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 الأكاديمية العلمية

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

كلية القانون
College of Law

Legal methods in detecting cybercrime

Dr. Takleef Awad Abaid
Police College, Baghdad, Iraq
takleef1989@gmail.com

Article info.

Article history:
- Received 9 Apr 2023
- Accepted 11 June 2023
- Available online 1 Aug 2023

Keywords:
- **Legal methodsk .**
- **Detection.**
- **Cybercrime.**

Abstract: Many countries have been concerned with the need to legislate a punitive law that combats cybercrime, because of the danger these crimes pose to society at all levels. In Iraq, there Is no special law to combat cybercrime. Electronic crimes such as human trafficking as well as drugs, and these In and of themselves have special laws governing them, such as the Narcotics and Psychotropic Substances Law No. (50) of 2017, as well as the Electronic Signature and Electronic Transactions Law No. (78) of 2012, which included many articles related to electronic signature, electronic contracts and documents, as well as Electronic commercial and financial contracts and electronic financial transfers, which are of high risk and damage to the Iraqi economy on the one hand, and on the other hand, there is difficulty In the procedures for investigating these crimes because of the ease of concealment, the speed of destruction of evidence, and the impossibility of examining all data on the Internet, and difficulties appear in how to collect Evidence from inspection, inspection, experience, testimony and other procedures.

© 2023 TUJR, College of Law, Tikrit University

الأساليب القانونية في الكشف عن الجرائم الإلكترونية

م.د. تكليف عواد عبيد
كلية الشرطة، بغداد، العراق
takleef1989@gmail.com

معلومات البحث :

تواريخ البحث:
- الاستلام : ٩ / نيسان / ٢٠٢٣
- القبول : ١١ / حزيران / ٢٠٢٣
- النشر المباشر : ١ / حزيران /٢٠٢٣

الكلمات المفتاحية :
- الاساليب القانونية.
- الكشف.
- الجرائم الالكترونية.

الخلاصة: أهتمت الكثير من الدول بضرورة تشريع قانون عقابي يكافح الجرائم الالكترونية لما لهذه الجرائم من خطورة على المجتمع على كافة الأصعدة، أمّا في العراق فلم يوجد قانون خاص لمكافحة الجرائم الالكترونية وانما هو مجرد مشروع قانون وتوقف بسبب الخلافات السياسية بسبب رغبة بعضها حول أدخال مواد قانونية لا تدخل ضمن الجرائم الالكترونية مثل الاتجار بالبشر وكذلك المخدرات وهذه بحد ذاتها لها قوانين خاصة تحكمها مثل قانون المخدرات والمؤثرات العقلية رقم (٥٠) لسنة ٢٠١٧، وكذلك قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (٧٨) لسنة ٢٠١٢ الذي تضمن الكثير من المواد المتعلقة بالتوقيع الالكتروني العقود والمستندات الالكترونية وكذلك العقود التجارية والمالية الالكترونية والتحويلات المالية الالكترونية والتي تعد ذات خطورة عالية وضرر على الاقتصاد العراقي هذا من جهة ومن جهة أخرى هنالك صعوبة في إجراءات التحقيق في هذه الجرائم لسهولة إخفائها وسرعة إتلاف الأدلة واستحالة إمكانية فحص كل البيانات على شبكة الانترنت ، كما تظهر الصعوبات في كيفية جمع الأدلة من المعاينة والتفتيش والخبرة والشهادة وغيرها من الإجراءات الأخرى.

© ٢٠٢٣, كلية القانون، جامعة تكريت

المقدمة :

تعد الجرائم الإلكترونية الاكثر شيوعاً في الوقت الحاضر لما تتمتع بإمتيازات تدفع المجرم الى إرتكابها منها الحصول على المال أو إثبات الذات والإنتصار على النظام المعلوماتي أو تعرضه للضغط والتهديد بأمور تتعلق بالمنافسة التجارية، أو الغاية من الابتزاز قد تكون إجبار الشخص على القيام بعمل أو الامتناع عن عمل ولو كان مشروع كما يمكن أن يكون دافع إرتكاب الجريمة الإلكترونية سياسياً مثل إختراق الشبكات الحكومية والاجهزة الامنية أو نشر أفكار تمس أمن الدولة الداخلي أو الخارجي أو نظام الحكم أو المساس بقيادات لها تأثير كبير والتشهير بها كما أصبحت من الجرائم المنظمة وظهر الارهاب الالكتروني بوجود الكثير من المواقع الخاصة بالإرهابيين التي تحرض على القتل ونشر الافكار الارهابية كون الانترنت أصبح وسيلة سريعة جدا لإيصال الافكار لعامة الناس والامر الذي يمكن أن يستغل من العصابات والجماعات الارهابية لارتكاب جرائم تتقاطع مع القوانين والأخلاق والأعراف والآداب.

أهمية البحث: لهذا البحث أهمية تتمثل في الخطورة التي تشكلها الجريمة الإلكترونية كونها تمس حرمة الحياة الخاصة للأفراد والحق في الحصول على المعلومات وكذلك تهدد الامن الوطني وفقدان الثقة بالتقنية الامر الذي يحدث إرباكاً في جميع مفاصل الحياة.

مشكلة البحث : إن صعوبة إجراءات التحقيق في هذا النوع من الجرائم هي المشكلة الاساس وذلك لسهولة إخفاء معالم الجريمة وتدمير أدلتها بسرعة، إضافة لذلك كثرة البيانات المراد فحصها على شبكة الانترنت ،كما تكمن الصعوبة في جمع الادلة والتفتيش والمعاينة والشهادة والخبرة وغيرها من الاجراءات الاخرى.

منهجية البحث: إن الاعتماد الرئيسي في هذا البحث يكون على المنهج التحليلي لكثير من القوانين والتعليمات الواردة في القوانين العراقية ومن ضمنها قانون أصول المحاكمات الجزائية ذي العدد (٢٣) لسنة ١٩٧١ وكذلك مشروع مكافحة الجريمة الإلكترونية.

تقسيم البحث: سنتناول في هذا البحث إجراءات التحقيق في جرائم الانترنت والتي تختلف بطبيعتها عن إجراءات الجرائم العادية، وعليه سنقسم هذا البحث على مبحثين الاول المعاينة والتفتيش في الجريمة الإلكترونية، والثاني الشهادة والخبرة في الجرائم الإلكترونية.

المبحث الأول

المعاينة والتفتيش في الجرائم الالكترونية

كفل الدستور للفرد الحق في الحفاظ على أسراره كونها جزء من حياته وتخصه وحده وعدم إنتهاكها سواء كان ذلك في مراسلاته أو مسكنه أو أي معلومات أخرى على موبايله الشخصي وعليه لا يمكن إنتهاك هذا الحق دون سبب قانوني.

وبناءً على ما تقدم سنقسم هذا المبحث على مطلبين وكالاتي:-

المطلب الأول / المعاينة في الجريمة الإلكترونية

ويقصد بها معاينة الاثار التي يتركها مستخدم الانترنت كالرسائل المرسلة أو الواردة اليه وكل الاتصالات سواء من شبكة الانترنت أو الهاتف المحمول، فالمستخدم عندما يتصفح الانترنت حتما سيترك أثارا خلفه في كل موقع يتصفحه لان المواقع تحفظ سجلات تتعلق بعنوان الموقع والمتصفح وكذلك (IP) الدائم والمتغير الذي يتصل منه[١].

(١) د. ممدوح عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر ، ٢٠٠٦، ص٦٩.

وبناءً على ما تقدم سنقسم هذا المطلب على فرعين نتطرق في الاول عن الية إنتقال للمعاينة في العالم الافتراضي، والفرع الثاني سنتناول فيه إجراءات المعاينة لمسرح الجريمة في العالم الافتراضي.

الفرع الأول / الية الانتقال للمعاينة في العالم الافتراضي

إن الانتقال للمعاينة على محل الجريمة لايكون في الواقع المادي في هذا النوع من الجرائم وإنما يقتصر على العالم الالكتروني فقط حيث يستطيع القائم بالتحقيق الانتقال الى هذا العالم من خلال عدة وسائل أمّا عن طريق الحاسوب الخاص بالمحكمة أو عن طريق مزودين خمة الانترنت، أو من خلال الخبير التقني في هذا المجال والمتخصص في المسائل الالكترونية[١].

الفرع الثاني / إجراءات المعاينة في جرائم الانترنت

كما ذكرنا سابقاً أن المعاينة في العالم الافتراض تختلف عنها في الواقع المادي من حيث الاجراءات، فعندما يراد لكشف الحقيقة في الجرائم الإلكترونية يجب على القائم بالمعاينة أن يقوم بتصوير الحاسبة والموبايل وكافة المحتويات ويثبت وقت وتاريخ كل صورة ومكان التقاطها، كما يقوم بأعداد خطة تفصيلية ويفضل أن تكون موضحة بالرسوم من أجل تنفيذها بكل دقة، وأيضا الاهتمام بالطريقة التي تم بها إعداد النظام الالكتروني من أجل معرفة نوع الجهاز وموقعه، كما يجب على القائم بالمعاينة أن يدقق ويمنع إتلاف أي دليل الكتروني والحفاظ على الاقراص والاشرطة ورفع البصمات من عليها كونها ذات صلة بالجريمة[٢] وأن يقوم بحفظ كل مستندات الادخال والاخراج الورقية للحاسبة المرتبطة بالجريمة، وكذلك الاستعانة بالخبراء والباحثين الذين تتوافر فيهم الخبرة الفنية في هذا الجانب، فكل هذه الامور يجب أن تكون ضمن الاطار القانوني الذي نصت عليه القوانين الجنائية[٣].

المطلب الثاني / التفتيش في الجريمة الإلكترونية

يعرّف تفتيش الجرائم الإلكترونية بأنه" إجراء يسمح بجمع الادلة المخزنة أو المسجلة بشكل الكتروني بواسطة وسائل التفتيش الإلكترونية للبحث عن البيانات أو الادلة المطلوبة[٤].

---

(١) المصدر نفسه، ص١٥٧.

(٢) عميد الشرطة أحمد فخري رشيد: المواجهة الامنية للجريمة المعلوماتية، مكتبة السمهوري، بيروت، ٢٠١٨، ص١٠١.

(٣) د. محمد أبو العلا عقيدة: التحقيق وجمع الادلة في مجال الجرائم الإلكترونية، من بحوث المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد١، السنة ٢٠٠٣، دبي، الامارات العربية المتحدة، ص ٣٠.

(٤) المصدر نفسه، ص٣٢.

وبناءً على ذلك سنتناول موضوع تفتيش الجرائم الإلكترونية عي فرعين: نتناول في الفرع الاول القواعد الموضوعية لتفتيش شبكات الانترنت، أمّا الفرع الثاني سنتطرق فيه الى محل التفتيش في الجرائم الإلكترونية.

الفرع الأول / القواعد الموضوعية لتفتيش جرائم الانترنت

التفتيش في الجرائم الالكترونية قد يطال المكونات المادية وقد يطال المكونات المعنوية لها، فالتفتيش المتعلق بالكيانات المادية يسهل تفتيشه وتنطبق عليه قواعد التفتيش العادية، بمعنى أن البحث عن كل ما يتصل بالجريمة من خلال الدخول للمكونات المادية للأجهزة قد يفيد في كشف الجريمة ومعرفة مرتكبها وبالتالي فأن تفتيش تلك المكونات يختلف بحسب طبيعة المكان الموجودة فيه فقد يكون مكان عام أو خاص، فإذا وجد في مكان عام فعندئذٍ ينطبق عليه قواعد تفتيش الاشخاص أما إذا وجد في مكان خاص فينطبق عليه قواعد التفتيش التقليدية بحسب القوانين النافذة[١].

أمّا التفتيش المتعلق بالمكونات المعنوية فعند الرجوع الى قانون الاصول العراقي النافذ نجد أنه ذكر كلمة (أشياء) على اطلاقها أكثر من مرة ولم يتقيد بنوع معين من التفتيش بحسب المكونات ، وهذا يعني أن التفتيش في ظل الجرائم الإلكترونية يمكن أن يمتد الى جميع المكونات المادية والمعنوية ولكن ضمن ضوابط يجب مراعاتها عن تفتيش هذه الكيانات[٢].

وبالتالي فأن القواعد الموضوعية لتفتيش الاجهزة المرتبطة بالأنترنت تخضع لعدة شروط منها: أن تكون هنالك جريمة من جرائم الانترنت، وأن تُنسب الى شخص محدد بأدلة كافية سواء كان فاعل أصلي أو شريك، وأن تكون هناك أدلة كافية تبيح له عملية تفتيش الاجهزة الإلكترونية، وأن يتم تحديد محل التفتيش حيث يعتبر الهاتف المحمول والحاسوب بكل المكونات المادية والمعنوية محلاً للتفتيش[٣].

الفرع الثاني / القواعد الشكلية لتفتيش شبكات الانترنت

يتم تفتيش شبكات الانترنت بطريقة آلية الكترونية من القائم بالتفتيش[٤] بشكل سريع، ويتم ذلك من خلال أبعاد المشتبه فيهم والعاملين على تلك الاجهزة عن المكان والبدء بعملية التفتيش للوصول الى

---

(١) ينظر: المواد من (٧٢ – ٨٦) من قانون أصول المحاكمات الجزائية رقم (٢٣) لسنة ١٩٧١.

(٢) ينظر: المواد (٧٤، ٧٥، ٧٨، ٧٩) من القانون نفسه.

(٣) د. صالح البربري: دور الشرطة في مكافحة جرائم الانترنت، مؤتمر الجوانب القانونية والامنية للعمليات الإلكترونية، دبي، ٢٠٠٣، ص٣٩٢.

(٤) ذكرت المادة (٧٢) من قانون الاصول الجهة القائمة بالتفتيش وهي (قاضي التحقيق أو المحقق أو أي عضو ضبط قضائي بأمر من القاضي أو من يخوله القانون إجراءه).

المعطيات المخزّنة فيها ونقل مايفيد منها لكشف الجريمة بنسخ احتياطية ويشترط أن يكون التفتيش صحيح وضمن القواعد القانونية كونه شرطاً لصحة الدليل، كما يجب أن يكون القائم بالتفتيش لديه مهارة فنية في هذا المجال لكي يعمل بصورة سريعة من أجل الحفاظ على الادلة من الاتلاف كون هذه الادلة تتغير بسرعة[١].

المبحث الثاني

الشهادة والخبرة في الجريمة الإلكترونية

تعد الشهادة والخبرة من وسائل إثبات الجريمة الإلكترونية كونها تتميز بسهولة إخفاء الادلة الناتجة عن الجريمة وكذلك سرعة ارتكابها، الامر الذي يلزم الجهات القائمة بالتحقيق أن تطور من الاجراءات المتبعة في التحقيق والمحاكمة بالشكل الذي يلائم تطور هذه الجرائم[٢].

وعليه سنقسم هذا المبحث على مطلبين نتناول في المطلب الاول الشهادة وفي المطلب الثاني نتناول الخبرة في الجريمة الإلكترونية.

المطلب الأول / الشهادة في الجريمة الإلكترونية

في القواعد العامة تعرّف الشهادة بأنه مارآه الشاهد أو سمعه أو أدركه بحواسه[٣]. وبذلك سنتناول موضوع الشهادة الإلكترونية في فرعين الاول نتطرق فيه الى الشهادة الإلكترونية عن بعد، والفرع الثاني نتناول فيه الشاهد المعلوماتي والتزاماته.

الفرع الأول / الشهادة الإلكترونية عن بعد

الشهادة الإلكترونية هي نوع من الشهادة التي لايكون فيها الشاهد حاضراً جلسة التحقيق بذاته وانما يحضر عبر وسائل الكترونية من خلال شبكة الانترنت وبالتالي فأن الشهادة من هذا النوع تعتبر من الادلة وهي على نوعين: الشهادة المسجلة مسبقاً، والشهادة الإلكترونية الفورية[٤].

---

(١) د. عادل خميس العميري: التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة – القيادة العامة لشرطة الشارقة، المجلد ٢٢، العدد٨٦، الامارات، ٢٠١٣، ص٢٦٥.

(٢) بن بادر عبد الحليم: إجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والاشكالات، مجلة الحقوق والعلوم الانسانية، جامعة زيان عاشور بالجلفة، العدد٢٣، الجزائر، ٢٠١٥، ص٩٤.

(٣) الدكتور تكليف عواد عبيد: الاجراءات الجزائية في مرحلة المحاكمة لمنتسبي قوى الامن الداخلي، مكتبة القانون المقارن، ط١، بغداد، ٢٠٢٠، ص ١٦٧.

(٤) د. صالح البربري : المصدر السابق ، ص٢٦٠.

أولاً:- الشهادة المسجلة:-

ويقصد بها الشهادة التي يمكن عرضها على المحكمة فيما بعد كونها مسجلة مسبقاً وبالتالي فأن الجهات القائمة بالتحقيق يمكن أن تلجأ لهذا الاسلوب من الشهادة لضمان عدم وقوع أيّ تهديد على المتهم، وبالتالي صحة أقواله كونه على علم وإدراك بكافة المعلومات المتصلة بالنظام الالكتروني[١].

ثانياً:- الشهادة الفورية:-

هذا النوع منظام من الشهادة يتم غالباً عبر الدوائر الاتصالية الإلكترونية بحيث يظهر الشاهد بشكل مباشر وكامل كما لو كان حاضراً أمام المحكمة ويسمع أسئلة الاتهام والدفاع أثناء التحقيق كما إن معرفته بالنظام الالكتروني والمعلومات الإلكترونية محل الواقعة يعد شرطاً جوهرياً يلزم الشاهد بالشهادة الصحيحة عن الجريمة الالكترونية[٢] .

الفرع الثاني / الشاهد المعلوماتي والتزاماته

أولاً:- الشاهد المعلوماتي

هو صاحب الخبرة والفني في مجال البرمجة والتقنية الإلكترونية سواء كان في الهاتف المحمول أو الحاسوب بحيث لديه خبرة جيده في كيفية الدخول لها ومعالجتها إذا كان للتحقيق مصلحة في ذلك لكشف الجريمة[٣] وبذلك فأن الشاهد المعلوماتي يشمل عدة فئات منها: مشغل الحاسوب المسؤول عن تشغيل الانظمة الإلكترونية سواء في الحاسوب أو الهاتف المحمول والاجهزة المرتبطة بهما ويكون ذو خبرة واسعة في هذا المجال، بالإضافة الى الاشخاص المتخصصين في لإدخال البيانات ومعالجتها والذين يشترط أن تكون لديهم خبرة في هذا المجال إضافة الى الخبرة الفنية[٤]، والفئة الثانية هم المبرمجون المتخصصون في عمل البرامج الخاصة بالحاسوب والهاتف المحمول[٥] فبعضهم متخصص في عمل برامج التطبيقات حيث يقومون بمعرفة مواصفات وخصائص التطبيق المطلوب من محلل النظم ثم يقوم بصنع البرنامج المطلوب ضمن الشروط المطلوبة وقد ينفذ هذا العمل شخص واحد أو عدة أشخاص حسب حجم النظام والبرنامج المطلوب، والاخر متخصص في برامج الانظمة الإلكترونية والذين

---

(١) يحيى الشديدي: الشهادة في الجريمة الإلكترونية، مجلة البعث، المجلد ٣٨، العدد٥٠، دمشق، ٢٠١٦، ص٥٩.

(٢) يحيى الشديدي: المصدر نفسه، ص ٥٩ ومابعدها.

(٣) عبد الله الهلالي: تفتيش نظام الحاسب الالي وضمانات المتهم المعلوماتي، القاهرة، ٢٠٠٠، ص٤٣.

(٤) جميل عبد الباقي الصغير: الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة،٢٠٠١،ص٣٨٦.

(٥) عبد الفتاح حجازي: مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة ٢٠٠٧، ص١٥٨.

يقومون بتجهيز الحاسبة بالبرامج التي تتحكم بوحدات الادخال والاخراج وأي تعديلات يمكن أن تطرأ على هذه البرامج[١]، أمّا الفئة الثالثة فهم المحللون الذين يقومون بتجميع البيانات وتحليل الخطوات ودراستها من خلال تتبعها داخل النظام ومعالجة الامور بواسطة الحاسوب والانترنت والاجهزة المرتبطة بهما[٢] والفئة الرابعة هم مهندسون الصيانة والاتصالات وهم المسؤولون عن كافة أعمال الصيانة الخاصة بالحاسوب والهواتف المحمولة والانترنت وشبكات الاتصال المتعلقة بها[٣].

ثانياً:- التزامات الشاهد المعلوماتي

من التزامات الشاهد أن يذكر الحقيقة في شهادته ومعلوماته دون أن يغالط الحقيقة أو يجزم بالباطل أو يكتم ما يعرفه من الواجبات المفروضة عليه وهذا يتيح للشهادة أداء دورها بوصفها دليل اثبات يتيح للقاضي تقديراً سليماً للواقع وتطبيقاً صحيحاً للقانون[٤]، أمّا الشاهد المعلوماتي يلتزم بتقديم مايحوزه من معلومات جوهرية للدخول الى نظام المعالجة والحصول على أدلة الجريمة الى سلطة التحقيق للتوصل الى مرتكب الجريمة الإلكترونية، لكن فيما يتعلق بالإفصاح عن كلمات المرور لهذه الحسابات الإلكترونية فقد أختلف الفقه في هذا المجال فمنهم من يرى انه ليس من واجب الشاهد المعلوماتي الافصاح عنها وهذا ما سار عليه الفقه الالماني، بينما يرى جانت آخر من الفقهاء أنه من التزامات الشاهد المعلوماتي هو الافصاح عن كلمات المرور لهذه البرامج ولكن عدم إعطاء كلمة المرور غير معاقب عليه جنائيا الا في مرحلة التحقيق والمحاكمة وهذا ماسار عليه الفقه الفرنسي[٥].

أمّا موقف المشرع العراقي من مسألة الشهادة في جرائم الانترنت فنرى أن مشروع قانون الجرائم المعلوماتية يخلو من أي تنظيم لهذه المسألة عدا أشارة بسيطة نصت عليها المادة (٣٠/ب) منه يحيل مالم ينص عليه قانون الجرائم المعلوماتية الى قانون أصول المحاكمات الجزائية النافذ، الامر الذي يحيل تنظيم مسالة الشهادة في جرائم الانترنت الى القواعد العامة، ونرى ضرورة أن يتم تنظيم الشهادة في الجرائم الإلكترونية لاختلافها عن القواعد العامة للشهادة المنصوص عليها في قانون اصول المحاكمات العراقي، وذلك لان الشاهد في الجرائم العادية يكون ممن شاهد أو سمع أو أدرك بحواسه الجريمة أو أي

---

(١) عبد الله الهلالي: التزامات الشاهد بالأعلام عن الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٠،ص٢٠٥.

(٢) عبد الفتاح حجازي: المصدر السابق، ص١٥٩.

(٣) د. عبدالله حسين علي محمود: إجراءات جمع الادلة في مجال سرقة المعلومات، بحث مقدم الى المؤتمر العلمي الاول حول الجوانب القانونية والامنية للعمليات الإلكترونية، محور القانون الجنائي ، دبي، للفترة من (٢٦ – ٢٨) أبريل ٢٠٠٣، ص٦١٦.

(٤) الدكتور أحمد السولية: الحماية الجنائية والامنية للشاهد، دار الفكر الجامعي، ط١، الاسكندرية، ٢٠٠٧، ص٨٦.

(٥) د. يحيى الشديدي: المصدر السابق: ص٥٣.

دليل منها، اما الشاهد المعلوماتي فأنه يكون أحد الاشخاص الذين يعملون في مجال الحاسوب والانترنت من مشغلين ومهندسين ومبرمجين ومحللين.

كما نرى أنه يجب أن ينص قانون الجرائم المعلوماتية على الزام الشاهد المعلوماتي بأداء الشهادة إذا كان يمتلك معلومات جوهرية وضرورية للحصول على الادلة بشرط عدم إكراهه وحمله على الادلاء بالمعلومات والا شاب الشهادة عيباً وبالتالي بطلانها ويمكن تصور الاكراه في هذه الحالة إجبار الشاهد للأدلاء بكلمات المرور السرية.

المطلب الثاني / الخبرة في الجرائم الإلكترونية

الخبراء هم الاختصاصيون من ذوي الخبرة العلمية والفنية لأخذ آرائهم لإزالة غموض الجريمة وإعطاء الرأي العلمي بصددها[١] فالقائم بالتحقيق يعمل من أجل كشف الغموض عن الجريمة وبالتالي الاستعانة بذوي الخبرة في هذا المجال إستناداً لمبدأ التخصص كون الخبرة هي تقدير ذهني ومادي يبديه أصحاب الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق معرفتها بمعلوماته الخاصة سواء كانت تلك المسألة متعلقة بشخص المتهم أم بالجريمة أم في المواد المستعملة في إرتكابها وآثارها[٢]، وبالتالي فأن تشكيل فريق متخصص للتحقيق في الجرائم قد يعد أمراً ضرورياً، أمّا التشكيل على مستوى الجرائم الإلكترونية فالأمر مختلف نظراً لطبيعة الجرائم الإلكترونية التي تختلف عن الجرائم العادية كون الاولى مرتبطة بمسائل فنية وتقنية دقيقة وبالتالي يصبح لزاماً على القائم بالتحقيق الاستعانة بالخبراء والمختصين، لان تصديهم لفحص الشي وأبداء الرأي فيه دون اللجوء الى أصحاب الاختصاص يجعل قراره معيباً ويعوق الوصول للحقيقة، وعليه يتطلب من المتخصصين أن تكون لديهم خبرة فنية وتقنية في هذا المجال فقد تكون الجريمة المرتكبة تزوير مستندات أو الغش أثناء نقل أو بث البيانات أو أطلاق الفايروسات أو قرصنة أو التجسس[٣]، ولكن لايشترط في الخبير الكفاءة العالية في مجال التخصص فحسب وإنما يجب أن تضاف اليه سنوات من أعمال الخبرة في مجال التقنية والحاسوب، ومع قد يتفوق

(١) المحقق الجنائي عمار مزاحم مهدي: فن التحقيق الجنائي، ط٢، المكتبة القانونية، بغداد، ٢٠٢١، ص٧٥.

(٢) د. سليم حربة، أ.عبد الأمير العكيلي: شرح قانون أصول المحاكمات الجزائية، ج١، بيروت، ٢٠٠٩، ص١٢٦.

(٣) راشد بشير إبراهيم: التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية عن أمارة أبو ظبي) بحث منشور في مجلة دراسات استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية ، العدد٢٠٠٨،١٣١،ص٦٩.

المجرم المعلوماتي على رجال القانون لمعرفتهم الكبيرة بالمعلومات الإلكترونية وقلة خبرة رجال التحقيق الامر الذي يزيد صعوبة التحقيق وإثبات الجرائم[١].

ومن خلال ما تقدم نعرّف الخبير في الجرائم الالكترونية بأنه " هو الشخص الذي تعمق في دراسة عمل من الاعمال الإلكترونية وتخصص في أداءه لفترة طويلة واكتسب خلالها خبرة فنية عملية بحيث أصبح ملماً بتفصيلاته مما جعله متفوقاً على الشخص العادي ويستطيع أبداء الرأي الالكتروني في الامور المتصلة بهذا العمل".

أمّا فيما يتعلق بأنواع الخبرة وأساليب عمل الخبير المعلوماتي سنتطرق لهما في الفرعين الآتيين:-

الفرع الأول / الخبرة الشخصية

هي من أهم الخبرات في مجال التكنلوجيا لأنها تنطلق من مفهوم خلق منافسة حقيقية وهي تضم الى جانبها الخبرة الفردية والتي لها أهمية كبيرة في مال الانترنت والحاسوب، فهنالك الكثير من الشركات الكبرى المتخصصة في الانترنت والحاسبات تسعى لاستقطاب أصحاب الخبرات الشخصية في عملهم ممن أثبتوا كفاءة عالية في عملهم التكنلوجي حتى عصاة القانون منهم، فبعض الاتجاهات الاقتصادية تحاول الاستفادة منهم دون التخلص منهم كالقراصنة والهاكر، بل أن بعض الدول تسعى جاهدة للتوصل الى هؤلاء القراصنة الذين أصبحوا رموزاً وطنية جراء تصرفاتهم عبر الانترنت، وعليه فأن الجهات القائمة بالتحقيق في الجرائم الإلكترونية يجب أن تكون لديها خبرة ومهارة فنية دقيقة وسرعة في استخلاص الدليل الامر الذي يكون له أهمية كبيرة في كشف الجريمة والحيلولة دون إفلات المجرمين[٢].

الفرع الثاني / جهات الضبط القضائي

أعدت بعض الدول جهات متخصصة في مجال الخبرة في الجرائم الإلكترونية ومنها الولايات المتحدة الامريكية والتي تجاوز نشاطها في الاطار الدولي المتمثل بمنظمة الانتربول، حيث كان لآخر نشاط هو الفرع الجديد الذي تأسس في المباحث الفيدرالية الامريكية والذي أُطلق عليه المعمل الاقليمي الشرعي للحاسوب ومقره في سان دييغو والذي أفتتح عام ٢٠٠٠ لكي يكون جهة متخصصة في الخبرة الإلكترونية غرضه مكافحة التصعيد الخطير للجرائم الإلكترونية، وذلك بتحليل وتصنيف البيانات الرقمية

---

(١) د. بوحيه وسيلة: صعوبات التحقيق وإثبات الجرائم الإلكترونية قانوناً وقضاءً وأساليب مواجهتها، المؤتمر الدولي الاول لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الامام محمد بن سعود الاسلامية، السعودية، ٢٠١٥، ص١٢٤.

(٢) اوباح زينب سارة: الخبرة القضائية في الجريمة المعلوماتية، رسالة ماجستير مقدمة الى كلية الحقوق والسياسة، جامعة الجزائر، ٢٠١٤، ص٧٢.

وتدقيقها ومتابعتها والذي تكون له أهمية كبيرة في نطاق العمل على تكثيف الجهود لمواجهة الجرائم عبر الانترنت[١].

وبذلك نوصي للمشرع العراقي في مشروع الجرائم الإلكترونية أن ينص على أنشاء جهات متخصصة في مجال الخبرة الإلكترونية من ذوي الخبرة والكفاءة والاختصاص وبالإمكانية الاستعانة فبهم من القاضي المختص [٢].

الخاتمة:

أولاً: النتائج:

١- إن الجريمة الإلكترونية تتطور بشكل مذهل ومتسارع ويجب أن يلاقي هذا التطور قوانين عقابية تواكب هذا التطورات لغرض مكافحة هذه الجرائم الإلكترونية .

٢- هنالك الكثير من البرامج والتي من خلالها حذف كافة الادلة وتدميرها بشكل نهائي وبالتالي لايمكن معها معرفة تلك الادلة المساهمة في كشف الجريمة .

٣- إن الجريمة الإلكترونية في بعض الحالات يمكن أن تصنف من الجرائم الدولية كونها يمكن أن تقع في دولة وتحدث أثارها في دولة أخرى.

ثانياً: التوصيات:

١- نوصي القضاء العراقي بإنشاء جهة متخصصة للتحقيق في جرائم الانترنت كون ذلك سيسهم السلطة التشريعية بكل تطورات الجرائم الإلكترونية والتي بدورها تعمل على سن القوانين المناسبة لمعالجة هذه الجرائم المتطورة.

٢- نوصي المشرع العراقي بضرورة الاسراع في إقرار قانون مكافحة الجريمة الإلكترونية لما له أهمية كبيرة في مكافحة جرائم الانترنت التي تتسارع بشكل كبير وملحوظ ووضع عقوبات مناسبة لها للحد من إرتكابها، مع تمكين كافة الجهات الامنية من متابعة هذه الجرائم من خلال الاختراق وغيرها وكشف الادلة منها.

٣- نوصي المشرع العراقي عقد الاتفاقيات الدولية في هذا المجال بما يضمن التعاون الدولي في مكافحة الجرائم الإلكترونية وتسهيل عمل السلطات القضائية بشكل عام.

---

(١) اوباح زينب سارة: المصدر السابق، ص٦١.

(٢) نصت المادة (٢٥/رابعا) من المشروع المذكور على إنه :" للقاضي المختص في مرحلتي التحقيق والمحاكمة الاستعانة بالخبرة الفنية من داخل العراق وخارجه ".

المصادر :

أولاً: الكتب

١- الدكتور تكليف عواد عبيد: الاجراءات الجزائية في مرحلة المحاكمة لمنتسبي قوى الامن الداخلي، مكتبة القانون المقارن،ط١، بغداد، ٢٠٢٠

٢- عميد الشرطة أحمد فخري رشيد: المواجهة الأمنية للجريمة المعلوماتية، مكتبة السنهوري، بيروت،٢٠١٨

٣- عمار مزاحم مهدي: فن التحقيق الجنائي، ط٢، المكتبة القانونية، بغداد، ٢٠٢١

٤- أحمد خليفة الملط: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.

٥- عباس غيدان العبيدي: الضبط الإداري تجاه وسائل التواصل الاجتماعي، مركز الدراسات العربية للنشر والتوزيع، ط١، الجيزة، ٢٠٢٢.

٦- د. أحمد السولية: الحماية الجنائية والامنية للشاهد، دار الفكر الجامعي، ط١، الاسكندرية،٢٠٠٧.

٧- د. ممدوح عبد الحميد عبد المطلب: البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، مصر ، ٢٠٠٦ م.

٨- عبدالله الهلالي: تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، بدون ذكر دار النشر، القاهرة،٢٠٠٠.

٩- جميل عبد الباقي الصغير: الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة،٢٠٠١، .

١٠- عبد الفتاح حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، ٢٠٠٧.

١١- عبد الله الهلالي: التزامات الشاهد بالإعلام عن الجرائم المعلوماتية، دار النهضة العربية ، القاهرة، ٢٠٠٠.

١٢- أ.عبد الأمير العكيلي، د.سليم حربة : شرح قانون أصول المحاكمات الجزائية، ج١، بيروت،٢٠٠٩.

ثانياً: الرسائل والبحوث والمصادر الاخرى

١- أوباح زينب سارة : الخبرة القضائية في الجريمة المعلوماتية، رسالة ماجستير مقدمة الى كلية الحقوق والسياسة ، جامعة الجزائر ، ٢٠١٤.

٢- ناصر بن محمد البقمي: مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، سلسلة محاضرات الإمارات تصدر عن مركز الإمارات للدراسات والبحوث الإستراتيجية ، العدد ١١٦،٢٠٠٨.

٣- د . محمد أبو العلا عقيدة ، التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية ، من بحوث المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي، مركز البحوث و الدراسات ، العدد ١ ، السنة ٢٠٠٣ م ، دبي / الإمارات العربية المتحدة .

٤- د. صالح البربري : دور الشرطة في مكافحة جرائم الإنترنت ، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، ٢٠٠٣م.

٥- الدكتور عادل خميس العميري: التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، المجلد ٢٢، العدد٨٦، الامارات، ٢٠١٣.

٦- بن بادره عبد الحليم: إجراءات البحث والتحري عن الجريمة المعلوماتية – الخصوصية والإشكالات، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد٢٣، الجزائر،٢٠١٥.

٧- يحيى الشديدي: الشهادة في الجريمة الالكترونية، مجلة البعث، المجلد٣٨، العدد٥٠، دمشق،٢٠١٦.

٨- د. عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات ، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، محور القانون الجنائي ، دبي ، للفترة (٢٦- ٢٨) أبريل ٢٠٠٣ م .

٩- راشد بشير إبراهيم : التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية على إمارة أبو ظبي)، بحث منشور في مجلة دراسات إستراتيجية، مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد ١٣١، ٢٠٠٨.

١٠- د. بوحيه وسيلة: صعوبات التحقيق وإثبات الجرائم المعلوماتية قانونا وقضاءً وأساليب مواجهتها، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية ICACC ، كلية علوم الحاسب والمعلومات ، جامعة الإمام محمد بن سعود الإسلامية، السعودية، ٢٠١٥.

ثالثاً: القوانين والانظمة

١- قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١.

٢- قانون التوقيع الالكتروني العراقي رقم ٧٨ لسنة ٢٠١٢.

٣- نظام خدمات الدفع الالكتروني للأموال العراقي رقم ٣ لسنة ٢٠١٤.

Sources :

First: books

1- Dr. Talif Awad Obaid: Criminal procedures during the trial stage for members of the Internal Security Forces, Library of Comparative Law, 1st edition, Baghdad, 2020.

2- Police Brigadier Ahmed Fakhri Rashid: The Security Confrontation with Information Crime, Al-Sanhouri Library, Beirut, 2018

3- Ammar Muzahim Mahdi: The Art of Criminal Investigation, 2nd edition, Legal Library, Baghdad, 2021

4- Ahmed Khalifa Al-Malat: Information Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, 2005.

5- Abbas Ghaidan Al-Obaidi: Administrative Control towards Social Media, Arab Studies Center for Publishing and Distribution, 1st edition, Giza,2022.

6- Dr. Ahmed Al-Sulayya: Criminal and Security Protection of the Witness, Dar Al-Fikr Al-Jami'i, 1st edition, Alexandria, 2007.

7- Dr. Mamdouh Abdel Hamid Abdel Muttalib: Digital forensic research and investigation into computer and Internet crimes, Dar Al-Kutub Al-Qanuni, Egypt, 2006 AD.

8- Abdullah Al-Hilali: Inspection of the computer system and information guarantees for the accused, without mentioning the publishing house, Cairo,2000.

9- Jamil Abdel Baqi Al-Saghir: The Internet and Criminal Law, Dar Al-Nahda Al-Arabiya, Cairo, 2001.

10- Abdel Fattah Hegazy: Principles of Criminal Procedure in Computer and Internet Crimes, Dar Al-Kutub Al-Lawaniyya, Cairo, 2007.

11- Abdullah Al-Hilali: Witness Obligations to Report Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

12- A. Abdel Amir Al-Ukaili, Dr. Salim Harba: Explanation of the Code of Criminal Procedure, Part 1, Beirut, 2009.

Second: Theses, research and other sources

1- Aubah Zainab Sarah: Judicial experience in information crime, a master's thesis submitted to the Faculty of Law and Politics, University of Algiers,2014.

2- Nasser bin Muhammad Al-Baqmi: Combating information crimes and their applications in the Gulf Cooperation Council countries, UAE Lecture Series issued by the Emirates Center for Strategic Studies and Research, Issue 116, 2008.

3- Dr. Muhammad Abu Al-Ala Aqeedah, Investigation and Collection of Evidence in the Field of Cybercrimes, from the research papers of the First Scientific Conference on the Legal and Security Aspects of Electronic Operations, Dubai Police Academy, Research and Studies Centre, Issue 1, year 2003 AD, Dubai/United Arab Emirates.

4- Dr. Saleh Al-Barbari: The role of the police in combating cybercrime, Conference on Legal and Security Aspects of Electronic Operations, Dubai, 2003 AD.

5- Dr. Adel Khamis Al-Amiri: Inspection of information crimes, Police Thought Magazine, Police Research Center, Sharjah Police General Command, Volume 22, Issue 86, UAE, 2013.

6- Ben Badra Abdel Halim: Procedures for research and investigation into information crime - privacy and problems, Journal of Law and Human Sciences, Zian Achour University in Djelfa, Issue 23, Algeria, 2015.

7- Yahya Al-Shadidi: Testimony in Electronic Crime, Al-Baath Magazine, Volume 38, Issue 50, Damascus, 2016.

8- Dr. Abdullah Hussein Ali Mahmoud, procedures for collecting evidence in the field of information theft, research presented to the first scientific conference on the legal and security aspects of electronic operations, criminal law axis, Dubai, for the period (26-28) April 2003 AD.

9- Rashid Bashir Ibrahim: Criminal investigation into information technology crimes (an applied study on the Emirate of Abu Dhabi), research published in the Journal of Strategic Studies, Emirates Center for Strategic Studies and Research, Issue 131, 2008.

10- Dr. Inspired by a means: Difficulties in investigating and proving information crimes legally and judicially and methods of confronting them, The First International Conference on Combating Information Crimes ICACC, College of Computer and Information Sciences, Imam Muhammad bin Saud Islamic University, Saudi Arabia, 2015.

Third: Laws and regulations

1- Iraqi Code of Criminal Procedure No. 23 of 1971.

2- Iraqi Electronic Signature Law No. 78 of 2012.

3- Iraqi Funds Electronic Payment Services System No. 3 of 2014.