Investigation and Difficulties Facing the Crime of Electronic Extortion

Emad Jawad Moussa
College of Education for Humanities, University of Anbar, Ramadi, Iraq
emad.jawad@uoanbar.edu.iq

KEYWORDS: **Electronic Blackmail, Investigation, Inspection, Search, Evidence.**

https://doi.org/10.51345/.v33i4.588.g310

ABSTRACT:

The crime of electronic extortion is a difficult crime and is shrouded in mystery during the stages of its commission, especially since it is committed by people who have sufficient knowledge in the field of information technology. The perpetrator is also characterized by characteristics that differ from the rest of the perpetrators of traditional crimes. In addition to the development in the field of informatics which requires the use of advanced methods in the field of investigation and evidence, It also requires the presence of experts and specialists within the investigation team, the investigative judge and members of the judicial police who have sufficient experience to seize the data related to the crime and follow up on their source to identify the perpetrator and arrest him taking into account the recording and keeping of those procedures to constitute evidence and conviction against the perpetrators of crime. Therefore, the investigators in such crimes must be people who have full experience and knowledge in the field of information technology than the perpetrators of the crime of extortion. The aim of our research is to identify the investigation procedures and the appropriateness of those procedures to reduce and control all the difficulties facing the crime of electronic extortion. the procedures for investigating the crime taken by investigators and judicial officers is the second aim. To achieve the first aim, the researcher dealt with the investigation procedures starting from going to the crime scene to conducting an inspection and search. The second aim was achieved by dealing with the difficulties encountered in the investigation as the difficulties in international cooperation.

التحقيق والصعوبات التي تواجه جريمة الابتزاز الإلكتروني

م.م. عماد جواد موسى
كلية التربية للعلوم الانسانية، جامعة الأنبار، الرمادي، العراق
emad.jawad@uoanbar.edu.iq

الكلمات المفتاحية | الابتزاز الإلكتروني، تحقيق، معاينة، تفتيش، الأدلة.

https://doi.org/10.51345/.v33i4.588.g310

ملخص البحث:

تعّد جريمة الابتزاز الالكتروني من فئة الجرائم الصعبة ويكتنفها الغموض اثناء مراحل ارتكابها، وخصوصاً أنها ترتكب من اشخاص لهم الدراية الكافية في استخدام وسيلة تقنية المعلومات، وكذلك يتصف مرتكبوها بصفات تختلف عن باقي مرتكبي الجرائم التقليدية، اضافة الى التطور حاصل في مجال المعلوماتية ممّا يتطلب استخدام أساليب متطورة في مجال التحقيق وجمع الأدلة، كذلك يتطلب وجود خبراء ومختصين ضمن فريق العمل المكلف بالتحقيق، وايضاً يجب تمتع قاضي التحقيق وأعضاء الضبط القضائي بالخبرة الكافية لغرض ضبط البيانات المتعلقة بالجريمة ومتابعة مصدرها لمعرفة الفاعل والقبض علية مع الأخذ بعين الاعتبار تسجيل تلك الإجراءات وحفظها لتشكل دليل إثبات وإدانة ضد مرتكبي تلك الجريمة، لذلك يجب على المحققين في مثل تلك الجرائم ان يكونوا من الاشخاص الذين يمتلكون الخبرة والدراية التامة في مجال تكنلوجيا المعلومات تفوق مرتكبي جريمة الابتزاز، الهدف من بحثنا الوقوف على إجراءات التحقيق ومدى ملائمة تلك الإجراءات للحد والسيطرة على كافة المشاكل التي ترافق الجريمة، كذلك معرفة إجراءات التحقيق المتخذة من المحققين ورجال الضبط القضائي اثناء سير التحقيق في الجريمة، لتحقيق الهدف الاول، تناول الباحث إجراءات التحقيق بدأ من التوجه الى مسرح الجريمة وصولا الى إجراء المعاينة والتفتيش. وتحقق الهدف الثاني بتناول الصعوبات التي تواجه التحقيق وكذلك الصعوبات في التعاون الدولي.

المقدمة:

تختلف جريمة الابتزاز الإلكتروني بشكل عام عن الجرائم التقليدية، ممّا يشكل ضغط على سلطات التحقيق في كيفية ملائمة تلك الإجراءات بصفة عامة وجريمة الابتزاز الالكتروني بصفة خاصة، وتبقى الإجراءات الجزائية في قواعد التحقيق هي نفسها مع الأخذ بالفروقات الموضوعية للتحقيق، وتتشابه تلك الإجراءات لكافة الجرائم سواء كان جريمة الكترونية ام جريمة عادية كون جميعها تحتاج الى المعاينة والتفتيش والاستجواب وعمليات جمع الأدلة وفحصها، والاهم من ذلك على المحقق اتخاذ الحرص التام للمحافظة على الأدلة المضبوطة في مسرح الجريمة من العبث او الضياع.

تظهر صعوبات من خلال سير التحقيق حسب طريقة ارتكاب الجريمة كونها من الجرائم العابرة للحدود والتي تتطلب التعاون الدولي المعلوماتي وابرام المعاهدات بين الدول، والتحقيق بجريمة الابتزاز ليس بالأمر الهين، السبب ما يكتنف تلك الصعوبات من غموض ويصاحبها العديد من العراقيل، تكمن أهمية البحث لمعرفة إجراءات التحقيق في جريمة اصبحت ظاهرة تهدد أمن الافراد والمجتمعات على حد سواء بل امتدت آثارها لتهدد المؤسسات بكافة أنواعها سواء كانت اهلية ام مؤسسات حكومية، فيما يخص الاشكالية للبحث تكمن في مدى قدرة رجال التحقيق والضبط القضائي للتوصل الى أهم النتائج لإدانة مرتكبي جريمة الابتزاز الإلكتروني وتقديمهم الى القضاء لينالوا الجزاء العادل، وسوف نستعرض هذه الإجراءات من خلال مطلبين الأول إجراءات التحقيق في جريمة الابتزاز الالكتروني والمطلب الثاني صعوبات التحقيق في جريمة الابتزاز واهم الصعوبات الدولية.

المطلب الأول :إجراءات التحقيق في جريمة الابتزاز الالكتروني

نظراً للتطور حاصل لتقنية المعلومات والانتشار الحاصل لشبكة الانترنيت ممّا يتطلب استخدام أساليب متطورة في مجال التحقيق وجمع الأدلة، وكذلك يتطلب وجود خبراء ومختصين ضمن فريق العمل المكلف بالتحقيق، وايضاً يجب تمتع قاضي التحقيق وأعضاء الضبط القضائي بالخبرة الكافية لغرض ضبط البيانات المتعلقة بالجريمة ومتابعة مصدرها لمعرفة الفاعل والقبض علية مع مراعات تسجيل تلك الإجراءات وحفظها لتشكل دليل إثبات[1]. سوف نتناول ذلك بفرعين على النحو الآتي:

الفرع الأول: التحقيق في جريمة الابتزاز الالكتروني

التحقيق في جريمة الابتزاز الالكتروني نفسها في الجرائم التقليدية، لأنّ الجريمتين تحتاج إلى التفتيش وجمع الأدلة المتحصلة، وأنّ من أهم الإجراءات التي يجب الالتزام بها من المحقق هي المحافظة على الأدلة المضبوطة في مسرح الجريمة خوفا من العبث بها أو فقدانها، وان التحقيق عرف على انه ((الإجراءات المتبعة من المحقق وتؤدي الى معرفة تفاصيل الجريمة وتحديد الفاعل وتقديمة الى المحاكم المختصة)، وتكون هذه الإجراءات عبارة عن عملية تفتيش او تكون فنية كمضاهاة البصمات، او برمجة لتحديد كيفية الدخول إلى المعطيات المخزنة في أجهزة الحاسوب[2]. وبالإمكان استخلاص أهم الإجراءات التي يجب ان تتبع من المحقق والتقييد بها في البحث أو التقصي عن الجرائم الالكترونية و تتمثل بالآتي[3]:

1- مراعاة حرمة الحياة الخاصة والحرص على عدم انتهاكها، والمحافظة على الإسرار الموجودة داخل الحاسب الآلي حتى لا يشوب الدليل اي عيب وممّا يؤدي الى بطلانه.

2- الحصول على اذن مسبق من الجهات المختصة عند تفتيش الحاسب الآلي وملحقاته وضبط تلك الاجهزة.

3- المحافظة على الادلة المتحصلة والاهتمام بطرق حفظها وتقديمها إلى المحكمة بالحالة التي ضبطت عليها.

4- ان يكون هدف المحقق الرئيسي التوصل الى النتائج التي تظهر الحقيقة الكاملة وتحقيق العدالة من خلال امتلاكه موهبة التحقيق[4].

المحقق هو من يضبط سير التحقيق كونه المؤتمن على الإسرار والحرص على عدم إفشائها ويتعرض للمسؤولية في حالة مخالفة ذلك، كما أشار قانون أصول المحاكمات الجزائية العراقي بنص المادة (**40**) الفقرة ب (يخضع أعضاء الضبط القضائي لرقابة حاكم التحقيق وله ان يطلب من الجهة التابعين لها النظر في آمر من تقع منه مخالفة لواجباته او التقصير في عملة ومحاكمته انضباطياً ولا يخل ذلك بمحاكمتهم جزائياً إذا وقع منهم ما يشكل جريمة)، ونصت المادة **42** منه (على أعضاء الضبط القضائي ان يتخذوا جميع الوسائل التي تكفل المحافظة على ادلة الجريمة) ونجد ان القانون العراقي أضاف العقوبات الانضباطية إضافة للعقوبات الجزائية في نص المادة (**40**) كون المحقق موظفاً عاماً ويخضع إلى قانون انضباط موظفي الدولة رقم (**14**) لسنة **1991**.

من إجراءات المحقق هو استجواب المتهم ومن خلال الاستجواب يتوصل الى فهم شخصية المتهم ويتحاور معه بشكل مفصل عن الفعل الجرمي المرتكب من قبلة و بالأدلة المتوفرة ضده ويطالبه بالرد على تلك الأدلة أما بالنفي او التسليم والاعتراف بها[5]، ويعد الاستجواب من أهم إجراءات التحقيق فهو يجمع بين وسيلة أثبات أو وسيلة دفاع والاستجواب يكون في مرحلة التحقيق الابتدائي.

التحقيق في جريمة الابتزاز الإلكتروني تحكمه قواعد التحقيق نفسها في الجريمة العادية، والخلاف يكون بالمعرفة وامتلاك المؤهلات للتعامل مع مقتضيات الجريمة لدى المحقق من الأجهزة الالكترونية والأدلة الرقمية، وذلك لتمتع مجرم تلك الجرائم بالذكاء وله دراية كافية بتقنية المعلومات، ونصت الإجراءات في التحقيق على عدم الضغط والتأثير على المتهم وانتزاع الأقوال منه بالإكراه، وهو مبدأ مستقر علية في النظام الجنائي، وإذا صدر الاعتراف من المتهم بالإكراه يعدّ باطلاً، وهذا الإجراء نص علية بالمادة **127** من قانون أصول المحاكمات الجزائية العراقي[6] إذ نصت على (لا يجوز استعمال أية وسيلة غير مشروعة للتأثير على المتهم للحصول على إقراره، ويعتبر من الوسائل غير المشروعة إساءة المعاملة والتهديد بالإيذاء والإغراء والوعد والوعيد والتأثير النفسي واستعمال المخدرات والمسكرات والعقاقير).

الفرع الثاني: المعاينة والتفتيش في جريمة الابتزاز الالكتروني

أن إجراءات التحقيق في جريمة الابتزاز تختلف عن الجرائم الأخرى من ناحية المعاينة والتفتيش والخبرة في تلك الجريمة، ونتطرق لذلك بالنقاط التالية:

اولا: المعاينة

الهدف من المعاينة التوصل الى آثر الدليل المتبقي في مسرح الجريمة لمستخدم شبكة الانترنيت، وتشمل الرسائل المرسلة والمستقبلة منه وكل الخطوات التي استخدمت في الجهاز المتصل بشبكة الانترنيت، ومستخدم تلك الشبكة يترك أثراً لأن الموقع المستخدم يفتح سجلاً خاصاً به يحتوي عنوان الموقع، ونوع والمتصفح الذي يستخدمه وعنوان رقم (IP) الدائم والمتغير للكمبيوتر الذي يتصل منه، وفي حالات معينة ممكن التوصل الى عنوان البريد الالكتروني واسم المستخدم[7]، إنّ الآثار الرقمية المستخرجة من أجهزة الكمبيوتر لها فائدة كبيره في عملية جمع الأدلة وضبطها لما تحتويه من معلومات قيمة مثل صفحات المواقع والبريد الالكتروني والفيديو الرقمي وغرف الدردشة والمحادثات والملفات المخزونة في الكمبيوتر والصور المرئية والدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمة[8].

عند انتقال أعضاء الضبط القضائي إلى مسرح الجريمة في حالة وقوع جريمة عن طريق استخدام شبكة الانترنيت لمعاينتها، ولأهمية المكان كونه مسرح وقوع الجريمة ومركزها وله الأولوية لبدء التحقيق بالبحث والتحري عن الأدلة والآثار الناشئة عن ارتكاب تلك الجرائم بهدف إيضاح الأسلوب الأمثل للكشف عن كامل إبعادها دون إغفال موقع او جزء او جانب منها، وعلى الرغم من ان الانتقال إلى مسرح الجريمة يتم بالطريقة نفسها للجرائم الأخرى، إلا ان الانتقال في جريمة الابتزاز يكون الى عالم افتراضي وليس عالم مادي. هناك عدة طرق بالإمكان المحقق أو اي عضو من أعضاء الضبط القضائي ان ينتقل بها عبر الفضاء الالكتروني ومن تلك الطرق هي:

1- أفضل مكان لإجراء المعاينة الانتقال لمقر عمل مزود خدمة الانترنيت.

2- يستطيع المحقق الانتقال إلى العالم الافتراضي للمعاينة من خلال الخبير التقني إذا اباح له القانون بذلك [9].

ولكي تكون المعاينة في جريمة الابتزاز الإلكتروني لها فائدة في كشف الحقائق ،كشف مرتكبيها، على المحقق مراعاة الخطوات الآتية:

أ. القيام بتصوير جهاز الكمبيوتر والأجهزة المرتبطة به مع ملاحظة تصوير الجزء الخلفي لجهاز الكمبيوتر مع مراعاة توثيق وقت ومكان تلك الإجراءات.

ب. ملاحظة الطريقة التي تم بها اعداد النظام والآثار الالكترونية وخصوصاً السجلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المستخدم في الولوج إلى الموقع او الدخول معه في حوار.

ت. عدم نقل أي معلومة في مكان ارتكاب الجريمة الا بعد إجراء الاختبار الخاص بخلو المحيط الخارجي لموقع الحاسوب من المجالات المغناطيسية التي تسبب مسح البيانات المسجلة [10].

أنّ القيام بإجراء إعادة المعاينة المستمرة لمسرح الجريمة قد تكشف دائماً عن أدلة جديدة، قد يكون هناك دليل مخفي من الجاني[11]، ونستخلص من ذلك أن المعاينة في الجرائم الالكترونية لمسرح الجريمة قد لا تكون مجدية كما هي في الجرائم العادية، لوجود صعوبات أثناء التنفيذ كونها تكون متخصصة بالبحث في جهاز الكمبيوتر وملحقاته ويتعامل المحقق مع معلومات وبيانات مخزنة فيه.

ثانيا: التفتيش

البحث والتفتيش في الاجهزة الالكترونية لا يمكن القيام به الا باستخدام الوسائل الالكترونية وأنّ تفتيش نظم الحاسب الآلي هو تفتيش للفضاء الالكتروني وان أوعية التخزين وتفتيش البيانات المحفوظة فيه ان كان مزوداً بحافظات الكترونية للعمليات المنجزة عن طريقه، وهو أمر يتعلق بالقدرة على تحديد المطلوب للبحث في نظام معلوماتي الكتروني، لأنه يمكن ان تكون هناك عواقب قانونية لأنها من خلال البحث قد تكشف أشياء عن خصوصية البيانات المخزنة في النظام[12]، ان قواعد التفتيش الجرائم الالكترونية تنقسم على نوعين قواعد موضوعية وقواعد شكلية ونتناول ذلك كما يأتي:

اولا: القواعد الموضوعية للتفتيش

في حالة وقوع جريمة ونسب تلك الجريمة إلى شخص او عدة أشخاص، فيجب ان تتوفر في حق المراد تفتيشه دليل كاف للاعتقاد بأنّ الجاني قد ارتكب تلك الجريمة سواء كان الفاعل أصيلا او مشاركا فيها، ولا يقتصر الأمر علىَ جمع الأدلة والقرائن ونسبها إلى فاعلها، بل يجب أنّ تتضمن تلك الأدلة على معلومات تعزز موقف المشتبه به وتنفي عنة ارتكاب الجريمة[13].وأنّ توفر الأدلة الكافية شرط لاتخاذ أي إجراء يتضمن المساس بحرمة الشخص أو المسكن، وأنّ الجرائم الواقعة عبر الانترنيت فان أذن التفتيش يصدر لضبط أدلة تفيد في وقوعها، والقصد من الأدلة الكافية أنها مجموعة المظاهر والإمارات التي تكفي وفقاً للسياق الفعلي والمنطقي وترجع ارتكابها ونسبتها إلى شخص محدد كان المرتكب الاصلي لها او الشريك[14]، الأدلة والاجهزة الموجودة في مسرح الجريمة لها الاثر في اكتشاف الحقيقة ويجب توفر الاسباب لدى المحقق واليقين

على وجود تلك الاجهزة في مكان الحادث استخدمت في الفعل الجرمي، وذلك تحديد مكان التفتيش ومحلة في الجرائم الالكترونية هو الكمبيوتر بجميع محتوياته والشبكة المتصل بها والمستخدمين له[15]، ونستخلص تلك الشروط، السبب، والمحل، السلطة المختصة.

أ. السبب يقصد به وقوع جريمة بالفعل، واتهام شخص او عدة أشخاص سواء كانوا فاعلين اصليين للجريمة او مشاركين فيها، إضافة إلى وجود أدلة تساعد في اظهار الحقيقة، ان هدف التفتيش هو العثور على أدلة اثبات الجريمة والكشف عن الفاعل، فان الجريمة قد تقع على الشبكة او تقع باستخدامها.

ب. محل التفتيش وهو المكان أو المستودع الذي يحتفظ الشخص بالأشياء المادية المتضمنة إسراره، وان الحاسب الآلي المتصل بشبكة الانترنيت ومكوناتها المزود الخادم الآلي والمضيف وملحقاته هو محل التفتيش في جريمة الابتزاز،، ان الدليل الذي يوجد بالحاسب الآلي بطبيعته دليل مادي كالمنزل او شخصه كما هو في الحاسوب المحمول او الهاتف النقال، ولذلك رجال الضبط القضائي عند طلب الأذن بالتفتيش عليهم تحديد المحل بدقة والغرض منه وان يتأكد انه مما يجوز تفتيشه، وإلا كان الإجراء باطلاً فمقر الهيئات الدبلوماسية مثلا لا يجوز تفتيشها [16].

ثانيا: القواعد الشكلية للتفتيش

القواعد الشكلية فيها شروط بما ان التفتيش يتم بأسلوب الكتروني من القائمين به يجب أنّ يتم بالشكل الصحيح والسريع مع طلب تفريغ المكان من الاشخاص المشتبه بهم والعاملين على أجهزة الحاسوب، وبعد ذلك يتم إجراء التفتيش على الأجهزة ومحتوياتها والاتصالات التي أجريت في مكان الجريمة ومن ثم القيام بنسخ كافة المعلومات للرجوع اليها، يتطلب لصحة الدليل ان يكون مستمداً من إجراء تفتيش بشكل صحيح. وانه يتطلب مهارات فنية خاصة موجودة لدى المحقق ليتمكن من السرعة في العمل والحفاظ على تلك الأدلة من الإتلاف أو الحذف او التعديل لسرعة تغير الأدلة الرقمية[17]، ولكي يقوم المحقق بالتفتيش علية الاستعانة بالفنين والمختصين بالحاسوب والانترنيت، وعلى الجهات المختصة ان تمنحهم الإذن بالتفتيش والتحقيق، وعلى ذلك يجب ان تضم سلطات التحقيق الخاصة بالتفتيش أعضاء من ذوي الاختصاص في الحاسوب والأنظمة الالكترونية ليتمكنوا من القيام بعملهم بالشكل الصحيح.

وهناك بعض الاستثناءات التي منحت صلاحية القيام بالتفتيش من المحققين دون منحهم الأذن المسبق مثل الجرائم المشهودة التي يشاهد فيها الجاني حال ارتكابه للجريمة والتي يسمح فيها القانون لرجال السلطة وللمواطنين بضبط الأشياء التي يحملها الجاني، والجرائم الواقعة داخل المسكن عند طلب ذلك من صاحب

المسكن للتدخل في حالة قيام الجناة استخدام جهاز الحاسوب الخاص به للاعتداء على غيره، وهذا ما جاء بنص المادة **73** من قانون أصول المحاكمات الجزائية العراقي[18].

ان إصدار أمر التفتيش من القاضي المختص يجب ان يكون مسبباً ويكون له غاية محددة كان يكون قائم بقصد التوصل إلى ما يفيد ارتكاب جريمة اعتداءات على نظم التشفير او قرصنة، وان لا يكون التفتيش شاملاً وإنما ينبغي ان يكون أكثر تخصصاً لكي يكون مبرراً القيام به. ان قرار التفتيش محدد المدة وعلى القائم بالتفتيش علية الالتزام بتلك المدة المحددة ويقوم بالتفتيش عن طريقها، وان قاضي التحقيق علية مراعاة تلك المدة عند إصدار الأذن وان لا تكون طويلة لعدم بقاء المأذون بتفتيشه مهدداً في حريته وحرمة مسكنة لمدة طويلة، وتحسب المدة من يوم إصدار الأذن لا من يوم وصوله لمن أحيل إلية الأذن إذا كان الأذن ينص على احتساب مدته بالأيام، أما إذا صدر الأذن محدد بالساعات فيجب احتساب الساعات من اليوم التالي لصدوره، ما إذا حدد أمر التفتيش بأجل معين فإنه لا يشترط ان يتم تنفيذه فور صدوره بل يكفي ان يكون ذلك في وقت يدخل في المدة المحددة للأمر[19].

فللمحقق ان يرى الوقت المناسب لكي يكون مثمراً ولا يترتب على انقضاء المدة المحددة لا جراء التفتيش البطلان بل يشترط عدم تنفيذه بعد ذلك إلى ان يجدد مفعوله لمدة أخرى كتابة، ويجوز لقاضي التحقيق بان يصدر أكثر من أمر لتفتيش المتهم، ولكن تداخل قواعد سريان أوامر التفتيش لا يعني أنها أوامر مفتوحة غير محدده المدة طالما ان كل أمر منها صدر صحيحاً وفق القانون. ان التفتيش في جريمة مرتكبة عبر الانترنيت هو جهاز الكمبيوتر وملحقاته والأجهزة المتصلة به والشبكة التي تشمل مزود الخدمة، وهذا كله ينصب على مكونات مادية (hardware) او ما يطلق عليها بالقطع الصلبة، وكذلك مكونات منطقية (software) او ما يطلق عليها بالبرمجيات[20]، وسوف نتعرف على طريقة التفتيش في هذه المكونات على النحو الآتي:

1. تفتيش المحتوى المادي لجهاز الحاسوب

الكمبيوتر يحتوي مجموعة من الوحدات متصلة بعضها ببعض بصورة تجعلها تعمل كنظام متكامل مثل الشاشة ولوحة المفاتيح ووحدة الذاكرة جميعها تشكل الحاسوب، التي تقبل إدخال البرامج وتنسيق وتبادل البيانات والأوامر[21]، ان الولوج إلى محتويات الحاسب الالي لكشف الجريمة و هوية مرتكبها لإخلاف علية اذا كان ضمن السياقات القانونية للتفتيش، وان التشريعات التي نصت صراحة على تفتيش مكونات الكمبيوتر قليلة فقط قانون إساءة استخدام الكمبيوتر الانكليزي الصادر لسنة **1990**، وقانون القسم **(16-1)** من قانون المنافسة الكندي الذي يعطي الاذن للمفتش استخدام اي نظام للحاسب الالكتروني،

وأما ما يخص المشرع العراقي فقط أشار إلى تفتيش جهاز الكمبيوتر ضمن المادة (**26** اولا) من مشروع قانون الجرائم المعلوماتية المقترح.

2. تفتيش المحتوى غير المادي لجهاز الحاسوب

جهاز الحاسوب الآلي أثار خلافاً في الفقه بشأن جواز التفتيش على مكوناته غير المادية، فهناك آراء تقول يجوز التفتيش بأي شكل بموجب صدور مذكرة التفتيش لأنها تعطي الأذن بضبط أي شيء داخل محتويات الكمبيوتر، وهذا الأمر دفع المشرع الفرنسي إلى تعديل المادة **94** من قانون الإجراءات الجزائية[22] وإضافة عبارة المعطيات المعلوماتية إذ أصبحت تلك المادة من القانون (يباشر بالتفتيش جميع الأماكن التي يمكن العثور فيها على أشياء او معطيات معلوماتية تفيد في كشف الحقيقة". ويذهب الرأي الأخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية او غير الملموسة)، لذلك ان هذا الاتجاه يقترح النص الواضح على تفتيش جهاز الحاسوب في التشريعات القانونية لان الغاية من التفتيش البحث عن الأدلة المادية او اي مادة معالجة بواسطة الحاسب[23]. وهناك رأي استند إلى الواقع العلمي والذي يتطلب ان يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلا ماديا، أما الرأي الذي استقر علية هو ان معطيات الحاسوب تصلح للتفتيش عن الأدلة الجرمية وضبطها لان غاية التفتيش هي الحصول على الأدلة الخاصة بالجريمة وكشف الغموض بها وتقديم البرامج غير المشروعة المخزنة على الحاسب الآلي الخاص بالمتهم كدليل اتهام يؤخذ بة أمام المحكمة المختصة[24].

المطلب الثاني: صعوبات التحقيق في جريمة الابتزاز واهم العوائق الدولية

تتطلب جريمة الابتزاز الالكتروني لغرض الكشف عنها إلى وسائل تقنية حديثة ويعود ذلك لحداثة تلك الجريمة ولاحترافية مرتكبيها، الأمر الذي يضع أمام المحققين صعوبات في إثبات تلك الجريمة، فهي تحتاج إلى أساليب متطورة وخبرة يتمتع بها أعضاء التحقيق في التعامل مع الأدلة الرقمية التي يتحصل عليها وكيفية تنفيذها للوصول الحقيقة وملابسات الجريمة لغرض مواجهة المتهم بما يتوفر لدية من الأدلة وضمان عدم مراوغته إثناء التحقيق ليصل في النهاية لاكتشاف الحقيقة التي يبحث عنها.

الفرع الاول: الصعوبات التي تواجهه التحقيق

التحقيق في جريمة الابتزاز الالكتروني يواجهه العديد من الصعوبات والعراقيل التي قد تسبب للمحققين ان لا يخرج بنتائج ايجابية يتوصل فيها إلى مرتكبي تلك الجريمة، بل قد تؤدي تلك الصعوبات إلى خروج المحقق بنتائج سلبية تؤدي إلى فقدان ثقة المجتمع والضحايا في الأجهزة الأمنية وكذلك فقدان المحقق للثقة في نفسه

لعدم قدرته على معالجة تلك القضايا والتي تمس امن المجتمع بشكل كبير[25]، وان من أهم تلك الصعوبات تتمثل في الآتي:

اولا: حق الإنسان في الخصوصية

من ابرز التحديات التي تواجه المحقق في جريمة الابتزاز الالكتروني هو حق الإنسان في الخصوصية، والسبب في ذلك يرجع إلى صعوبة التوازن بين الحرمة الشخصية للإنسان وبين المصالح التي يتطلبها تنفيذ القانون، وأن الخصوصية أحد حقوق الإنسان الرئيسية المتعلقة بكرامته وبقيمته، مثل الحق في الرأي والتعبير والمشاركة السياسية وذلك أصبح من أهم حق للإنسان، وان كافة الدساتير والتشريعات للدول اعترفت بتلك الخصوصية وعملت على حمايتها، كما جاء بنصوص الإعلان العالمي لحقوق الإنسان[26]، وفي المعهد الدولي للحقوق المدنية والسياسية، وفي غالبية اتفاقات حقوق الإنسان الدولية والإقليمية، وفي ميثاق الامم المتحدة المادة **15** منه. وكل الدول في العالم ضمنت في دساتيرها حكماً بشأن الخصوصية، قد أصدرت الولايات الأمريكية عام **1986** قانون يقضي بحرمة وخصوصية الاتصالات الالكترونية ومن ضمنها المعلومات والبيانات الحاسوبية[27]، وأصدرت الحكومة الفرنسية عام **1958** قرار يمنع نشر الحقائق المتعلقة بخصوصية الإفراد وفرض عقوبات من يقوم بمخالفة أمر هذا القرار، تضمن الدستور العراقي لسنة **2005** فقد أورد ضمن نصوصهما على حماية الحق في الخصوصية الشخصية بموجب المادة **17** من الدستور العراقي، وفي مشروع قانون الجرائم المعلوماتية المقترح في العراق لسنة **2011** جاء في المادة **26** الفقرة د (تتبع المعلومات إلى نظم الحاسوب والشبكات محل الاشتباه، على ان تبلغ الجهات التي تملك هذه النظم والشبكات بالإجراء ونطاقه على ان ينحصر نطاق هذا الإجراء بما يتعلق بالتصرف محل التحقيق دون انتهاك او مساس بحقوق الغير"[28]).

ثانياً: قلة الخبرة لدى جهات التحقيق

من اكبر المعوقات التي تواجهه التحقيق في جريمة الابتزاز الالكتروني هو قلة الخبرة، لأنها تعدّ الأداة إمام القضاء في التعامل مع تلك الجرائم، كون ضعف التعامل مع الأدلة الرقمية ومعرفة دلالتها وطريقة الحصول عليها، وكذلك التعامل مع الأقراص الصلبة او المغنطة والتعامل مع مصطلحات الحاسوب الآلي تشكل نقطة ضعف لدى المحقق والقاضي الذي ينظر في مثل تلك الجرائم، وخاصة إذا التعامل مع متهم مثل المجرم الالكتروني الذي لدية المهارة والمراوغة في التصرف للتخلص من التهم المسندة إلية إذا كان المحقق الذي إمامة غير ملم لجوانب الحاسب الآلي وخفاياه[29].

ثالثاً: سيادة القانون والحاجة لتطوير القوانين

من الأهمية والضرورة إلى إيجاد اتفاق دولي وآلية موحدة دولياً للتعامل مع جريمة الابتزاز الالكتروني لحداثة تلك الجريمة وانتشارها في كافة الدول، ان اختلاف التشريعات والقوانين للدول تشكل حاجزاً إمام اكتشاف العديد من المجرمين، وذلك كونها بيئة خصبة لهم لتنفيذ مخططاتهم الإجرامية، فيجب توحيد تلك الإجراءات الدولية لتسهيل متابعة مجرمي الحاسب الآلي، وتوفير المساعدة والتعاون بينهم للإطاحة بهم واكتشاف جرائمهم، وعلى ذلك تم التأكيد من الأمم المتحدة في تقريرها عن إعمال الدورة التاسعة للمجلس الاقتصادي والاجتماعي على ضرورة وضع توصيات ذات توجه علمي لمنع ومكافحة الجرائم المتعلقة بالحاسب الآلي وتعزيز القدرات على منع تلك الجرائم والتحري عنها[30].

ان الدور الذي تلعبه الشرطة الدولية (الانتربول) لمنع ارتكاب الجرائم الالكترونية يحتاج إلى مزيد من التفاعل بين الدول ومواصلة التعاون فيما بينهم للحد من خطورة تلك الجرائم، وأنّ القانون الدولي لم يتوصل إلى الجهد المطلوب للتعامل مع هذه الجرائم، فما زال يحتاج إلى جهود مكثفة ومزيد من التعاون والعمل المتواصل لوضع أسس كفيلة لتحقيق التعاون الدولي لمواجهة الجرائم الالكترونية ومن ضمنها جريمة الابتزاز الالكتروني.

الفرع الثاني: الصعوبات الدولية للتحقيق في جريمة الابتزاز الإلكتروني

ان حصول المحقق على المعلومات غالباً تكون تلك المعلومات مملوكة لبعض الإفراد أو الشركات أو مؤسسات والدول في بعض الاحيان، والصعوبة هنا أن أصحاب المعلومات يحاولون اتخاذ إجراءات لحماية تلك المعلومات فالإفراد والمؤسسات يحاولون تسخير كل إمكانياتهم من أجل حماية الأنظمة المعلوماتية الخاصة بهم دون تعاون مشترك بهدف حمايتها بشكل عام وأنّ غياب التعاون والتنسيق يلعب دوراً رئيسياً يؤثر في عدم انحسار دور الجريمة الالكترونية وبالتالي صعوبة إثباتها[31]، بالمقابل وجود تعاون بين محترفي الإجرام المعلوماتي، فضلاً عن ذلك البرامج المستخدمة من المجرمين في نشاطهم الإجرامي هناك تعاون فيما بينهم ويتبادلون النصائح والخبرات المتعلقة بأنشطتهم ممّا يزيد خطورة هجومهم[32]، وهناك عوائق تحول دون التعاون الدولي في مكافحة الجريمة الالكترونية وأهمها:

1- اختلاف الإجراءات القانونية

ان الإجراءات القانونية من تحري وتحقيق وإجراء المحاكمات قد تثبت فائدتها في دولة ما وتنعدم تلك الفائدة في دولة اخرى وقد يمنع القيام بإجراء تلك الإجراءات من المراقبة الالكترونية والتسليم المراقب وغيرها من الإجراءات فان طريقة جمع الاستدلالات والتحقيق القانوني في دولة ما قد تكون الطريقة نفسها غير متاحة في دولة ثانية، لذلك الدول المطبقة للقانون قد تصاب بالخذلان لعم تطبيق تلك الإجراءات من الدول

الاخرى، إضافة إلى ان السلطات القضائية في الدول غير المطبقة قد لا تسمح باستعمال أي ادلة اثبات توصل اليها في هذه الدولة غير مشروعة، وان تم الحصول علية بطرق مشروعة.

2- عدم وجود معاهدات ثنائية او جماعية بين الدول

ان المعاهدات والاتفاقيات بين الدول تساهم بسرعة اكتشاف الجرائم الالكترونية، وفي حال وجودها فأنها قاصرة على تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم وبرامج الحاسب وشبكة الانترنيت، وأنّ هذا التطور في الجريمة يؤدي إلى أرباك المشرع وسلطات الأمن في الدول، وبعدها يظهر الاثر السلبي في التعاون الدولي(33). وبناء على ما جاء أصبح أنّ التعاون الدولي لمكافحة الجرائم المعلوماتية ومن ضمنها جريمة الابتزاز الإلكتروني أمر حتميّ يتطلب الاهتمام الجاد بالموضوع و تعزيز فاعلية الإجراءات الموجودة، وان نقطة البداية هي ضرورة رسم سياسة جنائية متناسقة من اجل معالجة الإجرام ألمعلوماتي عن طريق تقويم الأنشطة الإجرامية مع أهمية الاتفاق على ماهية الأنشطة التي يضفي عليها التجريم ألمعلوماتي حتى يؤدي هذا التجريم ثماره وتسد الثغرات في وجه مرتكبي الجرائم الالكترونية، فان تلك الإجراءات إذا لم يتم التعاون والتنسيق الدولي سيجعل مرتكبي تلك الجرائم إلى التمادي بتحقيق ما يريدون دون الوقوع تحت طائلة القانون.

3- نقص خبرة سلطات الاستدلال

ان التحدي الذي تواجهه أجهزة العدالة الجنائية في جرائم الحاسب الآلي وشبكة الانترنيت وأنّ الجناة في هذه الجرائم لهم مفردات ومصطلحات خاصة بهم لدرجة إنهم يطلقون على أنفسهم اسم النخبة بدعوى إنهم على معرفة بإسرار الحاسوب ولغاته، ويطلق على رجال الشرطة والقضاء صفة الضعفاء، ولذلك يجب عليهم تطوير وتحديث مهاراتهم في تقنية المعلومات لمواجهة تلك الجرائم من خلال برامج للتدريب وإدارات متخصصة للاستدلال وايجاد وسائل تحقيق متخصصة في مثل تلك الجرائم، وهناك بعض المحاولات الجادة من بعض الدول في استيعاب رجال الشرطة والقضاء ضمن المتخصصين في المعلوماتية ولم تنفذ تلك المحاولات لوجود بعض الصعوبات منها(34):

أ- ضعف الميزانية المالية لدى أجهزة الأمن والقضاء بالنظر إلى خبرة المتخصصين في علوم الحاسوب، عكس ما تنفقه مؤسسات القطاع الخاص على العاملين في مجال الحاسب الآلي لديها.

ب- الخبرة العلمية لدى سلطات الضبط والتحقيق الجنائي المتأتية من ممارسة إعمال الضبط والتحقيق في الجريمة الالكترونية، لم تقع حتى بالعدد والشكل الذي يوازي الجرائم التقليدية كالسرقة والقتل لذلك الخبرة لديهم مازالت حديثة مع التطور الحاصل في الجريمة المعلوماتية.

الخاتمة:

التحقيق في جريمة الابتزاز الإلكتروني من المواضيع المهمة، كون الجريمة تمس الفرد والمجتمع بشكل مباشر لمساسها بأهم حق من حقوق الإنسان إلا وهو حقة بحرمة حياته الخاصة، إذ ان المعلومات والبيانات تعد من أهم ممتلكاته التي اهتم بها على مر العصور بدأ من تدوينها على جدران المعابد وصولاً الى الأقراص الممغنطة، وان الحداثة في تقنية المعلومات وانتشار شبكة الانترنيت ادى الى ظهور صور مستحدثة لجرائم اطلق عليها تسميات عديده منها الجرائم الالكترونية والجرائم المعلوماتية وأخطرها جريمة الابتزاز الالكتروني التي أطلق عليها جريمة العصر، ان التشريعات القانونية والإجراءات المتعبة اغلبها تنطبق على الجريمة التقليدية، ولذلك واجهة المحققين في جريمة الابتزاز صعوبات في التحقيق والاثبات وجمع الأدلة، بعد الانتهاء من بحثنا الخاص بالتحقيق وأهم الصعوبات التي تواجه المحقق في جريمة الابتزاز الالكتروني ولو بشكل موجز توصلنا الى عدة استنتاجات وتوصيات عسى ان يكون فيه فائدة للمتلقي سواء رجال التحقيق او الباحثين وان كان هناك تقصير غير متعمد فهذا عمل بشري يعتريه النقص مهما بذلنا من جهد ويبقى الكمال لله وحدة.

الاستنتاجات:

1- ان أساس ارتكاب الجريمة هو استخدام التكنلوجيا الحديثة المتمثلة بشبكة الانترنيت ومواقع التواصل الاجتماعي وهو الواقع الافتراضي لمسرح الجريمة.
2- يعد الابتزاز الالكتروني جريمة عابرة للحدود كونها ذات طابع دولي وبالإمكان ارتكابها من عدة دول.
3- سهولة ارتكابها من قبل المبتز كونها لا تتطلب جهد عضلي او الانتقال الى مكان الحادث.
4- وجود فجوة واختلاف في التشريعات القانونية بين الدول مما زاد من صعوبة ملاحقتها.
5- عدم امتلاك الخبرة والمهارة لدى رجال التحقيق مما يؤدي الى ضياع او اتلاف الدليل.

التوصيات:

1- ضرورة أنشاء اجهزة أمنية وقضائية متخصصة لمكافحة جرائم بالابتزاز.
2- اخضاع رجال التحقيق لبرامج تدريبية بشكل دوري تخص الجريمة تساعدهم على تحديث معرفتهم واطلاعهم على أخر التطورات الحاصلة في مجال تكنلوجيا المعلومات.

3- العمل الجاد في مجال التحقيق بين الدول من خلال أبرام الاتفاقيات والمعاهدات الثنائية ومتعددة الاطراف.

4- ضرورة اعادة النظر بالنصوص المتعلقة في التحقيق واثبات الادلة في قانون اصول المحاكمات الجزائية رقم 23 لسنة 1971 وتضمينها نص لجريمة الابتزاز الالكتروني لأنها تختلف في وسائل التحقيق عن الجرائم التقليدية.

المصادر:

1. جمال ابراهيم الحيدري، الجرائم الالكترونية وسبل معالجتها، مكتبة السنهوري، ط**1**، العراق، **2012**.
2. سالم برايز الحقباني، مهارات التحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، **2015**.
3. عبد الصبور عبد القوي، المحكمة الرقمية والجريمة المعلوماتية، مكتبة الاقتصاد والقانون، الرياض، **2012**.
4. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية. القاهرة، ط**3**، **1988**.
5. طه السيد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات العربية، مصر، **2001**.
6. رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، اطروحة دكتوراه، جامعة ابو بكر بلقايد، تلمسان، كلية الحقوق والعلوم السياسية، **2018**.
7. قانون اصول المحاكمات الجزائية رقم **23** لسنة **1971**.
8. فتحية محمد قواري، المبادئ العامة في قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، ط**3**، الأفاق المشرقة، الأردن، **2013**.
9. قانون أصول لمحاكمات الجزائية العراقي رقم **23** لسنة **1971**.
10. خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، **2004**.
11. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، من بحوث المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، مركز بحوث والدراسات، العدد **1**، **2003**، الإمارات العربية المتحدة.
12. أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، دراسة مقارنة للتشريعات العربية والأجنبية، ط**1**، **2016**، مكتبة الوفاء القانونية، إسكندرية.
13. سامي حسين الحسيني، النظرية العامة للتفتيش في القانون المصري والقانون المقارن، دار النهضة العربية، القاهرة، **1972**.
14. مسودة مشروع قانون الجرائم المعلوماتية ( ) لسنة **2011**.
15. قانون الإجراءات الجزائية الفرنسي رقم **(49- 653)** لسنة **1994**.
16. داليا عبد العزيز، المسؤولية الجزائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، بحث منشور في مجلة جيل الابحاث القانونية المعمقة العدد **27**،**2018**.
17. المادة **12** من الاعلان العالمي لحقوق الانسان لسنة **1948**.

الهوامش:

(1) جمال ابراهيم الحيدري، الجرائم الالكترونية وسبل معالجتها، مكتبة السنهوري، ط1، العراق، 2012، ص83.

(2) سالم برايز الحقباني، مهارات التحقيق في الجرائم المعلوماتية، ص66

(3) عبد الصبور عبد القوي، المحكمة الرقمية والجريمة المعلوماتية، مكتبة الاقتصاد والقانون، الرياض، 2012، ص274

(4) محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية. القاهرة، ط3، 1988، ص 501

(5) طه السيد الرشيدي، الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، ص60

(6) رابحي عزيزة، الاسرار المعلوماتية وحمايتها الجزائية، ص 258

(7) قانون اصول المحاكمات الجزائية رقم 23 لسنة 1971

(8) فتحية محمد قواري، المبادئ العامة في قانون الإجراءات الجزائية الاتحادي لدولة الإمارات العربية المتحدة، ص 224.

(9) قانون أصول لمحاكمات الجزائية العراقي رقم 23 لسنة 1971

(10) المصدر السابق.

(11) خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، **2004**، ص **69**

(12) المصدر السابق، ص **155**

(13) لعل ذلك متوفر في مصر من خلال إدارة مكافحة جرائم المعلوماتية التابعة لوزارة الداخلية، انظر المصدر السابق، ص 157

(14) محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في مجال الجرائم الالكترونية، ص، 30

(15) ففي فرنسا يقوم فريق مكون من 13 شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إلية وكلاء النيابة والمحققين وجميعهم تلقوا تدريباً خاصاً إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بمرافقة المحققين إثناء التفتيش حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الالكتروني، وهم يقومون بعمل تقرير يرسل إلى قاضي التحقيق، اما عن المعدات والبرامج فهم يستخدمون برامج تستطيع استعادة المعلومات من على الاسطوانة الصلبة، كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة كما يوجد تحت تصرفهم برامج من قراءة الحاسبات المحمولة، انظر خالد ممدوح ابراهيم، مصدر سابق، ص 158.

(16) أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، ص302

(17) المصدر السابق، ص301

(18) خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مصدر سابق، ص194

(19) خالد ممدوح ابراهيم، المصدر نفسه، ص **212**

(20) أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مصدر سابق، ص**304**

(21) سامي حسين الحسيني، النظرية العامة للتفتيش في القانون المصري والقانون المقارن، ص210

(22) أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية والاختصاص القضائي بها، مصدر سابق، ص**305**

(23) قانون أصول المحاكمات الجزائية رقم **32** لسنة **1971**

(24) أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية، مصدر سابق، **306**

(25) خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مصدر سابق، ص**195**

(26) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، مصدر سابق، ص**158**

(27) انظر الفصل السابع الخاص بالقواعد الإجرائية المتعلقة بضبط الأدلة المعلوماتية وحفظها من قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي رقم 81 لسنة 2018 المواد من 121 إلى 123

(28) مسودة مشروع قانون الجرائم المعلوماتية ( ) لسنة **2011**

(29) خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، مصدر سابق، ص**197**

(30) قانون الإجراءات الجزائية الفرنسي رقم (**49- 653**) لسنة **1994**

(31) خالد ممدوح ابراهيم، المصدر نفسه، ص **198**

(32) أمير فرج يوسف، الإثبات الجنائي للجريمة الالكترونية، مصدر سابق، ص**311**

(33) داليا عبد العزيز، المسؤولية الجزائية عن جريمة الابتزاز الالكتروني في النظام السعودي، دراسة مقارنة، ص 27

(34) المادة **12** من الاعلان العالمي لحقوق الانسان لسنة **1948**