ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

إجراءات التحقيق الإبتدائي في جريمة تزوير التوقيع الالكتروني

أ.م.د. يحيى حمّود مراد الوائلي
فرع القانون العام، كلية القانون ، جامعة كربلاء، كربلاء - العراق.
البريد الالكتروني: yahya.h@uokerbala.edu.iq

ID No. 2045	Received: 05/04/2024	الكلمات المفتاحية:
(PP 129 -149)	Accepted: 13/04/2025	التوقيع الالكتروني ، التزوير ، الجرائم
https://doi.org/10.21271/zjlp.23.sp.8	Published: 29/04/2025	الالكترونية ، اجراءات التحقيق .

تزوير التوقيع الإلكتروني يشير إلى استخدام علامة شخصية تتألف من حروف أو أرقام أو رموز أو إشارات أو أصوات أو غيرها، مع طابع فريد يشير إلى نسبتها للشخص أو المؤسسة الموقعة عليها. إنَّ إجراءات التحقيق في جرائم تزوير التوقيع الإلكتروني تشمل على العديد من الإجراءات القانونية تقوم بها السلطات القضائية المختصة لتحديد الجناة وتقديمهم للعدالة. فالتحقيق في جرائم تزوير التوقيع الإلكتروني يتميز عن التحقيق التقليدي في الجرائم غير الالكترونية بتطور المفاهيم المستخدمة والذاتية الخاصة به. ويعتمد التحقيق على جمع الأدلة الرقمية وتحليل التوقيع الإلكتروني، مع صعوبة إثبات الجرائم الإلكترونية أمام المحكمة. ويشدد البحث على ضرورة وجود قضاة وخبراء متخصصين في مجال تقنية المعلومات، لفهم التفاصيل الفنية والتكنولوجية المتعلقة بالجريمة.

وتواجه إجراءات التحقيق الابتدائي عن جمع الأدلة والكشف عن الحقيقة في جرائم التزوير الإلكتروني، منها كيفية استجواب المجرم الإلكتروني الذي يتميز بالذكاء والمهارات التقنية، مما يجعل التحقيق أكثر تعقيداً، كذلك مشكلة التفتيش وضبط الادلة وماهي نوع الادلة التي يمكن ضبطها، كذلك يجب ان تتوفر في خبير الادلة الجنائية والشاهد صفات غير متوفر في صفات هذه الفئات في الجرائم التقليدية .

المقدمة

أولاً :موضوع البحث

تعيش المجتمعات اليوم في عصر رقمي يتسم بالتطور التكنولوجي السريع، إذ أصبحت التقنيات الإلكترونية جزءًا لا يتجزأ من حياتنا اليومية. يتسارع التبادل الإلكتروني للمعلومات والمعاملات، ومن بين التطورات الهامة في هذا السياق هو استخدام التوقيع الإلكتروني كوسيلة لتأكيد الهوية وتوثيق المعاملات، ومع هذا التطور تبرز جريمة تزوير التوقيع الإلكتروني كتحدي أمني يهدد النظام الرقمي ويطرح تحديات كبيرة أمام الأمان الإلكتروني. يأتي هذا البحث لاستكشاف إجراءات التحقيق الابتدائي في جريمة تزوير التوقيع الإلكتروني وتحليل تلك الإجراءات لتحديد كيفية تعزيز فعالية التحقيق في هذا السياق المعقد .

يعد التحول الذي شهدته المعاملات الالكترونية في مجال تكنولوجيا المعلوماتية، في تغيير بعض المفاهيم القانونية خاصة التي تتعلق بجرائم التزوير الالكترونية، والتي لا يقل خطرها على جرائم التزوير التقليدية، فجريمة التزوير في المحررات الإلكترونية هي من الجرائم التي تخل بالثقة العامة، ويعود سبب تجريمها أساساً بالنظر إلى ما لها من أهمية في وقتنا الحالي، إذ أصبحت واسعة الاستعمال وفي مجالات عديدة، وهو ما استغله مجرمو المعلوماتية في ارتكاب جرائمهم، فطبيعة التزوير الإلكتروني تقتضي أن تكون طرقه متعددة ومتطورة تبعا للتطور التكنولوجي، فالتزوير

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

يتم إما بإضافة بيانات لم تكن موجودة أصلا أو بحذف بيانات ضرورية كانت موجودة، أو تغيير وتبديل بعض البيانات، وذلك بحذف بيان أو إضافة آخر بدل منه، وطالما أن المحرر الإلكتروني يتضمن كتابة وتوقيع، فإنه من الممكن أن يتعرَّض للتزوير، بل أن أكثر ما تتعرض له المحررات الإلكترونية هو التزوير وذلك لسهولة القيام به، لذلك عمدت أغلب التشريعات المقارنة على تجريم التزوير في المحررات، لما لهذه الأخيرة من تهديد للثقة العامة للمتعاملين بها، وما لها من إخلال باستقرار المعاملات التي تتم عن طريقها، فآثارها لا تقتصر فقط بالنسبة للأفراد، أو في إطار محلي محدود، بل على مستوى واسع وفي فضاء دولي مفتوح، كما أن سرعة تطورها وازدياد حجمها بشكل مطرد مع التطورات التي تشهدها التكنولوجيا الحديثة، جعل منها محل اهتمام أغلب النظم التشريعية الحديثة، فلجرائم التزوير في المحررات الورقية طرقاً تقليدية باتت معروفة وذات حجية قانونية متفق عليها، إلّا إنَّ التزوير في المحررات الإلكترونية لا يمكن كشفه بذات الطرق وإنما يتطلَّب استحداث آليات جديدة تحظى بحجية قانونية توازي أو تفوق تلك الحجية التي اتفق عليها في كشف جرائم التزوير التقليدية، باعتبار أن جريمة التزوير لا تقع إلّا إذا كان لهذا المحرر الإلكتروني قيمة قانونية .

طرح تزوير التوقيع في المجال الإلكتروني العديد من التحديات للتحقيق. إن الخسارة المالية والضرر الذي يلحق بالسمعة الأمنية التي تتكبدها التعاونيات ومنظمات الأعمال بسبب تزوير التوقيع يشكل مصدر قلق كبير . وتشكل عمليات التزوير الماهرة، على وجه الخصوص، تحديًا كبيرًا في أنظمة التحقق من التوقيع عبر الإنترنت . ويتطلب اكتشاف عمليات التزوير الماهرة تقنيات متقدمة يمكنها التمييز بدقة بين التوقيعات الحقيقية والمزورة . بالإضافة إلى ذلك، إنَّ التحديات التي تواجه التحقيق في جرائم تزوير التوقيع الإلكتروني تدعو الى الحاجة عن الكشف الفعّال عن عمليات التزوير الماهرة، والوصول إلى مجموعات البيانات الشاملة، وتطبيق تقنيات التعلم الآلي المتقدمة .

ثانياً: مشكلة البحث

إن تزايد استخدام التوقيع الإلكتروني وتكامله في مجالات متعددة يثير قضية أمنية حادة، وهي جريمة تزوير التوقيع الإلكتروني. إذ تعد هذه الجريمة تحديًا كبيرًا يحتاج كشفها والحد منها إلى تقنيات تحقيق متقدمة في مجال المعلوماتية وإجراءات دقيقة. لذا يعالج البحث كيفية التعامل مع هذه المشكلة بفعالية، وكيف يمكن تحسين إجراءات التحقيق الابتدائي لكشف الجرائم المتعلقة بتزوير التوقيع الإلكتروني .

ثالثاً : منهجية البحث

سوف نعتمد في هذا البحث المنهج الوصفي التحليلي ، ومن خلال رد الفروع الى اصولها لبلوغنا الى الهدف من هذا البحث في التعامل مع مشكلة البحث المثارة ، والرغبة منا الى الوصول الى جملة من النتائج والمقترحات بشأن حيثيات الموضوع ، ونطمح أنْ نعالج جزئية ولو بسيطة في هذا المجال، ونرجو أنْ يكون بمستوى علمي رصين .

رابعاً: أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف الرئيسة :

1. تحليل إجراءات التحقيق الابتدائي في جريمة تزوير التوقيع الإلكتروني .
2. فهم التحديات التي قد تواجه المحققين أثناء التحقيق في جرائم تزوير التوقيع الإلكتروني .
3. دراسة أفضل الممارسات والتقنيات المستخدمة لتعزيز كفاءة التحقيقات الابتدائية في هذا المجال .

خامساً : خطة البحث

سوف نقسم خطة البحث على مبحثين نخصص المبحث الأول لماهيّضة اجراءات التحقيق في جريمة تزوير التوقيع الالكتروني ، ونعرِّج في المبحث الثاني الى اجراءات التحقيق الابتدائي ، ثم نختتم البحث في خاتمة تتضمن اهم النتائج والمقترحات التي توصلنا لها.

1- ماهية اجراءات التحقيق جريمة تزوير التوقيع الالكتروني

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

للوقوف على معرفة ماهية اجراءات التحقيق في جرائم تزوير التوقيع الالكتروني ، لابدَّ من التطرَّق لبحث مفهوم محل الجريمة وهو التوقيع الالكتروني ومن ثمَّ بيان هذه الجريمة وماهي مفهوم اجراءات التحقيق في هذه الجريمة وكيف نمييز بينها وبين اجراءات التحقيق التقليدي وكالآتي:

1- 1 - مفهوم التوقيع الالكتروني واجراءات التحقيق

سوف نتطرق لتحديد مفهوم التوقيع الالكتروني على صعيد الفقه والقضاء والقانون:

فعلى صعيد الفقه ، فإنَّ التعريف الذي يؤيده غالبية الفقه، فهو ذلك التعريف الذي يبرز كيفية إنشاء التوقيع تاركاً للتشريع القيام بتحديد الصور المختلفة له، والذي يعرف التوقيع الإلكتروني بأنه: (مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته)[1].

اما تعريفه قضائياً: فقد سلكت محكمة النقض الفرنسية في تعريفها للتوقيع الإلكتروني مسلك تعريفه على ضوء التوقيع التقليدي، فبعدما عرَّفت هذا الأخير بأنَّه (شهادة بخط اليد تكشف عن رضاء الموقع بهذا التصرف وتمكن من التحقق من إسناد التوقيع لصاحب الوثيقة)[2]، وهنا قررت المحكمة بأنَّ هذه الطريقة الحديثة للتوقيع الإلكتروني تقدم الضمانات نفسها للتوقيع اليدوي الذي يمكن أن يكون مقلداً، بينما الرمز السري لا يمكن أن يكون إلّا لصاحب الكارت فقط[3].

كما كرس القضاء بعد ذلك أحكامه نحو الاعتداد بهذا النوع الجديد من التوقيعات، وبيَّن بأنه يشكِّل توقيعاً صحيحاً معتداَ به قانوناً،كل رمز خطي مميز وخاص يسمح بتحديد وتشخيص صاحبه دون لبس ولا غموض، وانصراف إرادته الصريحة الالتزام بمحتوى ما تمَّ التوقيع عليه، وقد أقر هذا الاتجاه للقضاء الفرنسي في حكم لمحكمة النقض المصرية في 1989/11/08 بخصوص قبول التوقيع الرقمي في حالات الوفاء بالبطاقة البنكية تطبيقا لحكم محكمة النقض الفرنسية في حكمها السابق المشهور بقضية (كريكيداس)[4].

من مجمل هذه الأحكام يتضح بأن التوقيع الإلكتروني وسيلة حديثة لتحديد هوية صاحب التوقيع ويُبيِّن قبوله ومعبراً عن رضائه بالتصرف القانوني الموقع عليه[5]،، وبالتالي يقوم بوظائف التوقيع التقليدي ذاتها ،لكنَّه ينشأ عبر وسيط إلكتروني،استجابة لنوعية المعاملات التي تعتبر بدورها إلكترونية ووجب توقيعها إلكترونياً، إذ لا يمكن تحققها بالإجراءات اليدوية، وأياً كانت الألفاظ أو العبارات المستعملة في تعريفه فإنّها تتحدد في المضمون وهو تحديد هوية الشخص الموقع وتمييزه عن غيره،إذ العبرة بالمساواة الوظيفية بين النوعين من التوقيعات[6].

1- علي أبو مارية، التوقيع الإلكتروني ومدى قوته في الإثبات ، مجلة جامعة الخليل للبحوث، المجلد 5، العدد 2010، ص 109.

2- محمد ناصر حمودي، العقد الدولي الإلكتروني المبرم عبر الإنترنت،ط1، دار الثقافة للنشر والتوزيع،عمان، 2012 ،ص327.

3-Ce procédé moderne présente les même garanties que la signature manuscrite la quelle peut être imitée tandis quele code secret n'est connu que du seul titulaire de la carte..

4- محمد ناصر حمودي، مصدر سابق ، ص327.

5- Santiago Cavanillas Mugica et autres, commerce électronique, Edition delta, beyrouth liban 2004,p57.

6-محمد ناصر حمودي، مصدر سابق ، ص328

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

أما على صعيد التشريع : فقد عرَّفت لائحة التوقيع الالكتروني للمملكة المتحدة لسنة (2002) التوقيع الالكتروني بأنَّه (بيانات في شكل الكتروني ملحقة أو متحدة منطقياً بغيرها من البيانات الالكترونية والتي تصلح كوسيلة للتوقيع)[1].

أما المشرِّع الفرنسي فقد عرَّفت المادة (249) من قانون التوقيع الفرنسي لسنة 2000 بأنَّه (التوقيع المُثبت بشكل الكتروني صحيح فقط باستخدام عملية تسمح بتحديد هوية الموقِّع ، ويضمن ارتباط التوقيع مع الفعل الذي يعلق عليه ويضمن سلامة هذا العمل ، والتوقيع الرقمي يتكون من توقيع مكتوب بخط اليد في شكل رقمي بعد تثبيته على شاشه تعمل باللمس من قبل جهاز لضمان سلامة الفعل بمجرد توقيع التوقيع)[2]، وبيَّن الدور الذي يضطلع به التوقيع الالكتروني في الإثبات، وهذا مانراه من خلال تشريع القانون رقم (2000/230) لسنة 2000 [3]، بموجب المادة (1316، ف 4) المضافة بموجب القانون أعلاه الى نصوص القانون المدني الخاصة بالاثبات ، إذ بيَّنت بأنَّ (التوقيع الإلكتروني ضروري لاكتمال التصرف القانوني وهو يحدد هوية مَنْ يحتج به عليه ويعبر عن رضا الأطراف بالالتزامات الناشئة عن هذا التصرف،وعندما يتّم بواسطة موظف أو مكلف بخدمة عامة يكتسب هذا التصرف صفة الرسمية. و الت يقتضي التوقيع إلكتروني إستخدام وسيلة آمنة لتحديد الشخص، بحيث تضمن صلته بالتصرف الذي وقَّع عليه، ويفترض أمان هذه الوسيلة ما لم يوجد دليل مخالف بمجرد وضع التوقيع الإلكتروني الذي يجري بموجبه تحديد شخص الموقع. ويضمن سلامة التصرف، وذلك بالشروط التي يتم تحديدها بمرسوم يصدر عن مجلس الدولة)[4].

أما المشرِّع الأمريكي فقد نظَّمه تنظّيماً محكماً سواء على المستوى الفدرالي أم على مستوى الولايات، غير أننا نركز على القانون الفدرالي والذي عرَّف التوقيع الإلكتروني في قانون المعاملات الإلكترونية لسنة 2000 بأنَّه (أصوات أو إشارات أو رموز، أو أي إجراء آخر يتصل منطقياً بنظام معالجة المعلومات إلكترونياً، ويقترن بتعاقد أو مستند أو محرر، ويستخدمه الشخص قاصداً التوقيع على المحرر)[5].

1- محمد الشهاوي شرح قانون التوقيع الالكتروني ، دار النهضة العربية ، القاهرة ، 2010، ص23.

2-Alain Bensoussan, La signature numérique et électronique en procédure pénal. www. De alain.bensoussan. com.

3- محمد المرسي ابو زهرة ، الدليل الكتابي وحجية مخرجات الكمبيوتر في الاثبات في المواد المدنية والتجارية ، من بحوث مؤتمر القانون والكمبيوتر والانترنت ، 1، 3 مايور ، جامعة الامارات العربية المتحدة ، ص21.

4- نورجان محمد علي ، التوقيع الالكتروني في ظل قانون المعاملات الالكترونية الاردني، ط1 ، 2003، ص58.

_ 2L'article 1316- 4 ,loi 2000 - 230 , (La signature nécessaire à la perfection d'un acte juridique identifie celui quil'appose elle manifeste le consentement des parties aux obligation qui découlent de cet acte quand elle est apposéepar un de officier public, elle confère l'authenticité à l'acte lorsqu'elle est électronique ,elle consiste en l'usage d'unprocédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache la fiabilité de ce procédé estprésumée du signataire assurée et l'intégrité de l'acte garantie, dans des condition fixées par décret en conseil d'état)

ينظر: إلياس ناصيف، العقد الإلكتروني في القانون المقارن،ط1،منشو ا رت الحلبي الحقوقية،بيروت، 2009 ،ص239 .

ينظر أيضاً: امير فرج يوسف ، الجديد في التوقيع الالكتروني ، ط1 ، مكتبة الوفاء القانونية ، الاسكندرية ، 2011، ص.92

5- محمد ناصر حمودي، مصدر سابق ، ص232.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

وعرَّفة المشرع العراقي بانه (علامة شخصية تتخذ حروف او ارقام او رموز او اشارات أو اصوات او غيرها ، وله طابع متفرد يدل على نسبته الى الموقع ويكون معتمداً من جهة التصديق)[1]. وأكدت المادة (13/ اولاً) من القانون نفسه بأنْ (تكون للمستندات الالكترونية والكتابة الالكترونية والعقود الالكترونية ذات الحجية القانونية لمثيلتها الورقية...).

يمُكن أنْ نستخلص من هذه التعريفات بأنَّها تشترط في التوقيع الإلكتروني قدرته على تحديد هوية الشخص الموقع انسجاماً مع التطورات في مجال الإعتراف بالتوقيع الإلكتروني والمحررات الإلكترونية، وتمتعها بحجية مشابه للتوقيع التقليدي والسندات والمحررات التقليدية في الإثبات .وتثير عملية الإثبات ذاتها إشكالية نظراً لأن التوقيع الإلكتر وني يسهل التلاعب به ويمكن تزويره عبر العديد من الشبكات الإجرامية في الخارج وهو ما يمكن أن يحقق صعوبات أخرى.

ومن خلال ماتقدَّم يمكن تعريف جريمة تزوير التوقيع الاكتروني بدلالة المادة (286) من قانون العقوبات العراقي رقم (111) لسنة 1969 النافذ، التي عرفت التزوير بانَّها (تغير الحقيقة في علامة شخصية تتخذ حروف او ارقام او رموز او اشارات أو اصوات او غيرها ، وله طابع متفرد يدل على نسبته الى الموقع ويكون معتمداً من جهة التصديق).

أما اجراءات التحقيق في جرائم التزوير الالكتروني فقد عرفَّها البعض بانَّها (عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة إلكترونية من فاعل بها لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لاقامة العدل)[2].

وهناك من عرَّفهابأنَّه (البحث في مستودع السر للمتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع السر بصاحبه فيمكن أن يكون المحل جهاز الكمبيوتر أو أنظمته أو الانترنت للاستدلال بها على صدق نسبة الفعل إلى شخص معين أو كذبه)[3].

وبذبك يمكننا تعريف التحقيق الجنائي في جرائم تزوير التوقيع الإلكتروني على أنه (الإجراءات التي يقوم بها قضاة التحقيق أوالمحققين القضائيين عبر العالم الافتراضي لضبط جريمة تزوير التوقيع الإلكتروني والتثبت من أدلتها ومعرفة فاعلها تمهيداً لإحالتهـــــــــم للمحاكمة).

1-2- التمييز بين التحقيق الجنائي الإلكتروني والتحقيق الجنائي التقليدي

هناك إجماع حول المنظور العالمي للجريمة الإلكترونية من حيث طبيعتها ونطاقها وارتباطها بشبكات دولية مما اثر علي الاقتصاد العالمي والتنمية وقابليتها للانتشار السريع[4]. مما جعل التحقيق في الجرائم الإلكترونية يتميز عن التحقيق الجنائي في الجرائم التقليدية بعدة جوانب منها:

1 - التحقيق في الجرائم الإلكترونية يتميز بتطور المفاهيم المستخدمة فيه، فأصبح هنالك مصطلحات جديدة تعد أكثر قرباً وملائمة من البيئة الافتراضية والتقنية الذي تباشر فيه إجراءات التحقيق، فمثلاً استخدام مصطلح (الولوج) بدلاً من مصطلح (التفتيش) واستخدام مصطلح (النسخ) بدلاً من مصطلح ا(لضبط) وهذه المصطلحات تتلائم مع البيئة

1- ينظر: الفقرة رقم (4) من المادة (1) من قانون التوقيع الالكتروني والمعاملات الالكترونية رقم 78 لسنة 2012 ، منشور بجريدة الوقائع العراقية بالعدد (4256) لسنة 2012/11/5 .

2- مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الالكترونية"،طبعه الاولى،مطابع الشرطه،القاهره، 2009 ،ص.169.

3- محمد صلاح محمد عبد المنعم، الجرائم الالكترونية وتحدياتها ، دارسة مقارنة ، اطروحة دكتوراة ـ كلية الحقوق ، جامعة المنصورة ،2005، ص.432.

4- د. محمد الأمين البشري، "الاساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، محاضرة مقدمة في الحلقة العلمية تحليل الجرائم المستحدثة والسلوك الإجرامي المنعقدة في الفترة من 17 - 19 / 1 / 2011 بمقر جامعة نايف العربية للعلوم الأمنية، ص 12 .

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

الافتراضية عنها في الجريمة التقليدية[1].

2 - يعد التحقيق في الجرائم الإلكترونية له ذاتية خاصة ومستقله مستمدة من الطبيعة الخاصة والمميزة للجريمة الإلكترونية عن الجريمة التقليدية، فالتحقيق بها لا يعد استثناء على التحقق في العالم المادي، فاكثر المساحات الافتراضية التي تنمو فيها الجريمة الإلكترونية هي بيئة شبكات الانترنت وقواعد البيانات والبريد الإلكتروني والنقود الإلكترونية والتجارة الإلكترونية والاسهم والسندات والأنظمة الأمنية الحساسة ونشر الفيروسات والإرهاب الإلكتروني[2].

3 - غالباً ما يتخذ الدليل في الجرائم الإلكترونية شكلاً مغايراً للشكل التقليدي للدليل، فالجريمة التي ترتكب بواسطة الكمبيوتر تنشأ في الخفاء وينصب الاعتداء فيها على معطيات الكمبيوتر ، فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الدليل يجعلها تتميز بالتحقيق عنها في الجرائم التقليدية[3]، وبالتالي يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وماتخلفه من آثار غير مرئية.

4 - التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية إذ يصعب توضيحها لهيئة المحكمة ويسهل زرع الشك في وجدانها، ويرجع ذلك إلى صعوبة إدراك المفاهيم التي يشملها موضوع التحقيق والبحث محل الادعاء، سيما عدم وجود سلطات تحقيق ومحاكمة متخصصة للتحقيق والفصل في الجريمة الإلكترونية[4]. فاذا كان التحقيق يعتمد على ذكاء القاضي، أو المحقق وفطنته وقوة ملاحظته ومحاولته بكل جهد ممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث عنها وصولاً للكشف عن الحقيقة إنه يتطلب تطوير اساليبه من أجل مواكبة حركة الجريمة وتطور اساليب ارتكابها في البيئة الافتراضية [5].

5 - إن التحقيق في الجرائم الإلكترونية امام متهم من نوع خاص يتميز بنسبة عالية في الذكاء والخداع فضلا عن امتلاكه لقدرات فنية ومعرفة بجهاز الكمبيوتر وتقنياته مما يتطلب امكانيات مادية وتشريعات وإجراءات تختلف عن التحقيق في الجرائم التقليدية، مما أدى إلي ظهور ما يسمي بأزمة القانون الجنائي سواء من حيث طبيعة السلوك الإجرامي الإلكتروني فإن القانون لا يستطيع تجريم أفعال لم ينص عليها المشرع حتى لو كانت هذه الأفعال مستهجنة لما مقيد به بمبدأ الشرعية الجنائية[6].

1- عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، اطروحة دكتوراه ،كلية الحقوق،جامعة عين شمس، 2004 ، ص .885

2- د. محمد امين البشري، مصدر سابق، ص 11 .

3- خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الاردن، 2011 ، ص 143 وما بعدها.

4- د. أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها ، المركز القومي للإصدارت القانونية، القاهرة، 2017 ، ص.75

5- محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها ، مصدر سابق ، ص 225 .

6- فاطمة زهرة بوعناد ، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية،العدد الأول، 2013 ، الجزائر،ص63.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

اما من حيث غياب الإمكانيات المادية لمواجهة التقنيات الفنية العالية والنقص بالتشريعات المتعلقة بالتحقيق يقود إلى أدنى مستوى أداء لجهات التحقيق في الجرائم الإلكترونية سيما أن بعض إجراءات التحقيق والإجراءات المتبعة في التفتيش والضبط وتكوين فرق العمل لها سمات خاصة وتحتاج إمكانيات مادية باهظة للكشف عن الجريمة الإلكترونية[1].

6 - ان التحقيق في الجريمة الالكترونية يختلف عنه في التحقيق في الجريمة التقليدية حيث يعاني المجتمع في كثير من الدول من عدم منح الجرائم المرتكبة بواسطة جهاز الكمبيوتر وتقنيات الاتصال الاهتمام التشريعي والقضائي اللازمين، سيما مع غياب الاطار التشريعي الموحد بين الدول وضعف التعاون الامني بينهما ، وهذا الامر ترك المجال مفتوحاً لتنفيذ العديد من جرائم الكمبيوتر الدولية مثل تبيض الاموال والاتجار بالمخدرات والاعتداء على قواعد البيانات الى جانب ذلك فانه يقصد العمليات الجرمية الالكترونية التي تتجاوز في العادة الحدود الجغرافي للبلدان حيث جعلت من مرتكبي الجرائم الالكترونية يتحدَّون جهات التحقيق التلقيدية للدول ذات السيادة ، فبتنظيمهم هجوماً منظماً من اي جهاز كمبيوتر في اي مكان في العام ثم تمرير الهجوم عبر الحدود الوطنية المختلفه مما اتاح الفضاء الالكتروني لمرتكبي هذه الجرائم مجالاً لاخفاء هوياتهم او تمويهها وبات الامر بالقبض على مجرمي هذا النوع من الجرائم بالنسبة لجهات التحقيق محفوفاً بالخطر والعقبات التقنية على جهات التحقيق[2].

وبناءاً على ما تقدم ولما لهذا التمييز للتحقيق الجنائي في الجرائم الإلكترونية عنه في الجرائم التقليدية فإنه يستوجب وجود تعديلات جوهرية وتشريعات خاصة في منطق واجراءات التحقيق وتعاملها مع الأدلة الجنائية الحديثة التي تتلائم مع تطور الجريمة سيما إن الأحكام العامة المنصوص عليها في قوانين العقوبات لا تفي بالغرض لأنه قد ينشأ عن طبيعة وخصوصية هذه الجريمة عدم إمكانية معاقبة مرتكبيها ويبقي مرتكبو هذه الجرائم دون عقاب[3].

2- اجراءات التحقيق الابتدائي

سنتطرق إلى إجراءات جمع الأدلة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، وكذلك إلى إجراءات التحقيق الهادفة إلى الكشف عن الحقيقة. في المطلبين الآتيين:

2-1 - إجراءات جمع الأدلة في جرائم تزوير التوقيع الالكتروني

سنقتصر في شرح وتوضبح بعض هذه الاجراءات وتتمثَّل بمايأتي:

2-1-1 الاستجواب

الإستجواب إجراء ضروري وهام من بين إجراءات التحقيق الإبتدائي ، وهو يعني (مجابهة المتهم بالأدلة المختلفة

1- مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وأثباتها في فلسطين ، بحث منشور مجلة علوم الشريعة والقانون، الجامعة الأردنية، المجلد 45 ، عدد 4 ، ملحق 2 ، 2018 ، ص .292

2- د. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الالكترونية، ط3 ،دار الثقافه للنشر والتوزيع، عمان، 2019 ، ص187 - 188 .

3- وحسناً فعل المشرع المصري لسنه للقانون رقم (175)لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات الذي يهدف الى حماية البيانات والمعلومات الحكومية والانظمه والشبكات المعلوماتية الخاصة بالدولة او احد الاشخاص الاعتبارية العامه من الاعتراض او الاختراق او العبث بها او اتلافها او تعطيلها بأي صورة كانت ففي فهذا القانون كان تنظيم اجرائي دقيق ينظم اجراءات الضبط والتحقيق والمحاكمة المتعلقه بالجرائم ، فضلاً عن حالات الدفاع واجراءاتها وتنظيم عمل الخبراء المتخصصين في مجال الجرائم لمكافحة تقنية المعلومات والقرارات والاوامر الجنائية المتعلقه بتنفيذ القانون.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

قِبله، ومناقشته فيها مناقشة تفصيلية ، كيما يفندها إنْ كان منكراً للتهمة ، أو يعترف بها إذا شاء الإعتراف) [1]. وعُرِّف أيضاً بأنَّه (مسائلة المتهم ومناقشته عن وقائع القضية المنسوب إليه إرتكابها ومجابهته بالأدلة المختلفة وسماع ما لديه من دفوع لتلك التهمة)[2]، وعلى صعيد القضاء عرّفته محكمة النقض المصرية بأنَّه (إجراء من إجراءات التحقيق يستطيع المحقق من خلاله التثبّت من شخصية المتهم ويتم عن طريق مجابهة المتهم بالأدلة المختلفة القائمة ضده ومناقشته مناقشة تفصيلية في التهمة المنسوبة إليه على وجه مفصّل في الأدلة القائمة في الدعوى إثباتاً ونفياً)[3].

إذن الاستجواب مجابهة المتهم بالأدلة المحشودة ضده ومناقشته فيها مناقشة تفصيلية بهدف استجلاء ظروف وملابسات الجريمة وكشف الحقيقة فيما تعلق بالجرم الواقع، والأدلة التي أمكن لإعضاء الضبط القضائي، أو رجال الشرطة أو المحققين التوصل إليها، والاستجواب على هذا النحو قد يفضي بالمتهم إلى الاعتراف بجرمه، وقد يحدو به على العكس إلى إنكار الجرم المنسوب إليه[4].

واستجواب المتهم في جرائم تزوير التوقيع الالكتروني تحكمه ذات القواعد العامة للاستجواب في أي جريمة تقليدية، لكن الفرق يكمن في ضرورة تأهيل وتكوين قضاة تحقيق في جرائم الحاسوب والانترنت حتى يمكن له استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة ومصطلحاتها، سيما وأن المجرم الذي يتم التحقيق معه ليس مجرماً عادياً، ذلك أن المجرم الالكتروني له طبيعة خاصة في استخدام تقنيات الحاسوب الآلي[5] ، وهو يضع المحقق في موضع صعب حين استجواب المجرم الالكتروني أو في محاولة الحصول على اعتراف منه ، ذلك أن المجرم الالكتروني على عكس المجرم التقليدي يتميز بالذكاء، ومتمرس بتفاصيل الحاسوب، والشبكات والبرمجيات، وتشير المعلومات إلى أن أغلب مرتكبي الجرائم المرتكبة بالوسائل الالكترونية يقيمون ـ كما يدعى ـ في دول العالم الثالث المتخلفة في كل شيء إلّا في مجرميها الالكترونيين الأذكياء[6]، وهذا ما يدعو لصعوبة الاستجواب مع مرتكبي جرائم تزوير التوقيع الالكتروني لقدرتهم على التهرّب من المسؤولية الجزائية، لذا يتطلّب من قاضي التحقيق أن يكون ملماً بملف التحقيق في مواجهة المتهم، ويتمتع بقدرات فنية للتحقيق، والأكثر من ذلك إلمامه بتقنيات الحاسوب لكي يستطيع ان ينتزع اعترافاً منه. واجراء الاستجواب في الموضوع لجرائم تزوير التوقيع الالكتروني يتطلّب من قاضي التحقيق ايضاً الحنكة والتبصر فيه من خلال مواجهة المتهم بالدلائل القائمة ضده، ومواجهته أيضا بالشهود وأي شخص يراه في مواجهته لإظهار الحقيقة، وما يمكن أن يساعد قاضي التحقيق ويعطي له إضافة في الاستجواب مواجهته بالخبرة الالكترونية والخبرة في مجال الحاسوب الآلي، وايضاً معرفة الطرق التي يتم بها ارتكاب هكذا جرائم مما يؤدي الى اصابة المتهم بالدهشة والذهول.

1- د.حسن صادق المرصفاوي ، أصول الإجراءات الجنائية، منشأة المعارف ، الإسكندرية ،مصر ، 1977 ،ص393 . جمعة سعدون الربيعي ،الدعوى الجزائية وتطبيقاتها، مطبعة الجاحظ ، بغداد ، العراق، 1996 ،ص.31

2- عبدالأميرالعكيلي و د.سليم حربة ،، أصول المحاكمات الجزائية ، ج2، المكتبة القانونية ، بغداد ، بلا تاريخ طبع ، ص.156

3- أحمد المهدي وأشرف شافعي ، التحقيق الجنائي الإبتدائي وضمانات المتهم وحمايتها ، دار الكتب القانونية ، مصر ، 2006 ، ص.80

4- جلال ثروت، سليمان عبد المنعم، أصول المحاكمات الجزائية، ط 1 ، المؤسسة الجامعية للدراسات، بيروت، 1997ن ص115 .

5- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ، ط 1 ، منشأة المعارف، الإسكندرية، 2009، ص.681

6- خالد ممدوح ابراهيم، فن التحقيق في الجرائم الالكترونية، ط 1 ، دار الفكر الجامعي ، الإسكندرية، 2018، ص 240.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

2-1-2 التفتيش (الولوج)

يُقرر القانون لكـلِّ شخص حق في أنْ يحتفظ بسرِّية شيءٍ ما ، ومنع الغير من الإطلاع عليـه ، والأشياء التي يعتبرها القانون محلاً للأسرار الفردية ومستودعاً لحقِّ السر ويحمي حق صاحبها في منع الغير من الإطلاع عليها إلَّا بـأذنه ورضائه هي (جسم الإنسان ومسكنه ورسائله) ، ومن هنا جاءت تعابير حرمـة الشخص وحرمـة المسكن وحرمـــة الرسائل [1]، ويعـرّف التفتيش بأنَّه (الإطـلاع على محل منحـهُ القانـون حرمةً خاصة بأعتباره مستودعاً لسِّر صـاحبه ، لضبط ماعسى يوجـد مما يفيد في كشـــفِ حقـيقةِ جريمةٍ مُعينةٍ)[2] ، ويُعرّف أيضاً بأنَّه (أمرٌ تحريري يصدر مدوناً على أوراق الدعوى من قاضي التحقيق أو المحكمة المختصة ، يُكلّف فيه المحقق أو عضو الضبط القضائي تفتيش أي شخص أو الدخول الى أي منزل أو مكان يتمتع بحرمة المسكن ، للبحث عن أي دليل يمكن الإستفادة منه والإستعانة به للوقوف على حقيقة الجريمة المرتكبة)[3] ، يتضح من التعاريف السابقة بأنَّ التفتيش يُعدْ وسيلة للحصول على الدليل وليس دليلاً في ذاته ، فهو من أعمال التحقيق التي تهدف الى كشف الحقيقة بشأن الجُرم الواقع ، ولكنَّ هذا الإجراء لايؤدي دائماً إلى إدانة المتهم بل على العكس قد يستفيد المتهم منه[4]،

التفتيش بحسب الأصل إجراء من إجراءات التحقيق يدخل في صلاحية قاضي التحقيق أو المحكمة المختصة ، ولمشروعية أمر التفتيش يجب أنْ يُعهد تقريره الى جهة قضائية[5]، والتفتيش بوصفه هذا يُعد من الإجراءات المقيدة للحرية .

إنَّ التفتيش هو عمل من أعمال التحقيق التي تستهدف كشف الحقيقة بشأن الجرم الواقع ومدى ثبوته في مواجية المتهم، ولقاضي التحقيق اللجوء إلى التفتيش إما بنفسه، واما أن يأذن بذلك للمحققين أو الشرطة[6] ، أو هو اجراء من إجراءات التحقيق يهدف إلى البحث عن دلائل، أو أشياء موجودة في مكان مغلق تفيد في كشف الحقيقة عن الجريمة، وهو ليس من اجراءات كشف الجرائم قبل وقوعها، بل هو من اجراءات التحقيق فيها بعد ارتكابها[7].

يعد التفتيش أحد أهم الآليات الإجرائية للبحث عن الدليل في الجرائم الالكترونية والتقليدية، الذي قد يكون في حيازة شخص المتهم أو مسكنه، كالبحث في الشخص الذي يحمل مواد مخدرة في جيبه، أو في المسكن المخبئة فيه، أما إذا ارتكبت الجريمة في وسط الكتروني فيكون محل التفتيش الوسائل الالكترونية الحديثة المادية منها أو المعنوية كالنظام المعلوماتي.

1- جواد الرهيمي ، أحكام البطلان في قانون أصول المحاكمات الجزائية ، ط2 ، المكتبة القانونية ، بغداد، العراق ، 2006 ، ص.180.

2- جمال محمد مصطفى ،، شرح قانون أصول المحاكمات الجزائية العراقي ، مطبعة الزمان ، بغداد ، 2005 ، ص.66

2- محمود عبد العزيز محمد ، التفتيش الاذن والاجراء والدليل والتدليل فقهاً وقضاءً ، دار الكتب القانونية ، مصر ، 2009 ، ص.5

3- علي وجيه حرقوص ، قاضي التحقيق في قانون اصول المحاكمات الجزائية الجديد ، ط1 ، مشورات زين الحقوقية ، بيروت ، لبنان، 2005 ،ص.46

4- د. علي عبد القادر القهوجي ، القانون الدولي الجنائي ، ط1 ، منشورات الحلبي ، بيروت ، لبنان، 2001، ص.58

5- جلال ثروت، سليمان عبد المنعم ،مصدر سابق ،.499

6- د.أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، دار النيضة العربية، القاهرة، 1985 ، ص 946.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

يتكون الحاسب من مكونات مادية ومكونات منطقية، وكذا شبكة إتصالات سلكية ولاسلكية، فقابلية تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه "عام أو خاص"، فإذا كانت موجودة في مسكن المتهم أو أحد ملحقاته، لا يجوز تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المقارنة، ومحل التفتيش الخاص بنظم الحاسب الآلي هي كل مكونات الحاسب سواء كانت مادية أو معنوية، أو شبكات الإتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش[1].

والتساؤل الذي يرد هنا عن مدى امكانية خضوع البيانات المعنوية للتفتيش ؟

اختلف الفقه بشأن التفتيش عن البيانات الموجودة في إطار غير مادي، كالتي يتم استدعائها بواسطة شبكة الانترنت أو البريد الالكتروني والمواقع الالكترونية[2].

فذهب البعض إلى أن التفتيش يشمل جميع الأدلة المادية الضرورية للتحقيق، فلا يمتد إلى البيانات والمعلومات الموجودة في حاملات البيانات المادية كالملفات والحقول وبرامج النظام وبرامج التطبيقات، أو في الذاكرة الداخلية، لكن الصعوبة تثور في حالة البيانات غير المحسوسة كتلك المخزنة في وحدة المعالجة المركزية يرتبط بها الحاسوب، فهنا لا يجوز لسلطة التحقيق التفتيش عن المعلومات في هذا النظام لما فيه من مساس بحقوق الغير في النظام الآخر محل التفتيش، ويتم التغلب على هذه الصعوبة بمطالبة حائز البيانات المطلوب الإطلاع عليها بتقديمها إلى جهات التحقيق عند طلبها، وفي حالة رفضه يكون قد أخل بالتزام التعاون مع سلطة التحقيق.

بينما ذهب جانب آخر من الفقه إلى أن التفتيش يمتد ليشمل كل البيانات المحسوسة وغير المحسوسة كالسجلات الإلكترومغناطيسية التي تتميز بطبيعتها غير المرئية التي ينبغي تحويلها إلى سجلات مرئية عن طريق وحدات الإخراج الخاصة بالحاسوب أو غيره من الوسائل الحديثة التي تتميز بهذه الميزة حتى يمكن تفتيشها، وقد أخذ الفقه في كل من فرنسا وانجلترا وأمريكا واليابان بهذا الرأي ، وهذا مانؤيده لأن سرعة انتقال البيانات والمعلومات المطلوب التفتيش عنها من جهاز المتهم إلى نظام آخر تستدعى تتبعها لأجل ضبطها في أنظمة أخرى بالسرعة نفسها التي تمت انتقالها من حاسوب المتهم إلى نهاية طرفية في مكان آخر[3].

2-1-3 - ضبط (نسخ) الأدلة الالكترونية

لكي يحقق التفتيش غايته في جمع الأدلة على الجريمة التي ارتكبت فلابد من وسيلة بموجبها يتم وضع اليد على شيء يتصل بها، ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وهذه الوسيلة تتمثل في الضبط، والتي عن طريقها يتم الوصول إلى الأدلة التي تهدف إليها إجراءات الإثبات الجنائي، لذلك سنتطرق إلى مفهوم الضبط في جرائم التوقيع الالكتروني، ثم محل الضبط في جرائم التوقيع الالكتروني .

أولا: مفهوم الضبط في جرائم تزوير التوقيع الالكتروني

يقصد بضبط الأشياء بوجه عام أن تقوم سلطة التحقيق بوضع يدها على كافة الأشياء المتعلقة بالجريمة والتي تفيد في كشف حقيقة الجرم الواقع أو في إثبات أو نفي التهمة في مواجية المتهم، ويستوي أن تكون الأشياء المضبوطة مملوكة للمتهم أو لغيره، كما لا يهم طبيعتها أو نوعها سواء أكانت منقولاً أم عقاراً ، وسواء كانت من وسائل الجريمة أم

1- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، ط 1، دار الفكر الجامعي 2011، ص 196. شيماء عبد الغني محمد عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، د ط، المنصورة، كلية الحقوق,). 2005 ، ص281 .

2- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 1، دار الفكر الجامعي، الإسكندرية، 2011، ص70-71 .

3- بكري يوسف بكري، المصدر السابق، ص72.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

متحصلة عنها[1]. والضبط بالنسبة لجرائم تزوير التوقيع الالكتروني التي تقع على الوسائل الإلكترونية، أو عن طريقها يشتمل على كل ما استعمل في ارتكابها، أو أعدَّ لهذا الغرض كأجهزة نسخ وتسجيل برامج الحاسوب ، أو أجهزة الربط مع الشبكات الإلكترونية، وكذلك أجهزة اختراق الاتصالات وتحميل الشفرات وكلمات السر، وكافة البرامج المقلدة والمنسوخة، وأيضاً المحررات الإلكترونية، والتوقيعات الإلكترونية المزورة والملفات المعنوية التي تعد وسيلة لارتكاب الجريمة، والضبط هنا يقصد به الضبط القضائي والذي يستهدف الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة، والضبط قد يقع على مكونات الوسائل الإلكترونية، وقد يكون محله أيضاً المراسلات الإلكترونية[2].

إن المواد المراد ضبطها قد لا تكون على الأجهزة المضبوطة، فقد تكون على جهاز غير موجود بمكان مسرح الجريمة، ويقوم العاملون بتشغيله فقط من المكان محل التفتيش، وقد تكون البيانات على ذات الأجهزة ولكنها مشفرة ولا يعرف فك الشفرة سوى شخص أو أكثر من العاملين، فهنا فيثور التساؤل عن مدى مشروعية إجباره على فك الشفرة، أو قد تكون المعلومات مشفرة، ولكن يتمكن أحد العاملين من محو البيانات الموجودة على الجهاز أو الأجهزة بمجرد العلم باجراء التفتيش[3].

ثانياً : محل الضبط

يتنوع ضبط الوسائل الالكترونية بحسب الوسيمة المراد ضبطها، إذا ما كانت من الوسائل المادية أو المعنوية، وهناك أيضاً ما يسمى بضبط المراسلات الالكترونية والبريد الالكتروني.

أ. ضبط الكيانات المادية والمعنوية في الوسائل الإلكترونية

المكونات المادية للحاسوب لا يثير ضبطها أي إشكال، فيمكن ضبط الوحدات المعلوماتية الآتية، مثل وحدة المدخلات بما تشمله من المفردات كلوحة المفاتيح وشاشة اللمس، نظام الإدخال المرئي، نظام الإدخال الصوتي، نظام الفأرة، نظام القلم الضوئي، نظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات، ويمكن أيضاً ضبط وحدة الذاكرة المركزية سواء أكانت ذاكرة للقراءة فقط أم الكتابة معاً، وضبط وحدة الحساب والمنطق بما تشمله من دائرة إلكترونية ومسجلات، وضبط وحدة التحكم وضبط وحدة المخرجات وما تشمل عليه من وسائل كالشاشة الطابعة والرسم والمصغرات الفيلمية وضبط وحدات التخزين الثانوية بما تشمل عليه من أقراص مغناطيسية بنوعيها المرن والصلب والأشرطة المغناطيسي [4].

ويلحظ كذلك أنه يمكن ضبط كافة الأدوات والمستندات التي تكون قد استعلمت أو تحصلت من الجرائم التي تقع على العمليات الإلكترونية، فيمكن ضبط الأوراق المالية المزورة وقد تضبط هذه الأوراق بداخل الحاسبات الآلية أو تضبط أدواتها بداخل نظم الحاسوب، ويمكن أيضاً ضبط التوقيعات الالكترونية في المحررات الإلكترونية المزورة

1- جلال ثروت، سليمان عبد المنعم ، مصدر سابق ، ص497 .

2- د.اشرف عبد القادر قنديل ، الاثبات الجنائي في الجريمة الالكترونية ، دار الجامعة الجديدة للنشر ، الاسكندرية ، 2015 ، ص 60-61 .

3- مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة ، 2000، ص71.

4- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ، ط 2، دار النهضة العربية، القاهرة،2008، ص198.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

كمخرجات أو بيانات داخل ذاكرة الحاسوب أو داخل أنظمة الصراف الآلي طبقاً لما هو مسجل من بيانات داخل هذه الأنظمة[1].

وقد أثير ضبط الكيانات المعنوية للحاسوب خلافاً بين الفقه، فهناك من يرى بأنَّه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البيانات الالكترونية بمشتملاتها من ملفات وسجلات وحقول سواء اتخذت برامج نظام أم برامج تطبيقات[2].

فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي تستهدف الوصول إليها فإن المعالجة التي تجرى عليها لجعلها مرئية للإطلاع عمليا واثباتها أو بإخراجها من الحاسوب بصورة مستندات مطبوعة لا تعد تفتيشاً عن أدلة الجريمة، ولكنها تمثل وصولاً إلى هذه الأدلة، ومن ثمَ تعد ضبطاً لها، وتجدر الإشارة إلى أن ضبط الأدلة المتحصمة من الوسائل الإلكترونية قد تكتنفه الصعوبة البالغة عندما يكون متعلقا بنظام آلي بأكمله ، إذ أن هذا الأمر يحتاج إلى تعاون دولي لأجل إتمام هذا الضبط دون إعاقة سير النظام المعلوماتي[3]، لذلك قد يصادف ضبط الأنظمة المعلوماتية صعوبتان، الأولى وهي أن الضبط سيؤدي إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر مما قد يتسبب عنه أضرار بالجهة مستخدمة النظام، أما الثانية فهي عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل أو الفعال مع سلطات التحقيق مما يعني لها الضبط بأنه مساس بحقوق الغير[4].

ومن التشريعات التي تجيز ضبط أي شيء منها المكونات المعنوية للوسائل الالكترونية نجد التشريع اليوناني الذي يجيز في المادة (201) من قانون الإجراءات الجنائية التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضرورياً لجمع وحماية الدليل، ويفسر الفقه اليوناني عبارة (أي شيء) بأنها تشمل ضبط البيانات المخزنة أو المعالجة الكترونياً، لذلك فإن ضبط البيانات المخزنة في حاملات البيانات المادية أو في الذاكرة الداخلية لا تسبب أي مشكلة في اليونان، إذ يجوز للمحقق أن يعطي أمراً للخبير بجمع البيانات التي تكون مقبولة كدليل في المحاكمة الجزائية ، كما تجيز أيضا المادة (260) من قانون نفسه استخدام القوة القسرية أثناء ضبط المستندات المتعلقة بالجريمة في حالات البنوك أو المؤسسات الخاصة والعامة، ولهذا فإن المحققين بمقدورهم أن يأخذ البيانات المخزنة في حاملات البيانات، وفي كندا تجيز المادة (487) من القانون الجنائي الكندي سلطة إصدار إذن لضبط (أي شيء) طالما تتوافر أسس معقولة للاعتقاد بأن الجرم ارتكب أو يشتبه في ارتكابه أو أنه سينتج دليلاً على وقوع الجريمة[5].

أما بالنسبة للمكونات المعنوية فالبرغم من عدم نص قانون التوقيع الالكتروني والمعاملات الالكترونية رقم (78) لسنة 2012 العراقي على جريمة تزوير التوقيع الالكتروني وعقوباتها والإجراءات النتخذه . فنرى امكانية ضبط وتفتيش المكونات المعنوية ، فالبرجوع الى قانون اصول المحاكمات الجزائية رقم (23) لسنة 1971 ، نجد من مفهوم المادة (75) أنَّ لقاضي التحقيق إذا تراءى له وجود اشياء تفيد التحقيق فله أن يأمر المتهم بتقديمها ، وإذا خُشي منه أنْ يهربها فله تفتيشها.وبالتالي ضبطها. وكان من الاجدر كما اسلفنا لو نص بشكل صريح ومفصَّل لهذه الاجراءات في قانون التوقيع او القوانين الجنائية ذات الصلة.

1- اشرف قنديل ، مصدر سابق ، ص .63

2- هلالي عبد اللاه احمد ، مصدر سابق ، ص199-200 .

3- اشرف قنديل ، مصدر سابق ، ص 62-63 .

4- عفيفي كامل عفيفي، فتوح عبد الله الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، منشورات الحلبي الحقوقية ،بيروت، 2007، ص 354 .

5- هلالي عبد اللاه احمد ، مصدر سابق ، ص200.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

ب. ضبط المراسلات الإلكترونية التي تحتوي على المحررات المزورة

إنَّ المراسلات الالكترونية ما هي إلَّا مراسلات ذات صبغة تقليدية من ناحية المضمون، ولا تختلف عن المراسلات العادية إلَّا من حيث الوسيلة التي تستخدم لنقلها، في حين أن المراسلات التقليدية تتم عبر البريد العادي فإنَّ المراسلات الالكترونية تتم عبر الياتف المحمول أو الحاسوب المربوط بشبكة الانترنيت حيث يخصص لكل شخص موقع الكتروني ، وهذا الموقع عبارة عن ملف يستخدم لاستقبال الرسائل بواسطة معالج الرسائل وعندما يريد أي مستخدم الحصول على الرسائل الخاصة به فإنه يستدعيها باستخدام أي وصلة طرفية بالانترنيت أو بإرسال رسائل إلى أي مكان في العالم باستخدام خطوط التيلفون أو الموجات اللاسلكية أو الأقمار الصناعية[1]. بذلك فان هذه المراسلات تتوفر لها الحماية الدستورية والقانونية ولايجوز الإطلاع عليها إلَّا بإذن من الجهة القضائية المختصه.

ج. ضبط مراسلات البريد الإلكتروني

يعد البريد الالكتروني من الخدمات المهمة التي تقدمها شبكات المعلومات حتى أنه أصبح واحداً من أكثر وسائل الاتصال شيوعاً، وهو شكل من أشكال الاتصال الالكتروني يسمح للافراد بتبادل الرسائل بشكل فوري من خلال شبكات المعلومات التي تعرف مجتمعة بالانترنت[2]. بمعنى آخر يقصد بالبريد الإلكتروني استخدام شبكات الانترنت لنقل الرسائل بدلاً من الوسائل التقليدية ، وبالنظر إلى سهولة استخدامه فقد أصبح من أكثر وسائل الانترنت شيوعاً واستخداماً في الوقت الحالي. وقد عرف القانون الأمريكي بشأن خصوصية الاتصالات الالكترونية الصادر سنة 1986 البريد الالكتروني بأنَّه (وسيلة اتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية خاصة أو عامة، وغالباً يتم كتابة الرسالة يتم إرسالها الكترونياً إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه حيث يتم إرسالها عبر نظام خطوط التليفون إلى كمبيوتر المرسل إليه). وعرفه القانون الفرنسي بشأن الثقة في الاقتصاد الرقمي الصادر في 2004 بأنه(كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صوت أو أصوات ويتم ارسالها عبر شبكة اتصالات عامة، وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها).

أما عن طريقة ضبط البريد الالكتروني، فعلى قاضي التحقيق الدخول إلى صندوق البريد الخاص بالمتهم في جريمة تزوير التوقيع الالكتروني بطريقتين، تتمثل الأولى في أن المتهم يعطي عنوان بريده الالكتروني ورقمه السري لقاضي التحقيق لأجل الدخول، أما الطريقة الثانية فهي الولوج إلى بريده الالكتروني عن طريق تشفير رقمه السري، ثم يذهب إلى قائمة البرنامج الرئيسة للبريد الالكتروني، فتظهر القائمة بها خيارات الصادر، الوارد، الحفظ، المهملات، فيدخل للرسائل الواردة التي استقبلها المتهم، أو اختياره للرسائل الصادرة والتي أرسلها المتهم، أو مجموعة الرسائل التي كتبها

1- بكري يوسف بكري، مصدر السابق، ص.138

2- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ط 1 ، منشوارةن الحابي الحقوقية، بيروت، 2005، ص44.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

المتهم ثم قام بحفظها، أو باسترجاع الرسائل التي قام المتهم بحذفها من قائمة سلة المهملات[1].

2-2 - إجراءات التحقيق الهادفة إلى الكشف عن الحقيقة

سوف نقصر البحث في هذا المجال على اجرائين من اجراءات التحقيق ، والتي تكون لها اهمية كبيرة وعلى الخصوص في جريمة تزوير التوقيع الالكتروني :

2-2-1- الخبرة في الجرائم الواقعة على التوقيع الالكتروني

قد يحتاج الأمر إلى الإستعانة بالخبير لإيضاح بعض المسائل التي تقابله وتستعصي ثقافته العامة على فهمها، والخبرة لها أهمية خاصة في مجال جريمة تزوير التوقيع الإلكتروني، نظراً لكون شبكات الحاسبات وشبكات الاتصالات بينها أنواع مختلفة, كما يحق للخصوم الحضور أثناء عمل الخبير، وغالبا ما يحتاج قاضي التحقيق إلى خبير خاصة في الأمور الأكثر تعقيداً، وذات التقنية العالية[2].

أولاً: شروط الخبير في جريمة تزوير التوقيع الالكتروني

إذا كانت الوسائل الإلكترونية وشبكات الاتصال متنوعة، فإن طبيعتها الفنية تجلعها موزعة على تخصصات فنية وعلمية دقيقة، ما يستوجب من جهات التحقيق والمحاكمة أن تراعي ذلك عند اختيارها للخبير، فيجب أن تتيقن أنه تتوفر لديه الإمكانات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة، وانما يجب أن تتوفر لديه أيضاً الخبرة العملية التي تمكنه من اكتساب كفاءة فنية عالية، وبالنظر إلى الطبيعة الفنية والعملية للخبرة في مجال الجرائم الإلكترونية فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية [3]:

1- الإلمام بتركيب الحاسوب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر أو كود التشفير.

2- طبيعة البيئة التي يعمل في ظلها الحاسوب من حيث تنظيم ومدى تركيز أو توزيع عامل المعالجة الآلية وتحديد أماكن التخزين المستخدمة في ذلك.

3- قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك عطب أو تدمير للأدلة المتحصلة من الوسائل الإلكترونية.

4- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل ععى دعائمها الممغنطة.

ثانياً: مجالات الخبرة في جريمة تزوير التوقيع الالكتروني

تتنوع العمليات الإلكترونية باستخدام الوسائل الإلكترونية، فنجد أمثلة لها في الأعمال المصرفية وفي الإدارة الإلكترونية وفي التجارة الإلكترونية، ولذلك فإنه يتصور تنوع الجرائم التي تقع على هذه العمليات وفقاً لنوع الوسائل الإلكترونية المستخدمة في ارتكابها وأمثلتها تزوير التوقيع الالكتروني في المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة عن بعد المعالجة، وأيضاً التلاعب في بيانات التوقيع الالكتروني، وكذلك الغش أثناء نقل وبث بيانات التوقيع الالكتروني ، وقد يكون التزوير في التوقيع الالكتروني الخاص ببطاقة الائتمان، أو في التوقيع الالكتروني المستعمل إذا ما كنا أمام جريمة استعمال التوقيع الالكتروني من قبل الغير، أو في أجيهة وتطبيقات وبرامج صناعة التوقيع الالكتروني

1- هلالي عبد اللاه احمد ، مصدر سابق ، ص214 .

2- الشحات إبراهيم محمد منصور، مصدر سابق، ص .199

3- اشرف قنديل ، مصدر سابق ، ص 59-60.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

إنَّ جمع الدليل بالنسبة لهذه الجرائم يحتاج إلى بحث مسائل علمية وفنية، فالأدلة قد تكون غير مرئية ويلزم تحويلها إلى أدلة مقروءة، وقد تكون نتيجة تلاعب في حسابات معينة أو في نظم التوقيع الالكتروني بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب، وقد يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل الإلكترونية نتيجة استخدام الشفرات والتوقيعات الالكترونية السرية، وبالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية الواقعة على التوقيع الالكتروني فإن إماطة اللثام عنها قد يحتاج في أغلب الحالات إلى خبرة فنية تظهر الحاجة إليها منذ بدأ مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مرحلتي التحقيق والمحاكمة نظراً للطابع الفني الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء.

ثالثاً: أساليب عمل الخبير

الخبير التقني في سبيل التحري عن الحقيقة في جرائم تزوير التوقيع الالكتروني يستخدم الأساليب العلمية التي يقوم عليها تخصصه، هناك أسلوبان لعمل الخبير التقني:

1- القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة الكترونية في ذاتها، كجريمة الدخول لقاعدة بيانات متعلقة بالتوقيع الالكتروني ، ثم القيام بعملية تحميل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسباها إلى مسارها التي أعدت فيه وتحديد عناصر حركتها وكيف التوصل إلى معرفتها ، ومعرفة برتوكول الانترنيت الذي ينسب إلى جهاز الحاسوب الذي صدرت منه الجريمة.

2- القيام بتجميع وتحصيل المواقع التي لا تشكل موضوعها جريمة في حد ذاتها، وانما تؤدي حال تتبع موضوعها إلى مساعدة مرتكب الجريمة كالمواقع التي توضع كيفية اختراق وتغيير التواقيع في المستندات[1].

2-2-2- الشهادة في مجال جريمة تزوير التوقيع الالكتروني :

لم تضع التشريعات موضوع المقارنة تعريفاً لها ، أما الفقه فقد عرّفها بأنها (إدلاء الشخص فيما لديه من معلومات وأقوال أدركها بإحدى حواسه بشأن جريمةٍ وقعت أوبشأن واقعة تتعلق بهذه الجريمة ، أو بشأن المتهم بأرتكاب هذه الجريمة)[2]، وعُرّفت أيضاً بأنها (مايقرره الإنسان بخصوص واقعة أدركها بحاسةٍ من حواسه أمام جهة قضائية وفقاً للإجراءات المقررة قانوناً لذلك)[3].

وللشهادة أهمية خاصة في المسائل الجزائية لأنها إحدى الأدلة التي يُعتمد عليها في تقرير مصير المتهم ، فكثيراً مايكون للشهادة سواء أثناء التحقيق الإبتدائي أم المحاكمة أكبر الأثر في القضاء بالإدانة أو البراءة ، وإذا كانت الشهادة على هذا القدر الكبير من الأهمية ، فمن غير المستغرب أن تُقرر العديد من التشريعات بعض الضمانات التي من شأنها أن

1- خالد ممدوح ابراهيم، مصدر سابق ، ص299 .

2- د.سليمان عبد المنعم ، أصول الإجراءات الجنائية ، دراسة مقارنة ، منشورات الحلبي ، بيروت ، 2005 ، ص .839

3- د.محمود صالح العادلي ، إستجواب الشهود في المسائل الجنائية ، دراسة مقارنة في القانون الوضعي والشريعة الاسلامية ، دار الفكر الجامعي ، الأسكندرية ، 2005 ، ص8.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

تكفل سلامة الشهادة وهي بذات الوقت تحمي المتهم تجاه هذا الإجراء[1].

يقصد بالشاهد في الجريمة الإلكترونية؛ الفني صاحب الخبر والتخصص في تقنية و علوم الحاسب الآلي, والذي تكون لديه معلومات جوهرية ولازمة للدخول في نظام المعالجة الآلية للمعلومات إذا كانت مصلحة التحقيق تقتضي التنقيب على أدلة الجريمة داخله، ويطلق عل هذا النوع من الشهود الشاهد المعلوماتي" يشمل " الشاهد المعلوماتي " عدّة وظائف، أهمها: القائم على تشغيل الحاسب الآلي، والمبرمجون، زالمحللون، ، مهندسو الصيانة[2].

1- د. حسن بشيت خوين ، ضمانات المتهم في الدعوى الجزائية خلال مرحلة التحقيق الإبتدائي ، دراسة مقارنة ، ط1 ، مكتبة دار الثقافة ، عمان ، الأردن ، 1998 ،ص.109

2- الشحات إبراهيم محمد منصور، مصدر سابق، ص197.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

الخاتمة

في نهاية البحث كان لزاماً علينا ان نوجزه بخاتمة تتضمن اهم النتائج التي توصلنا اليها والمقترحات:

اولاً: النتائج

1- التوقيع الالكتروني علامة شخصية تتخذ حروف أو أرقام أو رموز أو إشارات أو اصوات او غيرها ، وله طابع متفرد يدل على نسبته الى الموقع ويكون معتمداً من جهة التصديق. أما اجراءات التحقيق في جرائم التزوير الالكتروني فهي (عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة إلكترونية من فاعل بها لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لاقامة العدل). أو هي الإجراءات التي يقوم بها قضاة التحقيق أوالمحققين القضائيين عبر العالم الافتراضي لضبط جريمة تزوير التوقيع الإلكتروني والتثبت من أدلتها ومعرفة فاعلها تمهيداً لإحالتهـــــــــم للمحاكمة.

2- يتميز التحقيق في جرائم تزوير التوقيع الالكتروني عن التحقيق بالطريقة التقليدبه من عدة نواحي، إذ يتميز بتطور المفاهيم المستخدمة فيه ، وله ذاتية خاصة ومستقله مستمدة من الطبيعة الخاصة والمميزة للجريمة الإلكترونية عن الجريمة التقليدية، فالتحقيق. و غالباً ما يتخذ الدليل في الجرائم الإلكترونية شكلاً مغايراً للشكل التقليدي للدليل. كذلك التحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم التقليدية إذ يصعب توضيحها لهيئة المحكمة ويسهل زرع الشك في وجدانها.

3- وتتمثل إجراءات التحقيق الابتدائي في هذه الجريمة بإجراءات جمع الأدلة في الجرائم المرتكبة بالوسائل الالكترونية الواقعة على التوقيع الالكتروني، وكذلك إلى إجراءات التحقيق الهادفة إلى الكشف عن الحقيقة.

4- أن المجرم الالكتروني على عكس المجرم التقليدي يتميز بالذكاء، ومتمرس بتفاصيل الحاسوب، والشبكات والبرمجيات، وهذا ما يدعو لصعوبة الاستجواب معه ، وكذلك صعوبة تفتيش وضبط ادوات الجريمة ، كذلك يحتاج القضاة أن يتمتع القضاة بمعلومات علمية وعملية في مجال البرامجيات .وكذلك انتداب خبراء مختصين ولهم خبرة في هذا المجال . وايضاً الشاهد في هكذا جرائم يجب ان تتوفر فيه شروط خاصة .

ثانياً: المقترحات

1- ندعو المشرِّع العراقي لتضمين قانون التوقيع الالكتروني أو الاسراع باصدار قانون جرائم المعلوماتية من خلال تبيان بشكل مفصل اجراءات التحقيق في هذه الجرائم لازالة اللبس والغموض والنقص التشريعي .

2- ضرورة تأهيل القضاة والمحققين واعضاء الضبط القضائي ، من خلال دورات علمية تبيِّن الاساليب التقنية المستحدثة والمستخدمة في ارتكاب جرائم تزوير التوقيع الالكتروني ، وتدريبهم على كيفية كشف هذه الجرائم ، وايضاً كيفية اعتراض محنوى المحرر الالكتروني.

المصادر

أولاً: الكتب

1- أحمد المهدي وأشرف شافعي ، التحقيق الجنائي الإبتدائي وضمانات المتهم وحمايتها ، دار الكتب القانونية ،مصر، 2006 .

2- د. أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها ، المركز القومي للإصدارت القانونية، القاهرة، 2017 .

3- د.أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية ، دار النيضة العربية، القارة، 1985 .

4- د.اشرف عبد القادر قنديل ، الاثبات الجنائي في الجريمة الالكترونية ، دار الجامعة الجديدة للنشر ، الاسكندرية ، 2015 .

5- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، ط 1، دار الفكر الجامعي 2011..

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

6-إلياس ناصيف، العقد الإلكتروني في القانون المقارن،ط1،منشو ا رت الحلبي الحقوقية،بيروت، 2009.
7- امير فرج يوسف ، الجديد في التوقيع الالكتروني ، ط1 ، مكنبة الوفاء القانونية ، الاسكندرية ، 2011.
8- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، ط 1، دار الفكر الجامعي، الإسكندرية، 2011.
9- جلال ثروت، سليمان عبد المنعم، أصول المحاكمات الجزائية، ط 1 ، المؤسسة الجامعية للدراسات، بيروت، 1997.
10- جمال محمد مصطفى ،، شرح قانون أصول المحاكمات الجزائية العراقي ، مطبعة الزمان ، بغداد ، 2005 .
11- جمعة سعدون الربيعي ،الدعوى الجزائية وتطبيقاتها، مطبعة الجاحظ ، بغداد ، العراق، 1996 .
12- جواد الرهيمي ، أحكام البطلان في قانون أصول المحاكمات الجزائية ، ط2 ، المكتبة القانونية ، بغداد، العراق ، 1. 2006
13- د. حسن بشيت خوين ، ضمانات المتهم في الدعوى الجزائية خلال مرحلة التحقيق الإبتدائي ، دراسة مقارنة ، ط1 ، مكتبة دار الثقافة ، عمان ، الأردن ، 1998 .
14- د.حسن صادق المرصفاوي ، أصول الإجراءات الجنائية، منشأة المعارف ، الإسكندرية ،مصر ، 1977 .
15-خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الاردن،2011. 16- خالد ممدوح ابراهيم، فن التحقيق في الجرائم الالكترونية، ط 1 ، دار الفكر الجامعي ، الإسكندرية، 2018.
17-د.سليمان عبد المنعم ، أصول الإجراءات الجنائية ، دراسة مقارنة ، منشورات الحلبي ، بيروت ، .2005
18- شيماء عبد الغني محمد عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، د ط، المنصورة، كلية الحقوق, 2005 .
19- د. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الالكترونية، ط3 ،دار الثقافه للنشر والتوزيع، عمان، 2019 .
20- عبدالأميرالعكيلي و د.سليم حربة ،، أصول المحاكمات الجزائية ، ج2، المكتبة القانونية ، بغداد ، بلا تاريخ طبع .
21- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، ، ط 1 ، منشأة المعارف، الإسكندرية، 2009 .
22- عفيفي كامل عفيفي، فتوح عبد الله الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ، منشورات الحلبي الحقوقية ،بيروت، 2007 .
23- د. علي عبد القادر القهوجي ، القانون الدولي الجنائي ، ط1 ، منشورات الحلبي ، بيروت ، لبنان، 2001 .
24- علي وجيه حرقوص ، قاضي التحقيق في قانون اصول المحاكمات الجزائية الجديد ، ط1 ، مشورات زين الحقوقية ، بيروت ، لبنان، 2005 .
25- مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة ، 2000.
26-محمد الشهاوي شرح قانون التوقيع الالكتروني ، دار النهضة العربية ، القاهرة ، 2010 .
27- محمد ناصر حمودي، العقد الدولي الإلكتروني المبرم عبر الإنترنت،ط1، دار الثقافة للنشر والتوزيع،عمان، 2012 .
28- د.محمود صالح العادلي ، إستجواب الشهود في المسائل الجنائية ، دراسة مقارنة في القانون الوضعي والشريعة الاسلامية ، دار الفكر الجامعي ، الأسكندرية ، 2005 .
29- محمود عبد العزيز محمد ، التفتيش الاذن والاجراء والدليل والتدليل فقهاً وقضاءً ، دار الكتب القانونية ، مصر ، 2009 .
30- مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الالكترونية"،طبعه الاولى،مطابع الشرطه،القاهره، 2009 .
31- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، ، ط 1 ، منشوارةن الحابي الحقوقية، بيروت، .2005
32- نورجان محمد علي ، التوقيع الالكتروني في ظل قانون المعاملات الالكترونية الاردني، ط1 ، .2003
33- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي ،ط 2، دار النهضة العربية، القاهرة،2008.

ثانياً: الاطاريح

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

1- عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، اطروحة دكتوراه ،كلية الحقوق،جامعة عين شمس، 2004 .

2- محمد صلاح محمد عبد المنعم، الجرائم الالكترونية وتحدياتها ، دارسة مقارنة ، اطروحة دكتوراة ـ كلية الحقوق ، جامعة المنصورة ،2005 .

ثالثاً : البحوث المنشورة

1- علي أبو مارية، التوقيع الإلكتروني ومدى قوته في الإثبات ، مجلة جامعة الخليل للبحوث، المجلد 5، العدد 2010 .

2- فاطمة زهرة بوعناد ، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية،العدد الأول، 2013 ، الجزائر .

3- د. محمد الأمين البشري، "الاساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، محاضرة مقدمة في الحلقة العلمية تحليل الجرائم المستحدثة والسلوك الإجرامي المنعقدة في الفترة من 17 - 19 / 1 / 2011 بمقر جامعة نايف العربية للعلوم الأمنية .

4- محمد المرسي ابو زهرة ، الدليل الكتابي وحجية مخرجات الكمبيوتر في الاثبات في المواد المدنية والتجارية ، من بحوث مؤتمر القانون والكمبيوتر والانترنت ، 1، 3 مايور ، جامعة الامارات العربية المتحدة .

5- مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وأثباتها في فلسطين ، بحث منشور مجلة علوم الشريعة والقانون، الجامعة الأردنية، المجلد 45 ، عدد 4 ، ملحق 2 ، 2018 .

رابعاً المصادر الاجنبية

1-Alain Bensoussan, La signature numérique et électronique en procédure pénal. www. De alain.bensoussan. com.

2- Santiago Cavanillas Mugica et autres, commerce électronique, Edition delta, 2 beyrouth liban 2004

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

ڕێکارەکانی لێکۆڵینەوەی سەرەتایی لە تاوانی ساختەکردنی واژۆی ئەلیکترۆنی

پ. ی. د. يحيى حمّود مراد الوائلي
لقی یاسای گشتی، کۆلێژی یاسا ، زانکۆی کەربەلا- عێراق
ئیمێل:yahya.h@uokerbala.edu.iq

پوختە

"ساختەکردنی واژۆی ئەلیکترۆنی ئاماژەیە بۆ بەکارهێنانی نیشانەیەکی کەسی کە پێکهاتووە لە پیت، ژمارە، هێما، نیشانە، دەنگ، یان شتی تر، لەگەڵ سیمایەکی ناوازە کە ئاماژەیە بۆ گەڕاندنەوەی بۆ ئەو کەسە یان ئەو دامەزراوەیەی واژۆی لەسەر دەکات. ڕێکارەکانی لێکۆڵینەوە بۆ تاوانەکانی ساختەکردنی واژۆی ئەلیکترۆنی چەندین ڕێکاری یاسایی لەخۆدەگرێت لەسەر بنەمای دەسەڵاتی دادوەری کارامەی هەیە بۆ ناسینەوەی تاوانباران و گەیاندنیان بە دادگا چەمکە بەکارهێنراوەکان و بابەتەکانی خۆی.لێکۆڵینەوەکە پەیوەستە بە کۆکردنەوەی بەڵگەی دیجیتاڵی و شیکردنەوەی واژۆی ئەلیکترۆنی، لەگەڵ سەختی سەلماندنی تاوانە ئەلیکترۆنییەکان لەبەردەم دادگادا.توێژینەوەکە جەخت لەوە دەکاتەوە پێویستی بە دادوەر و پسپۆڕی پسپۆڕ لە بواری تەکنەلۆژیای زانیاری هەیە بۆ تێگەیشتن لە وردەکارییە تەکنیکی و تەکنەلۆژییەکانی پەیوەست بە تاوانەکە.

ڕێکارەکانی لێکۆڵینەوە سەرەتاییەکان ڕووبەڕووی کۆکردنەوەی بەڵگە و ئاشکراکردنی ڕاستییەکان دەبنەوە لە تاوانەکانی ساختەکاری ئەلیکترۆنیدا، لەوانە چۆنیەتی لێپرسینەوە لە تاوانبارێکی ئەلیکترۆنی کە تایبەتمەندی هەواڵگری و لێهاتوویی تەکنیکی هەیە، ئەمەش لێکۆڵینەوەکە ئاڵۆزتر دەکات، هەروەها کێشەی پشکنین و دەستبەسەرداگرتنی بەڵگەکان و چ جۆرە بەڵگەیەک دەتوانرێت دەست بەسەردا بگیرێت، پێویستە شارەزایەکیش ئامادەبێت، بەڵگەی تاوان و شایەتحاڵ ئەو تایبەتمەندیانەن کە لە تایبەتمەندییەکانی ئەم پۆلانەدا لە تاوانە تەقلیدییەکاندا بەردەست نین."

کلیلەوشەکان :واژۆی ئەلیکترۆنی، ساختەکاری، تاوانی ئەلیکترۆنی، ڕێکارەکانی لێکۆڵینەوە.

Initial investigation procedures in the crime of forgery of electronic signature

Asst. Prof. Dr. Yahya Hamoud Murad Al-Waeely
Department of Public Law, College of Law, University of Karbala, Iraq.
Email: yahya.h@uokerbala.edu.iq

Abstract

" Forgery of an electronic signature refers to the use of a personal mark consisting of letters, numbers, symbols, signs, sounds, or others, with a unique character indicating its attribution to the person or institution signing it. The investigation procedures for crimes of forgery of an electronic signature include many legal procedures based on It has the competent judicial authorities to identify the perpetrators and bring them to justice. The investigation into electronic signature forgery crimes is distinguished from the traditional investigation into non-electronic crimes by the development of the concepts used and its subjectivity. The investigation depends on collecting digital evidence and analyzing the electronic signature, with the difficulty of proving electronic

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

crimes before the court. The research emphasizes There is a need for judges and experts specialized in the field of information technology to understand the technical and technological details related to the crime.

The primary investigation procedures are faced with collecting evidence and revealing the truth in electronic fraud crimes, including how to interrogate a cybercriminal who is characterized by intelligence and technical skills, which makes the investigation more complex, as well as the problem of inspecting and seizing evidence and what type of evidence can be seized. An expert must also be present. Criminal evidence and witnesses are characteristics that are not available in the characteristics of these categories in traditional crimes".

key words:Electronic signature, forgery, electronic crimes, investigation procedures.