تقوم به من نشر معلومات عن الجاني ، أو صورة له تمكن الجهات الأمنية من إلقاء القبض عليه . فضلاً عن ما تقوم به من مساعدة قوات الأمن بإطلاق تحذيرات ، حول ألية استخدام وسائل التواصل الاجتماعي ، والتنويه عن مخاطر استخدامها في حالة ما إذا كانت غير مشروعة [٢] .

أن من أكثر الاساليب التي من شأنها وضع العراقيل أمام وزارة الداخلية في أنجاز عملها في تحقيق الردع بحق الجاني وزجر غيره هو "خجل وحرج العائلات العراقية من الإعلان عن جرائم الابتزاز الإلكتروني ، فضلاً عن الجرائم الأخرى التي تتستر العوائل عن الإخبار وتحاول حل المشكلة بنفسها بعيداً عن علم الجهات الأمنية و الانصياع صوب تحقيق مطالب المبتز، ليمتنع عن نشر أو أفشاء الأمور الشخصية [٣] .

المطلب الثالث / التحقيق الإلكتروني

وجدت الجهات المختصة بالتحقيق ، أن التحقيق في الجرائم الإلكترونية فيه صعوبات وتحديات كبيرة في سبيل الكشف عنها ، و اتخاذ الإجراءات القانونية بشأنها. ما أستدعى ذلك الأمر إلى ضرورة إعداد برامج لتدريب الكوادر المختصة بالتحقيق وتأهيلها فنياً على نحو يمكنها من أنجاز أعمالها بدقة و أتقان وبحسب المطلوب ، بعيداً عن الغموض والالتباس

---

[١] عبد اللطيف محمود ربايعة، بحث بعنوان الجرائم الالكترونية (التجريم والملاحقة والاثبات)، فلسطين ، ٢٠١٦، ص ٣٤.

[٢] موقع هيئة تنظيم الاتصالات والحكومة الرقمية ، https://www.td-ra.gov.ae/ar/mediahub/cyberblackmailing.aspx تمت الزيارة بتأريخ ٢٠٢١/٧/٩ .

[٣] عبير نجم عبدالله أحمد الخالدي تداعيات الابتزاز الالكتروني .....، مرجع سابق .

والخلط الذي قد يغدو الأبرياء ضحية له . لذلك سنبين في هذا المطلب المدلول الاصطلاحي للتحقيق ، و ألية تنفيذه ، على وفق فرعين وكالآتي :-

الفرع الأول / المدلول الاصطلاحي للتحقيق الإلكتروني

يقصد بالتحقيق مجموعة من الإجراءات التي تباشرها السلطات المختصة قانوناً بالشكل المحدد قانوناً بهدف الكشف عن حقيقة الواقعة الإجرامية محل التحقيق وإسنادها إلى المتهم وتمحيص أدلتها و أتخاذ القرار المناسب في مدى ملائمة رفعها إلى القضاء من عدمه [١] . أن الاجراءات الإلكترونية تشبه التقليدية من حيث الكيفية والشروط والطبيعة ، إلا إنها تختلف عنها من حيث الوسيلة لأن الإجراءات الإلكترونية يتم تنفيذها إلكترونياً بوساطة جهاز الحاسوب و بالاعتماد على البرامج والشبكات المحملة فيه، و لا يعتبر الاعتقاد بضياع الأدلة أو محوها سبباً كافياً لإصدار الحكم القضائي على استعجال، باتخاذ بعض الإجراءات ، و أنما لا بد من القيام بجميع الإجراءات بصيغة إلكترونية . وعليه فأن تبني استراتيجية أمنية إلكترونية تعمل وفق منهجية التحقيق الإلكتروني، بعيداً عن التلاعب والتحريف ، لا تتم إلا بتعاون مؤسسات القطاع الخاص والمتمثلة بالمؤسسات الخاصة بإدارة وتنظيم مواقع التواصل الإلكتروني ، وأفراد المجتمع مع الجهات الحكومية المختصة بمكافحة الجرائم الإلكترونية في الفضاء الإلكتروني ليكون التقليل من آثارها والحد من أنتشارها ممكناً [٢]).

الفرع الثاني / ألية تنفيذ التحقيق الإلكتروني

إن المحققين يُواجهون العديد من الصعوبات عند ممارسة وظائفهم في إثبات الجرائم الالكترونية وهو ما يتطلب مجهوداً إضافياً وتدريباً وتعاوناً من الجهات ذات العلاقة لإثبات هذا النوع من الجرائم.لكن مع هذا تتم إجراءات الإثبات بالتحري وجمع والأدلة والتحقيق الابتدائي وسنوضح كلاهما كما يلي :-

---

[١] نقلاً عن د. حسين عبد علي عيسى ، د. شيلان شريف محمد ، التحقيق الابتدائي في جريمة الاحتيال الإلكتروني المجلة العلمية لجامعة جيهان – السليمانية ، المجلد ٢ ، العدد ٢ ، كانون الأول ، ٢٠١٨ ، ص٣٠٥.

[٢] ثيان ناصر آل ثيان ، إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية ، جامعة نايف للعلوم الأمنية ، ١٤٣٣، ص ٤٥.

اولاً / التحري وجمع الأدلة في الجرائم الالكترونية:-

إن الإخبار عن جريمة يتطلب أن يكون لدى المخبر معلومات صحيحة ، حول محل الجريمة والذي يمثل الموقع الإلكتروني ، الذي ارتكبت عليه الجريمة الإلكترونية حتى يتمكن قاضي التحقيق أو عضو الضبط القضائي من الانتقال إلى محل الحادث في الوقت المناسب وبشكلٍ إلكترونياً أيضاً ، للحفاظ على آثارها والوسائل المستخدمة في ارتكابها من المحو أو الضياع، مستعيناً بالبرامج الحاسوبية المخصصة للكشف عن الجريمة التي تكون محلاً للتحقيق الإلكتروني ، أي الجريمة التي وقع الإخبار بشأنها لا سيما جرائم التهكير وجرائم نشر السلوكيات الإباحية . تعد مسألة أعداد و استحداث الأدوات البرمجية الحاسوبية للتعرف على الأنماط الإجرامية ، مسألة في غاية الأهمية ليكون بالإمكان تشخيص الجريمة وكشفها بيسر ، نظراً لضخامة حجم المعلومات المتوافرة في شبكة الانترنت[١] .

أما بالنسبة للجريمة المشهودة ، التي يضبط فاعلها حال استخدامه لموقع الأنترنيت ، لتنفيذ جريمته ، فعلى عضو الضبط القضائي إخبار قاضي التحقيق والادعاء العام بوقوع الجريمة [٢]، وينتقل فوراً إلى الموقع الإلكتروني الذي من خلاله نفذ الجاني جريمته ، و أن يقوم بتوجيه الأسئلة للمتهم عن التهمة المُسندة إليه ، و أن كان توجيه تلك الأسئلة بشكل إلكتروني ، عن طريق الرسائل أو البصمات الصوتية الإلكترونية ، و أن يضبط كل ما يظهر إنه قد أستعمل في تنفيذ الجريمة الإلكترونية من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يُعتقد إن لها صلة بالجريمة ، وتحميلها من الموقع الذي نفذت من خلاله جريمة الابتزاز الالكتروني وكذلك يقوم عضو الضبط القضائي بسماع أقوال من يُمكن الحصول منه على معلومات وإيضاحات في شأن الحادثة ومرتكبها ، حتى لوكان السماع عن طريق الاتصال الفيديوي أو عن طريق تسجيل بصمة الصوت وإرسالها إلكترونياً عبر أحد التطبيقات الإلكترونية، على أن يُنظم محضراً بذلك [٣]. كما يجب على أعضاء الضبط

---

[١] جمال إبراهيم الحيدري ، الجرائم الإلكترونية وسبل معالجتها ، ط١، مكتبة السنهوري ،بغداد ،٢٠١٢،ص٧٦.

[٢] راشد بشير إبراهيم، التحقيق الجنائي في جرائم التقنيات، مركز الامارات للدراسات والبحوث الاستراتيجية ، العدد ٢٠٠٨،١٣١، ص٥٢.

[٣] المادة (٤٣) من قانون أصول المحاكمات الجزائية ، رقم (٢٣) لسنة ١٩٧١ المعدل .

القضاء أتخاذ كافة الوسائل التي من شأنها المحافظة على أدلة الجريمة [١] حتى و أن كانت تلك الوسائل إلكترونية كالتخزين بشكل إلكتروني في جهاز الحاسوب أو نقل أو نسخ الأدلة من الحساب الإلكتروني للجاني أو عن طريق التقاط الصور لها بوساطة كاميرا الهاتف المحمول أو السكنر أو غيرها من الوسائل المستحدثة .

ثانياً/ التحقيق الابتدائي في الجرائم الالكترونية:-

يتم التحقيق الابتدائي بإجراءات لازمة لابد من إتباعها ، حتى يكون استحصال الدليل الإلكتروني ممكناً ، إلا أننا سنركز البحث في هذه الفقرة على إجراء التفتيش والخبرة لأنهما الأهم من بين الإجراءات الأخرى في تحديد منهاج الإثبات الإلكتروني للجريمة الإلكترونية وكالآتي :-

١- **التفتيش:** ويقصد به الكشف عن محل الجريمة وأثرها ، و وسيلة ارتكابها ، وما أحاط بها وبمرتكبها من ظروف وملابسات أدت إليها . للمعلومات التقنية عالم خاص تتكون ذاتيته من شقين هما: الكيانات المادية والكيانات المعنوية [٢] ، وتبعاً لذلك فإن التفتيش باعتباره اجراء من اجراءات التحقيق الابتدائي يختلف في كلا الشقين، وعلى ذلك لا بُد من التفريق بين تفتيش الكيانات المادية وتفتيش الكيانات المعنوية وذلك في النقطتين الآتيتين:

أ) تفتيش الكيانات المادية : إن التفتيش المتعلق بالكيانات المادية في نطاق الجرائم الالكترونية يسهل إجراؤه وتنطبق القواعد التقليدية للتفتيش عليه ، إذ لا خلاف على إن الولوج إلى المكونات المادية للكمبيوتر بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يُفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى إن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هو من الأماكن العامة أم الخاصة، أذ إن لطبيعة المكان خصوصية ينبغي احترامها ، وعدم تجاوزها ، فإذا ما كانت الكيانات المادية في مكان خاص كمنزل المتهم أو أحد ملحقاته فلا يجوز اتخاذ إجراء التفتيش بخصوصها إلا في الحالات التي يجوز فيها القانون ذلك وبنفس

---

[١] المادة (٤٢) من قانون أصول المحاكمات الجزائية ، رقم (٢٣) لسنة ١٩٧١ المعدل .

[٢] م.م حسين خليل مطر ، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية ، بحث مقدم الى مؤتمر (الاصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد) الذي اقامته مؤسسة النبأ للثقافة والاعلام وجامعة الكوفة/كلية القانون ، بتأريخ ٢٥-٢٦ نيسان ، ٢٠١٨ ، منشور على الموقع الإلكتروني https://annabaa.org/arabic/studies/15926 تمت الزيارة بتاريخ ٢٠٢١/٨/٢ .

الإجراءات المقررة قانوناً . على شرط أن لا تتعلق تلك الماديات أو ترتبط بشخص غير المتهم.

أما بالنسبة لحالة وجود شخص في مكان عام (سواء كان طريق عاماً كالشوارع والطرق العامة أو عاماً بالتخصيص كالمقاهي والمساجد ... الخ) ، وفي حوزته كيانات مادية ، فهنا تتبع أليه التفتيش نفسها الخاصة بتفتيش الأشخاص[١] المتواجدين في المكان العام وقت إجراء التفتيش عليهم .

ب) تفتيش الكيانات المعنوية : اختلفت الآراء حول مسألة ، فرأي يجيز تفتيش الكيانات المعنوية وضبط البيانات الإلكترونية بمختلف أشكالها، مستنداً اصحابه بالقوانين الإجرائية التي تنص على إصدار الإذن بضبط (أي شيء) ،[٢] فإن ذلك يفسر بشموله لبيانات الكمبيوتر المحسوسة وغير المحسوسة ، أما الرأي الأخر فقد ذهب إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، و يقترح بأن يكون هناك تنظيم صريح وواضح، يمنح للجهات المختصة بالتحقيق صلاحية تفتيش المكونات المعنوية للكمبيوتر[٣] .

٢-الخبرة: من ضمن الإجراءات اللازمة التي يجب على المحقق الجنائي إجرائها عند التحقيق في جرائم الابتزاز الإلكتروني ، الاستعانة بأهل الخبرة ، أيماناً بمبدأ التخصص والذي يكون في غاية الأهمية بالنسبة للجرائم الإلكترونية ، فلا يجوز للمحق أو قاضي التحقيق اتخاذ أي إجراء إلكتروني بخصوص جريمة الابتزاز الإلكتروني من دون الرجوع لأهل الخبرة لأنهم أصحاب الاختصاص ، نظراً لكون الخبرة عبارة تقدير مادي أو ذهني يُبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في جريمة الابتزاز الإلكتروني بمعرفتها وبمعلوماته الخاصة سواء أكانت تلك المسألة الفنية متعلقة بشخص المتهم أم بجسم الجريمة أم المواد المستعملة في ارتكابها أم آثارها [٤] .

---

[١] خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ،ط١،دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠١١،ص٤٧.

[٢] ينظر نصوص المواد (٧٤ ، ٧٦ ، ٧٧، ٧٨ ، ٧٩) من قانون أصول المحاكمات الجزائية النافذ .

[٣] خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي ، الإسكندرية، ٢٠١٠، ص١٩٧.

(٤) عبد الأمير العكيلي ، سليم حربة ، شرح قانون أصول المحاكمات الجزائية ،ج١، بيروت،٢٠٠٩،ص١٢٦.

الخاتمة :

أن التطور التكنولوجي الهائل في مجال المعلومات الذي أسهم بشكل كبير في رخاء البشرية في جوانب عديدة من الحياة، هو نفسه الذي وفر ملاذاً أكثر أمانا لنوع جديد من المجرمين، وهيأ مجالا خصباً لنمو جرائم جديدة تتسم بالبساطة في ظاهرها ، وبالخطورة الشديدة فيما ترتبه من نتائج .

وإن كنا قد ركزنا في هذه الدراسة على جريمة الابتزاز الإلكتروني، فهذا لا يعني أن الجريمة الإلكترونية منحصرة فيه، فهناك كم هائل من الأفعال الجرمية التي وجدت في فضاء الانترنت الذي يعد وسطاً خصباً لنموها وتطورها . وبعد الانتهاء من كتابه بحثنا الموسوم بالابتزاز الإلكتروني تكييفه وسبل مواجهته فقد توصلنا إلى جملة من الاستنتاجات والمقترحات والتي سنبينها على وفق فقرتين وكالآتي :-

أولا : <u>الاستنتاجات</u>:

١-أن المشرع العراقي لم ينظم الابتزاز الالكتروني كجريمة مستقلة بذاتها، إلا أن ذلك لا يمنع من الالتجاء الى النصوص الجزائية الأخرى لمواجهة الابتزاز الإلكتروني .

٢- أن للقضاء العراقي دوراً بارزاً في الحد من جرائم الابتزاز الإلكتروني من خلال تطويع النصوص القانونية الواردة في متن قانون العقوبات العراقي بالكيفية التي من شأنها جعل الجاني محلاً لتنفيذ العقوبة المفروضة عليه ، نظراً لقيامة بابتزاز المجنى عليه وتهديده بفضح اسراره أو القيام بإفشائها في حالة عدم استجابة المبتز لطلباته فضلاً عن ذلك فقد يقترن الابتزاز الإلكتروني مع جريمة السرقة أو جريمة الفعل الفاضح أو جريمة هتك العرض أو الاغتصاب أو اللواط أو القتل وغيرها من الجرائم الواردة في متن قانون العقوبات النافذ ، فهنا ينبغي أن تكون العقوبة مناسبة لخطورة الجاني من جهة وللضرر الناشئ عن جريمة الابتزاز الالكتروني بمفردها او مقترنة بجريمة أخرى ، تحقيقاً لمتطلبات العدالة الجنائية .

٣- أن التطور المعرفي الحاصل، يستلزم بالضرورة وضع نصوص قانونية واضحة وصريحة لمعالجة هذه الجريمة وغيرها من الجرائم المعلوماتية التي ظهرت بفعل التطور، وذلك للحد من التوسع في تفسير النصوص القانونية الجزائية والذي يتعارض مع مبدأ "لا جريمة ولا عقوبة الا بنص".

٤-ضرورة الإسراع في تعديل الاجراءات الواردة في قانون أصول المحاكمات رقم (٢٣) لسنة (١٩٧١) حتى تكون ملائمة لطبيعة الجرائم الإلكترونية .

ثانيا: المقترحات :

١- تنظيم المشرع وعلى وجه الاستعجال نصوص بالجرائم الإلكترونية تحدد سلوكياتها المجرمة والعقوبات المناسبة لردع مرتكبها وزجر غيره .

٢- تعديل الإجراءات الواردة في قانون اصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧١ المعدل ، لتكون ملائمة وطبيعة الجرائم الالكترونية ، التي يتطلب لإثباتها والحد منها إتباع إجراءات خاصة تكون من ذات صنفها ، لأنه لا يمكن قياس الضرر وإثبات الأثر الناشئ عن الابتزاز الإلكتروني ، إلا من خلال الإجراءات الإلكترونية .

٣- إقامة دورات تدريبية متخصصة لأعضاء الضبط القضائي والقضاة من أجل تعريفهم بطبيعة الجرائم

الالكترونية وآلية التعامل معها.

٤- تفعيل الرقابة السابقة على مواقع التواصل الإلكترونية واللاحقة حتى يكون في الإمكان فرض السيطرة ولو بصورة جزئية ، أو شكلية على الجرائم الإلكترونية للحد من ارتكابها أو التقليل منها وبغض النظر عن النتيجة المتحققة سواء كانت مرضية أو بسيطة ، المهم أن يكون هناك ردعاً من شأنه أن يقلص من حجم جرائم الابتزاز الإلكتروني .

٥- ان تكون هناك محكمة مختصة بنظر القضايا الإلكترونية المرتكبة عبر الوسائل الإلكترونية. تكون ضليعة في المسائل المتعلقة بهذا الأمر، أي مختصة في المجال الإلكتروني ، ان يكون في المحكمة موظفين ذوي اختصاص في مجال هندسة المعلومات والتكنولوجيا.وظيفتهم تقديم الخبرة اللازمة للقضاة في الوقت المناسب ومن دون تأخير ، كما يجب أن تكون قراراتها ذات حجية قانونية وبمواجهة الجميع إذا ما اكتسبت حجيتها بفوات مواعيد الطعن ، أو بمصادقة الجهات العليا على ما اتخذته المحكمة المختصة بنظر دعاوى الجرائم الإلكترونية .

قائمة المصادر والمراجع

اولا: المصادر:-

-القوانين :

١-قانون العقوبات المصري رقم (٥٨) سنة ١٩٣٧.

٢- العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ .

٣- قانون اصول المحاكمات الجزائية رقم (٢٣) لسنة ١٩٧١.

ثانيا:المراجع:-

أ-المعاجم :-

١- أبو الفضل جمال الدين محمد بن مكرم (ابن منظور) ، لسان العرب ، دار صادر – لبنان- المجلد الثاني – حرف الباء- مادة (بزز) ، لا يوجد سنة نشر .

٢- الفيروز أبادي ، القاموس المحيط بيروت – لبنان،ط٨ ، باب الزاي ، فصل الباء،٢٠٠٥.

٣- محمد مرتضى الحسيني الزبيدي ، تاج العروس – ج٧- مطبعة حكومة الكويت- كويت – طبعة ثانية – ١٩٩٤ .

٤- معجم المصطلحات القانونية والقضائية المستخرجة من القوانين العربية والمعتمدة من قبل مجلس وزراء العرب – قوانين تنظيم المؤسسات العقابية – المركز العربي للبحوث القانونية والقضائية، الدورة ٢٦،القرار ٨٥٢ بتاريخ ٢٠ ديسمبر ٢٠١٠.

ب-الكتب :

١- احمد شوفي ، شرح الاحكام العامة لقانون العقوبات ، دار النهضة العربية ، القاهرة ،٢٠٠٣.

٢- أبو سعيدي ،مقال عن الابتزاز الالكتروني واثاره الاجتماعية والنفسية، بيروت ، لا يوجد دار النشر ، ٢٠١٦.

٣- أشرف احمد هلال ، الجرائم المعلوماتية في الاعتداء على الحق في الحياة الخاصة ، دار ال غالب للنشر والتوزيع، جدة ،١٤٣٦هـ .

٤- الحديثي، فخري، والزغبي، خالد، الجرائم الواقعة على الأشخاص، دار الثقافة للنشر والتوزيع ،عمان ،٢٠٠٩.

٥- الهميم، عبد اللطيف، احترام الحياة الخاصة، دار عمار، ٢٠٠٤ .

٦- ثنيان ناصر آل ثنيان ، اثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية ، جامعة نايف للعلوم الأمنية ، ١٤٣٣.

٧- جمال إبراهيم الحيدري ، الجرائم الإلكترونية وسبل معالجتها ، ط١، مكتبة السنهوري ،بغداد ،٢٠١٢،ص٧٦.

٨- حنان مبارك المضحكي ، الجرائم المعلوماتية " دراسة مقارنة" ، ط ١،منشورات الحلبي الحقوقية ، بيروت ٢٠١٤.

٩- خالد عياد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ،ط١،دار الثقافة للنشر والتوزيع ، الأردن ، ٢٠١١.

١٠- خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ،دار الفكر الجامعي ، الإسكندرية، ٢٠١٠.

١١- راشد بشير إبراهيم، التحقيق الجنائي في جرائم التقنيات، مركز الامارات للدراسات والبحوث الاستراتيجية ، العدد،٢٠٠٨.

١٢- رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون، العدد ٦٣ الصادرة عن كلية القانون جامعة الإمارات العربية المتحدة، السنة ٢٩، يوليو ٢٠١٥.

١٣- سالم عمر، المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج أسوار السجن، الطبعة الأولى، دار النهضة العربية، ، القاهرة،٢٠٠٠.

١٤- صفاء أوتاني، الوضع تحت المراقبة الإلكترونية "السوار الإلكتروني" في السياسة العقابية الفرنسية، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٥، العدد الأول ٢٠٠٩.

١٥- عبد الأمير العكيلي ، سليم حربة ، شرح قانون أصول المحاكمات الجزائية ،ج١، بيروت،٢٠٠٩.

١٦- عبد الفتاح بيومي حجازي ،مكافحة جرائم الكومبيوتر والانترنت في القانون العربي النموذجي ، ط١، دار الفكر الجامعي ، الإسكندرية ، ٢٠٠٦.

١٧- عبد اللطيف محمود ربايعة، بحث بعنوان الجرائم الالكترونية (التجريم والملاحقة والاثبات)، فلسطين ، ٢٠١٦.

١٨- عبد الهادي لهزيل، نظام السوار الإلكتروني وفق السياسة القضائية الجزائرية، لبنان، لا توجد سنة النشر.

١٩- عمار عباس الحسيني ، جرائم الحاسوب والانترنت الجرائم المعلوماتية ، ط١، مكتبة زين الحقوقية والأدبية ش.م.م. بيروت ،لبنان ،٢٠١٧.

٢٠- كاظم عبد جاسم الزيدي، المسؤولية الجنائية عن جرائم النشر والاعلام في القانون العراقي ، مكتبة صباح ، بغداد ،٢٠١٦.

٢١- كاظم عبد جاسم الزيدي ، جريمة الابتزاز الالكتروني (دراسة مقارنة) ، مكتبة القانون المقارن ، ط١، بغداد ، ٢٠١٩.

٢٢- مأمون محمد سلامة: الإجراءات الجنائية في التشريع المصري، ج١، دار النهضة العربية، القاهرة، ٢٠٠١.

٢٣- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، دار النهضة العربية ، القاهرة ٢٠٠٩.

٢٤- نمور، محمد سعيد، . شرح قانون العقوبات، القسم الخاص، الجزء الأول، الجرائم الواقعة على الأموال، دار الثقافة للنشر والتوزيع ،عمان ،٢٠٠٢ .

ج – البحوث والمقالات :

١- بن عسكر ، منصور عبد الرحمن ، استطلاع اراء الشباب السعودي : دور المؤسسات الاجتماعية في التبصير بالجرائم الالكترونية، مجلة دراسات وابحاث، المجلد ٤،العدد٦ ٢٠١٢.

٢- بوشنافة جمال، تنفيذ العقوبة بالوضع تحت المراقبة الإلكترونية، دراسة في ظل القانون رقم ١٨/٠١ المعدل والمتمم لقانون تنظيم السجون الجزائري، مجلة الدراسات القانونية، المجلد ٤، العدد١، جامعة يحي فارس بالمدية – الجزائر ٢٠١٨.

٣- خالد حساني، نظام المراقبة الإلكترونية في النظم العقابية الحديثة نحو أنسنة العقوبة الحلقة ١، مقال منشور بجريدة الشعب العدد ١٧٢١٩ ، ٢٠١٦.

٤- يحيى خطاطبه – د عز الدين النعيمي صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين /

سليمان الغديان – / –مجلة البحوث الأمنية العدد ٦٩ ربيع الآخر ١٤٣٩هـ / يناير ٢٠١٨ . الإسلامية، جامعة الملك سعود،٢٠١٣.

د – الرسائل والاطاريح:

١- أفراح بنت خميس بن عامر اللويهية ،مشكلة الابتزاز الإلكتروني لدى طلبة مرحلة التعليم ما بعد الأساسي ، رسالة مقدمة لنيل شهادة الماجستير في الآداب ، كلية الآداب والعلوم الاجتماعية ،جامعة السلطان قابوس ،سلطنة عمان ،٢٠١٨.

٢- زاهر خالد صباح ، دور الوسائل العلمية الحديثة في الإثبات الجنائي في فلسطين ، رسالة مقدمة لنيل شهادة الماجستير في القانون العام ، جامعة القدس ، أبو ديس ، فلسطين ، ٢٠١٧.

هـ – الكتب والبحوث والمقالات الإلكترونية :

١- د. حسين عبد علي عيسى ، د. شيلان شريف محمد ، التحقيق الابتدائي في جريمة الاحتيال الإلكتروني المجلة العلمية لجامعة جيهان – السليمانية ، المجلد ٢ ، العدد ٢ ، كانون الأول ، ٢٠١٨ ، ص٣٠٥. منشور على الموقع الإلكتروني https://sj.sulicihan.edu.krd/files/2018/12/303-319.pdf ، تمت الزيارة بتاريخ ٢٠٢١/٨/٣ .

٢- حسين خليل مطر ، إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية ، بحث مقدم الى مؤتمر (الاصلاح التشريعي طريق نحو الحكومة الرشيدة ومكافحة الفساد) الذي اقامته مؤسسة النبأ للثقافة والاعلام وجامعة الكوفة/كلية القانون ، بتأريخ ٢٥-٢٦ نيسان ، ٢٠١٨ ، منشور على الموقع الإلكتروني https://annabaa.org/arabic/studies/15926 تمت الزيارة بتاريخ ٢٠٢١/٨/٢.

٣- فاطمة الزهراء عبد الفتاح ، آليات وضوابط مراقبة مواقع التواصل الاجتماعي ، بحث منشور على الموقع https://futureuae.com/ ، تمت الزيارة بتأريخ ٢٠٢١/٦/٩ .

٤- **فايز عبد الله الشهري ، دور مؤسسات المجتمع في مواجهة ظاهرة الابتزاز وعلاجه ، الابتزاز الإلكتروني نموذجاً، بحث مقدم لندوة الابتزاز ((المفهوم-الاسباب- العلاج))، مركز باحثات لدراسات المرأة بالتعاون مع قسم الثقافة الإسلامية بجامعة الملك سعود ، ط١ ، ١٤٣٢ هـ**

منشور على الموقع . https://feqhup.com/uploads/١٤٥٦١٢٣٧٧٦٣٤٤٨١.pdf تمت الزيارة بتاريخ ٤/٨/٢٠٢١ .

٥- عبير نجم ،تداعيات الابتزاز الالكتروني على الشباب والاحداث الصغار وسبل المواجهة والعلاج ، ٢٠١٩، https://www.alnahrain.iq/post/448 تاريخ زيارة الموقع ٤/٧/٢٠٢١

٦- مجموعة مؤلفين ، الابتزاز الإلكتروني جريمة العصر الحديث ، سلسلة ثقافاتنا الأمنية ، العدد الثاني ، ٢٠١٩ ، ص ١٢٨-١٢٩، منشور على الموقع https://moi.gov.iq/upload/upfile/ar/925.pdf تمت الزيارة بتاريخ ٣/٨/٢٠٢١ .

٧- موقع هيئة تنظيم الاتصالات والحكومة الرقمية ،تمت زيارة موقع بتاريخ ٩/٧/٢٠٢١. https://www.tdra.gov.ae/ar/mediahub/cyber-blackmailing.aspx

٨- مقال بعنوان " أغلب ضحايا الابتزاز الالكتروني "فتيات" والجناة غرضهم "الأموال" ، منشور على موقع مجلس القضاء الأعلى https://www.hjc.iq/view.3774/ ، تمت الزيارة بتاريخ ٢/٨/٢٠٢١

٩- قرار لمحكمة جنايات المثنى منشور على الموقع https://www.dorar-aliraq.net/threads/1083279، تمت الزيارة بتاريخ ٣/٨/٢٠٢١ .

List of sources and references;

First, the sources:

Laws:

1 - Egyptian Penal Code No. (58) of 1937.

2 - Iraqi Sanctions No. 111 of 1969.

3 - Criminal Procedure Law No. 23 of 1971.

Second: References:-

A- Dictionaries:-

1 -Abu al-Fadl Jamal al-Din Muhammad ibn Makram (Ibn Manzur), Lisan al-Arab, Dar Sader - Lebanon - Volume Two - Letter Ba - Material (Buzz), no publication year.

2 -Al-Fayrouz Abadi, The Ocean Dictionary, Beirut - Lebanon, 8th edition, Bab Al-Zai, Chapter Al-B, 2005.

3 -Muhammad Murtada Al-Hussaini Al-Zubaidi, The Crown of the Bride - part 7 - Kuwait Government Press - Kuwait - second edition - 1994.

4 -A Dictionary of Legal and Judicial Terms Extracted from Arab Laws Approved by the Council of Arab Ministers - Laws Regulating Punitive Institutions - Arab Center for Legal and Judicial Research, Session 26, Resolution 852 of December 20, 2010.

b-books:

1 - Ahmed Shufi, Explanation of the General Provisions of the Penal Code, Dar Al-Nahda Al-Arabiya, Cairo, 2003.

2 - Abu Saidi, an article on electronic blackmail and its social and psychological effects, Beirut, no publishing house, 2016.

3- Ashraf Ahmed Hilal, Information Crimes in Attacking the Right to Private Life, Dar Al Ghalib for Publishing and Distribution, Jeddah, 1436 AH.

4 - Al-Hadithi, Fakhri, and Al-Zoghbi, Khaled, Crimes against Persons, House of Culture for Publishing and Distribution, Amman, 2009.

5 - Al-Hamim, Abdul Latif, Respect for private life, Dar Ammar, 2004.

6 - Thanayan Nasser Al-Thunayan, Proving Cybercrime, An Applied Rooting Study, Naif University for Security Sciences, 1433.

7 -Jamal Ibrahim Al-Haidari, Electronic Crimes and Ways to Treat It, 1st Edition, Al-Sanhoury Library, Baghdad, 2012, p. 76.

8- Hanan Mubarak Al-Mudhaki, Information Crimes “A Comparative Study”, i 1, Al-Halabi Human Rights Publications, Beirut 2014.

9-Khaled Ayyad Al-Halabi, Investigation and Investigation Procedures in Computer and Internet Crimes, 1st Edition, House of Culture for Publishing and Distribution, Jordan, 2011.

10- Khaled Mamdouh Ibrahim, The Art of Criminal Investigation in Electronic Crimes, Dar Al-Fikr Al-Jamii, Alexandria, 2010.

11-Rashid Bashir Ibrahim, Criminal Investigation of Technology Crimes, Emirates Center for Strategic Studies and Research, Issue, 2008.

12- Rami Metwally Al-Qadi, Electronic Monitoring System in French and Comparative Law, Sharia and Law Journal, Issue 63 issued by the College of Law, United Arab Emirates University, Year 29, July 2015.

13 - Salem Omar, Electronic Surveillance, a Modern Method for Executing a Freedom-Depriving Punishment Outside Prison Walls, First Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

14 - Safaa Otani, Placement under Electronic Surveillance "Electronic Bracelet" in the French Punitive Policy, Damascus University Journal of Economic and Legal Sciences, Volume 25, Number One 2009.

15 - Abdul Amir Al-Akaili, Salim Harba, Explanation of the Code of Criminal Procedure, Part 1, Beirut, 2009.

16 - Abdel-Fattah Bayoumi Hegazy, Combating Computer and Internet Crimes in Arab Model Law, 1st Edition, Dar Al-Fikr University, Alexandria, 2006.

17- Abdul Latif Mahmoud Rabaya, a paper entitled "Criminalization, Prosecution, and Evidence" entitled "Criminalization, Prosecution and Evidence", Palestine, 2016.

18 -Abdelhadi Hazel, The electronic bracelet system according to the Algerian judicial policy, Lebanon, there is no year of publication.

19-Ammar Abbas Al-Husseini, Computer and Internet Crimes Information Crimes, 1st Edition, Zain Law and Literary Library LLC. Beirut, Lebanon, 2017.

20- Kazem Abdul Jassim Al-Zaidi, Criminal Responsibility for Publication and Media Crimes in Iraqi Law, Sabah Library, Baghdad, 2016.

21- Kazem Abdul Jassem Al-Zaidi, The Crime of Electronic Extortion (A Comparative Study), Comparative Law Library, 1st Edition, Baghdad, 2019.

22- Mamoun Muhammad Salama: Criminal Procedures in Egyptian Legislation, Volume 1, Dar Al-Nahda Al-Arabiya, Cairo, 2001.

23-Muhammad Obeid Al-Kaabi, Crimes Arising from the Illicit Use of the Internet, Dar Al-Nahda Al-Arabiya, Cairo 2009.

24- Tigers, Muhammad Saeed, . Explanation of the Penal Code, Special Section, Part One, Crimes against Money, House of Culture for Publishing and Distribution, Amman, 2002.

C - Research and articles:

1- Bin Askar, Mansour Abdel Rahman, Saudi Youth Opinions Poll: The Role of Social Institutions in Insight into Electronic Crimes, Journal of Studies and Research, Volume 4, Issue 6 2012.

2 -Bouchnafa Jamal, Execution of Punishment by Placement under Electronic Surveillance, Study under Law No. 01/18 amending and supplementing the Algerian Prison Organization Law, Journal of Legal Studies, Volume 4, Issue 1, Yahya Fares University in Medea - Algeria 2018.

3- Khaled Hassani, The Electronic Monitoring System in Modern Punitive Systems Towards Humanizing Punishment, Episode 1, an article published in Al Shaab newspaper, No. 17219, 2016.

4 -Yahya Khataba - Dr. Izz Al-Din Al-Nuaimi Pictures of the crimes of electronic extortion and their motives and the psychological effects of them from the point of view of teachers, men of the authority and psychological counselors / Suleiman Al-Ghadyan - / - Journal of Security Research Issue 69 Rabi' Al-Akhir 1439 AH / January 2018 Islamic, King Saud University, 2013.

D - Letters and theses:

1 -Afrah bint Khamis bin Amer Al-Luwayhiya, the problem of electronic extortion among post-basic education students, a thesis submitted for obtaining a master's degree in Arts, College of Arts and Social Sciences, Sultan Qaboos University, Sultanate of Oman, 2018 .

2- Zaher Khaled Sabbah, The Role of Modern Scientific Methods in Criminal Proof in Palestine, a thissis submitted for obtaining a master's degree in public law, Al-Quds University, Abu Dis, Palestine, 2017.

E - Books, research and electronic articles:

1 -Dr. Hussein Abdel Ali Issa, d. Shailan Sharif Muhammad, The preliminary investigation into the crime of electronic fraud, The Scientific Journal of Cihan University - Sulaymaniyah, Volume 2, Issue 2, December, 2018, pg. 305. Published on the website https://sj.sulicihan.edu.krd/files/2018/12/303-319.pdf , accessed on 3/8/2021.

2 -Hussein Khalil Matar, Investigation Procedures and Evidence Gathering in Cybercrime, a paper presented to the conference (Legislative Reform is a Path to Good Government and Combating Corruption), which was held by Al-Nabaa Foundation for Culture and Media and the University of Kufa/College of Law, on April 25-26, 2018, published on Website: https://annabaa.org/arabic/studies/15926, accessed on 2/8/2021.

3- Fatima Al-Zahra Abdel-Fattah, mechanisms and controls for monitoring social networking sites, research published on the website https://futureuae.com/, visited on 9/6/2021.

4- Fayez Abdullah Al-Shehri, The Role of Society Institutions in Confronting the Phenomenon of Extortion and its Treatment, Electronic Extortion as a Model, Research Presented to the Extortion Symposium ((Concept - Reasons - Treatment)), Research Center for Women's Studies in cooperation with the Department of Islamic Culture at King Saud University, 1, 1432 It is posted on the site. https://feqhup.com/uploads/145612377634481.pdf, accessed on 4/8/2021.

5- Abeer Najm, The Consequences of Electronic Blackmail on Young People and Young Juveniles and Ways of Confrontation and Treatment, 2019, https://www.alnahrain.iq/post/448, date of visit 4/7/2021

6- A group of authors, Electronic extortion, the crime of the modern era, Our Security Cultures series, second issue, 2019, pp. 128-129, published on the website https://moi.gov.iq/upload/upfile/ar/925.pdf Visited on 3/8/2021.

7- The Telecommunications Regulatory Authority and the Digital Government website, a website was visited on 7/9/2021. https://www.tdra.gov.ae/en/mediahub/cyber-blackmailing.aspx

8- An article entitled “Most of the victims of electronic blackmail are “girls” and the perpetrators are “money”, published on the website of the Supreme Judicial Council https://www.hjc.iq/view.3774/, visited on 2/8/2021

9- A decision of the Al-Muthanna Criminal Court published on the website https://www.dorar-aliraq.net/threads/1083279, visited on 3/8/2021.