جامعة نايف العربية للعلوم الأمنية
Naif Arab University For Security Sciences

فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني

د. عبد الله بن سعود محمد السراني

الرياض
الطبعة الأولى
١٤٣٢هـ - ٢٠١١م

ح (٢٠١١)، جامعة نايف العربية للعلوم الأمنية ـ الرياض ـ

المملكة العربية السعودية. ص. ب ٦٨٣٠ الرياض: ١١٤٥٢
هاتف ٢٤٦٣٤٤٤ (ـ١ـ٩٦٦) فاكس ٢٤٦٤٧١٣ (ـ١ـ٩٦٦)

البريد الإلكتروني: Src@nauss.edu.sa

ISBN 8- 65 - 8006- 603- 978

P.O.Box: 6830 Riyadh 11452 Tel. (+1 966) 2463444 KSA

Fax (966 + 1) 2464713 E-mail Src@nauss.edu.sa

ح (١٤٣٢هـ) جامعة نايف العربية للعلوم الأمنية

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

السراني، عبدالله بن سعود محمد

فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني/ عبدالله بن سعود محمد السراني، الرياض ١٤٣٢هـ

٤٤٢ ص ، ١٧ × ٢٤ سم

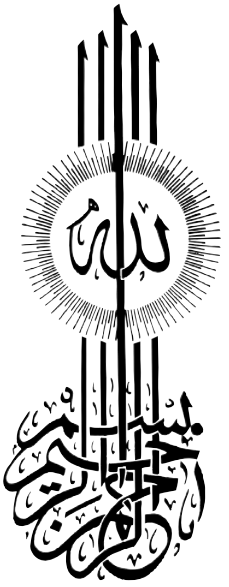
ردمك: ٨ـ٦٥ـ٨٠٠٦ـ٦٠٣ـ٩٧٨

١ ـ التزوير ٢ ـ الجريمة والمجرمون أ ـ العنوان

ديوي ٣٦٤,١٦٣ ١٤٣٢ / ٤٦٣٥

رقم الايداع: ١٤٣٢ / ٤٦٣٥

ردمك: ٨ـ٦٥ـ٨٠٠٦ـ٦٠٣ـ٩٧٨


بسم الله الرحمن الرحيم

المحتويـــات

الفصل الأول

مدخـل الدراسـة

١. مدخل الدراسة

١.١ مقدمة الدراسة

أصبح التعامل مع المعلوماتية نتيجة حتمية لمواكبة التطور التقني والتكنولوجي في ظل التحول الإلكتروني لمختلف نواحي الحياة وفي ظل عالم مفتوح تتسيّده المعلومات والتي أضحت بحق مصدر القوة والمعرفة، والمعيار الحقيقي لتطور ونمو الشعوب ومستقبلها.

إن التطور الكبير في تقنية المعلومات والاتصالات لم يقف عند حدود التعاملات التقليدية، بل امتد ليشمل كافة الأنشطة الاقتصادية، مما ترتب عليه ارتفاع المهارات التقنية للمستخدمين، وكمظهر من مظاهر الإساءة لاستخدام تقنية المعلومات والاتصالات ظهرت الجرائم الإلكترونية التي تختلف طبيعة ومضموناً عن الجرائم التقليدية، مما جعل النظم والقوانين الحالية غير كافية لمواجهة هذه الجرائم سواء في مجالات التجريم أو العقاب أو الوقاية، في ضوء اختلال التوازن بين الاستفادة من تقنية المعلومات، وبين إساءة استخدامها، مما يتطلب استحداث نظم وقوانين لتحقيق التوازن ما بين الاستخدام الحر والكامل للمعلوماتية من ناحية، وبين حماية المواطن وحرياته من ناحية أخرى.

لذلك تسعى الهيئات والجهات التي تتبنى نشاطاً معلوماتياً إلى الحفاظ على معلوماتها، وأسرارها، وتخزينها بعيداً عن أيدي مرتكبي جرائم المعلوماتية.

فالتزوير الإلكتروني على سبيل المثال يعني تزوير المستندات والبيانات الموجودة على جهاز الكمبيوتر، وتزوير المعلومات بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية، وتستهدف جريمة التزوير أيضاً المستندات والبيانات بشكل واسع للبيانات الممثلة للاستحقاقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات وأوامر الدفع وقوائم المبيعات وأنظمة التحويل الإلكتروني للأموال والودائع المصرفية (الكركي، ١٩٩٨م، ص٦٠).

وهناك جملة من المعوقات تعترض سبيل اكتشاف الجرائم الإلكترونية عامة وخاصة جرائم التزوير الإلكتروني، منها أساليب يستخدمها الجناة تتعدى تدمير الأدلة لتصل إلى فرض تدابير أمنية تمنع اكتشافهم، وتمنع الحصول على دليل ضدهم ومن هذه الأساليب استخدام كلمات المرور، أو كلمات السر حول مواقعهم تمنع من الوصول إليها ومن ثم تمنع التفتيش المتوقع الذي يكون القصد منه البحث عن أدلة، وإلى جانب هذا الأسلوب يستخدم الجناة أسلوب الترميز، والتشفير، بل إن الجناة وحسب ما يذهب البعض يلجأون إلى أسلوب حماية يصل إلى الحيلولة دون ضبطهم والإيقاع بهم (حجازي، ٢٠٠٢م، ص ٤٨).

ومما يثار في صدد إثبات جرائم الحاسب الآلي بوجه عام وجرائم التزوير الإلكتروني بوجه خاص إمكانية الاستناد إلى الدليل الرقمي باعتبار أن هذه الجرائم جرائم غير تقليدية ترتكب عن طريق نبضات إلكترونية يرسلها الجاني إلى جهاز الحاسب الآلي للمجني عليه فيسيطر عليه بعد اختراقه، أو أن يستقبلها منه، وهذه وتلك عملية لا يمكن البت فيها من قبل القضاء قبل أن تتولى سلطات التحقيق فيها، بل إن تحديد الآثار التي ترتبت، على اختراق

الحاسب الآلي، وعن الجريمة لا يمكن تحديدها إلا من خلال محقق ذي خبرة ودراية فنية.

وفي ضوء استقرار الأمر على التعاملات الإلكترونية في المملكة العربية السعودية، وتعاظم استخدام هذه التقنيات في كافة نواحي التعاملات الإلكترونية اعتماداً على هذه الآلات الحاسوبية، ظهرت الحاجة لتشريعات تواكبها من حيث الوقاية والمكافحة لمواجهة السلوك الإجرامي في استخدامها، وأصبح التوقيع التقليدي (اليدوي) عقبة من المستحيل تكيفها مع النظم الحديثة للإدارة والمحاسبة الآلية، فقد تم الاتجاه نحو بديل لذلك التوقيع التقليدي (اليدوي) بما يسمى بالتوقيع الإلكتروني، مما زاد من المخاطر نتيجةً لعدم توافر الضوابط الكافية لعدم استغلالها في تنفيذ معاملات مزورة (المسعودي والحلبي، ٢٠٠٧م، ص ٦٤٠-٦٤١).

وهذا ما حدا بالباحث باعتباره يعمل محققاً في أقسام مكافحة التزييف والتزوير بالأمن العام إلى دراسة جريمة التزوير الإلكتروني بصفة خاصة، ومحاولة إيجاد بعض الأساليب التي تساعد ذوي الاختصاص في مكافحة هذه الجريمة وإثباتها بوسائل علمية صحيحة.

١ . ٢ مشكلة الدراسة

في نطاق جرائم الحاسوب فإن التزوير الإلكتروني يعد تغييراً للحقيقة يرد على مدخلات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر المعلوماتي أن يكون مدوناً باللغة العربية أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات لا ورقية شرط أن تكون محفوظة على

دعامة ـ كبرنامج منسوخ في أسطوانة ـ وشرط أن يكون المحرر المعلوماتي ذا أثر في إثبات أو أثر قانوني معين (حجازي، ٢٠٠٥م، ص٣٢).

كما أن جريمة استعمال التوقيع الإلكتروني المزور بالتقليد أو الاصطناع وشهادة اعتماد هذا التوقيع المزور، وذلك فيما زورت لأجله هي جريمة استعمال مستقلة عن التزوير ذاته. ويمكن أن يتصور التعدد المادي هنا دون انفصال أو استقلال (العريان، ٢٠٠٤م، ص١٤٢).

وإذا تحقق التزوير بالتقليد أو الاصطناع قامت جريمة التزوير المعلوماتي في حق الجاني، وهنا تتكون صورتان للجريمة هما التزوير واستعمال المحرر المزور وهي جريمة عمدية، صورة الركن المعنوي فيها هو القصد الجنائي بعنصريه العلم والإرادة، حيث يجب أن يعلم الجاني بوقائع الجريمة وأن ذلك محظور وفقاً للقانون، ومع ذلك تتجه إرادته إلى الفعل المجرم ويقبل النتيجة المترتب عليها (حجازي، ٢٠٠٥م، ص ٥٨٣).

وزاد من أهمية المشكلة الاتجاه الحديث للمملكة العربية السعودية نحو تفعيل الحكومة الإلكترونية في التعامل اليومي بالدوائر الحكومية والمتعلق بمصالح المواطن. وكذلك صعوبة مواجهة المجرم الإلكتروني، وفداحة الخسائر، وزيادة احتمالات إفلات المجرم من العقوبة، مما جعل الباحث يشعر أنه مقبل على صور عديدة من التزوير الالكتروني تتطلب التعرف على فاعلية أساليب التحقيق ودورها في إثبات التزوير الإلكتروني سواء باستخدام الأساليب التقليدية أو المادية أو الإجرائية اللازمة لمكافحة هذه الجرائم وتقديم بعض التوصيات والمقترحات التي تساعد في إقناع القضاء بصورها وتكييفها القانوني.

ترد صور عديدة للتزوير الالكتروني تواجهها أقسام مكافحة التزوير منها مثلاً قيام شخص مصرح له بالدخول إلى النظام المعلوماتي بطريقة

مشروعـة أي أنه له كود أو رمز يدل عليه (توقيع الكتروني) يؤهله بالدخول إلى النظـام المعلومـاتي والتعامل معه إما لمصلحته هو أو غيره سـواء كان هذا بمقابـل أو بدون مقابل يتم تغيير الحقيقة بالنظام المعلوماتي بالحاسـب بطرق التزويـر المعتـادة في المحـرر الطبيعـي. ومن أهم صـور التزويـر الإلكتروني العمليات المالية في البنوك، حيث يتم التحويل تزويراً، بجانب تزوير بطاقات الائتـمان والتي تتـم حالياً بطرق عـبر وطنية، وقيام بعـض موظفي الأحوال المدنيـة بتغيـير بيانات المهنة تزويـراً في هويات بعض العسـكريين، لتمكينهم من السفر خارج المملكة دون علم مراجعهم، أو نسبة آخرين لغير آبائهم أو أمهاتهم، أو منح آخرين هوية سعودية يترتب عليها آثار اجتماعية واقتصادية سلبية.

كما أن انتشـار وتوفر وسـائل وبرامـج تقنية حديثة، وسـهولة الحصول عليها من الأسواق المحلية، وبأسعار في متناول الجميع التي تستخدم برنامج للتجسس الصناعي (C.T.A) على البيانات المخزنة مثل وسائل تقنية وبرامج إخفاء وحدات ناقلة للبيانات في البرنامج، واستخدام برنامج حصان طروادة بصورة خفية واستعمال هوائيات مع ربطها بحاسب خاص، واستخدام تقنية المصيدة أو الأبواب الخلفية وأجهزة الالتقاط للبيانات المنقولة الكترونياً.

وتزداد مشكلة التزوير الإلكتروني صعوبة يوماً بعد يوم، في ضوء التزايد المطـرد في ارتـكاب هــذه الجريمة بوسـائل متنوعة، وبصفـة خاصة من قبل بعـض العاملين في الدوائـر الحكومية الإلكترونية من المخـول لهم بالدخول عـلى النظـام الذين قـد يتلاعبـون في قاعـدة البيانـات دون إدراك للمخاطر الأمنيـة التـي تترتـب عـلى ذلك، في ضـوء الخلـط بـين التزويـر الإلكتروني والتزوير التقليدي خلال الإحصاءات الجنائية، فغالبية الإحصاءات تدمجهما

معـاً، وهـذا ما أكـده الباحث عنـد محاولة إيجـاد إحصائيات مسـتقلة لجرائم التزويـر الإلكتروني، وبعد مجهود شـاق تمكن من الحصول عـلى (٦٠) قراراً صـادراً عن الدوائـر الجزائية بديوان المظـالم بفروعه المختلفـة بإدانة مرتكبي جرائـم التزوير الإلكـتروني والتلاعب في قواعد البيانـات، وقد قام الباحث بتحليـل (٢٠) منهـا ليوضح وجود هذه الظاهرة وتفاقمهـا باطراد، وإظهار الأسـاليب التقليديـة والمادية والإجرائيـة في إثبات هذه الجرائـم التي تحتاج لتمتع مرتكبيها بخصائص تميزهم عن غيرهم.

ومـن خصائـص مرتكبـي هذه الجرائـم أن معظـم نشـاطاتهم تتركز في الحقـوق المالية للأفراد والشركات أو أن يكون الدافع إليها غرضي شـخصي كالتيـار الفكـري، أو أنهم مجرمـون يسـببون أضراراً اقتصاديـة باهظة دولية وإقليمية ومحلية كشفت عنها الإحصاءات الجنائية (شتا، ٢٠٠٠م، ص ٩٩).

لذلك يتصور وقوع التزوير في النظام المعلوماتي عن طريق تغير الحقيقة عـلى الشرائـط أو المسـتندات التـي تمثـل مخرجـات الحاسـب الآلي طالمـا أن التغيير ذاته قد طال البيانات الحاسـوبية في المحررات الرسـمية حالة التزوير المعلومـاتي في المحرر الرسـمي أو المسـاس بحق لأحد الأفـراد، وذلك حال التزويـر المعلوماتي في المحـرر العرفي، ذلك إن جرائم التزوير المادي تحصرها كل الأنظمة والتشريعات في خمس هي:

١ ـ وضع إمضاءات أو أختام أو بصمات مزورة.

٢ ـ تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات أو محوها.

٣ ـ وضع أسماء أو صور أشخاص آخرين مزورة.

٤ ـ التقليد.

٥ ـ الاصطناع.

أما جرائم التزوير المعنوي فهي:

١ ـ إقرار أولي الشأن.

٢ ـ جعل واقعة مزورة في صورة واقعة صحيحة.

٣ ـ جعل واقعة غير معترف بها في صورة واقعة معترف بها (حسنى، ١٩٨٨م، ص٢٢٧).

وهنا تبرز مشكلة رجال الشرطة والعدالة نتيجة لقصور الإمكانات المادية والبشرية في مواكبة مثل هذا النوع من جرائم التقنية المعلوماتية التي يحتاج فيها إلى الخبرة التحقيقية العملية وأساليبها العلمية اللازمة لإثبات جريمة التزوير الإلكتروني وتتبع خيوط هذه الجريمة، مما يدعو إلى إجراء دراسة علمية للتعرف إلى فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني من لحظة الاكتشاف ثم تلقي البلاغ والتحريات وجمع الاستدلالات والمعاينة والتفتيش لمحل الجريمة البيئة الإلكترونية) لإثبات جريمة التزوير الإلكتروني بأساليب علمية وفنية قادرة على إثباتها. ومن هنا تتبلور مشكلة الدراسة الحالية في التساؤل الرئيس التالي:

ما فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني ؟

١ . ٣ تساؤلات الدراسة

ويتفرع عن التساؤل الرئيس الأسئلة الفرعية التالية:

أ ـ التساؤلات المرتبطة بالدراسة المسحية: ويتم الإجابة عليها من خلال المسح الاجتماعي لآراء أفراد مجتمع الدراسة وتحليل مؤشرات هذه الآراء وهي:

١ ـ ما خصائص جريمة التزوير الإلكتروني ؟

٢ـ ما الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني ؟

٣ـ ما صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية؟

٤ ـ ما سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني ؟

٥ ـ ما سمات المجني عليه في جرائم التزوير الإلكتروني ؟

٦ ـ ما فاعلية الأساليب التي يتبعهـــا المحقق الجنائي في إثبات جرائم التزوير الإلكتروني ؟

٧ ـ ما فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني ؟

٨ ـ ما المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني ؟

٩ ـ هل هناك فروق ذات دلالة إحصائية في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية ؟

ب ـ التساؤلات المرتبطة بالإطار النظري للدراسة: ويتم الإجابة عليها باتباع المنهج المكتبي من خلال الاطلاع على الأدبيات المتصلة بالتساؤلات وهي:

١ ـ ما الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني ؟

٢ ـ ما موقف الشريعة الإسلامية من جرائم التزوير الإلكتروني ؟

١ . ٤ أهداف الدراسة

الهدف الرئيس لهذه الدراسة يتمثل في الآتي:

التعرف على فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني.

ويتفرع عن هذا الهدف الأهداف التالية:

١ ـ الوقوف على خصائص جريمة التزوير الإلكتروني.

٢ ـ التعرف على الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني.

٣ ـ التعرف على صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

٤ ـ التعرف على سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني.

٥ ـ التعرف على سمات المجني عليه في جرائم التزوير الإلكتروني.

٦ ـ التعرف على فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني.

٧ـ التعرف على فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني.

٨ـ التعرف على المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

٩ـ التعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية.

١٠ـ التعرف على الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني.

١١ـ التعرف على موقف الشريعة الإسلامية من جرائم التزوير الإلكتروني.

١ . ٥ أهمية الدراسة

التطور المتسارع لاستخدام الحاسب الآلي والإنترنت وسيطرة الجانب المعلوماتي والغموض الذي يحيط بالجريمة المعلوماتية ذاتها حتى في البلدان التي أدخلت في تشريعاتها أنماط من هذه الجرائم، منها جرائم التزوير الالكتروني، وعدم وضوح هذه الجريمة ومعالمها حتى على المشتغلين بها من المحققين والقضاة لقلة القضايا التي عرضت عليهم، وانعدام الأدلة المادية الملموسة في هذه الجريمة المعلوماتية (جريمة التزوير الالكتروني)، وتظهر أهمية هذه الدراسة في الآتي:

١ ـ الأهمية النظرية

تنبثق أهمية هذه الدراسة من حيوية الموضوع الذي تناولته وهو فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني.

كما تبرز الأهمية العلمية لهذه الدراسة فيما قد تسهم به من لفت الانتباه للأبعاد الجديدة لأحدث جرائم التزوير التي تتم عن طريق استخدام التقنيات الحديثة والمعاصرة، وهو ما دعت إليه كثير من المنظمات الدولية المعنية بهذا الأمر مثل المنظمة العربية للعلوم الأمنية، والمنظمة الدولية لحماية المعلومات، وذلك من خلال استعراض الباحث لنسق المعلومات التي توضح جريمة تزوير المحرر الإلكتروني، كمحل للحماية القانونية، وصور جريمة التزوير الإلكتروني، وما يتعلق بالتوقيع الإلكتروني، والتصديق الإلكتروني، وجهة التصديق، وخصائص جريمة التزوير الإلكتروني والمجرم الإلكتروني والمجني عليه في جريمة التزوير الإلكتروني، وفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني، وموقف الشريعة الإسلامية من جريمة التزوير الإلكتروني، والمعوقات التي تواجه المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

ومن المتوقع أن تسهم هذه الدراسة في استنباط دراسات جديدة تلقي الضوء على أهمية التوقيعات الرقمية والأختام الرقمية، والمعوقات التي تحول دون إثبات جريمة التزوير الإلكترونية.

٢ ـ الأهمية العملية

تنبثق الأهمية العملية للدراسة من دورها في تحديد فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني، ولفت نظر مخططي السياسة

الأمنية سـواء من حيث تشـخيص المشـكلة أو من حيث تقديـم الرؤى التي تسهم في التخطيط لمواكبة الجرائم المستحدثة تجريباً ومكافحة ومنعاً.

ولذلك يأمل الباحث أن تسهم هذه الدراسة في تزويد الأجهزة المسؤولة عـن مكافحة التزويـر بالآليات اللازمة لمواجهة جرائـم التزوير الإلكتروني، وطـرق اكتشـاف التزوير، ومن ثم اتخاذ الوسـائل اللازمـة لحماية المحررات والوثائق والتعاملات الإلكترونية الحكومية.

١ . ٦ حدود الدراسة

تحددت حدود ا لدراسة بالمجالات التالية:

١ . ٦ . ١ الحدود البشرية

تقتصر الدراسـة على المحققـين الجنائيين والفنيـين العاملين في مكافحة التزويـر في الأمـن العـام والجـوازات، والمعنيـين بمكافحـة جرائـم التزوير الإلكـتروني من الذين على رأس العمل في العـام ١٤٣٠هـ في الواقع الميداني لمدن المملكة.

١ . ٦ . ٢ الحدود المكانية

تقتصر الدراسـة على المحققـين الجنائيين والفنيـين العاملين في مكافحة التزويـر في الأمـن العـام، والجـوازات والمعنيـين بمكافحـة جرائـم التزوير الإلكتروني في مدن المملكة العربية السعودية.

١ . ٦ . ٣ الحدود الموضوعية

سـوف يقوم الباحث بتوزيع أداة الدراسـة (الاسـتبانة) عـلى المبحوثين المعنيـين بالتحقيق في إثبات جرائم التزوير الإلكتروني (جنائياً في مرحلة جمع

الاستدلالات والتحقيق وليس قضائياً) بالأمن العام والجوازات بالمملكة، من خلال الإجابة على محاورها الآتية:

أ ـ خصائص جريمة التزوير الإلكتروني.

ب ـ الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني.

جـ ـ صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

د ـ سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني.

هـ ـ سمات المجني عليه في جرائم التزوير الإلكتروني.

و ـ فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني.

ز ـ فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني.

ح ـ المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

ط ـ الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني.

ي ـ موقف الشريعة الإسلامية من جرائم التزوير الإلكتروني.

كما سيقوم الباحث بدعم الدراسة بتحليل قرارات أحكام صادرة عن الجهات القضائية المختصة بنظر هذه الجرائم المتمثلة بالدوائر الجزائية بديوان المظالم، حيث سيتم دراسة بعض أحكام هذه الدوائر الجزائية بديوان المظالم بمختلف فروعه في المملكة، وقد اشتملت على عشرين حكماً قضائياً.

١ . ٦ . ٤ الحدود الزمانية

سوف يجري الباحث الدراسة خلال العام الدراسي الجامعي ١٤٣٠ هـ.

١ . ٧ مفاهيم ومصطلحات الدراسة

١ . ٧ . ١ الجريمة في النظام

تعـرف الجريمة في نظام الإجراءات الجزائية السـعودي بأنها: «كل فعل يخالف الحق والعدل ويتضمن ارتكاب محظورات شرعية زجر الله عنها بحد أو تعزير» (الحجيلان، ٢٠٠٦م، ص٥).

تعـرف الجريمـة في القانـون بأنهـا: «كل عمـل أو امتناع ضـار له مظهر خارجـي ليـس اسـتعمالاً لحق ولا قيامـاً بواجـب، يُجرّمه القانـون، ويفرض لـه عقابـاً، ويقوم به إنسـان أهل لتحمل المسـؤولية الجنائيـة». (محيي الدين، ١٩٨١م، ص٩٥).

وتعرف جريمة التزوير الإلكتروني إجرائياً بأنها: ارتكاب جريمة التزوير الإلكتروني سـواء بالدخول المـشروع أو غير المشروع على النظـام المعلوماتي والتعامل مع بياناته تزويراً بطرق التزوير المادية والمعنوية باستخدام الحاسب الآلي وملحقاته للحصول على محرر أو وثيقة إلكترونية مزورة.

١ . ٧ . ٢ الفاعلية

هي: «اختيار أهداف مناسـبة وملائمة وواقعية وقابلة للإنجاز والعمل على إنجازها» (الخشروم وموسى، ١٩٩٩م، ص٢٥).

قيـام الأفراد بتحقيق أهـداف المنظمات وتنفيذ الأعـمال والمهام المطلوبة منهم (ماهر، ٢٠٠٠م: ٤٢-٤٣).

وتعـرف الفاعليـة إجرائيـاً بأنهـا: القـدرة عـلى إثبـات جرائـم التزوير الإلكتروني من قبل المحقق الجنائي والفني من لحظة الاكتشاف وتلقي البلاغ

والتحريـات والانتقال والمعاينة والتفتيش لمحل الجريمة (البيئة الإلكترونية) والبحـث عن الأدلة الفنية، وإثبات العلاقة السـببية بين الجاني والمجني عليه وكشف غموض الجريمة.

١ . ٧ . ٣ الأساليب المستخدمة

الطريقة العلمية المسـتخدمة والمتاحة التـي يتبعها المحقق في التحقيق في إثبات جرائم التزوير الإلكتروني من لحظة اكتشافها وتلقي البلاغ والتحريات وجمع الاسـتدلالات والمعاينـة والتفتيش لمحل الجريمـة (البيئة الإلكترونية) وهي مخرجات الحاسـب الآلي لإثبـات طريقة التزوير الإلكتروني بأسـاليب علمية (عليان وغنيم، ٢٠٠٠م، ص٣٣).

وعرفت الأسـاليب العلمية بأنها: الطرق التي أحدثت تغييرات جذرية في وسـائل الإثبات الجنائي، ولم تكن معروفة من قبلٍ، اعتمادا على النظريات العلمية والممارسات العلمية الميدانية بما لا يعطي مجالاً للجدل في حقيقتها، أو الطعن في صحتها (بوادي، ٢٠٠٥م).

كـما عرفت بأنها: الوسـائل التي تعتمد علي اسـتخدام النظريـات والحقائق العلميـة في مجـالات مكافحة الجريمـة، وذلك عن طريق إقامـة دليل الاتهام على الجـاني أو تبرئتـه، ويسـتخدم في ذلـك الأجهـزة العلميـة الحديثة التـي تعتمد في تطورهـا عـلى العلـوم والفنون، ومـن أمثلتها التصويـر الجنائـي، وأجهزة قياس السرعـة، وأجهـزة مقارنة البصـمات، والأسـلحة الناريـة، والمقذوفـات النارية (إبراهيم، ١٩٨١م).

وتعـرف الأسـاليب المسـتخدمة إجرائياً في هذه الدراسـة بأنها: الأسـاليب العلمية والفنية المتاحة التي يستخدمها المحقق الجنائي والفني للتعامل مع مسرح

جريمة التزوير الالكتروني لفحص أجهزة الحاسوب ونظم المعلومات والبرامج، وما تحتويه من بيانات ومعلومات، باستخدام تقنيات التحري والمعاينة والمحافظة على مسرح جريمة التزوير الإلكتروني ثم استخدام تقنيات التتبع الإلكتروني، والتفتيش الإلكتروني، وصولاً للإثبات الإلكتروني وهو ما يسعى إليه الباحث من خلال إثبات الجريمة لإدانة مرتكبي جرائم التزوير الإلكتروني.

١. ٧. ٤ الإثبات

يعرف الإثبات في المواد الجنائية بأنه: «إقامة الدليل على وقوع الجريمة، أو عدم حصولها وعلى إسنادها إلى المتهم أو براءته منها» (يونس، ٢٠٠٦م، ص٨).

وفي معناه القانوني (النظامي) هو إقامة الدليل على وجود واقعة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون (السنهوري، ١٩٥٦م، ص ١٣-١٤).

وهو الوسيلة الثبوتية التي يتوصل إليها قاضي الموضوع لإثبات التهمة على المتهم، ونفيها عنه، ومن ثم الحكم ببراءته. (السماك، ١٩٩٠م، ص ١٦٥).

ويعرف الإثبات إجرائياً في هذه الدراسة بأنه: إقامة الدليل على ارتكاب جريمة التزوير الإلكتروني ونسبة الجريمة إلى مرتكبها، وإقناع الجهات القضائية بحجية الدليل الإلكتروني في إثبات الجريمة.

١. ٧. ٥ الأثر المادي

عرف الأثر بأنه (كل ما يتركه الجاني في مكان الجريمة، أوفي الأماكن المحيطة أو المجاورة، أو الأماكن المتصلة بها)(إبراهيم ،١٩٨١م).

كما عرف بأنه: (كل مادة، أو جسم يعثر عليه في مسرح الجريمة، أو على أحد أطرافها سواء تم إدراكه بالحواس مباشرة، أو بالاستعانة بالأجهزة العلمية) (الردادي، ٢٠٠٠م، ص٧٦).

ويعرف الأثر المادي إجرائياً في هذه الدراسة بأنه: كل ما يتخلف عن الجاني، أو إحدى أدواته في مسرح جريمة التزوير الالكتروني ،مثل (أجهزة الحاسب ونظم المعلومات والبرامج والأقراص المدمجة وما تحتويه من أدلة رقمية وبيانات ومعلومات وما يرتبط بها من طابعات وأجهزة مسح ضوئي وما يصدر عنها من مخرجات ورقية حاسوبية تتضمن بيانات المحرر المزور سواء في موضوعه أو التوقيع الالكتروني عليه ـ أو جهة التصديق والتوثيق) وكل ما يتم العثور عليه من أثر في البيئة الالكترونية عامة من أحبار وأدوات قص أو تثبيت مستخدمة وماسحات ضوئية وأجهزة ملحقة بأجهزة الحاسوب.

١. ٧. ٦ تعريف الأدلة الجنائية

الدليل اصطلاحا هو ما يلزم من العلم به علم شي آخر. وغايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة (أحمد، ١٩٩٤م، ص ١٧٤).

وتعرف الأدلة الجنائية إجرائياً في هذه الدراسة بأنها: وسيلة إثبات جريمة التزوير الإلكتروني التي تشير إلى مرتكبها دون غيره وتوضح العلاقة بين الجاني والمجني عليه.

١ . ٧ . ٧ الأدلة الجنائية الرقمية

إن الأسس العلمية للدليل المادي بعد التطور العلمي في مجال علوم الأدلة الجنائية قد زرعت نوعاً من الثقة والارتياح لدى جهات التحقيق والقضاء، فخلفت لديهم حالة من الاقتناع اليقيني بأهمية الأدلة وقيمتها الإثباتية (إن الأدلة المادية طريقة وأسلوب للإثبات، يعلو في شأنه، ويسمو في قيمته على نظائره من الأدلة الأخرى، ومن ثم فهو يحتل مركز الصدارة في الإثبات الجنائي) (أبو القاسم، ١٤١٤هـ، ص٢٥٧).

وظهور ذلك النوع من الجرائم الالكترونية وخاصة جرائم التزوير الالكتروني أوجد الحاجة إلى البحث عن أدلة مادية للتعامل معها تكون نابعة من طبيعة تلك الجرائم المعلوماتية، حيث أدى ذلك إلى ظهور الأدلة الجنائية الرقمية (Digital Evidence) التي أصبح استخدامها في تزايد مستمر في الإثبات (MARR, 2003).

والجريمة الالكترونية هي الجريمة التي يكون للحاسوب والشبكات المعلوماتية دور فيها، بما في ذلك الجرائم التي تعتمد كثيراً على الحاسوب، والجرائم التي يكون الحاسوب بها مجرد مستودع للأدلة الجنائية.

وعرفت الأدلة الجنائية الرقمية بأنها عبارة عن البيانات الرقمية الموجودة في الحاسوب وملحقاته، أو المنقولة عبر شبكات الاتصال، والتي يمكن عن طريقها كشف وقوع الجريمة، أو إثبات وجود علاقة بينها وبين الجاني أو المجني عليه (البشرى، ١٤٢٣هـ).

وتعرف الأدلة الجنائية الرقمية إجرائياً في هذه الدراسة بأنه: البيانات الرقمية الموجودة في الحاسوب وملحقاته (البرامج والملفات) أو المنقولة

عـبر شـبكة الاتصال التـي يمكن مـن خلالها كشـف وقوع جريمـة التزوير الإلكتروني وإثباتها وإيجاد العلاقة بينها وبين الجاني والمجني عليه.

١ . ٧ . ٨ التزوير الإلكتروني

يعني «أي تغير للحقيقة يرد على مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسـومة عـن طريق الراسـم ويسـتوي في المحرر الإلكـتروني أن يكون مدونـاً باللغة العربيـة أو لغـة أخرى لهـا دلالتها، كذلك قـد يتم في مخرجـات ورقية شرط أن تكـون محفوظـة على دعامـة، كبرنامج منسـوخ على أسـطوانة، وشرط أن يكـون المحرر الإلكتروني ذا أثـر في إثبات حق أو أثر قانوني معين (حجازي، ٢٠٠٢م، ص١٧٠).

ويعرف التزوير الإلكتروني بأنه تغيير الحقيقة في المسـتندات المعالجة آلياً والمستندات المعلوماتية وذلك بنية استعمالها» (القهوجي، ١٩٩٢م، ص٦٣).

ويعرف التزوير الإلكـتروني إجرائياً بأنه: تغيير البيانات والمعلومات في المسـتندات المعالجة آلياً باسـتخدام أجهزة وبرمجيات اختراق وتعد للحصول عـلى مسـتندات تحاكي الأصـل، ولكن مـزورة في مضمونهـا وصيغتها، بنية استخدامها في تحقيق مصلحة لمرتكب التزوير أو لشخص آخر.

١ . ٧ . ٩ الجريمة المعلوماتية

أي فعل يرتكب متضمناً اسـتخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفـة لأحكام هذا النظام.(المادة الأولى نظام مكافحة جرائم المعلوماتية، ١٤٢٨هـ).

كما تعرف الجريمة المعلوماتية بأنها «كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادية أو المعنوية». (قشقوش، ٢٠٠٠م، ص٤).

وتعرف الجريمة المعلوماتية إجرائياً بأنها: استخدام تقنيات المعلومات في عمليات الاختراق والتعدي على البيانات أو إتلافها أو سرقتها أو محوها، أو تزويرها، أو سرقة منظومة التوقيع الإلكتروني واستخدامه بغير تصريح من مالكه الأصلي، أو الامتناع عن إجراء عمليات التغيير النظامية وفقاً لمسوغات صحيحة.

١٠.٧.١ المحرر في جريمة التزوير

يقصد بالمحرر في جريمة التزوير «مجموعة العلامات والرموز المكتوبة التي تعبر عن معنى معين يستشف من مجرد النظر إليها»، وإذا كان من اللازم نسبة المحرر إلى شخص معين إلا أنه لا يلزم كتابته بطريقة معينة، فقد يكون بخط اليد أو عن طريق آلة كاتبة أياً كانت درجة تقدمها، أو عن طريق آلة حافرة، ولا يدخل في بنيان المحرر كذلك المادة التي دون عليها، فقد تكون ورقاً أو خشباً أو جلداً أو مادة بلاستيكية (عبد الستار، ١٩٨٨م، ص٢٤٤).

ويعرف المحرر في جريمة التزوير إجرائياً بأنه: المستندات والوثائق المكتوبة التي تحتوي تفاصيل عن موضوع معين رسمي أو عرفي الذي يتم فيه تغيير الحقيقة في موضوعه بطرق التزوير المادية أو المعنوية حيث يتم تغيير بياناته بالحذف أو الإضافة (مثلاً) لتغيير المعنى ضمناً أو نسبته إلى شخص آخر.

١.٧.١١ جريمة المحررات المزورة

تعرف بأنها «جريمة عمدية يتخذ ركنها المعنوي صورة القصد الجنائي، وهـو يتمثل في اتجاه إرادة الجاني إلى اسـتعمال المحرر مع العلم بتزويره ويجب أن يثبت العلم باليقين لديه بالتزوير، فلا يغني عنه مجرد تمسكه بالورقة المزورة واحتجاجـه بها أومن المتصور التمسـك بها على الرغم مـن الجهل بتزويرها» (حجازي، ٢٠٠٥م، ص٥٨٣).

وتعـرف جريمة المحـررات المـزورة إجرائياً بأنهـا: تعمد تغيـير بيانات المحـررات وتحريفها جزئياً بالحذف أو الإضافة، أو كلياً بالتقليد والاصطناع باستخدام تقنية المعلومات والاتصالات، واستخدام المحرر المزور مع علمه بتزويره.

١.٧.١٢ الجريمة الإلكترونية

تعرف بأنها «النشـاط الإجرامي الذي تسـتخدم فيـه التقنية الإلكترونية الرقميـة بصورة مبـاشرة أو غير مبـاشرة، كوسـيلة لتنفيذ الفعـل الإجرامي المستهدف» (موسى، ٢٠٠٣م، ص٥٦).

كما تعرف بأنها أنماط من الجريمة تسـتخدم فيها التقنية الحديثة من أجل تسهيل عملية الإجرام»(اليوسف، ١٤٢٠هـ، ص١٣).

أمـا التعريـف الـذي تبنـاه مؤتمـر الأمـم المتحدة العـاشر لمنـع الجريمة ومقاومـة المجرمين، حيث عرّف الجريمـة المعلوماتية بأنها «أية جريمة يمكن ارتكابها بواسـطة نظام حاسـوب وتشـمل تلك الجريمة مـن الناحية المبدئية جميـع الجرائم التـي يمكن ارتكابها في بيئـة الكترونية» (مؤتمـر الأمم المتحدة العاشر، ٢٠٠٠م).

وتعرف الجريمة الإلكترونية بعدة تعريفات من أشـملها تعريف منظمة التعـاون الاقتصادي للتنميـة الذي عرّفها بأنها» كل فعل أو امتناع من شـأنه الاعتـداء على الأمـوال المادية والمعنوية، يكـون ناتجاً بطريقـة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية. (الملط، ٢٠٠٥م، ص٩٦).

أما الجرائم المشتقة من الجريمة الإلكترونية فيذكرها (Casey, 2000, 5) في «الخلاعة، والفسـق وإغـراء القصر على أداء أعمال الجريمة والتحرشـات والانتهاكات والتحايل والتجسس والتخريب والتدمير والتزوير».

وتهـدف هـذه الجرائـم إلى الإسـاءة للبيانـات والمعلومـات الموجـودة عـلى الشـبكة العالميـة للمعلومات والخاصة بشركـة معينة، ومـن أنواع تلك الإسـاءة الإلكترونية محو المعلومات أو تزويرها أو إلغائها أو تعديل مسارها (الشوابكة، ٢٠٠٤م، ص١٨).

وتعـرف الجريمـة الإلكترونيـة إجرائياً بأنها: اسـتخدام الحاسـب الآلي وتقنيـة الاتصال والمعلومـات في عمليات الاختراق والتعـدي على البيانات والملفـات والمعلومـات بسرقتهـا أو تغيير محتواهـا، أو تزويرها، لاسـتغلالها في عمليـات بيـع وشراء وهمية، أو تحويل حسـابات لصالح الجاني بعد سرقة بيانات بطاقات الائتمان الخاصة بالآخرين.

١٣.٧.١ المجرم الإلكتروني

يعرف المجرم الإلكتروني بأنه «المجرم الذي لديه قدرة على تحويل نواياه إلى لغـة رقميـة باسـتخدام التقنيـة الرقميـة المعلوماتية، وذلك بـأداء فعل أو الامتناع عنه، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة لمخالفته قواعد الضبط الاجتماعي محلياً أو دولياً» (موسى، ٢٠٠٣م، ص١٦).

ويعرف المجرم الإلكتروني إجرائياً بأنه: شخص يستغل مهاراته التقنية المتميزة في ارتكاب عمليات الاختراق والتعدي وتزوير البيانات والمحررات وتغييرها، وسرقة منظومة التوقيع الإلكتروني، وسرقة أرقام بطاقات الائتمان لتحقيق مصلحة شخصية له أو لغيره.

١٤.٧.١ التوقيع الإلكتروني

«وحدة قصيرة من البيانات التي تحمل علامة رياضية مع البيانات الموجودة في محتوى الوثيقة» (قشقوش، ص٥٢).

فمن خلال التوقيع الإلكتروني يمكن تحديد هوية المرسل والمستقبل إلكترونياً والتأكد من مصداقية الأشخاص والمعلومات وأنها نفس المعلومات الأصلية.

كما عرفه قانون التجارة الإلكترونية في دبي الصادر برقم (٢) لسنة ٢٠٠٢م بأنه توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذو شكل إلكتروني وملحق أو مرتبط منطقياً برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة كما عرف التوقيع الإلكتروني ـ المحمي ـ أي الذي يتمتع بحماية القانون وأن ذلك التوقيع استوفى الشروط المنصوص عليها في المادة (٢٠) من القانون المذكور.

ويعرف التوقيع الإلكتروني إجرائياً بأنه: بيانات مشفرة يتم التصديق عليها واعتمادها من قبل هيئة مختصة، تمنحه مصداقية وقوة التوقيع التقليدي اللازم لإجراء المعاملات الإلكترونية كافة.

١ . ٧ . ١٥ صاحب التوقيع الإلكتروني

فقد عرف بأنه «الشخص الطبيعي أو المعنوي الحائز لأداة توقيع الكتروني خاصة به، ويقوم بالتوقيع أو يتم التوقيع نيابة عنه على الرسائل الإلكترونية باستخدام هذه الأداة». (حجازي، ٢٠٠٧م، ص٢٣٥).

ويعرف صاحب التوقيع الإلكتروني إجرائياً بأنه: شخص يمتلك توقيعاً إلكترونياً مصدقاً من جهة معترف بها محلياً أو دولياً، ويستخدمه في توقيع معاملاته عبر التقنيات الإلكترونية في أي مكان في العالم، وهو يماثل التوقيع التقليدي وله نفس المصداقية.

١ . ٧ . ١٦ إدارة الأدلة الجنائية

هي إحدى الإدارات العلمية الفنية بجهاز الأمن العام ،والمرتبطة مباشرة بمدير الآمن العام، وهو ما يعطيها الحيدة والاستقلالية المطلوبتين في مجال عملها.ويرتبط بها فنياً إدارات للأدلة الجنائية في جميع مناطق المملكة، كما تضم في تشكيلها الداخلي عدداً من الإدارات، والشعب والأقسام المزودة بأحدث التقنيات، والأجهزة العلمية التي يعمل عليها خبراء سعوديون مؤهلون أكاديميا وما يهمنا منها شعب أبحاث التزوير في هذه الدراسة حيث تتولى فحص مسارح الحوادث، وما تحتويه من آثار متنوعة لأجهزة الحاسوب (الحاسوب ونظم المعلومات والبرامج حيث يقومون بالانتقال إلى أماكن وجودها وفحصها، بالإضافة إلى فحص ما يصل إليهم من مخرجات تتعلق بالتزوير الالكتروني (مثل البرنت أو البطاقات أو البرامج)، وتقديم الاستشارات، وإعداد التقارير العلمية الدقيقة اللازمة ومن ثم إرسالها إلى جهات التحقيق للاستفادة منها في التوصل إلى الحقيقة من خلال تقارير فنية عدلية.

الفصل الثاني

الإطار النظري والدراسات السابقة

٢. الإطار النظري والدراسات السابقة

٢. ١ الإطار النظري

أسـهمت التطـورات التقنية المتسـارعة في نهاية القـرن العشرين وبداية القـرن الحـادي والعشريـن في سرعة تحـول المجتمعـات من عـصر الصناعة إلى عـصر المعلومات، وتحولت أسـاليب وأنشـطة العمل تدريجيـاً إلى النمط الإلكتروني بعد زيادة قدرة الحاسـبات الآلية، والتمازج بين تقنية الاتصالات والمعلومـات التـي أسـفرت عن انطلاقـة قوية في عـالم تقنيـة المعلومات، مما جذب انتباه المنظمات الإدارية بصفة عامة والمنظمات الأمنية بصفة خاصة إلى محاولة الاستفادة من منجزات الحضارة التقنية فظهرت التجارة الإلكترونية، وتبعتها الحكومة الإلكترونية، وأخيراً الإدارة الإلكترونية كإيجابيات للتطور التقنـي المعـاصر، إلا أن الوجـه السـلبي للتقنيـة ترافق مع هـذه الإيجابيات، فظهرت جرائم المعلوماتية كأثر سـلبي لإساءة استخدام التقنية في ضوء عدم قـدرة القوانـين الحالية على فرض عقوبـات صارمة أو تحديـد هوية مرتكبي الجرائـم الإلكترونية بدقة، مما جعل اسـتخدام تطبيقـات التقنية الإلكترونية أمـراً محفوفـاً بالمخاطـر، نتيجـة إمكانية التعـرض لمخاطر الاخـتراق وسرقة منظومـة التوقيعـات الإلكترونية واسـتغلالها في صياغة محـررات مزورة قد يترتب عليها منح حقوق أو إعفاء من التزامات، أو استقدام أفراد مستبعدين أو إرهابيين أو ينتمون لجماعات الإرهاب المنظم.

ومن هذا المنطلق نشـأت الحاجة إلى بيان فاعلية الأسـاليب المسـتخدمة في إثبـات جريمة التزوير الإلكتروني، في ضـوء المعوقات التي تكتنف إثبات

جرائـم المعلوماتيـة، وحتى في حالة اكتشـاف أن هذه المحـررات التي تحمل التوقيـع الإلكتروني مـزورة، فمن الصعوبة بمكان تحديـد مرتكب الجريمة، ويقتـصر الأمر على اكتشـاف الموقـع الذي تم الاختراق منـه وسرقة منظومة التوقيـع الإلكـتروني، وإذا كان هـذا الموقع من جهة بعيـدة أو من دولة ليس بينها وبين الدول الأخرى تعاون في مجال تسـليم المجرمين، فلا يمكن توقيع العقوبـة عـلى الجـاني أو متابعة إجـراءات التحقيـق في ضوء اختـلاف النظم القانونيـة والعقابيـة والحاجة لتعـاون دولي لمواجهة جرائـم المعلوماتية ذات الطابـع الـدولي، ومن الصعـب إيقاف التعامـلات الإلكترونيـة التي تضفي المرونـة والسرعـة عـلى أداء المنظمات الأمنيـة في ظل التسـارع التقني للعصر الحالي الذي يتطلب الأخذ بأساليب التقنية الحديثة التي تزيد من فاعلية الفرد والمنظمة (الشاعر، ٢٠٠٤م، ص ١٥-١٦).

لذلـك يعـد التحكـم في تقنيـة المعلومـات والاتصـالات وتأمينهـا من مفاتيح تقدم المنظمات الأمنية وتطوير مسـتوى أدائها وقياس قدراتها، حيث بـات التخلـف التقني والمعلوماتي يشـكل خطراً مباشراً وخطـيراً على الأمن الوطني، فمن يمتلك التفوق في تقنية المعلومات والاتصالات يمتلك القدرة على السبق والريادة (عالم وشاهين، ٢٠٠٥م، ص١٦٣).

وقـد اعتمـد الباحث في إعداد الإطـار النظري على العديـد من أدبيات الفكـر الإداري في مجال الإدارة العامة، والسـلوك التنظيمـي، وإدارة الموارد البشرية، وتقنية المعلومات والاتصالات، وأمن المعلومات، واشتمل الإطار النظري على أربعة محاور تغطي فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني.

تنـاول المحـور الأول أمـن المعلومـات من خـلال اسـتعراض مفهومه وأهميتـه وعنـاصره، والأمـن المـادي لتقنيـة المعلومـات، وأمن الشـبكات،

والمجرم المعلوماتي. وتناول المحور الثاني الجرائم التي ترتكب بواسطة الحاسب الآلي وصعوبة إثباتها من خلال جرائم التزوير الإلكتروني، ومعنى الإثبات والقواعد التي تحكمه، والتعرف على فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني، وصعوبة التوصل للآثار المادية في جرائم الحاسب الآلي، وإثبات جرائم الحاسب الآلي بالأدلة العلمية، وتناول المحور الثالث التحقيق في جرائم التزوير الإلكتروني من خلال استعراض طرق اكتشاف جرائم التزوير الإلكتروني سواء فيما يتعلق بدور المحقق الجنائي في إثبات جرائم التزوير أو دور المحقق الفني في إثبات جرائم التزوير، والمحرر الإلكتروني. وتناول المحور الرابع مواجهة جرائم التزوير الإلكتروني من خلال استعراض الدور التشريعي والقضائي في مواجهة جرائم التزوير الإلكتروني، وموقف الشريعة الإسلامية من جرائم التزوير الإلكتروني.

٢. ١. ١ أمن المعلومات

أولاً: مفهوم أمن المعلومات

أمن المعلومات في ضوء تحديد صلاحية الاستخدام هو: فرض ضوابط على سبل وأساليب الوصول للمعلومات، بهدف إضفاء الشرعية على حدود وصلاحية استخدام المعلومات (العبود، ٢٠٠٥م، ص١٥٢).

وعرف أمن المعلومات من منطلق الحماية المادية وغير المادية بأنه: حماية المعلومات المختلفة والأدوات التي تتعامل معها وتعالجها، من منظمة وغرف تشغيل أجهزة، وأجهزة ووسائط تخزين وأفراد من السرقة، أو التزوير، أو التلف، أو الضياع، أو الاختراق باتباع إجراءات وسياسات وقائية (الحميد ونينو، ٢٠٠٧م، ص٣٤).

وعرف أمن المعلومات بأنه: اتخاذ الاحتياطات والتنظيمات التي تهدف إلى المحافظة على المعلومات في الحاسب الآلي بمأمن من الأعطال أو الحوادث أو الجرائم المتعمدة (الشمري، ١٩٩١م، ص١٠).

وعرف بأنه: مجموعة من الإجراءات الإدارية والفنية التي صممت لضمان حماية الأجهزة وملحقاتها والبرامج والبيانات من السرقة أو التوقف أو التلف المتعمد أو غير المتعمد أو التخريب أو التبديل أو مجرد الاطلاع دون تصريح بالاستخدام. وحماية شبكة المعلومات الداخلية والاتصالات الخارجية من الاختراق أو التعطيل المتعمد أو غير المتعمد (الشدي، ٢٠٠٠م، ص ٨٢-٨٣).

وعرف أمن المعلومات في إطار ما يجب أن تحظى به من سرية وخصوصية بأنه: ضمان الحفظ وعدم الإتلاف، أو التغيير، أو التعديل بالحذف أو الإضافة للمعلومات المخزنة، أو المنقولة عبر الشبكة (أبو مغايض، ٢٠٠٤م، ص ٢٧٠-٢٧١).

وفي ضوء التعريفات السابقة لأمن المعلومات، يتضح أنه ينطوي على:

أ ـ إجراءات وتدابير إدارية وفنية.

ب ـ تهدف إلى المحافظة على المكونات المادية للحاسب الآلي.

جـ ـ تسعى إلى المحافظة على المكونات غير المادية للحاسب الآلي.

د ـ وضع ضوابط وقيود لإضفاء الشرعية على حدود وصلاحية استخدام المعلومات والأجهزة.

هـ ـ الحماية ضد السرقة، أو التوقف، أو التلف المتعمد أو غير المتعمد، أو التخريب، أو التبديل، أو الاختراق، أو مجرد الاطلاع دون تصريح بالاستخدام.

ويعرف الباحث أمن المعلومات بأنه: اتخاذ الإجراءات والتدابير الإدارية والفنية والمادية لحماية المكونات المادية من أجهزة وملحقات وشبكات ووسائل اتصال وأقراص لبة ومرنة وضوئية، والمكونات غير المادية كالبرامج والتطبيقات والبيانات والمعلومات من السرقة، أو التوقف، أو التلف المتعمد أو غير المتعمد، أو التخريب، أو التبديل، أو الاختراق، أو مجرد الاطلاع دون تصريح بالاستخدام.

ثانياً: أهمية أمن المعلومات

للمعلومات أهمية وقيمة مادية ومعنوية للأفراد والشركات والدول، وتزداد أهميتها في المنظمات الأمنية والعسكرية، والاقتصادية ذات الطابع الاستراتيجي، لذلك ارتبط عنصر السرية بالمعلومات ودرجة توافرها، في ضوء ما يترتب على فقدانها من خسائر، وما يترتب على توافرها من مكاسب، حيث تلعب دوراً كبيراً في انتصار أو هزيمة الدول (الحمدان والقاسم، ٢٠٠٤م، ص٣٥).

وترجع أهمية أمن المعلومات إلى الحاجة للارتباط بنظم الاتصالات والإنترنت، وعدم إمكانية عزل الأجهزة عن الشبكات المحلية والشبكات واسعة النطاق لتوفير المعلومات لمن يحتاجها، واعتماد مختلف المنظمات على فعالية المعلومات في ظل صعوبة تحديد الأخطار والتحكم بها، أو متابعة المجرمين ومعاقبتهم لعدم توافر حدود جغرافية عند استخدام الإنترنت والاتصالات الإلكترونية لأنها تتيح الفرصة لاختراق الحدود المكانية، والنمو المطرد في الاستخدامات والتطبيقات الإلكترونية وظهور التجارة الإلكترونية والحكومة الإلكترونية والإدارة الإلكترونية التي تحتاج إلى بيئة معلوماتية آمنة (القاسم، ٢٠٠٥م، ص ٣٤-٣٥).

ثالثاً: عناصر أمن المعلومات

تتطلب المحافظة على أمن المعلومات توافر ثلاثة عناصر هي سرية المعلومات، وسلامتها وتوافرها.

١ ـ سرية المعلومات

تعني ضمان حفظ المعلومات المخزنة أو المنقولة عبر الشبكة وعدم الاطلاع عليها أو استخدامها إلا بموجب إذن (أبو مغايض، ٢٠٠٤م، ص٢٧٠).

وتهدف سرية المعلومات إلى التأكد من عدم اطلاع غير المصرح لهم عليها، فضلاً عن تحديد حدود وصلاحية الاستخدام سواء كان كلياً أو جزئياً، مع تحديد من له صلاحية التعديل أو الإدخال أو الحذف أو الإضافة أو القراءة فقط من بين المصرح لهم بوجه عام (الحميد ونينو، ٢٠٠٧م، ص٥٣).

٢ ـ سلامة المعلومة

تعني ضمان عدم تغيير المعلومات المخزنة أو المنقولة (أبو مغايض، ٢٠٠٤م، ص٢٧١)، حيث يتكون عنصر سلامة المعلومة من شقين: الأول سلامة المعلومة، والثاني سلامة المصدر، فالمفهوم الصحيح لسلامة المعلومة هو عدم تغييرها بشكل غير ملائم سواء بقصد أو بدون قصد، وأنها أدخلت بشكل صحيح يعكس الظروف الحقيقية للمعلومة. أما سلامة المصدر فيقصد بها الحصول على المعلومة من مصدرها الأصلي. وتشير سلامة المعلومات بصفة عامة إلى الإجراءات التي تضمن حفظ المعلومات خلال مراحل إدخالها أو نقلها بين الأجهزة والشبكات للمحافظة على سريتها وسلامتها (الحمدان والقاسم، ٢٠٠٤م، ص ٢٩-٣٠).

٣ـ توافر المعلومات

يعني ضمان بقاء المعلومات وعدم حذفها أو تدميرها (أبو مغايض، ٢٠٠٤م، ص٢٧١).

وأهم الأخطار التي تهدد توافر المعلومات:

١ـ رفض (منع) الخدمة: يعني الأعمال التي تعطل خدمات نظم الحاسب وشبكاته بصورة لا تُمكِّن المصرح لهم من استخدام الحاسب والاستفادة منها والوصول إلى المعلومات.

٢ـ فقدان القدرة على معالجة البيانات نتيجة الكوارث الطبيعية، أو الأفعال العمدية (القاسم، ٢٠٠٥م، ص٣١).

رابعاً: الأمن المادي لتقنية المعلومات

يعني الأمن المادي المحافظة على المعلومات بعيداً عن متناول غير المصرح لهم باستخدامها، من خلال منع المخترقين ومزوري المعلومات من الوصول إلى مركز المعلومات والجلوس على النهاية الطرفية لطلب المعلومات، ومنعهم من الوصول إلى أقراص التخزين، ومنعهم من فصل توصيلات شبكات المعلومات، أو إيقاف التيار الكهربائي عن النظام، أو تعطيل التكييف داخل غرفة النظام (الشدي، ٢٠٠٠م، ص١٩٥).

كما أن توفير الأمن المادي يتحقق من خلال توفير أمن المنظمة، وأمن الأجهزة ووسائط التخزين، وأمن غرفة تشغيل الحاسب، وأمن الأفراد (الحميد ونينو، ٢٠٠٧م، ص ٤٢-٥٢).

خامساً: أمن الشبكات

يتـم في أغلب الحالات نقل البيانات عن طريق الشـبكات؛ لذلك يجب الاهتمام بأمنها لضمان سرية وسلامة المعلومات ووصولها إلى الجهات المعنية. ويتحقق أمن الشبكات من خلال اتخاذ إجراءات الحماية اللازمة التي تنقسم حسب طبيعة المخاطر التي تتعرض لها إلى قسمين:

١ ـ إجراءات الحماية المادية

تتضمـن إجـراء التوصيـلات والتمديـدات بـين الأجهزة بشـكل أمن مـن خلال تمريرها عبر قنوات غير مكشـوفة يصعب الوصـول إليها، وعزل الكيابل داخل أنابيب بلاسـتيكية، مع وضع أجهزة استشـعار لإطلاق إنذار عند الخطر (الحميد ونينو، ٢٠٠٧م، ص١٥٣).

٢ ـ إجراءات الحماية غير المادية

١ ـ عنونـة الشـبكات: يجـب الالتـزام بوضـع عناوين لجميـع الأجهزة المرتبطة بالشـبكة؛ لكي يمكن التعرف عليها عند تشغيلها، ومن ثمَّ حمايـة جميـع العناوين والأجهزة التي تقوم بترجمـة وتحويل العناوين إلى الأشخاص غير المصرح لهم بالتعامل معها.

٢ ـ الاسـتفادة من الإعلانات التي تظهر على الشاشـة قبل إدخال كلمة المرور للمصرح لهم فقط بالدخول على الشـبكة؛ وذلك بتحذير غير المصرح لهم بخطورة محاولات الاختراق.

٣ ـ متابعـة جميـع محـاولات الدخـول عـلى النظـام سـواء الصحيحة أو الفاشلة.

٤ ـ توفير آليات الحماية بعد الدخول على النظام كإلزام المستخدم بالخروج من النظام عند عدم استخدامه، والخروج الآلي عند عدم استخدام النظام لفترة معينة، والخروج من النظام عند نهاية الدوام الرسمي.

٥ ـ يجب المحافظة على سرية رقم الهاتف الخاص بالدخول على النظام، إذا كان يتم عن طريق الهاتف، مع تجنب نشره بالدليل، وقصر المعرفة بهذا الرقم على من يستخدم النظام، ويفضل تغيير رقم الهاتف كل فترة (القاسم، ٢٠٠٥م، ص ٩٤-٩٦).

٦ ـ تشفير البيانات عند إرسالها عبر الشبكة لضمان عدم تحويرها أو الاطلاع عليها أو العبث بها.

٧ ـ استخدام كلمات المرور، والبطاقات الممغنطة، لتحديد صلاحية الاستخدام.

٨ ـ اتخاذ إجراءات مراقبة الشبكة بعد تشغيلها، والإشراف عليها من قبل إداريين وفنيين، بهدف اكتشاف مشاكلها وتحسين خدماتها باستمرار (الحميد ونينو، ٢٠٠٧م، ص ١٥٣-١٥٤).

٩ ـ استخدام أجهزة الليرز عند نقل المعلومات والبيانات للشبكات الداخلية والخارجية عبر الغلاف الجوي لتحسين نظام تأمين الشبكة (برينتون وهنت، ٢٠٠٣م، ص١٢٦).

١٠ ـ استخدام الكاشفات البيولوجية التي تحدد حدود وصلاحية الاستخدام من خلال تعريف المستخدم نفسه للنظام عن طريق الكاشفات البيولوجية المتصلة بالحاسب الآلي(Ashbourn, 2000: pp. 46-47)، للكشف عن: بصمة الأصبع، أو بصمة راحة اليد، أو شكل الوجه، أو تمييز شبكية العين، أو تمييز قزحية العين، أو

بصمة الصوت، ومن ثم لا يفتح النظام إلا عند التأكد من صلاحية المستخدم، كما أنه لا يمنحه سوى حدود معينة للاستخدام (Nana-vati, et. al., 2002: p. 102).

يتضح مما سبق تزايد الحاجة إلى أمن المعلومات في ضوء تزايد الحاجة إلى المعلومات، في ظل العصر الراهن الذي يطلق عليه عصر المعلوماتية، وفي ظل تزايد جرائم المعلوماتية نتيجة اكتساب غالبية الأفراد لمهارة استخدام الحاسب الآلي، فقد أصبحت الأمية معياراً يعبر عن عدم القدرة على استخدام الحاسب الآلي، فمن يمتلك المعلومة يمتلك القوة، وهذا يتطلب توفير الحماية المادية وغير المادية لتقنية المعلومات، بهدف تأمين المعلومات وحمايتها من التهديدات المختلفة التي لا تقتصر على السرقة والإتلاف والتدمير، بل واستغلال تلك المعلومات في تحقيق ميزات اقتصادية وسياسية وأمنية، لذلك تزداد أهمية أمن المعلومات في المنظمات الأمنية والعسكرية التي تحتاج لوسائل حماية فعالة لضمان أمن المعلومات، لعدم استغلال قدرة المستخدمين على الاختراق في الحصول على معلومات أمنية، أو تزوير المحررات والوثائق الرسمية باستخدام التوقيع الإلكتروني المزور أو تزوير البيانات الإلكترونية والحصول على محررات إلكترونية مزورة.

سادساً: المجرم الإلكتروني

الإجرام يعني الخروج عن قواعد الضبط الاجتماعي التي تحدد العلاقات والحقوق والواجبات السارية في المجتمع، ومن ثم فالمجرم المعلوماتي هو من يخرج عن هذه القواعد من خلال انتهاك حقوق الآخرين ومنح نفسه حق التعدي على معلوماتهم وأموالهم وخصوصياتهم من خلال اختراق نظم معلوماتهم، ومحاولة استغلال تعاملاتهم لصالحه، ومن ثم لم تعد

الجريمة المعلوماتية تقتصر على سرقة المعلومات والبيانات والتعدي عليها، بل اكتسبت منحى آخر كالتزوير الإلكتروني بعد استخدام تقنية المعلومات في التجارة الإلكترونية والحكومة الإلكترونية والإدارة الإلكترونية، ومن هنا وفي ظل تفعيل الخدمات الإلكترونية، ظهرت جرائم أخرى كالنصب والتحايل والتزوير التي يرتكبها المجرم المعلوماتي الذي لم يعد إجرامه يقتصر على سرقة المعلومات والبيانات بل تعدى إلى سرقة الأموال وتحويلها لحسابه الخاص، أو الشراء عن طريق استخدام أرقام بطاقات الائتمان الخاصة بالآخرين وأرقامهم السرية، وكذلك التوقيع الإلكتروني على معاملات الآخرين واستقدام عمالة أو توجيه معاملات وطلبات بأسماء آخرين دون علمهم، مما يعرضهم لعقوبات في حالة وقوع مخالفات هم أصلاً لا يعلمون عنها شيئاً، ولكنهم يتحملون مسؤولية عدم تأمين نظم معلوماتهم بالدرجة الكافية التي تقيهم من محاولات الاختراق والتعدي، فالمجرم المعلوماتي لا ينتج عن إجرامه خسائر مادية ومعنوية لمن يخترق نظم معلوماتهم، بل قد يترتب على ذلك الاختراق مشكلات أخرى خطيرة نتيجة إمكانية التعامل مع جهات مشبوهة وغسل الأموال أو تجارة السلاح، أو إيواء الإرهابيين أو استقدام جماعات وعصابات الإجرام المنظم وغيرها من الأفعال، كما أن انتشار الجرائم الإلكترونية قد يمنح من يرتكبون هذه الأفعال التذرع بالاختراق والتزوير للتوقيع الإلكتروني كوسيلة للهروب من المساءلة القانونية.

١ ـ صفات المجرم المعلوماتي

يختلف المجرم المعلوماتي عن المجرم التقليدي في إلمامه التام بوسائل وتقنيات الاتصال والمعلومات، من خلال إتقان التعامل مع الحاسب الآلي، بغض النظر عن تمكنه من صيانة نظم الحاسب الآلي، ولكن لابد من توافر قدر

مـن المهارة التي تمكنه من القيام بعمليات الاختراق غير المشروعة، والتنصت على المعلومات عبر انتقالها خلال الشبكة، أو نسخ المعلومات الخاصة بأجهزة الحاسب الآلي عبر الإشعاع المنبعث من الحاسب، لكي لا تعوقه عملية تشفير المعلومـات أو برامج الحماية من الاختراق، وسـواء حـاول المجرم المعلوماتي الاخـتراق بالطرق التقليدية أو اسـتخدام التقنيات الحديثة في الاسـتيلاء على المعلومات والبيانات، فإن من أهم صفاته التي تؤهله للقيام بعمله على الوجه الأكمل قوة العلاقات الإنسانية، والاحترافية والذكاء، والمثابرة.

٢ ـ قوة العلاقات الإنسانية

العلاقـات الإنسـانية عبارة عـن: «نوع مـن علاقات العمـل الذي يهتم بالجوانب الإنسـانية والاجتماعية في المنظمة. وهي بذلك تسـتهدف الوصول بالعاملـين إلى أفضـل إنتـاج في ظـل أفضـل ما يمكـن أن يؤثر عـلى الفرد من عوامـل نفسـية ومعنوية، باعتباره إنسـاناً وجدانيـاً وانفعالياً أكثر منه رشـيداً ومنطقيـاً» (النمـر وآخـرون، ٢٠٠٦م، ص٦٣). وهي ميـدان الإدارة الذي يهدف إلى تحقيق التكامل بين الأفراد في محيط العمل بشكل يدفعهم ويحفزهم إلى الإنتاجيـة والتعـاون وفي الوقت ذاته إشـباع حاجاتهم الطبيعية والنفسـية والاجتماعيـة (الشـنواني، ١٩٩٩م: ٤٩٧). والعلاقـات الإنسـانية تعـبر عن طرق تفاعـل الناس مع بعضهم البعض والتي تتحدد وفقـاً للثقافة التنظيمية والممارسـات الإدارية والقوى العامة الأخرى (راتشـمان وآخرون، ٢٠٠١م: ٢٤٩).

ولذلك يسـعى المجـرم المعلومـاتي إلى تدعيم علاقاته الإنسـانية، حيث عمله وسـط المجتمع، فهو إنسـان اجتماعـي بطبعه، وتطبيقـاً لذلك ترتكب كثـير مـن جرائـم المعلوماتية بدافـع الكبريـاء، أو للرد على تعرضـه للفصل

من العمل أو الاستغناء عن خدماته، أو بدافع النصب أو الحسد أو بدافع اللهو، أو لإظهار ما يتمتع به من مهارات تبرز تفوقه في مواجهة أنظمة أمن المعلومات، أو لمجرد الحصول على منفعة مالية (العريان، ٢٠٠٤م، ص٦٢).

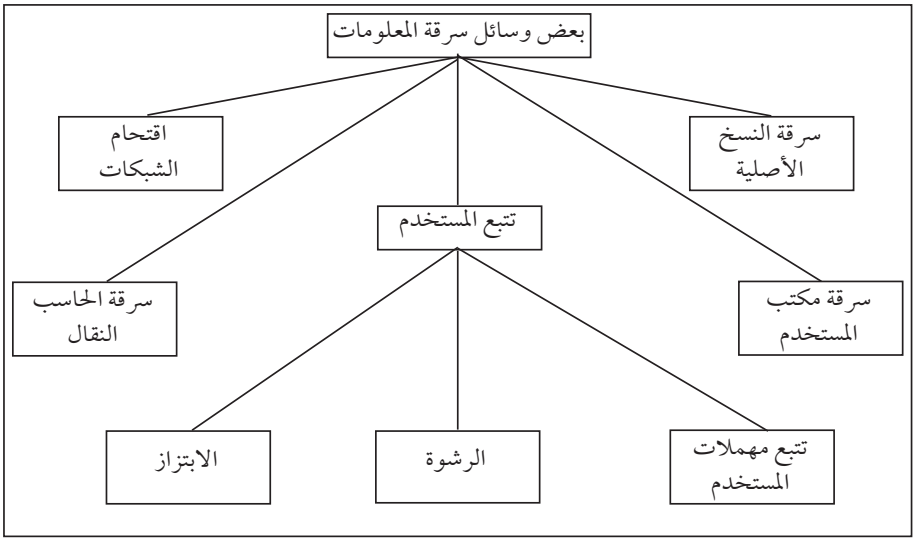
٣ ـ الاحترافية والذكاء

لا يحتاج المجرم المعلوماتي إلى قوة العضلات، بل يحتاج إلى قوة العقل والذكاء والاحترافية في عمله، من خلال إتقان مهارات استخدام الحاسب الآلي وتقنيات الاتصال، والقيام بعمليات الاختراق، والتنصت على حزم المعلومات أثناء مرورها عبر الشبكة وإمكانية فك رموز الشفرات، وغيرها من الأعمال التي يرتكبها المجرم المعلوماتي بسهولة. وبالرغم من قسوة الآثار المترتبة على التعدي والاختراق والقيام بعمليات النصب والتزوير الإلكتروني والسرقة، إلا أن الإجرام المعلوماتي ينشأ من تقنيات التدمير الناعمة التي تساعده على التلاعب ببيانات وبرامج الحاسب الآلي لمحو البيانات أو تعطيل استخدام البرامج (العريان، ٢٠٠٤م، ص٦٢) من خلال عدة وسائل تتضمن الاختراق، وفك الشفرات، واستقبال الأشعة الكهرومغناطيسية المنبعثة من الحاسب الآلي.

٤ـ الاختراق

هي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات، أو تخريبها، أو سرقتها (الحمدان والقاسم، ٢٠٠٤م، ص ٤٦-٤٨).

والشكل رقم (١) يوضح بعض وسائل سرقة المعلومات:



المصدر : (الحمدان والقاسم، ٢٠٠٤م، ص ص٤٦-٤٨).

الشكل رقم (١) بعض وسائل سرقة المعلومات

يفتقد الكثير من المنظمات والأفراد الوعي الأمني، ولا يتخذون أية إجراءات أمنية لحماية معلوماتهم، فلا توجد ميزانية مخصصة لأمن المعلومات، ولا يوجد إجراءات خاصة بكيفية التصرف عند حدوث الاختراق، ولا يوجد أية برامج تدريبية وقائية أو للتدريب على كيفية التصرف في حالة الاختراق (الشدي، ٢٠٠٠م، ص٢٧٤).

إن الهدف من الاختراق هو الحصول على معلومات خاصة عن المنظمة أو الفرد، فضلاً عن التعرف على خدمات الشبكة ومواطن الضعف في أجهزة الحاسب الآلي من خلال المنافذ أو بوابات عبور المعلومات الخاصة بالشبكة المحلية. أما أساليب الاختراق فتنحصر فيما يلي (الحمدان والقاسم،٢٠٠٤م، ص ٤٨-٥٠):

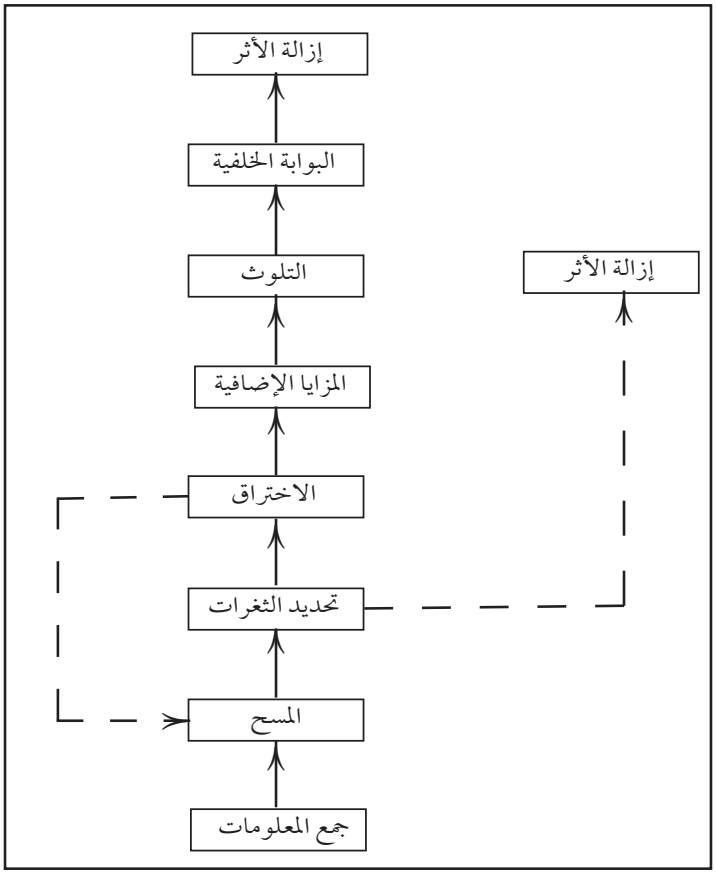
١ ـ يبدأ المخترقون بمحاولة السيطرة على جدران الحماية من خلال تحييد دور برامج الجدران النارية.

٢ ـ قد يقوم المخترقون بمهاجمة خادمات الملفات العامة للحصول على معلومات عن الشبكة بعد اختراق الخادم.

٣ ـ قد يسعى المخترقون للحصول على معلومات عن الشبكة باستخدام طرق غير هجومية، عن طريق الدخول كمستخدمين عاديين ـ إن كان لهم صلاحية ـ ثم يحاولون الحصول على معلومات تمكنهم من الوصول مباشرةً إلى شبكة المنشأة ومن ثم يتصل مباشرةً بالخادم، ويحصل على المعلومات التي يريدها، وتعد هذه الطريقة من أنجح وسائل الاختراق؛ لأنها لا تثير اشتباه مسؤولي أمن الشبكات، كما تسمح للمخترقين بالوصول إلى الشبكة والحصول على المعلومات التي يريدونها بأسرع وقت ممكن.

٤ ـ قد يحصل المخترق على معلومات خاصة عن شبكة المنشأة عن طريق الروابط المستخدمة من قبل مستخدمي الشبكة، فمن المعلوم أن تطبيقات الإنترنت تبين اسم الحاسب الخاص بدلاً من الاسم العام، وتستغل هذه المعلومة للحصول على معلومات أكثر عن الخادمات في الشبكة لاستخدامها في عملية الاختراق.

وللقيام بعملية الاختراق يجب البحث عن ثغرة في النظام على مستوى البروتوكولات أو نظم التشغيل أو التطبيقات أو حتى المستخدم نفسه، ثم القيام بالخطوات الموضحة في الشكل رقم (٢).



المصدر : (عبد الرحيم، ٢٠٠٧م، ص٦٨٢).

الشكل رقم (٢) خطوات الاختراق

ومن أهم الوسائل التي يستعين بها المجرم المعلوماتي لنجاح الاختراق

الفيروسات من أخطر المشكلات التي تهدد أمن المعلومات، لذلك يعد نشر فيروس جريمة من جرائم الحاسب يتعرض من قام بها للعقوبة إذا تم اكتشافه، فالفيروسات تهدف إلى السيطرة على الجهاز وتمكين المخترقين من الوصول للمعلومات بسهولة، أو تدمير الجهاز وإتلاف محتوياته وملفاته وبرامج تشغيله.

والفيروس عبارة عن برنامج حاسب مثل أي برنامج تطبيقي يتم تصميمه بواسطة أحد المبرمجين لتحقيق هدف معين، قد يكون إلحاق الضرر بنظام الحاسب، ولذلك تتم برمجته بحيث يكتسب القدرة على ربط نفسه بالبرامج الأخرى وإعادة إنشاء نفسه للانتشار بين برامج الحاسب المختلفة ومواقع الذاكرة بشكل يسمح له بتحقيق أهدافه التدميرية (الحميد ونينو، ٢٠٠٧م، ص١٥٩).

والفيروسات ذات هدف تخريبي تنتشر ذاتياً وبسهولة من حاسب لآخر، وتستطيع أن تصيب وتفسد الأجهزة والبرامج والشبكات المتصلة معها بشكل جزئي أو كلي.

وأهم أنواع الفيروسات:

ـ حصان طروادة

تختبىء هذه الفيروسات ضمن برامج يبدو مظهرها بريئاً، وعندما يشغل المستخدم أحد هذه البرامج ينشط الجزء الماكر ويقوم بممارسة عمله في السيطرة على الجهاز وإتلافه، من خلال جمع معلومات عن اسم المستخدم وكلمة السر، وإرسالها لصاحب الفيروس أثناء اتصال المستخدم بالشبكة، كما يسمح بتصفح الجهاز والتحكم بملفاته تحكماً كاملاً (الحميد ونينو، ٢٠٠٧م، ص١٦٠).

ـ الديدان

فيروسات تتميز بقدرة كبيرة على نسخ نفسها من وإلى الأقراص المرنة، أو عبر الشبكات، ويعتمد بعضها على بعض في إنجاز مهامها. وهي تنقسم إلى نوعين الأول الدودة المضيفة التي تستخدم الشبكة لنسخ نفسها على أجهزة

الحاسب الآلي المتصلة بالشبكة، والنوع الثاني الدودة الشبكية التي توزع أجزاءها على عدة أجهزة حاسب آلي وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن أن تظهر الدودة على أجهزة حواسيب منفصلة فتنسخ نفسها إلى أماكن متعددة على القرص الصلب. وأهم أضرار الديدان هي إبطاء سرعة عمل الشبكات (الحميد ونينو، ٢٠٠٧م، ص١٦٥).

ـ القنابل الموقوتة

برامج تتخفى بشكل معين ملتصقة بملف أو برسالة بريد إلكتروني، ويبدأ عملها أو نشاطها في وقت لاحق محدد بزمن أو حدث معين، وتحدث نفس الأثر التخريبي لأحصنة طروادة من حذف وتعديل للبيانات وتعطيل لنظم الحاسب الآلي (الحمدان والقاسم، ٢٠٠٤م، ص٩٣).

ـ فيروسات الشبكات

تنتشر عن طريق البريد الإلكتروني وخصوصاً من الرسائل التي تأتي لاحقاً.

ـ باب المصيدة

عبارة عن رمز يتم توزيعه عند تركيب باب الحماية، لكي يعطي المخرب حرية اختيار الوقت المناسب لعملية التخريب، حيث يسمح هذا الرمز بالنفاذ من خلال الشبكات في وجود نظم الحماية التي تعتاد على وجوده (الحميد ونينو، ٢٠٠٧م، ص١٦٦).

ـ فيروسات العتاد

تصمم لتصيب العتاد، حيث يبرمج الفيروس لتنفيذ ملايين العمليات الحسابية المتوالية دون استخدام أوامر للإخراج أو الإدخال، ومن ثم يلقي

عبئاً كبيراً على وحدة المعالجة المركزية، فيؤدي إلى ارتفاع درجة حرارتها واحتراقها (الحميد ونينو، ٢٠٠٧م، ص١٦٦).

ـ شبكة الشبح Goast Net

وهي عبارة عن شبكة كاملة لها قدرات عالية على اختراق المواقع في كافة الدول والأجهزة المحصنة، ولها القدرة على تحييد دور برامج الحماية، والقيام بعمليات الاختراق والتعدي والتزوير في زمن قياسي، وهي تمثل الجديد في عالم الاختراق؛ ويصعب الكشف عنها لأنها تمتاز بسرعة الاختفاء، وعدم إمكان رصدها وتحديد موقعها. وتدور الشبهات حالياً حول أربعة مواقع لها، ثلاث منها في الصين، والرابع في شمال كاليفورنيا. وقد تمكنت من اختراق القارات الأمريكية وأجهزة الـ FBI، وبعض البنوك في كل من سويسرا والهند وإيران (مؤنس محب الدين، ٢٠٠٦م).

١ ـ فك الشفرات

التشفير إحدى وسائل حفظ معلومات المنظمة عن طريق تغيير مظهرها لإخفاء معناها الحقيقي، باستخدام عدة طرق، فتظهر كلمات غامضة لا معنى لها، وطريق فك الشفرة هي عكس الإجراء الذي تم استخدامه في التشفير.

والتشفير هو عملية تحويل المعلومات إلى شفرات غير مفهومة وغير ذات معنى، لمنع الأشخاص غير المرخص لهم من فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة (القائفي، ٢٠٠٧م، ص١٥٠٣).

ومن أهم فوائد التشفير أنه يقي من التنصت على حزم المعلومات الخاصة بالأفراد والمنظمات أثناء انتقالها عبر الشبكة، والتنصت يعني نسخ حزم

المعلومـات عند انتقالها عبر الشـبكة، حيث يمكن من الناحيـة التقنية مراقبة أداء الشـبكة من خـلال حزم البيانات المتدفقة عبر الشـبكة؛ مما ييسر وصول المخترقين لهذه الحزم، ولكن يمكن منع التنصت باسـتخدام وسـائل التشفير المناسـبة؛ لأن عـدم معرفة الشـفرة معناه الحصـول على بيانـات ومعلومات مبهمة وغير مفهومة.

وبصفـة عامة ترتكز معظم نظم التشـفير القديمـة والحديثة على مبدأين رئيسين هما:

١ ـ مبدأ الاستبدال: استبدال حرف من أبجدية النص المقروء بحرف أو أكثر من أبجدية النص المشـفر حسـب قاعدة استبدال محددة تعرف بمفتاح التشفير.

٢ ـ مبدأ الإبدال أو القلب: تغير مواقع أو حروف النص المقروء حسب قاعـدة اسـتبدال محـددة تعرف بمفتاح التشـفير (المزيد والشـهري، ٢٠٠٧م، ص١٥٣٣).

ويعد التشفير وإخفاء المعلومات من الوسائل المهمة التي تستخدم لضمان تحقيق أهداف أمن المعلومات، وبالرغم من أن التشفير وإخفاء المعلومات لا يحل كل المشـكلات التي تعـترض أمن المعلومات؛ إلا أنه يسـتخدم للتغلب على عدد كبير من المهددات والأخطار الأمنية (محمد، ٢٠٠٧م، ص١٤٦٨).

ويتـم فك الشـفرات باسـتخدام أقراص مصممة لهـذا الغرض، ولديها القدرة على فك أية شفرة مهما بلغت صعوبتها، ومن ثم إمكانية الدخول على النظام والعبث به كيفما شاء المستخدم (الشدي، ٢٠٠٠م، ص٥٤).

٢ ـ استقبال الأشعة الكهرومغناطيسية المنبثعة من الحاسب

غالباً ما تنبعث موجات كهرومغناطيسية من الأجهزة وتقنية المعلومات، وقد أثبت العلم إمكان استغلال هذه الموجات التي تصدر في شكل إشعاعات من الأجهزة في سرقة محتويات الأجهزة من المعلومات والبيانات، حيث يمكن باستخدام جهاز الاستقبال والهوائي المناسب مع بعض الأجهزة المعاونة التقاط المعلومات التي يحتوي عليها أي جهاز حاسب آلي عن بعد من خلال الإشعاعات الكهرومغناطيسية المنبعثة من الجهاز (محمود، ٢٠٠٧م، ص١٣٣٢).

وتكمن الخطورة في أن المعلومات التي يتم سرقتها تكون غير مشفرة أو مخفاة، لأن الإشعاعات الصادرة تحمل المعلومات بنفس مواصفاتها الأصلية، ولا تمر خلال شبكة تقوم بتشفيرها من خلال برامج الحماية، مما يمكن من الحصول على المعلومات بوضوح (محمد، ٢٠٠٧م، ص١٤٧٧).

٣ ـ اللياقة البدنية والقوة الجسدية والمثابرة

يحتاج المجرم المعلوماتي إلى القدرة على التحمل، فقد يستغرق الأمر عدة ساعات لكي يقوم بعملية اختراق أو تحويل أو القيام بتوقيع إلكتروني، وذلك لنجاح عملية الاختراق وتفادي برامج الحماية. فالقوة الجسدية واللياقة البدنية العالية من السمات التي تساعد على رفع وتنمية مهارات المخترق، فتكرار محاولات الاختراق قد تستغرق وقتاً طويلاً يحتم تمتع المخترق بالمثابرة وكثرة المحاولات التي تحتاج إلى القوة البدنية واللياقة العالية (أبو شامة، ١٩٩٢م، ص٤١).

٢. ١. ٢ الجرائم التي ترتكب بواسطة الحاسب الآلي وصعوبة إثباتها

هناك العديد من الجرائم التي يتم ارتكابها عن طريق الحاسب الآلي، وهي تنقسم بصفة عامة إلى جرائم تقليدية، وجرائم تقنية، وجرائم دعم الأنشطة الإجرامية الأخرى، ونظراً لارتباط الجرائم التقنية بجرائم ذات صفة وطبيعة معينة، إلا أن ما يهمنا منها جرائم التزوير المعلوماتي (الإلكتروني)، حيث يمكن استخدام تقنيات وبرامج معينة للقيام بهذه الأعمال الإجرامية التي يصعب إثباتها في ضوء تعدد المستخدمين وصعوبة تتبع الدليل الرقمي. وتهتم الدراسة الحالية بجريمة التزوير الإلكتروني والأساليب المستخدمة في إثباتها.

أولاً: الجرائم التي ترتكب بواسطة الحاسب الآلي

تتنوع الجرائم التي ترتكب باستخدام الحاسب الآلي، وبالرغم من توافر إحصاءات عديدة توضح تركيز غالبية الجرائم المعلوماتية على جرائم المال والتلاعب في الحسابات وغسل الأموال والجرائم الأخلاقية، إلا أن هناك مؤشرات تؤكد استخدام الحاسب الآلي في جرائم سياسية وعسكرية وجرائم الإرهاب والقرصنة التي تكلف خسائر مادية ومعنوية باهظة، فضلاً عن ارتفاع معدلاتها يوماً بعد يوم بسبب التطور المستمر في مجال تقنية الحاسبات الآلية وابتكاراتها المتسارعة، الذي يقابله تطور في أساليب ووسائل وأدوات الاختراق والتعدي، خاصةً بعد انتشار ثقافة الحاسب الآلي وتعميم استخدامه، مما يترتب عليه تضاعف إساءة استخدام الحاسب الآلي في مجالات مختلفة، وزيادة أعداد جرائم الاحتيال والتزوير والنصب المعلوماتي بغرض تحقيق الكسب غير المشروع (البشرى، ٢٠٠٠م، ص ٣١٨-٣١٩).

١ ـ التزوير الإلكتروني

أ ـ مفهوم التزوير الإلكتروني

التزوير هو تغيير الحقيقة في محرر بإحدى الطرق التي وضحها القانون تغييراً من شأنه أن يسبب ضرراً (العريان، ٢٠٠٤م، ص١٣٧).

والتزوير هو تغيير الحقيقة في بيانات محرر ما، بإحدى الطرق المحددة نظاماً، مع ترتيب ضرر للغير، ومع توافر نية استعمال المحرر للحصول على منفعة أو قضاء مصلحة من أجلها تمت عملية التزوير (خضر، ١٩٨٨م، ص٢٥).

والتزوير الإلكتروني يختلف عن التزوير التقليدي؛ حيث يتضمن التزوير المعلوماتي إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو الإضافة، بالإضافة إلى أنه قد يتعلق بالكيان المادي للحاسب الآلي، أو البرامج ذاتها، وهو يندرج بصفة عامة تحت نطاق التزوير الإلكتروني كسلوك غير مشروع يتعلق بمعالجة المعلومات ونقلها، فهو سلوك غير قانوني وغير مسموح به يتعلق بالتعامل الفوري مع المعلومات والبيانات أو انتقالها (الهيتي، ٢٠٠٥م، ص٧٦).

والتزوير يتضمن نسخ الأقراص المدمجة على أقراص أخرى، وتغيير البيانات والمعلومات واستخدامها كوسيلة للتدليس، سواء تم استخدامها في ارتكاب عمل إجرامي أو لا، لأن تغيير الحقيقة في المحررات أو تغيير التوقيعات والصور من قبيل التزوير (النجيمي، ٢٠٠٧م، ص١١).

وتزوير البيانات يكون بالدخول بطريقة مشروعة أو غير مشروعة على قاعدة البيانات الموجودة في نظم المعلومات وتعديل البيانات سواء بإلغاء

بيانـات موجـودة بالفعـل، أو بإضافـة بيانات لم تكـن موجودة مـن قبل، مما يضع عراقيل أمام تنفيذ مشـاريع التجارة الإلكترونيـة والإدارة الإلكترونية نتيجـة إمكانيـة تزوير البيانـات وصعوبة القبض على مرتكبيهـا أو تحديدها، وإن تـم تحديـد الموقع المسـتخدم في عمليات التزوير، فمـن الصعوبة بمكان تحديد مسـتخدم الموقع، خاصةً إذا كان الموقع المستخدم مكاناً عاماً أو مقهى إنترنت، أو فندقاً، في ضوء تعدد المستخدمين وصعوبة تحديد الجاني (الجنبيهي والجنبيهي، ٢٠٠٥م، ص٩٠ـ٩١).

وهنـاك العديـد مـن الأمثلـة التـي تشـير إلى خطـورة جريمـة التزويـر الإلكتروني سواء في البيانات أو المحررات، فعلى سبيل المثال اكتشف موظف الميقات المسؤول عن إدخال بيانات ساعات العمل الإضافي لـ ٣٠٠ موظف في إحـدى المحلات التجارية أن جميع السـاعات الإضافية للموظفين تدخل في برنامـج حفـظ الوقت ودفتر الدفعيات باسـم الموظفـين وأرقامهم. وكان الحاسب الآلي معداً لاستخدام رقم الموظف فقط للتعرف على اسمه وعنوانه وطباعة شـيكات الدفعات، كما لاحظ أيضـاً أن المراجعة الخارجية مبنية على اسـم الموظف فقط، ولا يقـوم أحد بمراجعة حقوق الأشـخاص بأرقامهم، ومن ثمَّ انتهز هذه الفرصة في اسـتخدام أسماء الموظفين الأكثر عملاً إضافياً، وأدخـل رقمه الخاص بحيث يضاف أجر السـاعات الإضافية التي يعملونها لصالحه، ولكن تم اكتشـاف الأمر عندما كشـفت مراجعـة الضرائب ارتفاع دخله، فاعترف لها بجريمته (البشرى، ٢٠٠٠م، ص٣١٧).

ب ـ طرق التزوير

يتخذ التزوير الإلكتروني طرقاً متعددة من أهمها:

ـ وضع توقيعات أو أختام أو بصمات مزورة

التوقيعات المزورة تتم عن طريق محاكاة التوقيع الأصلي، أو رسمه، أو تصويره أو طباعته على المحرر (وقيع الله، ٢٠٠٣م، ص٥٩)، أما وضع الختم المزور فهو استخدام الختم الأصلي للشخص بسرقته واستخدامه في ختم المحرر، أو تقليد الختم واصطناع آخر مماثل له، والتزوير يقوم نتيجة عدم علم أو انصراف إرادة صاحب الختم الحقيقي إلى ختم المحرر، وتأخذ البصمة المزورة حكم التوقيع (حجازي، ٢٠٠٥م، ص١٨٢).

ويرى الباحث أن البصمة لا تكون مزورة ولكن تكون غير صحيحة إذا أخذت بطريق التحايل، كأن يتم إجبار الشخص على وضع بصمته رغماً عنه، أو إذا تم استخدام بصمته بعد وفاته مباشرةً، أو إذا تم عمل بصمات جيلاتينية مطابقة لبصمته واستخدامها على المحررات.

والتزوير الإلكتروني يعتمد على التلاعب في المعلومات، فالمعلومات ذات قيمة في ترتيب حق معين أو أثر قانوني معين، فمن السهل تزوير مخرجات الحاسب المتضمن هذه المعلومات، سواء كانت تمثل أثراً إدارياً أو قانونياً، ومن السهل إدخال صورة توقيع أي شخص أو بصمته أو صورة ختمه عن طريق الماسح الضوئي إلى جهاز الحاسب الآلي، مع إضافة التوقيع إلى المحرر الذي يحتوي على البيانات المزورة، وهنا تتحقق أركان جريمة التزوير بعد كتابة بيانات وتوقيعها أو ختمها أو طبع البصمة الشخصية عليها دون انصراف إرادة صاحبها، أي نسبتها إليه دون علمه، فالتقنية الحديثة مكنت من الحصول على مستند صحيح من الناحية الشكلية، ولكنه مزور نتيجةً بسبب نسبته إلى شخص آخر بعد أن حمل توقيعه أو بصمته أو ختمه بغير إرادته أو علمه (حجازي، ٢٠٠٥م، ص ١٨٣-١٨٤).

ويتم تزوير التوقيع الإلكتروني بطريقة مختلفة تماماً، فالتوقيع الإلكتروني المزور مطابق تماماً للتوقيع الأصلي، ولكن يتم التزوير من خلال سرقة منظومة التوقيع الإلكتروني من خلال التجسس الإلكتروني والتلصص، ومن ثم الحصول على التوقيع الإلكتروني وتوقيع الأوراق والمحررات به، فالتوقيع الإلكتروني توقيع سليم إذا تمت مضاهاته، ولكنه ليس صادراً من مالك منظومة التوقيع الإلكتروني، أي أنه صادر عن شخص آخر تمكن من سرقة منظومة التوقيع الإلكتروني للمالك الأصلي (الجنيبهي والجنيبهي، ٢٠٠٥م، ص١١٥).

ـ تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات

هو إدخال تغيير مادي على صلب المحرر أو التوقيع أو الختم، بهدف إحداث تعديل في معناه، ويتضمن ذلك أيضاً زيادة كلمات على المحرر، ويقصد بالزيادة هنا ما يحدث بعد اكتمال المحرر والتوقيع عليه (عبد الستار، ١٩٨٨م، ص٢٦١).

أما التزوير الإلكتروني فهو أبسط وأسهل بكثير من التزوير في المحررات العادية، لأنه لا يحتاج إلى إزالة باستخدام الأدوات والمواد الكيميائية لتغيير معاني الكلمات أو كشط توقيعات سابقة، ولكنه يحتاج فقط إلى إدخال كلمات أو تغيير معاني كلمات بالحذف أو الإضافة أو التعديل عليها، وبذلك يصدر المحرر النهائي مطابقاً للأصل وإن كان مزوراً في مضمونه (حجازي، ٢٠٠٥م، ص ١٨٨-١٨٩).

ـ وضع أسماء أو صور أشخاص آخرين مزورة

يتحقق التزوير المادي عندما يقوم الجاني بانتحال أو إبدال شخصيته بشخصية الغير سواء بتغيير الاسم أو الصورة، وتتضمن الأفعال المادية

التوقيع باسم من انتحل شخصيته، والإدلاء بأقوال ينسبها إلى الشخص في المحرر المدون (حسني، ١٩٨٢م، ص٢٣٦).

وباعتبار الصورة أحد البيانات الجوهرية في الوثيقة المعلوماتية، فمن السهولة تزويرها باستخدام الحاسب سواء عن طريق الانتحال أو الاستبدال باستخدام الماسح الضوئي، حيث توجد برامج متخصصة بتركيب الصور، وبذلك يمكن تزوير الصورة بسهولة باستخدام الحاسب الآلي والأجهزة المساعدة كالماسح الضوئي عن طريق رسم الصورة ضوئياً ونقلها إلى الحاسب الآلي واستخراجها ورقياً عن طريق الطابعة، أو إدخالها على بيانات مخزنة في ذاكرة الحاسب الآلي، وعرضها على الشاشة دون طباعة ورقية (الصغير، ١٩٩٩م، ص٤٤).

ـ التقليد

التقليد هو إنشاء محرر مماثل لمحرر أصلي، أو أن يقوم المتهم بتحرير مكتوب مشابه خط شخص آخر لنسبته إليه (حسني، ١٩٨٢م: ٢٣٨). وقد يسر استخدام الحاسب الآلي والماسح الضوئي من جرائم التقليد بشكل كبير، حيث يتم استخراج محرر طبق الأصل، ولا يشترط في التقليد أن يبلغ حد الإتقان، ولكن يكفي محاكاة المحررات بحيث ينخدع به الناس إلى حد إيهامهم بصحة المحرر (حجازي، ٢٠٠٥م، ص١٩٧).

ويشير جانب كبير من الفقه بوقوع جريمة التزوير عن طريق التقليد والمحاكاة للمحرر الأصلي للحصول على نسخة طبق الأصل باستخدام الحاسب الآلي والماسح الضوئي، بينما يشير البعض بعدم وقوع التزوير إلا في حالة توقيع المحرر أو وضع بصمة مقلدة عليه، أو ختم مزور منسوب إلى الضحية (حسني، ١٩٨٢م، ص٢٣٩).

ـ الاصطناع

الاصطناع هو إيجاد محرر بأكمله ونسبته إلى غير محرره، بمعنى إنشاء محرر على غرار أصل موجود مسبقاً، والاصطناع يختلف عن التقليد في عدم اهتمام الجانب بالتشابه في الخط، ولكن الغرض منه الإيحاء بأن كاتب المحرر شخص معين، أي استخدام أسلوبه وطريقته في الكتابة، وغالباً ما يتم التوقيع على المحرر المصطنع بتقليد مزور كي يستمد قيمته القانونية من هذا التزوير (عبد الستار، ١٩٨٨م، ص٢٦٥).

وبصفة عامة هناك صورتان للاصطناع إحداهما أن يوجد المتهم محرراً لم يكن موجوداً من قبل، أو يوجد محرر آخر وذلك بعد التعديل من شروط أو بدون تعديل منها (حسني، ١٩٨٢م، ص٢٤).

والاصطناع المعلوماتي يتم من خلال إدخال المصطنع ما يريد من معلومات أو بيانات إلى الحاسب الآلي، ومن ثمَّ ينسب صدورها إلى شخص ما أو جهة ما، ثم يستخرجها من الحاسب الآلي بوصفها منسوبة إلى ذلك الشخص أو تلك الجهة، ولذلك يعد تزييف العملة الورقية باستخدام الماسح الضوئي والحاسب الآلي من طرق الاصطناع كما هي من طرق التقليد؛ لأن الاصطناع هو إيجاد محرر بأكمله ونسبته إلى غيره، ولا توجد صعوبة في إدخال عناصر المحرر المراد تزويره إلى جهاز الحاسب الآلي سواء عن طريق الماسح الضوئي، أو عن طريق لوحة المفاتيح، بل وعن طريق استدعاء المعلومات من الإنترنت، ثم صياغته في هيئة المحرر المزور الذي يطلبه الجاني، ويطبعه ويستخدمه حسب رغبته (حجازي، ٢٠٠٥م، ص٢٠٢).

ـ بطاقات الائتمان المزورة

يتم تزوير بطاقات الائتمان من خلال تشكيل أرقام بطاقات خاصة ببنك معين من خلال تزويد الحاسب بالرقم الخاص للبنك مصدر البطاقة

عن طريق برامج تشغيل خاصة، ومن ثم استخدام البطاقة المزورة (التي لها مستخدم أصلي) والقيام بجميع العمليات بها، مما قد يترتب عليه تعرض بعض أصحاب البطاقات الأصلية لمشكلات نتيجة استخدام بطاقاتهم أو البطاقات المطابقة لبطاقاتهم في أعمال البيع والشراء، وقد اكتشفت بعض البنوك تكرار اعتراض بعض حاملي بطاقات الدفع الإلكتروني على عمليات لم يقوموا بإجرائها، وتبين للبنك أن هذه العمليات تم إجراؤها عن طريق الإنترنت من قبل بعض قراصنة الحاسب الآلي الذين يمتلكون تقنيات يستطيعون بها الحصول على أرقام البطاقات الخاصة بالعملاء والشراء بواسطتها (الصغير، ١٩٩٩م، ص٣٦).

وتندرج عملية استخدام بيانات بطاقة دفع إلكتروني خاصة بالغير تحت جريمة الاحتيال نتيجة انتحال اسم كاذب وصفة غير حقيقية للحصول على منفعة مادية (الشوابكة، ٢٠٠٦م، ص٢٠٢).

وأهم وسائل مكافحة تزوير بطاقات الائتمان هي (باتوباره، ١٩٩٨م، ص٢١١-٢١٤):

١ـ استخدام تقنية البطاقة الذكية لإنجاز المعاملات الدائنة والمدينة بشكل أكثر أماناً، وأقدر على مواجهة احتمالات التزوير، حيث أسهمت هذه البطاقة في انخفاض حوادث التزوير بنسبة (٥٠٪)، فضلاً عن تفوقها على البطاقات العادية في استيعابها لحوالي (١٦) كيلو بايت مقارنة بحوالي (٢٠٠) بايت للبطاقة التقليدية، ولذلك يمكن أن تستخدم البطاقة الذكية في تخزين برامج التعرف على الفرد من خلال السمات البيولوجية، ولذلك لا يتم إدخال الرقم السري (الذي يمكن معرفته وفك شفرته في حالة البطاقات العادية)، بل

يتم استخدام بصمة اليد، أو بصمة الكف، أو بصمة قزحية العين، كوسيلة للتأكد من هوية حامل البطاقة.

٢ ـ إعادة النظر في مستويات الصرف: يجب إعادة النظر في مستويات الصرف وجعلها بحدود دنيا تتطلب اعتماد الصرف من قبل مصدر البطاقة، مما يجعل المزورين لا يستطيعون الشراء إلا في حدود معينة وبمبالغ قليلة لكي لا يتم اكتشافهم، وقد تم تطبيق هذه الاستراتيجية في بريطانيا وأدت إلى انخفاض نسبة الحوادث بمعدل (٠,٢٠٪)، وانخفاض خسائر القطاعات التي استهدفتها بنسبة (٠,٧٥٪).

٣ ـ تثقيف العملاء: ينبغي تبصير حامل البطاقة بأهمية المحافظة عليها، وعدم الإدلاء ببياناتها للمواقع المشبوهة.

٤ ـ تطوير تقنية أجهزة الصرف الآلي وأجهزة نقاط البيع لزيادة قدرتها على اكتشاف وتشخيص البطاقات المزورة، وتمييزها عن البطاقات الأصلية.

٥ ـ جمع المعلومات عن حوادث التزوير، لتكوين صورة شاملة عن أساليب التزوير، ووضع أساليب العلاج المناسبة.

٦ ـ سن القوانين الرادعة لمزوري البطاقات.

٧ ـ تدريب موظفي البنوك والمتاجر على أساليب اكتشاف بطاقات الائتمان المزورة.

جـ ـ أركان جريمة التزوير الإلكتروني

لقيام جريمة التزوير الإلكتروني يجب توافر ركنين هما الركن المادي والركن المعنوي الذي يتضمن القصد الجنائي العام والقصد الجنائي الخاص.

ـ الركن المادي

يتضمـن الركن المادي النشـاطات الماديـة للتزوير والتـي تتضمن تغيير الحقيقة،والتزوير في محرر معلوماتي إلكتروني وطرق (أنواع) التزوير والضرر.

ـ تغيير الحقيقة

التزويـر عبـارة عن تغيـير الحقيقة، فـإذا كان المحرر لا يشـتمل على أمر كاذب، بـل كان يتضمـن أمـوراً حقيقيـة، فـلا تزويـر ولا عقـاب، حتى إن كان الغـرض من تحريـره تغيير الحقيقة والإضرار بالغير (حسـني، ١٩٨٢م، ص٢١٨). والهدف من تغيير الحقيقة إنشـاء حقيقة مخالفة، أو تحريف حقيقة قائمـة، فجوهـر تغيـير الحقيقة هو الزيـف والكذب، وعلى ذلـك لا يرتكب تزويـراً مـن يدلي أمـام الموظـف المختص ببيانـات يعتقد أنها غـير صحيحة، فيدونهـا الموظف في المحرر، ثم يتضح أنها صحيحة، أو يقلد توقيع شـخص بناء على إذن شفهـي بتقليد توقيعه (العريان، ٢٠٠٤م، ص١٣٨).

ولابـد أن يتـم تغيـير الحقيقة في المحرر بشـكل واضح لا يقبل الشـك، بمعنى تغيير الحقيقة القانونية النسـبية وليس تغيـير الحقيقة الواقعية المطلقة، فجريمـة التزوير تقع إذا ثبت انعدام إرادة الشـخص كأن يكون قد وقع على المحرر تحت التهديد، أو بالإكراه (خضر، ١٩٨٨م، ص٣١).

ـ المحرر المعلوماتي

يجـب أن يكـون التزويـر للحقيقـة قد وقع في محـرر مكتـوب، أي محرر موجـود من الأصل، ولا يهم اللغة التي كتب بها المحرر سـواء كانت العربية أو أيـة لغة أجنبية، ولذلك لا يعد تزويـراً تزوير الحقيقة الذي يقع دون كتابة بقول أو فعل. وفي جرائم المعلوماتية فإن البيانات المخزنة آلياً سواء في ذاكرة

الحاسب أو أسطوانات ممغنطة أو أشرطة أو برامج غير مقروءة، ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق البصر أو المشاهدة؛ لأنها تسجل على هيئة نبضات إلكترونية مثبتة على دعامة بشكل يسمح للحاسب فقط بقراءتها، مما استدعى إدخال تعديلات على التشريعات، ففي فرنسا أدخل المنظم الفرنسي التزوير الذي يقع في المستندات المعالجة آلياً في نطاق التجريم بموجب المادة ٤٦٢/ ٥ من القانون رقم ١٩ لسنة ١٩٨٨م بشأن تجريم التزوير في المحررات المبرمجة والتي تنص على: «كل من زور وثائق مبرمجة أياً كان شكلها، إذا سبب ذلك ضرراً للغير يعاقب بالحبس...»، وكذلك القانون الفرنسي الصادر وفقاً لتوجيهات المؤتمر الأوروبي والذي ينص على: «يعاقب بالحبس... كل من قام بتزوير مستندات معالجة آلياً أياً كان شكلها، إذا سبب ذلك ضرراً للغير» ويشير تعبير المستند آلياً إلى المستند المعلوماتي (العريان، ٢٠٠٤م، ص١٤٠).

وقد استحدث التشريع الألماني المادة (٢٦٩) من قانون العقوبات الألماني التي تشير إلى تجريم التزوير في المحررات المعلوماتية وفرض عقوبة السجن على « «كل من باشر بغرض التحايل على الروابط القانونية: ١) التخزين (الإلكتروني أو المغناطيسي غير المشروع أو بأية وسيلة أخرى غير مرئية أو غير مقروءة مباشرةً) لبيانات متخصصة لكي تستعمل كوسائل لإثبات وقائع قانونية مناسبة الصلة. ٢) أو التعديل غير المشروع لهذه البيانات المختزنة سواء بوسيلة قانونية أو غير قانونية. ٣) أو استعمل البيانات المختزنة...» (العريان، ٢٠٠٤م، ص١٤١).

أما التشريع البريطاني الصادر في ٢٨/ ١١/ ١٩٨١م فقد أفرد تشريعاً خاصاً بالتزوير في المحررات وتقليدها، وعرف السند القابل للتزوير بأنه كل

أسطوانة أو شريط ممغنط أو شريط صوتي أو أي جهاز آخر سجل فيه أو عليه معلومات أو حفظت بوسائل ميكانيكية أو إلكترونية أو بوسائل أخرى (العريان، ٢٠٠٤م، ص١٤٢).

وكذلك عالج المنظم السعودي ذلك في الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير الصادر بناء على تعميم وزير العدل رقم ١٣/ ت/ ٢٧٠٥ في ٢٤/ ٧/ ١٤٢٦هـ والمرسوم الملكي رقم م/ ١٦ في ٨/ ٧/ ١٤٢٦هـ وقرار مجلس الوزراء رقم ١٦٧ في ٣/ ٧/ ١٤٢٦هـ المتضمن إضافة مادتين إلى نظام مكافحة التزوير الصادر بالمرسوم الملكي رقم (١١٤) في ٢٦/ ١١/ ١٣٨٠هـ، والتي نصت على ما يلي: «كل من زور الصور الضوئية أو المستندات المعالجة آلياً أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو أسطوانة ممغنطة أو غيرها من وسائط، أو استعملها وهو عالم بتزويرها يعاقب بالعقوبات الواردة في هذا النظام».

ـ أنواع التزوير

هناك نوعان من التزوير: الأول مادي، والثاني معنوي، فالتزوير المادي يقع بخمسة طرق هي:

أ ـ وضع إمضاءات أو أختام مزورة.

ب ـ تغيير المحررات أو الأختام أو الإمضاءات أو زيادة الكلمات.

جـ ـ وضع أسماء أو صور أو أشخاص آخرين مزورة.

د ـ التقليد.

هـ ـ الاصطناع (العريان، ٢٠٠٤م، ص ١٤١-١٤٢).

وقد عالجت الصور السابقة المواد السادسة والتاسعة والعاشرة من نظام مكافحة التزوير السعودي الصادر بالمرسوم الملكي رقم (١١٤) في

٢٦/ ١١/ ١٣٨٠هـ، حيث نصت المادة السادسة على ما يلي: «يعاقب الأشخاص العاديون الذين يرتكبون الجرائم المنصوص عليها في المادة السابقة أو الذين يستعملون الوثائق والأوراق المزورة والأوراق المنصوص عليها في المادة السابقة على علم من حقيقتها بالعقوبات المنصوص عليها في المادة المذكورة، وبغرامة مالية من ألف إلى عشرة آلاف ريال»، ونصت المادة التاسعة على ما يلي: «من انتحل اسم أو توقيع أحد الأشخاص المذكورين في المادة السابقة لتزوير الوثيقة المصدقة أو حرف أو زور في وثيقة رسمية أو في حفيظة نفوس أو جواز سفر أو رخصة إقامة أو تأشيرة من التأشيرات الرسمية للدخول أو المرور أو الإقامة أو الخروج من المملكة العربية السعودية عوقب بالسجن من ستة أشهر إلى سنتين وبالغرامة من مائة إلى ألف ريال»، بينما نصت المادة العاشرة على ما يلي: «من زور أو قلد توقيعاً أو خاتماً لشخص آخر أو حرف، بطريق الحك أو الشطب أو التغيير، سنداً أو أي وثيقة خاصة عوقت بالسجن من سنة إلى ثلاث سنوات».

أما التزوير المعنوي فيتضمن تغيير إقرارات ذوي الشأن، أو جعل واقعة مزورة في صورة واقعة صحيحة، أو جعل واقعة غير معترف بها في صورة واقعة معترف بها (العريان، ٢٠٠٤م، ص١٤٢)، وقد عرض لها نظام مكافحة التزوير في المملكة العربية السعودية في المادة رقم (٥) التي نصت على ما يلي: «كل موظف ارتكب أثناء وظيفته تزويراً بصنع صك أو أي مخطوط لا أصل له أو محرف عن الأصل عن قصد أو بتوقيعه إمضاءً أو خاتماً أو بصمة إصبع أو أتلف صكاً رسمياً أو أوراقاً لها قوة الإثبات سواء كان الإتلاف كلياً أو جزئياً، أو زور شهادة دراسية أو شهادة خدمة حكومية أو أهلية، أو أساء التوقيع على بياض اؤتمن عليه، أو بإثباته وقائع وأقوال كاذبة على أنها وقائع صحيحة وأقوال معترف بها، أو بتدوينه بيانات وأقوال غير التي

صـدرت عن أصحابها، أو بتغيير أو تحريف الأوراق الرسـمية والسـجلات والمستندات بالحك أو الشطب أو بزيادة كلمات أو حذفها وإهمالها قصداً، أو بتغيير الأسـماء المدونة في الأوراق الرسـمية والسـجلات، ووضع أسماء غير صحيحة أو غير حقيقية بدلاً عنها، أو بتغيير الأرقام في الأوراق والسجلات الرسمية بالإضافة أو الحذف أو التحريف، عوقب بالسجن من سنة إلى خمس سنوات».

ـ الضرر

لكـي يكتمـل الركن المادي في جريمة التزوير لابـد أن يترتب على تغيير الحقيقـة في محـرر مكتوب بإحدى الطرق المحددة قانونـاً إحداث الضرر على الآخريـن، أو احتـمال تعريضهم لهذا الضرر، فإذا لم يقـع ضرر على الآخرين لا يكتمـل الركن المـادي وتنتفي جريمة التزوير، فالـضرر هو كل إخلال أو احتـمال الإخـلال بمصلحـة يحميهـا القانون، ويجـب على القـاضي بيان هذا الـضرر في حكم الإدانـة، وبغض النظر عـن نوع الضرر سـواء كان مادياً أو أدبياً محضاً، أو عاماً أو خاصاً (الربيعان٢٠٠٤م، ص١٤٢).

ـ الركن المعنوي

جرائـم التزويـر في المحررات المعلوماتيـة جرائم عمدية يلـزم لوقوعها توافر القصد الجنائي بشـقيه العام والخـاص، فالجاني يكون عالماً بأن الأفعال التـي يرتكبها تجرمهـا القوانين والأنظمة، وأنه يسـعى لتغيير الحقيقة في محرر وأن ذلك يترتب عليه الإضرار بالغير، وأن ينصرف علمه إلى أنه يغير الحقيقة بسـلوكه، فإذا ثبت جهلـه انتفى القصد الجنائي. أما العنـصر الثاني فهو اتجاه إرادة الجاني إلى تغيير الحقيقة، بإثبات بيانات غير صحيحة في المحرر المعلوماتي بإرادتـه، فإذا قام بذلك بالإكراه أو تحـت التهديد ينتفي القصد الجنائي العام

وتسقط عنه التهمة (خليل، ١٩٩٣م، ص٣٣)، فالقصد الجنائي العام يقوم على عنصري العلم والإرادة، فالعلم والإرادة شرطان أساسيان لتوافر القصد الجنائي العام (تاج الدين، ٢٠٠٤م، ص٢٧٤).

أما القصد الجنائي الخاص فيتمثل في نية استعمال المحرر المزور فيما زور من أجله سواء لتحقيق مصلحة شخصية، أو دفع ضرر، أو تحقيق مصلحة شخص آخر، أو إيقاع الضرر بشخص آخر (العريان، ٢٠٠٤م، ص ١٤٣-١٤٤).

٢ ـ خصائص جريمة التزوير الإلكتروني

تتسم جريمة التزوير الإلكتروني بعدة خصائص من أهمها:

أ ـ جريمة فنية غير ملموسة

جريمة التزوير الإلكتروني جريمة غير ملموسة، فلا يوجد أثر مادي ملموس، حيث تتم الجريمة من خلال الوصول إلى المعلومات، وتغيير مضمونها، فهي جريمة من جرائم أصحاب الياقات البيضاء التي تعتمد على قوة العقل والإدراك وليس على قوة العضلات، فلا تتضمن استخدام العنف، أو سفك الدماء، بل هي جريمة فنية غير ملموسة لا ترتكب بمحض الصدفة، بل تحتاج إلى التخطيط والمعرفة الفنية، فجرائم الاختراق والتعدي التقليدية، قد تتم بالمصادفة، أما جرائم التزوير الإلكتروني فتحتاج للتخطيط والدقة في التنفيذ، والمعرفة الفنية باختراق الحواجز الأمنية وتدميرها، والوصول إلى المعلومات والبيانات الخاصة بالأفراد أو المنظمات التي تمثل قوة اقتصادية، وتغييرها لتحقيق أرباح ومكاسب مادية أو معنوية لصالح مرتكب الجريمة أو لصالح شخص آخر (الشهري والعطوي، ٢٠٠٧م، ص٨٢١).

ب ـ جريمة عابرة للحدود

جريمة التزويـر الإلكتروني جريمة عابرة للحدود، فلا يوجد لها حدود معينة، بل يمكن ارتكابها من أي مكان في العالم، ولا يحتاج المجرم الإلكتروني إلى بـذل الجهـد والانتقال مـن مكان لآخـر للتخطيط لارتـكاب جريمته أو تنفيذها، بل يتمتع بكافة الأمان النفسي والراحة التامة عند تنفيذها (الصغير، ١٩٩٩م، ص٣٥).

جـ ـ تحتاج إلى خبرات فنية عالية

جريمـة التزوير الإلكتروني جريمة غير تقليدية، فهي لا ترتكب بطريقة عشـوائية أو غير مدروسـة، بل يحتاج ارتكابها إلى خبراء على درجة عالية من التخصص والكفاءة في اسـتخدام الحاسـب الآلي والإنترنت، فضلاً عن تمتع مرتكبهـا بسـعة الأفق والحيلة، فهـم أفـراد ذوو مكانة في المجتمـع يتمتعون بقـدر كافٍ من العلم والإلمام بالتقنية، حيث يتطلب ارتكاب جريمة التزوير الإلكـتروني الإلمـام بمعـارف ومهارات فنيـة متقدمة في مجال الحاسـب الآلي والإنترنت (مدني، ٢٠٠٧م، ص٤٨).

د ـ التمكن من مجال المعالجة الإلكترونية للبيانات

يتدخل الجاني من خلال ارتكاب جريمة التزوير الإلكتروني في مجال المعالجة الإلكترونيـة للبيانات سـواء من حيث تجميعها، أو تجهيزهـا، أو إعادة صياغتها وتهيئتها لإدخالها على جهاز الحاسب الآلي بغرض الحصول على المعلومات التي يريد تغييرها أو تزويرها (العريان، ٢٠٠٤م، ص٤٧).

هـ ـ التمكن من مجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية

يتدخل مرتكب جريمة التزوير الإلكتروني في مجال المعالجة الإلكترونية للنصوص والكلمات باسـتخدام طريقة أوتوماتيكية تمكن مستخدم الحاسب

الآلي من كتابة الوثائق المطلوبة أو تغيير محتواها بدقة متناهية، بفضل استخدام الأدوات التي تحت يده، وبفضل إمكانات الحاسب الآلي التي تتيح التعديل والتصحيح والمحو والتخزين والاسترجاع والطباعة، وجميع الأفعال المادية التي لها علاقة وثيقة بارتكاب جريمة التزوير الإلكتروني (العريان، ٢٠٠٤م، ص٤٧).

ثانياً: الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني

تتنوع الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني بهدف الحصول على الدليل الرقمي أو الأدلة المادية التي تشير إلى ارتكاب جريمة التزوير الإلكتروني ونسبتها إلى مجرم محدد، أو حصر التهمة في أضيق نطاق، ومن ثَمَّ التحقيق مع المشتبه بهم أو المتهمين لتوجيه الاتهام لهم جميعاً أو لبعضهم أو لأحدهم.

وتتضمن هذه الأساليب استخدام أساليب تقليدية، وأساليب مادية، وأساليب إجرائية تتنوع بحسب حالات التزوير، وما يتم التوصل إليه مع المتهمين والمشتبه به من نتائج أثناء التحقيق من قبل المحقق الجنائي والمحقق الفني. وتتوقف فاعلية استخدام هذه الأساليب في إثبات هذه الجرائم حسب ظروف وملابسات القضية، والدليل المثبت لها.

١ ـ الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني

هي الأساليب التي تعتمد على استخدام الأجهزة الفنية والخبرة العملية اللازمة لاكتشاف عمليات التزوير عند الكشف والمضاهاة من قبل المحقق الفني من خلال استخدام أجهزة تقنية تتمتع بفاعلية وقدرة عالية على إجراء المضاهاة، وكشف التزوير المادي الموجود فيها كمحررات أو وثائق يتم

إجراء الكشف عليها من خلال هذه الأجهزة حسب نوع الفحص، وهي أجهزة ذات كفاءة عالية في إثباتها، والتي من أهمها (إدارة الأدلة الجنائية، ٢٠٠٩م، ص ١-٢):

أ ـ جهاز ديكو سنتر (٣٠٠٠) وجهاز ديكوسنتر (٥٠٠٠)

جهاز إلكتروني يحتوي على مجموعة من الفلاتر الضوئية ذات موجات مختلفة تساعد في الكشف عن عمليات التزوير والتزييف للوثائق والمستندات المحررة يدوياً أو آلياً، من خلال الكشف عن الكتابات المطموسة على المستندات باستخدام المزيل، والكشف عن بعض البيانات التي تحتوي عليها الأوراق المحترقة إذا كانت جزيئات الورق المحترقة كبيرة أو متصلة، والكشف عن العملات المزيفة باستخدام الأشعة فوق البنفسجية والأشعة تحت الحمراء، ومعرفة نوعية الطباعة المستخدمة في العملات المزيفة والمستندات المزورة والوثائق الثبوتية، ومضاهاة الصور المثبتة على الوثائق الثبوتية مع الصور الفوتوغرافية للشخص المراد فحص صورته، وكذلك معرفة إذا كانت الصورة منزوعة أم لا من الوثيقة الرسمية، ومضاهاة الخطوط والتواقيع من خلال عدسات ذات قوة تكبير عالية، ومقارنة طبعات الأختام وإيضاح أوجه التطابق بينها، وفحص الوثائق الثبوتية الرسمية كرخص القيادة والإقامة والبطاقات الشخصية والجوازات للتأكد من صحتها.

ويتميز جهاز ديكوسنتر (٥٠٠٠) بأنه أكثر كفاءة في كشف التزوير في المحررات والوثائق من خلال عمله بميكانيزمات عمل تعتمد على تركيز الأشعة فوق البنفسجية والأشعة تحت الحمراء لاكتشاف أدنى فروقات في الخطوط والأختام والتوقيعات في المحررات التقليدية.

ب ـ جهاز زايس

جهاز إلكتروني يختص بفحص البطاقات الممغنطة والتأكد من صحتها.

جـ ـ جهاز زايزدي

جهاز إلكتروني يختص بكشف الضغوط على المستندات.

د ـ برنامج العملات

برنامج يحتوي على جميع العملات المالية التي تخص كل دولة في العالم، ويوضح ما تحتويه كل عملة من علامات أمنية.

هـ ـ المجاهر الإلكترونية

مجاهر ذات قوة تكبير وتوضيح عالية جداً تساعد في عمليات الفحص للأوراق والمستندات المشتبه بها.

و ـ جهاز رامان لتحليل الأحبار

جهاز إلكتروني يستخدم في التفرقة بين أنواع الأحبار المستخدمة على المستندات.

٢ ـ الأساليب المادية في إثبات جريمة التزوير الإلكتروني

هي الأدوات الفنية التي تستخدم في بيئة نظم المعلومات لتنفيذ إجراءات وأساليب التحقيق الجنائية والفنية المختلفة، بهدف إثبات وقوع جريمة التزوير ونسبتها إلى متهم محدد. وهذه الأساليب ذات فاعلية وكفاءة عالية في التحقيق الجنائي، حيث تسهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجاني والمجني عليه، ومن أهمها:

أ ـ عناوين (IP و MAC) والبريد الإلكتروني وبرامج المحادثة

عنوان (IP) هو المسؤول عن تراسل حزم البيانات عبر الإنترنت وتوجيهها إلى أهدافها، وهو يتكون من أربعة أجزاء: يشير الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه (Arabiat, 2002).

ولذلك ففي حالة وجود جريمة اختراق وتعد لارتكاب جريمة التزوير يقوم المحققون بالبحث عن عنوان الـ (IP) للجهاز مصدر الجريمة، ومن ثم العثور عليه وتحديد موقع الجهاز وتاريخ الاختراق (حجازي، ٢٠٠٥م، ص٦٣).

وهذا الأسلوب من الأساليب التقنية المستخدمة التي تتسم بفاعلية عالية إذا استخدمت في ظروف ملاءمة تمكن من الوصول إلى مصدر الجريمة من خلال التحديد لموقع ارتكابها.

ب ـ البروكسي

يعمل البروكسي كوسيط بين الشبكة ومستخدميها، لكي تتمكن الشبكة المقدمة للخدمة من إدارة الشبكة، وضمان توفير الأمن، بجانب توفير خدمات الذاكرة الجاهزة، حيث يتلقى البروكسي طلباً من المستخدم للبحث عن الصفحة المطلوبة ضمن ذاكرة كاشي المحلية المتوافرة، فيتحقق البروكسي إذا ما كانت هذه الصفحة قد جرى تنزيلها من قبل، فإذا كانت كذلك يقوم بإعادتها إلى المستخدم دون الحاجة إلى إرسال طلب إلى الشبكة العالمية، أما إذا لم يجدها فيقوم بإرسال طلب إلى الشبكة العالمية لاستخدام عناوين (IP). وأهم مزايا البروكسي إمكانية احتفاظه بالعمليات التي تمت عليه، مما يمكن

مـن اسـتخدامها كدليل إثبات قـوي، خاصةً وأن المعلومـات لا توجد لدى المستخدم، بل توجد لدى مقدم الخدمة (عبد المطلب، ٢٠٠١م، ص٢١٩).

جـ ـ برامج التتبع

تقوم هذه البرامج بالتعرف على محاولات الاختراق ومن قام بها وإشعار الجهة المتـضررة من عملية الاختراق والتعدي وتزوير المعلومات (الشـدي، ٢٠٠٠م، ص١٠٠)، حيث يتكون البرنامج من شاشة رئيسة تقدم للمستخدم بياناً شـاملاً بعمليات الاختراق التي تحدث ضد جهازه وتحمل اسـم الحدث وتاريخ حدوثه، وعنوان الـ (IP) الذي تم من خلاله، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت، ومعلومات أخرى، وعند حدوث أية محاولة للاختراق تظهر أمام المسـتخدم شاشة أخرى صغيرة مصحوبة بتحذير صوتي ويظهر على الشاشة عنـوان الـ (IP) الخاص به، ويمكن للمسـتخدم الاختيار ما بين أربعة أوامر موجودة في هذه الشاشـة الفرعية منه Report it والأمر الثاني هو Trace it، وبمجرد الضغط على هذا الأمر تظهر شاشـة أخرى عليها اسـم الدولة التي تمت منها محاولة الاختراق، وعلى المسـتخدم أن يضغط على أمر Next حتى يقـوم البرنامج باسـتكمال عملية اقتفـاء الأثر بعدها تظهر شاشـة ثالثة عليها خريطـة العالم وخط طويل ممتد من المدينة التي تمت منها محاولة الاختراق إلى المدينة التي يقيم فيها المسـتخدم، ويوجد أسفل الخريطة مجموعة من العوامل هي Map، وبالضغط عليها تظهر خريطة توضح خط سـير محاولة الاختراق (Arabiat, 2002).

الأمر الثاني هو Trace، وبالضغط عليه يظهر اسـم الشركة المسـتضيفة وعنـوان الــ (IP)، ورقـم المنفـذ Port أو البوابة الخاصـة بهـا. وهنـاك أمـر

Network وبالضغط عليه تظهر البيانات الكاملة للشبكة التي تتبعها الشبكة المستضيفة للمخترق بما فيها أرقام الهواتف والفاكسات الخاصة بها، وآخر تحديث قامت به في جهاز الخدمة الخاصة بها، وهناك أمر Registrant ويقدم معلومات الشركة المستضيفة، ثم أمر اقتفاء الأثر وتحديث المعلومات، ويظهر على شكل دائرة عليها خطان متقاطعان، ويمكن الحصول على هذه البرامج من موقع www.zdnet.com (Arabiat, 2002) وتكمن فاعليتها في أنه من خلالها يمكن تحديد جهة مرسل الرسالة عن طريق البريد الإلكتروني باستخدام برامج تتبع مصدر الرسائل، وهي لا تحدد المستخدم فقط، بل تحدد الدولة وكذلك الشركة المقدمة لخدمات الإنترنت التي يمكن التأكد من خلالها بحصول الاختراق والتعدي والتزوير.

د ـ أدوات الضبط

هي أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وأدوات التنصت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، وأدوات الضبط الأخرى، ويمكن استخدام الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للمواقع كبرمجيات Java Applets أو Java X أو Cookies والبرامج الأخرى.

هـ ـ الأدوات المساعدة بالتحقيق

من خلال عمليات التحري الإلكتروني يمكن استخدام أدوات استرجاع المعلومات من الأقراص التالفة مثل View Disk، وبرامج كسر كلمة المرور، وبرامج الضغط، وفك الضغط Pkzip، وبرامج البحث عن الملفات العادية والمخفية مثل Xtreepro Gold، وبرامج تشغيل الحاسب

مثل Bootable Diskette، وبرامج نسخ البيانات مثل Lap Link، بالإضافة إلى برامج منع الكتابة على القرص الصلب التي تستخدم بعد ارتكاب الجريمة لحماية مسرحها، وكذلك برامج استرجاع الملفات المحذوفة التي يلجأ المجرم إلى حذفها للتخلص من الدليل الإلكتروني مثل Win-dows For Rescue File وبرنامج Research Regnerud، وذلك بهدف جمع الاستدلالات إلكترونياً.

وتظهر فاعليتها عند اتباع الإجراءات العلمية والفنية للتحري، حيث تمنع من تغيير المواد والبرامج المستخدمة في الاختراق والتعدي والتزوير.

و ـ أدوات فحص ومراقبة الشبكات

هي الأدوات التي تستخدم في فحص البروتوكول TCP/IP لمعرفة المشكلات المتعلقة بالشبكات والعمليات التي تعرضت لها (العنزي، ٢٠٠٣م، ص١٠٢).

وترجع فاعليتها إلى قدرتها الفائقة في الدخول على الشبكات، وتلمس برامج السرقة والتلصص، وكذلك الفيروسات التي تستخدم في عمليات الاختراق والتعدي والتزوير، وتحديد مصدرها بدقة.

ز ـ برامج فحص الشبكة المحلية LAN وبرامج التشارك في الموارد

هي برامج تستطيع فحص الشبكة المحلية، وكذلك التعرف على البرامج المشاركة في الموارد، ومن ثم تتبع حالات الاختراق والتعدي، حتى اكتشاف الـ (IP) الخاص بالمخترق الذي قام بارتكاب جريمة التزوير والتعرف على موقع الجهاز (Arabiat, 2002).

وترجع فاعليتها إلى قدرتها الفائقة على اكتشاف الـ (IP) الخاص بالجاني داخل الشبكة المحلية، وتحديد موقع الجهاز بدقة.

حـ ـ تتبع برامج الاختراق الموجودة على شبكة الإنترنت

يتـم ذلـك باسـتخدام بروتوكـول تخاطب خاص بهـذه البرامـج، لتتبع نشـاطاتها خلال فترة زمنية محددة، والتعرف على البرنامج الذي اسـتخدم في الاختراق والتعدي من خلال خادمات الملفات التي يمكن من خلالها تحديد موقع الاختراق والتعدي (عبد المطلب، ٢٠٠١م، ص٢٢٠).

وترجع فاعليتها إلى قدرتها الفائقة على اكتشاف الـ (IP) الخاص بالجاني داخـل الشـبكة الدولية، وتحديـد موقع الجهـاز بدقة، وتختلف عن سـابقتها باختلاف الشبكة، فهي ذات قدرة أعلى على التوغل في الشبكات الخارجية.

ط ـ اكتشاف الثقوب التي تتخلل البرامج الموجودة على النت

توجـد بعـض البرامـج على شـبكة الإنترنـت، وهـذه البرامج تسـاعد المستخدم على القيام بأعمال مهمة كالاتصال، وزيادة سرعة الإنترنت، ولكن المشكلة في إمكانية ترك المخترقين لثقوب بهذه البرامج يستطيعون من خلالها النفـاذ إلى النظـام واختراقـه من خلال البحـث عن هذه البرامـج والدخول مـن خلالهـا إلى نظم المعلومات والسـيطرة عليهـا وارتكاب جرائـم التزوير الإلكتروني (الحمدان والقاسم، ٢٠٠٤م، ص ٥٣).

ويمكـن اكتشـاف الثقوب الموجـودة عـلى البرامج باسـتخدام جدران الحمايـة، أو برمجيـات Cookies والبرمجيـات الأخرى التي تسـاعد في معرفة مصدر الاختراق (Arabiat, 2002).

ي ـ برامج فك الشفرات

من أهم فوائد التشفير أنه يقي من التنصت على حزم المعلومات الخاصة بالمنظـمات، والتصنت يعني نسـخ حزم المعلومات عند انتقالها عبر الشـبكة،

حيث يمكن من الناحية التقنية مراقبة أداء الشبكة من خلال حزم البيانات المتدفقة عبر الشبكة؛ مما ييسر وصول المخترقين لهذه الحزم، ولكن يمكن منع التنصت باستخدام وسائل التشفير المناسبة؛ لأن عدم معرفة الشفرة معناه الحصول على بيانات ومعلومات مبهمة وغير مفهومة (الحميد ونينو، ٢٠٠٧م، ص٥٤)، إلا أن هناك برامج يمكنها فك الشفرات، وبصفة خاصة للبرامج والمواقع التي تقوم بعمليات الاختراق والتعدي والتزوير، وهذه البرامج تحتوي على مليارات من الشفرات،وتقوم باستغلال الحاسب الآلي في تجربة هذه الشفرات في ثوانٍ معدودة حتى تقوم بفتح الموقع المشفر، ومن ثم متابعته، ومعرفة ما إذا كان قد استخدم في عملية الاختراق والتعدي والتزوير (عبد المطلب، ٢٠٠١م، ص٢٢٠).

وتتميز هذه البرامج بفاعلية عالية في فك أية شفرة، ومن ثمَّ إمكانية الدخول على البرامج المشفرة التي استخدمت في الاختراق والتزوير والتعدي، ومعرفة مصدرها.

٣ـ الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني

هي الأساليب التي تستخدم لإثبات وقوع الجريمة، وتحديد شخصية مرتكبها، وهذه الأساليب ذات فاعلية في التحقيق الفني، حيث تسهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجاني والمجني عليه من قبل المحقق الفني باستخدام تقنيات وبرامج التتبع الإلكتروني والتفتيش الإلكتروني والضبط الإلكتروني التي تتميز بقدرات فائقة على القيام بمهام التتبع والاسترجاع للبرامج والأدوات التي استخدمت في الاختراق والتعدي والتزوير، ومن أهمها:

أ ـ اقتفاء الأثر

هو اقتفاء أثر مرتكب جريمة التزوير في الحاسب الآلي الخاص بالمجني عليه للبحث عن دليل الإدانة سواء كان بريداً إلكترونياً، أو سجلاً لغرف المحادثة أو غيره، ولذلك يحرص المخترقون على إزالة آثارهم بعناية (الفنتوخ، ٢٠٠١م، ص١٨)، وذلك من خلال القيام بإجراءات التتبع الإلكتروني التي يقوم بها المحقق الفني أثناء الانتقال والمعاينة.

ب ـ الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

يجب على المحقق الفني الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات، وكذلك قاعدة البيانات وإدارتها،وخطة تأمينها، وموارد النظام، والمستفيدين، والملفات، والإجراءات، وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، والوقت المخصص لكل مستفيد في حالة تعدد المستخدمين، وإجراءات أمن العاملين، وأسلوب النسخ الاحتياطي، وبرامج الحماية المتوافرة.

جـ ـ الاستعانة بالذكاء الاصطناعي

يمكن الاستعانة بالذكاء الاصطناعي في حصر الحقائق والاحتمالات والأسباب والفرضيات، واستنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي وفق برامج لتغطية كافة الاحتمالات وتقديم الاحتمال الأقوى (البشرى، ٢٠٠١م، ص١٨٦).

د ـ التوقيف خلال فترة التحقيق

هو سلب المتهم الذي تثور دلائل وشبهات قوية نحو ارتكاب جريمة التزوير الإلكتروني حريته خلال فترة التحقيق حسب مقتضيات التحقيق

ومصلحتـه، وهو إجراء من إجراءات التحقيق، ويطلق عليه مسـمى الحبس الاحتياطـي، وينتهي بـبراءة المتهم والإفـراج عنه، أو إصـدار الحكم بتوقيع العقوبـة عليه، والغرض من تقييد حريـة المتهم في الجرائم المعلوماتية الخوف من اسـتغلال مهارته في طمس وتدمير الأدلـة المادية والإلكترونية (العنزي، ٢٠٠٣م، ص١٠٦).

هـ ـ إظهار الحقائق

يجـب على المحقـق إظهـار الحقائق خـلال مرحلـة جمع الاسـتدلالات الإلكترونيـة، وإثباتهـا في محـضره نظـراً لأهميتهـا في تحديـد الجريمة،ورسـم خطـوات البحث من خلال التثبت من توافـر أركان الجريمة، وتحديد مكان الجريمـة ووصفـه، وتحديد وقت وقـوع الجريمة، وتحديد أسـلوب ارتكاب الجريمـة، وأداة ارتـكاب الجريمـة، والظـروف المحيطـة بالجريمـة، ودوافع الجريمة (كامل، ١٩٩٩م، ص ٦٦-٦٩).

و ـ اتباع القواعد الفنية لكشف الجريمة

لكشـف غمـوض الجريمـة، يجب عـلى المحقـق أن يتقيـد بالإجراءات التالية:

١ ـ مراعاة الاحتمالات الشائعة في الجرائم: كأن تكون الجريمة لم تقع، أو وقعت بالصدفة، أو نتيجة ظروف عارضة، وعدد الجناة، وأساليب ارتكاب الجريمة.

٢ ـ تقديـر احتـمالات وقوع الجريمة: يجب على المحقـق تقدير خطوات ارتـكاب الجريمـة بدايـةً من التحضـير لها، ثـم التخطيـط والتنفيذ اعتماداً على الأدلة والوقائع.

٣ ـ فحص الاحتمالات: بعد الحصول على الاحتمالات يقوم المحقق بفحص كل احتمال متبعاً في ذلك القواعد الفنية، مع البدء بالاحتمال الأقوى، وعدم التشبث باحتمال واحد، وعدم تعجل الوصول إلى نتيجة إيجابية من خلال فحص الاحتمالات (كامل، ١٩٩٩م، ص٣١٤).

و ـ الاستعانة بخبراء الحاسب الجنائي

في حالة عدم إلمام المحقق الجنائي بمجال الحاسب الجنائي، فعليه أن يستعين بخبراء الحاسب الآلي بهدف تأمين الحاسب الآلي والحفاظ على الأدلة الموجودة به من التلف أو تعطيلها من قبل مرتكب الجرائم التزوير الإلكتروني (الحبشي، ١٩٩٠م، ص١٢).

ز ـ التفتيش في مرحلة جمع الاستدلالات

يجب الحصول على إذن من السلطة المختصة في حالة تحديد الموقع الذي قام بعمليات الاختراق والتعدي وارتكاب التزوير الإلكتروني، لتفتيش هذا الموقع وتفتيش الموجودين به، وإثبات ذلك في المحضر مع إرفاق المستند الكتابي (كامل، ١٩٩٩م، ص ٢٨٢-٢٨٣).

ح ـ التحفظ على الأجهزة المشتبه بها وتقنيات الاتصال المتصلة بها

يجب التحفظ على الأجهزة المشتبه بها، وكذلك تقنيات الاتصال المرتبطة بها التي يشك المحقق في استخدامها في عمليات الاختراق والتعدي والتزوير الإلكتروني، لكي لا يقوم الجاني بتدميرها أو إتلافها، مع ضرورة تحريز جميع المضبوطات بعد إجراء الفحص عليها وتدوين ذلك في محضر الضبط،وتحريز ما يجب تحريزه من الأجهزة والتقنيات، والبدء بفحص الأجهزة التي يمكن

حفظهـا في المكان أو نقلها إلى مكان الفحص بعد تحريزها حسـب ما يتراءى للخبير والمحقق الجنائي والفني (العريان، ٢٠٠٤م، ص١٣٥).

ط ـ ترتيب استجواب المتهمين

يجب ترتيب اسـتجواب المتهمين حسب طبيعة جريمة التزوير المرتكبة، وحسب مرئيات خبير الحاسب الآلي الذي يجب أن يشارك في وضع الأسئلة مـع المحقق، وترتيبها وفقاً للخطوات الإجرائية، وكذلك ترتيب المتهمين إذا كان هنـاك أكثـر من متهم حسـب توجيهات خبير الحاسـب الآلي (البشرى، ٢٠٠٠م، ص ٣٦٦-٣٦٧).

ثالثاً: معوقات إثبات جرائم التزوير الإلكتروني

يواجـه إثبـات جرائم التزويـر الإلكتروني صعوبات بالغـة نظراً لطبيعة الجريمة المعلوماتية التي يرتكبها جناة على علم ودراية كبيرة بأسـاليب عمل برامـج الحاسـب الآلي، وذوي قـدرات عـلى اختـراق نظم المعلومـات بعدة وسـائل، ومـن ثم فهم أقدر عـلى محو الآثار الدالة على ارتـكاب جريمته بعد ارتكابهـا، بجانب إمكانية ارتكاب هذه الجرائم مـن أماكن بعيدة تماماً، ومن دولـة لا يوجد بينها وبـين الدولة التي تم ارتكاب الجريمـة فيها أو على أحد مواطنيها أو مؤسساتها أي نوع من التعاون في مجال تسليم المجرمين، بل وقد تطغـى الخلافـات السياسـية بين الدولتين وتشـجع على عمليـات الاختراق والتعـدي، ممـا يتطلب وجود تعـاون دولي لمواجهـة جرائـم المعلوماتية لأنها ذات طابـع دولي، فهناك عدة معوقات تعترض إثبات جرائم الحاسـب الآلي مـن أهمها قـدرة الجاني على تدمـير أدلة الإدانـة، وعدم تخلف الآثـار المادية، وعدم رؤية النشـاط الإجرامي، وقلة الخبرات للسلطات المسؤولة عن ضبط

الجرائم والتحقيق فيها، والتكتم على نشاطات الاختراق والتعدي من قبل الجهات والمراكز التي تتعرض لذلك خوفاً من فقدان ثقة العملاء، ووجود معوقات تعود لطبيعة النظام الآلي.

ومن ثم فإن المعوقات التي تكتنف الجريمة الإلكترونية تعزى إلى عدد من الصعوبات:

١ ـ صعوبات التحري في جرائم التزوير الإلكتروني

من أهم صعوبات التحري:

١ ـ أنها تختلف عن الجريمة التقليدية في أنها غير عشوائية أو غير مدروسة، بل يحتاج القيام بها إلى مهارة في استخدام الحاسب الآلي والإنترنت وسعة الأفق والحيلة والدهاء، فمن يقوم بها من أصحاب المكانة في المجتمع الحديث ممن يتمتعون بقدر كافٍ من العلم اللازم لاستخدام وتطويع التقنية.

٢ ـ اختراق الحدود والحواجز، فالجريمة المعلوماتية ترتكب في بلد من بلد آخر يبعد آلاف الأميال، وتنتشر أدلتها في عدة بلدان، فأي قانون يحكم هذه الجريمة فهو يصعب من عمليات التحري عنها.

٢ ـ صعوبة الضبط في جرائم التزوير الإلكتروني

من أهم صعوبات الضبط (مدني، ٢٠٠٧م، ص ٤٨-٤٩):

١ ـ استخدام تقنية عصرية متطورة للحاسبات الآلية والشبكات والاتصالات في ارتكابها، مما يكسبها تأثيراً أشد من الجرائم التقليدية، بل وتسهم في زيادة تأثير الجرائم التقليدية إذا استخدمت أو ساعدت في ارتكابها.

٢ ـ يمكـن أن يشـترك فيها مجموعـة من العصابـات الدولية كعصابات الإجرام المنظم أو المافيا أو الجماعات الإرهابية أو الجماعات المتطرفة ذات الاتجاهـات العقائدية المتباينة والتوجهات الفكرية والسياسـية والدينيـة المختلفـة، حيث تسـهم التقنية في زيادة معدلات التنسـيق بـين هذه الفئات، وتزيد من خطورتها نتيجة توجيه المنفذين من قبل المخططين من مسافات بعيدة، وسهولة توجيه الأوامر والتعليمات، مما يزيد من خطر الإرهاب.

٣ ـ سهولة تدمير المعلومات المؤدية إلى معرفة شخصية المجرم أو موقعه بمجرد علمه بصدور إذن بضبطه وتفتيشـه، ومن ثم صعوبة تقديم دليـل إلكتروني أو رقمـي لتحقيق الإقناع اليقينـي للمحكمة بإدانة المجرم الإلكتروني.

٤ ـ يمكن أن تدخل في أغلب أنواع الجرائم التقليدية إن لم يكن جميعها.

٥ ـ بعـض الجرائـم الإلكترونيـة لا يشـترط لهـا توافـر خـبرة عاليـة في اسـتخدام الحاسـب الآلي والإنترنت، فكثير من المراهقين يتجولون عبر الإنترنت وينسخون برامج قد تخـالف الدين أو الأخلاق.

٣ ـ صعوبة التحقيق في جرائم التزوير الإلكتروني:

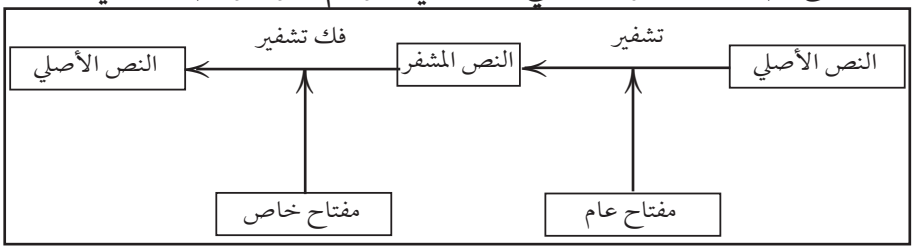
١ ـ عـدم تخلـف آثار مادية عـن جريمة التزوير الإلكـتروني أو الجريمة المعلوماتية، لأن الآثار التي قد تتخلف عنها ذات طبيعة غير ظاهرة.

٢ ـ اتخـاذ الجنـاة لتدابير أمنية تمنع اكتشـافهم أو الحصول على دليل على جرائمهـم ككلمات المـرور التي تمنع اختراق مواقعهـم، أو التفتيش المتوقـع للبحـث عن أدلـة، فضلاً عـن اسـتخدام أسـلوب الترميز

والتشـفير الذي يمنع من قراءة المعلومـات إلا لمن يحمل مفتاح حل الشفرة (حجازي، ٢٠٠٥م، ص٤٨).

والشكل رقم (٣) يوضح استخدام المفتاح العام والخاص في التشفير.

أ ـ معنى الإثبات والقواعد التي تحكمه في جرائم التزوير الإلكتروني



المصدر : (المزيد والشهري، ٢٠٠٧م، ص١٥٤١).

الشكل رقم (٣) استخدام المفتاح العام والخاص في التشفير

الإثبات في معناه العام هو كل ما يؤدي إلى كشـف الحقيقة، أما الإثبات في معنـاه القانـوني فهو إقامة الدليل عـلى وجود واقعة قانونيـة تترتب آثارها أمام القضاء بالطرق التي حددها القانون، وهو الوسـيلة التي يتم من خلالها إقـرار وقوع الجريمة، وهو كل ما يؤدي إلى ثبوت إجرام المجرم أو براءته من التهمة المنسوبة إليه (الهيتي، ٢٠٠٥م، ص٢٢٢).

والإثبـات هـو إقامة الدليل على وقوع الجريمـة أو عدم حصولها، وعلى إسنادها إلى المتهم، أو براءته منها (مصطفى، ١٩٧٧م، ص١٥٠).

والدليـل هو أداة الإثبـات، وهو إما دليل إثبـات أو دليل نفي، فالدليل هو الأداة التي يسـتخدمها القاضي للبرهـان على إثبات اقتناعه بالحكم الذي ينتهـي إليه، فالإثبات أعم وأشـمل من الدليل، فلـكل منهما مدلوله الخاص (النمر، ١٩٩١م، ص ٣-٤).

وتفـترض الواقعـة الجنائية وقـوع الحدث المجرَّم بموجـب نص جنائي

يجرمه ويحدد مقدار العقوبة، وإسناد الحدث إلى شخص معين بحيث يوجه إليه الاتهام من خلال الدعوى العمومية أو الدعوى الجزائية (العكيلي وحربة، ١٩٨١م، ص٢١).

ومن أهم القواعد التي تحكم الإثبات قاعدة «لا حاجة لإقامة الدليل على ما تنهض الشواهد على تقرير ثبوته، وإنما يلجأ إلى الإثبات من يدعي عكس ما تؤيده الشواهد» (عوض، ١٩٦٣م، ص٤٤١)، ولذلك لا يتم اللجوء إلى الإثبات إلا في حالة وجود ادعاء بارتكاب جريمة» لأن الأصل في الإنسان هو البراءة، وما تقوم عليه الشواهد هو براءة الإنسان، والادعاء بارتكاب جريمة ادعاء يخالف الأصل ويناقضه، فلابد من توافر الدليل، ولذلك أوكل المنظم للجهات التي خولها حق الاتهام تقديم الدليل، فالأصل يمكن نقضه بما خالفه، فقرينة البراءة التي يفترضها المنظم بالإنسان قرينة بسيطة قابلة لإثبات العكس، فقرينة البراءة من القرائن القانونية البسيطة لكونها قابلة لإثبات العكس (الهيتي، ٢٠٠٥م، ص٢٢٣)، وهذا يرتكز أيضاً على قاعدة «المتهم برىء حتى تثبت إدانته».

أي أن سلطة الاتهام هي التي يقع عليها عبء الإثبات من خلال تجميع أدلة الاتهام، بمعنى إثبات عناصر الجريمة بجميع أركانها ما لم يشترط القانون عكس ذلك، فإثبات الجريمة لا يعني التحقق من وقوعها فحسب، بل يمتد ليشمل نسبتها إلى شخص معين من خلال أدلة تثبت ارتكابه الجريمة، أو تحدد صلته بها في نطاق الجريمة، والأدلة إما مادية أو معنوية، أو قولية كالإقرار والشهادة، أما الأدلة المادية فهي المخلفات والآثار المحسوسة التي تتخلف في مسرح الجريمة نتيجة احتكاك الجاني بالمجني عليه أو الأدوات التي يستعملها في ارتكاب الجريمة، أو العلاقات المكانية في مسرح الجريمة نتيجة الاضطراب أو الصراع الذي يدور بين الجاني والمجني عليه، فمقتضى

إثبـات الجريمة هـو وجود أدلة كالاعتراف أو الشـهادة، أو وجود آثار مادية كالبقـع الدموية، وبصمات الأصابع، وغير ذلك من الأدلة المادية (الشـاذلي، ١٩٩٨م، ص١٢٧).

ب ـ صعوبة التوصل للآثار المادية في جرائم التزوير الإلكتروني

تتميـز جرائـم التزوير الإلكتروني بصعوبة التوصل للآثـار المادية، نظراً لأن جرائـم الحاسـب الآلي أصلاً عبـارة عن نبضات إلكترونيـة تملأ الكون، وتنساب كما تنساب الأشعة التي تخترق الحواجز وتنفذ منها، ويمكن إرسالها واسـتقبالها من قبل الجـاني عن طريق النهايات الطرفية، أو محطات اسـتقبال النبضات والإشـعاعات المنبعثة من كابلات الربط، كـما تختلف الآثار المادية عـن الآثـار المادية الناتجة عـن ارتكاب الجرائـم التقليديـة، في إمكانية تدمير الآثـار التـي تثبت ارتكاب جريمتـه في ثوانٍ معدودة. ومـما يصعب الأمر أن مرتكـب الجريمـة قد يرتكبها مـن منزله، وفي هذه الحالة تسـقط أهمية وقيمة الأدلـة الماديـة التقليديـة كبصـمات الأصابع التـي توجد على لوحـة المفاتيح والتي تثبت اسـتخدامه للحاسـب، أما في المنظمات فتسقط قيمة الأدلة المادية لمواجهتهـا بتعـدد المسـتخدمين، وربما يتم العبـث والدخول عـلى النظام من خارج المنظمة، أومن خارج الدولة بأكملها. كما أن جرائم الحاسب الآلي من الجرائم الناعمة التي لا يتكبد فيها الجاني مشـقة الصراع مع المجني عليه عند اكتشـاف أمره، فهي جرائـم خالية من العنف، لا تحتـاج إلى كسر الأقفال أو الاعتداء على الحراس، أو كسر الخزائن ونهب محتوياتها، فالآثار التي تتخلف عـن الجريمـة المعلوماتية ذات طبيعـة غير مادية هي بذاتها تمثـل صعوبة أمام إثباتها. وتقتصر الآثار المادية التي تتخلف عن ارتكاب الجريمة المعلوماتية في الأوراق التـي قد توجد لـدى الجاني عند محاولة اختباره نتيجة التعديل الذي

أجراه على البرنامج، أو المعلومات المخزنة، أو سقوط ورقة أو مجموعة أوراق التي نسخ عليها الجاني البرامج، أو المعلومات التي استولى عليها (الهيتي، ٢٠٠٥م، ص٢٢٥-٢٢٨).

رابعاً: إثبات جرائم التزوير الإلكتروني بالأدلة العلمية

يحتاج إثبات جرائم التزوير الإلكتروني إلى الدليل العلمي كوسيلة لإثبات ارتكاب جريمة الاختراق والتعدي على البيانات والمعلومات سواء بسرقتها أو إتلافها أو تزويرها، أو سرقة منظومة التوقيع الإلكتروني الخاص بفرد معين أو منظمة معينة لصالح الفرد أو الغير، والدليل العلمي يتطلب استخدام طرق غير تقليدية في الإثبات، والدليل العلمي يقتصر على إجراء تجارب علمية ومعملية على جهاز الحاسب الآلي الذي استخدم في الاختراق أو التعدي لتعزيز دليل سبق تقديمه سواء بالنفي أو الإثبات للواقعة التي ثار الشك بشأنها (حجازي، ٢٠٠٥م، ص ٤٩-٥٠)، ويحتاج إجراء هذه التجارب إلى محقق جنائي وفني متخصص يمتلك مهارات فنية وتقنية لاستخلاص الأدلة الرقمية (الخليفة، ٢٠٠٧م، ص١٠١٧)؛ لأن الفصل في الدعوى الجزائية في هذه الحالة يتوقف على الرأي الفني الذي يثبت أو ينفي ارتكاب الجريمة من قبل المشتبه به (حسني، ١٩٨٨م، ص٤٧٤).

والدليل العلمي هو النتيجة التي تسفر عنها التجارب العملية والمعملية لتعزيز دليل سبق تقديمه، سواء للإثبات أو نفي واقعة ثارت شكوك حولها، وهو لا يعدو كونه رأياً فنياً يعتمد على خبرة ومهارة فني متخصص يحدد إذا كان الاختراق والتعدي قد تم من الحاسب المشتبه به أم لا (الهيتي، ٢٠٠٥م، ص٢٣٢).

وبالرغم من الاختلاف بين شراح القانون في اعتبار الخبرة الفنية دليلاً

أو قرينة، إلا أن واقع التقدم التقني المعاصر استدعى الاستعانة بالمختصين والخبراء وأصحاب الرأي الفني في دراسة الوقائع المتصلة بالجريمة ونسبتها إلى المتهم، في ضوء تحري الدقة في تحديد المتهم، وهي في الفقه تعد بمثابة قرائن لا ترقى إلى أدلة الإثبات المادية، ولكنها تعد بمثابة إحدى طرق الإثبات كقرائن (حجازي، ٢٠٠٥م، ص٥١). والرأي السابق قد جانبه الدقة؛ لأن الخبرة العلمية والفنية تستخدم في حالات كثيرة لإثبات الوقائع المختلفة، كتحديد الحالة العقلية للمتهم لتحديد مسؤوليته، وكذلك في حالة استخدام البصمة الوراثية لتحديد الجاني أو إثبات النسب والبنوة والقرابة للفصل في قضايا النسب والميراث وغيرها (حسني، ١٩٨٨م، ص٤٧٥).

إن عدم الاعتداد بالخبرة الفنية كوسيلة لإثبات الجريمة المعلوماتية، وإنما اعتبارها بمثابة قرائن فقط، يضيف صعوبة أخرى إلى صعوبات اكتشاف المجرم المعلوماتي وتحديده في ضوء عدم التسليم بالأمور التي تحكم الدليل العلمي في الفكر الجنائي خارج نطاق تلك الجرائم، بمعنى أنه لم يتم التسليم بالقواعد التقليدية في الإثبات بوزن الدليل العلمي في الجريمة المعلوماتية وعدم اعتماده كدليل إثبات، وإنما اعتباره قرينة، ما لم تؤازره أدلة أخرى، فإن ذلك يترتب عليه إفلات مرتكبي جرائم المعلوماتية أو التزوير الإلكتروني من العقاب؛ لأنه لا توجد وسيلة لإثبات ارتكاب هذه الجريمة في العصر الحديث سوى الدليل العلمي، والخبرة الفنية، خاصةً أن كثيراً من القضايا في العصر الحالي يعتمد الفصل فيها على الخبرة الفنية والعلمية (الهيتي، ٢٠٠٥م، ص ٢٣٣-٢٣٤).

ويرى الباحث ضرورة اعتبار الخبرة الفنية في جرائم المعلوماتية وجرائم التزوير الإلكتروني دليلاً مادياً فهي وسيلة علمية في مواجهة جرائم المعلوماتية في ضوء طبيعة هذه الجريمة التي تعتمد على نبضات إلكترونية

تتـم من خـلال التلاعب بقواعد البيانـات في المنظمات، وذلـك بالإضافة أو الحذف أو التعديل وإخراج مخرج أو وثيقة إلكترونية مزورة بصورة صحيحة مسـتغلاً مهاراته في الدخول على النظام والقيام بعمليات التزوير والتلاعب التـي يصعب كشـفها بالطرق التقليدية، مما يحتم الاسـتعانة بأسـاليب علمية وخـبرات فنية ذات فاعليـة في إثبات جريمة التزوير الإلكتروني والعمل على تطويرها والاستفادة من فاعليتها في إثبات هذه الجرائم.

٢. ١. ٣ التحقيق في جرائم التزوير الإلكتروني

نظراً لطبيعة الجرائم الإلكترونية بصفة عامة وجريمة التزوير المعلوماتي بصفة خاصة، فإنها تتطلب أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمـي ودعمه مـن قبل الفنيين المختصين، وذلك يسـتدعي اتخاذ إجراءات سريعـة؛ لأن الدليل الإلكـتروني غير مادي، ويمكن التخلص من أية أدلة أو آثـار من قبل مرتكبـي الجرائم المعلوماتيـة، كما تختلف أسـاليب تلقي البلاغ وإجراء المعاينة والقيام بالتحريات والتفتيش والاسـتجواب عنها في الجرائم التقليدية نظراً لطبيعة الجرائم المعلوماتية وخصائصها، كما هو الحال في تزوير التصديـق الإلكتروني الذي يسـتدعي أيضـاً اتخاذ الإجراءات السـابقة، لأن تزويـر التوقيـع الإلكتروني لا يعني تقليده، بل الاسـتيلاء عليـه من منظومة التوقيـع الإلكتروني المسـؤولة عن تصديقه، واسـتخدامها دون معرفة مالكه الأصلي.

ويتطلـب التحقيـق في جرائـم التزويـر الإلكـتروني في مجـال الضبـط والتفتيـش انتقـال المحقق إلى مسرح جريمة التزوير الإلكتروني، واسـترجاع ومعالجـة الدليل المادي، أما اكتشـاف المعلومات فيشـمل وصول المحقق إلى مصـادر المعلومات من غير المـواد المضبوطة مثل سـجلات الملفات وقواعد

البيانـات، بهـدف تحديد ومعالجة المعلومـات التي قد تثبـت أو تنفي التهمة. وقد تتطلب القضية تفتيشاً وضبطاً بالإضافة إلى اكتشاف المعلومات،ويمكن تلخيص مراحل التفتيش والضبط واكتشاف المعلومات في الشكلين التاليين:

أما الشكل رقم (٥) فيوضح مراحل اكتشاف المعلومات:

(أ)	(ب)	(ج)	(د)	(هـ)	(و)
معالجة الأدلة	الذهاب وتأمين مسرح الجريمة	توثيق وضع مسرح الجريمة	البحث عن أدلة	استرجاع الأدلة	معالجة الأدلة

المصدر : (www:http://online.securityfocus.com/infocus/124/8-4-2009).

الشكل رقم (٤) مراحل التفتيش والضبط

وهناك مراحل مشـتركة بين الشـكلين، فالشـكل الأول أكثر تعمقاً لأن

(أ)	(د)	(و)
تكوين الخطة	البحث عن الأدلة	معالجة الأدلة

المصدر : (www:http://online.securityfocus.com/infocus/124/8-4-2009).

الشكل رقم (٥) مراحل اكتشاف المعلومات

التفتيش والضبط يتعامل مع الدليل المادي الموجود في مسرح الجريمة كأجهزة الحاسوب والعناصر المكونة له والوسائط (حسن، ١٩٩٩م، ص٢١٩) وهي مهمـة المحقق الجنائي التقليدي، أما اسـترجاع الأدلـة ومعالجتها فهي مهمة المحقق الفني.

أولاً: طرق اكتشاف جرائم التزوير الإلكتروني

تواجه طرق اكتشاف التزوير الإلكتروني صعوبات متعددة شأنها شأن طرق اكتشاف الجرائم الإلكترونية، حيث تستدعي هذه الطرق في المقام الأول اكتشاف جريمة التزوير الإلكتروني، ومحلها، وبيئتها، ومن ثم البلاغ عن جريمة التزوير الإلكتروني، وأخذ إذن الجهات المختصة قبل القيام بالمعاينة والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الإلكتروني بالطرق الفنية، ومن ثم إجراء التحريات، وبعد تحديد المشتبه به الذي تقوم دلائل قوية على ارتكابه أو ارتكاب الجريمة الإلكترونية من جهازه أو موقعه الإلكتروني في مرحلة جمع الاستدلالات، حيث يتم تحديد الموقع المشتبه به، وصاحب الجهاز، ويتم سؤاله، وإجراء المعاينة والتفتيش الدقيق بمساعدة المحقق الفني الذي يتولى البحث عن الدليل الإلكتروني وتقييمه، وإعداد التقرير الفني الجنائي، وتقديمه لجهة التحقيق تمهيداً للمحاكمة في مرحلة جمع الاستدلالات، وفي الوقت ذاته التقاط القرائن والأدلة المساندة التي تثبت إدانته بارتكاب جريمة التزوير الإلكتروني.

١ ـ دور المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

يتضمن دور المحقق عمليات تلقي البلاغ، وإجراء التحريات، والمعاينة، والتفتيش، والسؤال في مرحلة جمع الاستدلالات قبل الاستجواب، وإقامة الدعوى، كما يتضح مما يلي:

أ ـ البلاغ عن جرائم التزوير الإلكتروني

ـ تقديم البلاغ

يعد البلاغ هو المشكلة الحقيقية التي تواجه الجريمة الإلكترونية، فغالبية المنظمات تخشى من الإبلاغ لكي لا تفقد ثقة عملائها، ومن ثم يفلت مرتكب الجريمة الإلكترونية بفعلته نتيجة إحجام المنظمات والشركات والمؤسسات المالية عن الإبلاغ خوفاً على سمعتها، حيث تفضل هذه المرافق عدم إبلاغ السلطات المختصة للمحافظة على ثقة عملائها أكثر من اهتمامها بكشف الجريمة ويفضلون الترضية المالية لعملائهم ومنحهم الأموال التي سلبت منهم نتيجة الاختراق والتعدي (الهيتي، ٢٠٠٥م، ص٢١٨).

والبلاغ: «إجراء يصدر عن الغير أو عن المجني عليه في غير الجرائم التي يتوقف تحريك الدعوى الجنائية فيها على شكوى، بهدف إحاطة المختص علماً بوقوع جريمة أو واقعة مخالفة للقانون» (الصيفي، ٢٠٠٢م، ص٢٢٥).

والأصل أن يقبل رجل الضبط الجنائي جميع البلاغات والشكاوى التي ترد إليه بشأن الجرائم بغض النظر عن شخصية الشاكي أو صفته، فقد يكون المتقدم بالبلاغ أو الشكوى الجاني أو المجني عليه، أو أي فرد من عامة الناس (سلامة، ١٩٩١م، ج١، ص٤٧٤).

وفي هذا الصدد نصت المادة (٢٧) من نظام الإجراءات الجزائية السعودي على أن: «على رجال الضبط الجنائي كل حسب اختصاصه أن يقبلوا البلاغات والشكاوى التي ترد إليهم في جميع الجرائم، وأن يقوموا بفحصها وجمع المعلومات المتعلقة بها في محضر موقع عليه منهم... ».

و«الإبلاغ عن الوقائع الجنائية حق لكل إنسان، بل هو واجب مفروض عليه، فلا تصح معاقبته واقتضاء التعويض منه إلا إذا كان قد تعمد الكذب

فيه وتوافرت في شأنه أركان جريمة البلاغ الكاذب» (سرور، ١٩٨٥م، ص٤٧٩).

وتتضمن الإجراءات قيام رجل الضبط الجنائي بتدوين البلاغات والشكاوى بجميع تفاصيلها وجمع المعلومات وتدوين ملخصها وتاريخها في محضر رسمي، ومن ثم إرسالها إلى الجهة المختصة (هيئة التحقيق والادعاء العام في المملكة العربية السعودية)، وأن يبلغها بالبلاغ أو الشكوى فور ورودها (طنطاوي، ١٩٩٧م، ص٢٦٣)، وهذا ما تنص عليه المادة (٢٧) من نظام الإجراءات الجزائية السعودي المشار إليها أعلاه.

والبلاغ هو أول خطوة في إجراءات التحقيق في جرائم التزوير الإلكتروني التي تبدأ من خلال:

١ـ تلقي جهات التحقيق معلومات أمنية تشير إلى ممارسة شخص معروف أو غير معروف أنشطة التزوير المعلوماتي بتغيير الوثائق والمستندات، أو المحررات الإلكترونية، أو الاستيلاء على التوقيعات الإلكترونية في مكان معروف وعلى أجهزة محددة ووفق لغات برمجية معلومة.

٢ ـ ضبط شخص وبحيازته أموال مشبوهة أو محررات غير خاصة به، أو بطاقات ائتمان مزورة، أو بطاقات تعريف مشبوهة.

٣ ـ بلاغ يصل إلى علم جهة التحقيق من متضرر يفيد بوقوع تلاعب أو ممارسات خاطئة في حقه أو في حق آخرين، سواء كان ذلك في شكل عجز مالي نتيجة تزوير بطاقات الائتمان، أو سرقة أرقامها، أو ضياع حقوق أو تغييرات في الودائع (دون أن يدرك أن ذلك من جرائم الحاسب الآلي أم لا).

٤ ـ توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الإنترنت.

٥ـ توفر معلومات عن وقوع عمليات اعتراض أو قرصنة فضائية للمعلومات (Douglass & Burger, 1992: p. 216).

ـ مسرح جريمة الحاسب الآلي

بعد تلقي البلاغ عن جريمة التزوير الإلكتروني، يتم اتخاذ إجراءات التحرك إلى مسرح الجريمة، وذلك بعد الحصول على إذن من الجهات المختصة سواء كان هذا الإذن يصدر من الجهات الإدارية، أو الشرطة أو النيابة أو القضاء أو المعامل الجنائية، لكي يتم استيفاء الشروط القانونية اللازمة (عبد المطلب، ٢٠٠٧م، ص٥٣٣).

وقبل الوصول لمسرح الجريمة يجب اتخاذ الاحتياطات التالية (البشرى، ٢٠٠٠م، ص٣٥٦):

١ ـ توفير معلومات مسبقة عن مكان الجريمة، ونوعية وعدد الأجهزة المتوقع مداهمتها وشبكاتها.

٢ـ إعداد خريطة للموقع الذي تتم الإغارة عليه وتفاصيل المبنى أو الطابق من المبنى موضع البلاغ، وتحديد مواقع الأجهزة والخزائن والملفات عن طريق المصادر السرية.

٣ ـ تحديد عدد وأنواع الأجهزة المحتمل تورطها في ارتكاب جريمة التزوير لتحديد إمكانات التعامل معها فنياً من حيث الضبط والتأمين وحفظ المعلومات.

٤ـ الحصول على الاحتياجات الضرورية من أجهزة وبرامج صعبة ومرنة للاستعانة بها في الفحص والتشغيل.

٥ ـ إعـداد قائمـة بالاحتياجات العامة لجميع الغارات مسـبقاً ومراجعة توافر احتياجات كل حالة على حدة.

٦ ـ إعـداد فريـق التفتيـش مـن المتخصصـين وفـق قائمة تحدد الأسـماء والاختصاصات والمهام الموكولة بدقة.

٧ ـ إخطـار أعضـاء الفريـق قبـل التحرك لمـسرح الجريمة بوقـت كافٍ لتمكينهم من إعداد خططهم الخاصة.

٨ ـ كتابـة بيانات بالمهـام المطلوبة من كل عضو في الفريق وتوزيعها على الجميع لضمان الإنجاز مع عدم التداخل.

٩ـ إعـداد خطـة هجـوم واضحـة ومفهومـة للجميـع، مـع تفصيلهـا بالرسـومات ومراجعتهـا مـع أعضاء الفريـق قبل التحـرك لمسرح ارتـكاب الجريمة مع مراعاة الحالة، والرسـالة، والتنفيذ، والمداخل والمخارج، والاتصالات.

١٠ـ الاحتفاظ بسرية الغارة حتى نهاية التفتيش: لتلافي إتلاف المعلومات التي يتم البحث عنها من قبل المتهمين أو المتورطين.

١١ ـ تأمين التيار الكهربائي لكي لا يتم التلاعب أو التخريب عن طريق قطع التيار الكهربائي.

أمـا بعـد الوصول لمـسرح جريمة ارتـكاب التزوير الإلكـتروني (موقع المخترق) فيتم اتخاذ الإجراءات التالية (حجازي، ٢٠٠٥م، ص ٦٣-٦٦):

١ـ تحديـد أجهـزة الحاسـب الآلي الموجـودة في مـكان المعاينـة، وتحديد مواقعها بأسرع وقت ممكن، وفي حالة وجود شـبكة اتصالات يجب البحـث عن خـادم الملفات، بهدف تعطيل الاتصـالات لمنع تخريب

الأدلـة الموجودة أو محوهـا، مع تصوير الأجهـزة الموجودة، وبصفة خاصة أجزاؤها الخلفية.

٢ ـ وضـع حراسـة كافية على مـكان المعاينة، ومراقبـة التحركات داخل مسرح الجريمة، ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة مع إبطال مفعول أجهزة الهاتف المتحرك التي قد تسـاعد عن طريق تقنيـة معينـة عـلى تدمير أدلـة جريمة التزويـر المعلوماتي متـى ما تم توصيلها بالأجهزة محل المعاينة.

٣ ـ ملاحظـة الطريقـة المعد بهـا النظـام المعلوماتي والآثار التـي يخلفها، ومعرفـة السـجلات الإلكترونية التي تزود بها شـبكات المعلومات لمعرفـة موقع الاتصـال ونوع الجهاز المتصل عـن طريق الدخول إلى النظـام أو الموقع أو الدخول معه في حوار، وبروتوكولات الاتصال عـبر الإنترنـت وإن تعلقـت الجريمـة بهـذه الشـبكة والتـي تعرف اختصـاراً بـ (IP). ويتعين أيضاً ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام لكي يمكن تحليل البيانات ومقارنتها والوصول منها إلى دليل عند عرض الأمر على القضاء.

٤ ـ عـدم نقل المواد المعلوماتية خارج مـسرح الجريمة إلا بعد التأكد من خلـو المحيط الخارجي للحاسـب من مجـالات القوى المغناطيسـية (الممـرات المغناطيسـية) التـي قـد تتسـبب في محـو البيانـات، ولـن يتأتـى ذلك إلا عـن طريق خـبراء الحاسـب الآلي، ولذلك يجب أن يتضمـن الفريق الذي يتـولى ضبط وتحريز الأدلة عـلى اثنين أو أكثر مـن خبراء الحاسـب الآلي لضبـط وإدخال المعلومـات المضبوطة في الحاسب، وتصنيف الأدلة وتحريزها في صناديق، ووضع العلامات الدالـة عليها، ويقوم الفريـق بنقل أجهزة الحاسـب الآلي المضبوطة

بعد استكمال إجراءات الرسم والتصوير، مع مراعاة تنوع خبراء الحاسب الآلي ما بين محققين وآخرين مدربين على التعامل مع الأدلة الرقمية وتقييمها.

٥ـ التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وشرائط وأقراص ممغنطة وغير سليمة أو محطمة ورفع البصمات التي قد توجد عليها، والتحفظ على مستندات الإدخال والمخرجات الورقية لجهاز الحاسب الآلي، والتي قد تكون ذات صلة بالجريمة.

٦ـ قصر المعاينة على المحققين الجنائيين والفنيين أصحاب الخبرة والدراية والكفاءة العلمية والفنية في مجال الحاسبات والشبكات واسترجاع المعلومات من الذين تلقوا تدريبات متخصصة في ذلك، ويفضل أن يضم فريق المعاينة أشخاصاً من مأموري الضبط القضائي والمحققين للحصول على الاستدلالات أو تحليل الأدلة القائمة وسؤال الشهود، ويضمن كذلك آخرين للرسم والتصوير، لرسم كروكي لمسرح الجريمة، وتحديد مواقع الأجهزة والملفات والأشخاص، ولتفتيش الموجودين في مسرح الجريمة.

ـ أنواع الأدلة المطلوبة في جرائم التزوير الإلكتروني

الدليل بصفة عامة هو «الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم» (سلامة، ١٩٩١م، ج٢، ص١٢٤).

وجريمة التزوير المعلوماتي شأنها شأن أية جريمة وتمر بمراحل التفكير والتخطيط والتحضير، فالتنفيذ، ومن ثم التخلص من معالج الجريمة وإخفاء وطمس أدلتها من خلال عمليات الإتلاف أو الإزالة للملفات والملفات المساعدة والبرامج التي استخدمت في تيسير عمليات الاختراق والتعدي.

ويمكـن إثبات جريمـة التزوير المعلوماتي بالأدلة المعروفـة، كاعتراف الجاني بارتكابها، فالاعتراف سـيد الأدلة، وشـهادة الشـهود أيضـاً، والقرائن التي تدعـم الأدلة وشـهادة الشـهود، كـما أن هناك بعـض الآثار الماديـة المهمة في إثبـات ارتكاب جريمة التزوير المعلومـاتي، والتي يأتي في مقدمتها (البشرى، ٢٠٠٠م، ص ٣٦١-٣٦٤):

١ـ الأوراق: هـي الأوراق الناتجـة عـن طباعـة المعلومـات لأغـراض المراجعة، أو التأكد من الشـكل العام للمستند أو الرسالة أو المحرر أو الصور أو الرسـومات التي تم تزويرها إلكترونياً، أو الورقة التي تتضمـن التوقيع الإلكتروني الذي تم الاسـتيلاء على منظومته، فقد يقوم الجاني بطباعتها للتأكد من نجاحه، وسواء كانت هذه الأوراق مسـودات تتضمن التغيير المبدئي، أو أوراق تالفة، أو أوراق أصلية أو أوراق أساسـية محفوظة في الملفات العادية، فإنها تعد بمثابة دليل مـادي على ارتكاب الجريمة، ولذلك يجب على المحقق تفتيش سـلة المهمـلات بحثـاً عـن هـذه الأوراق، وفي الوقـت نفسـه البحث في السـجلات والملفـات الموجودة في مـكان ارتكاب جريمـة التزوير المعلوماتية.

٢ ـ جهاز الحاسـب الآلي وملحقاته: يشـير وجود جهاز الحاسـب الآلي وملحقاته كالطابعة والماسـح الضوئي وأجهزة الاتصالات المرتبطة به إلى إمكانية ارتكاب جريمة التزوير المعلوماتي.

٣ ـ أقـراص الليـزر: قـد تحتوي الأقراص على نسـخ من برامـج الاختراق والتعـدي، والبرامـج المسـاعدة عـلى ذلـك وبرامج نشر الفيروسـات وغيرها، لذلك تعد دليلاً مادياً في حالة وجود هذه المحتويات بداخلها.

٤ ـ الشرائط الممغنطة: تستخدم للحفظ الاحتياطي، وهذا يعني أيضاً إمكانية احتوائها على برامج الاختراق والتعدي والفيروسات وغيرها من البرامج التي تساعد في ارتكاب جرائم التزوير المعلوماتي.

٥ ـ المودم: يعبر وجود المودم عن إمكانية اتصال أجهزة الحاسب الآلي ببعضها، وقد تطورت أنواعه، ومنها ما له القدرة على إرسال الفاكس والرد على المكالمات الهاتفية، وتبادل البيانات وتعديلها، ويمكن من خلاله الاتصال بالحاسب وتدمير الملفات والبيانات.

٦ ـ الطابعات: تتعدد أنواعها، وتستخدم في طبع المحررات بعد تزويرها للتعرف على مدى مطابقتها.

٧ ـ البطاقات: تستخدم في أجهزة الحاسب الآلي الصغيرة، وتأخذ شكل البطاقات الائتمانية.

٨ ـ البرامج اللينة والمراشد: تفيد المراشد المصاحبة للحاسب الآلي في التعرف على الجهاز والبرامج المستعملة.

٩ ـ البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستخدمة في إعداد تلك البطاقات تعد قرائن للإثبات في جرائم تزوير بطاقات الائتمان.

وبالرغم من أهمية الأدلة، إلا أن رأي الفقه الجنائي قد انقسم حول جمعها في مرحلة التحريات، حيث يذهب الرأي الراجح لدى شراح القانون إلى عدم إمكان استخلاص الدليل من مرحلة جمع الاستدلالات؛ «لأنه لا يمكن أن ينتج عنها الدليل الكامل الذي تطمئن إليه المحكمة؛ لأن مرحلة

جمع الاستدلالات لا تتوافر فيها الضمانات التي تتطلب نشأة الدليل الجنائي، فبداية تكوين الدليل لا تبدأ إلا مع مرحلة التحقيق الابتدائي، ولا يكتمل هذا الدليل إلا في مرحلة المحاكمة وبعد استيفاء الشروط القانونية المطلوبة» (أحمد، ١٩٨٧م، ص٣٤٥).

ويذهب رأي آخر إلى: «جواز استخلاص الدليل من مرحلة جمع الاستدلالات؛ لأن الأدلة في نظر المنظم وفي نظر القاضي متساوية ما دام مصدرها مشروعاً» (طنطاوي، ١٩٩٧م، ص١٩٩).

ويؤيد الباحث الرأي الثاني الذي يفيد بجواز استخلاص الدليل في مرحلة جمع الاستدلالات في حالة الجريمة الإلكترونية بصفة عامة، وجريمة التزوير الإلكتروني بصفة خاصة؛ لأن إجراءات الاستدلال من حيث المبدأ تسعى إلى كشف الغموض والتوصل إلى أدلة وقرائن تساعد جهة التحقيق على أداء عملها، فالدليل الذي تبحث عنه جهة الاستدلال هو مجرد وسيلة أو مفتاح يستفيد منه المحقق في البحث عن الحقيقة والوصول إلى أدلة تدين المشتبه به، وعلى الرغم من ذلك فقد تنتج خلال هذه المرحلة أدلة تبرر قيام سلطة الاتهام برفع الدعوى بناءً عليها وتكون كافية لتوجيه الاتهام لدرجة الإدانة، ومع ذلك يختلف دليل الاتهام عن دليل الإدانة، فإذا كان يكفي لرفع الدعوى على المتهم مجرد الظن والاحتمال بأنه ارتكب الجريمة الإلكترونية وذلك بتحديد موقع الاختراق والتعدي من خلال معاينة الحاسب الآلي الذي تعرض لذلك لتحديد الـ (IP) للمخترق ومن ثم تحديد موقعه باستخدام تقنيات التتبع، فإن دليل الإدانة يجب أن يبنى على الجزم واليقين وذلك من خلال مداهمة موقع الجهاز المشتبه به، واستخدام تقنيات استرجاع المعلومات المحذوفة والمتلفة كدليل آخر معضد للدليل الأول، ولكن يمكن

القول انه في الغالب لا يكفي ما يحتويه محضر جمع الاستدلالات لكي يؤسس القاضي حكمه بالإدانة، بل لابد أن يجري تحقيقاً لاستخلاص دليل الإدانة من إجراءات الاستدلال التي تمت.

ب ـ التحريات في جرائم التزوير الإلكتروني

التحري: «إجراء يباشره رجل الضبط الجنائي أو مرؤوسيه تجاه شخص يشتبه في ارتكابه جريمة وقعت بالفعل بهدف الوقوف على ملابسات وقوعها وتحديد شخصية مرتكبها» (الصيفي، ٢٠٠٢م، ص٢٢٦).

والتحري لا يقتصر على التحقق من صحة الوقائع المبلغة لرجل الضبط الجنائي ضمن الشكوى أو البلاغ، ولكن يمتد ليشمل جمع كافة القرائن والأدلة التي تشير إلى حصول الواقعة أو نفي وقوعها (طنطاوي، ١٩٩٧م، ص٢٦٥)، حيث حددت المادة (٢٤) من نظام الإجراءات الجزائية السعودي المسؤولين عن إجراءات البحث والتحري، بقولها: «رجال الضبط الجنائي هم الأشخاص الذين يقومون بالبحث عن مرتكبي الجرائم وضبطهم وجمع المعلومات والأدلة اللازمة للتحقيق وتوجيه الاتهام».

ولكي تنتج التحريات آثارها الإجرائية يجب أن تتسم بما يلي:

أ ـ أن تتعلق بجريمة ارتكبت فعلاً؛ لأن إذن جهة التحقيق الذي يصدر استناداً عليها هو إجراء من إجراءات التحقيق، ولا يصدر عن جريمة لم تقع أو محتملة، فلصدور إذن التفتيش يجب إجراء تحريات جدية تشير بوضوح إلى ارتكاب شخص معين جريمة تزوير معلوماتية وفق دلائل وإمارات قوية تحدده وتنسب الجريمة إليه دون غيره تجنباً للمساس بحريته وحرمة مسكنه.

ب ـ استخدام الوسائل المشروعة في إجراء التحريات، وعلى ذلك فلا يجوز استراق السمع أو التجسس من ثقوب الأبواب.

جـ ـ عدم التدخل في جلب الجريمة بالتحريض عليها وذلك لكي يسهل على رجل الضبط الجنائي اكتشافها وتحديد مرتكبها، لكونه على علم مسبق بها (الموجان، ٢٠٠٣م، ص ٤١-٤٢).

د ـ التقيد بقواعد الاختصاص النوعي والمكاني، لكي تكون إجراءاته منسجمة مع ما تنص عليه التعليمات، فلا تبطل التحريات.

هـ ـ كفاية التحريات وجديتها بحيث تتضمن معلومات وافية وصحيحة وكاملة وغير مغلوطة، بحيث يتخذها المحقق أساساً لتحقيقه فيما بعد (الصيفي، ٢٠٠٢م، ص٢٢٨).

وترجع أهمية التحريات إلى دورها في التحقق من صحة ما ورد في البلاغات والشكاوى، ففي الجريمة الإلكترونية لا يمكن إجراء التحريات إلا بعد تقديم الجهة المتضررة لبلاغ يفيد بتعرضها لذلك، أو تقديم شخص بلاغ يفيد بالسحب من رصيده وشراء أغراض لم يشترها، أو قيام فرد أو شركة باكتشاف وجود عمالة مخالفة على كفالتها دون علمها نتيجة استخدام توقيعه الإلكتروني في تزوير طلبات الاستقدام، ويفضل التحقق من ذلك على سبيل التخفي لكي لا يتخذ الجناة حذرهم، وقد يكتشف رجل الضبط الجنائي كذب البلاغ أو أن الشكوى كيدية، ومن ثم يوفر الجهود في عدم إشغال جهات التحقيق فيما لا جدوى منه، كما أن بعض إجراءات التحقيق لا يمكن مباشرتها إلا إذا توافرت تحريات جدية أمام سلطة التحقيق لكي تأذن بها، فلا يمكن إصدار إذن بتفتيش المتهم أو مسكنه في الجريمة الإلكترونية إلا بعد توافر تحريات جدية على ارتكابه الجريمة أو الواقعة

الإجرامية (طنطاوي، ١٩٩٧م، ص٢٦٦-٢٦٧)، وذلك باستخدام تقنيات التتبع والتأكد من وقوع الاختراق والتعدي على جهاز المجني عليه أو موقعه الإلكتروني سواء كان فرداً أو هيئة تصديقات أو نحوهما، أو من خلال مخاطبة الجهات المشرفة (كمركز المعلومات) في المنظمات الأمنية بالجوازات والأمن العام والأحوال المدنية باعتبار العاملين يحملون أرقاماً كودية تحدد هوياتهم وهذه غالباً في المنظمات التي لديها عدد كبير من المستخدمين وفي مناطق مختلفة.

جـ ـ المعاينة في جرائم التزوير الإلكتروني

المعاينة هي: «المناظرة بالعين لمكان أو شخص أو شيء»، ويقصد بها في مجال التحقيق الجنائي «وصف وفحص مكان الجريمة، وذلك بهدف تحديد صفات المكان وما يحويه من أشخاص وأشياء وكشف ما يحويه من آثار أو أدلة جنائية» (كامل، ١٩٩٩م، ص٢٤٦).

والمعاينة كإجراء لها مدلولان:

أ ـ الأول: يتعلق بذات الجريمة، وما يتصل بها وجوداً وعدماً، زماناً ومكاناً.

ب ـ الثاني: يتعلق بشخص الجاني أو المجني عليه أو الشهود.

فالمدلول الأول ذو طبيعة موضوعية بمعنى أنه يتناول الفعل الإجرامي المرتكب وزمان ومكان وقوع الجريمة، أما الثاني فيغلب عليه الطبيعة الشخصية لأنه يتناول الجاني والمجني عليه والشهود (الردادي، ١٩٨٩م، ص١٠-١١).

وترجع أهمية المعاينة في جريمة التزوير الإلكتروني إلى أنها وسيلة للكشف عن الآثار المادية المتخلفة في مسرح الجريمة، سواء أكان الحادث

عمدياً أو غير عمدي أو عرضياً، ومن ثم اتخاذ الإجراءات اللازمة حيالها، كما أن المعاينة:

أ ـ الوسيلة الأساسية للتحقق من وقوع الجريمة، والتعرف على ما إذا كانت الجريمة عمدية أو عرضية من خلال مناظرة الآثار المادية المتخلفة في مسرح الجريمة من أجهزة حاسوب وتوصيلات وملحقاتها والأدوات المستخدمة.

ب ـ وسيلة تكوين الفكرة الأولى عن كيفية ارتكاب الجريمة، ومحاولة إخفاء معالم الجريمة، وأسلوب الجريمة والآلات والأدوات المستخدمة وعدد الجناة (كامل، ١٩٩٩م، ص ٢٤٦-٢٤٧).

جـ ـ تسهم في الكشف عن الأدلة والآثار المادية التي تقود إلى التعرف على ظروف الجريمة وأسبابها.

د ـ تنقل للمحكمة صورة حية عن مسرح الجريمة، وكيفية وقوعها، ومن ثم معرفة مرتكبها في حالة التعمد (الحبشي، ١٩٩٠م، ص٢).

هـ ـ تساعد في معرفة وتحديد الأسلوب الإجرامي المتبع والآلات المستخدمة، وطريقة دخول وخروج الجاني، وعلاقة المتهم بموقع الحادث وظروفه وملابساته (الملا، ١٩٩٤م، ص٧٨).

و ـ المعاينة تسهم في الاستدلال على شهود الحادث بتحديد الأشخاص الذين تقع محال أعمالهم أو مساكنهم بجوار موقع الجريمة أو بالقرب منه، وبصفة خاصة الذين يمكنهم مشاهدة الموقع بوضوح، من خلال أوقات تواجدهم وإمكانية مشاهدتهم لموقع الحادث.

ز ـ أنها تمكن المحقق من استيفاء العديد من الحقائق الأساسية عن الجريمة مثل وقت وقوعها، والظروف المحيطة بها، مما يجعله أكثر قدرة على

استنتاج ما إذا كانت الواقعة والحادث عمدياً أم غير عمدي أو عرضياً، مع الربط بالأدلة اللازمة في حالة الحادث العمدي مثل العبث الشديد بمحتويات موقع الجريمة نتيجة الصراع أو محاولة الضحية الفرار.

ح ـ تساعد المعاينة في وضع وإرساء خطة البحث الجنائي في الحادث العمدي من خلال النتائج المستخلصة من المعاينة، وذلك بتحويل الحادث إلى الشرطة لوجود شبهة جنائية، ومن ثم تبدأ الشرطة في أعمال البحث والتحري والقبض والتفتيش والاستعانة بالخبراء والفنيين لرفع وتحريز الآثار المادية وتحليلها بالطرق الكيميائية المتطورة.

ط ـ تسهم المعاينة في رد الحق العام والحق الخاص إلى أصحابها.

ـ الحق الخاص: يحكم فيه القاضي بعد إظهار الحقائق وتصديق الشهود والمتضررين المطالبين برد حقوقهم شرعاً من خلال إدراج تلك المطالبات في خطاب رسمي موجه إلى رئيس المحكمة مرفق به جميع الأوراق اللازمة لإصدار الحكم. وتحال مطالبات العمال إلى مكتب العمل والعمال لاستكمال إجراءات التعويض المناسب.

ـ الحق العام: يطالب بإقامته ضد من يرتكب فعلاً يمس الحق العام ويلحق به الضرر عند مخالفة النظم الإدارية أو الوقائية حسب النظم الأمنية المتبعة واللوائح التنفيذية، أو التعليمات المنظمة لذلك (كامل، ١٩٩٩م، ص٢٤٧).

وتتطلب المعاينة الانتقال الفوري لمسرح جريمة التزوير الإلكتروني من قبل رجل الضبط الجنائي للحيلولة دون العبث بمعالم مسرح الجريمة

وتغيير العلاقات المكانية، أو إتلاف الأدلة المادية أو إخفائها، أو تغيير معالم مسرح الجريمة، أو إخفاء المسروقات وإزالة الآثار المادية بمسرح الجريمة (طنطاوي، ١٩٩٧م، ص٧٠)، وفي هذا الصدد نصت المادة (٧٩) من نظام الإجراءات الجزائية على ما يلي: «ينتقل المحقق ـ عند الاقتضاء ـ فور إبلاغه بوقوع جريمة داخلة في اختصاصه إلى مكان وقوعها لإجراء المعاينة اللازمة قبل زوالها أو طمس معالمها أو تغييرها».

ويرى الباحث أنه لابد من تدريب المحقق في الجرائم الإلكترونية بصفة عامة، وجرائم التزوير الإلكتروني بصفة خاصة على الأقل على تأمين الأجهزة من خلال إيقافها عن العمل،وفصل التيار الكهربائي عنها، فور الوصول وكذلك تدريبه على الأقل كيفية التعامل مع خادم الملفات بإيقاف الاتصالات السلكية واللاسلكية، لتفويت فرصة إتلاف الأدلة الإلكترونية من قبل الجاني، ومن الأفضل اصطحاب المحقق الفني مع المحقق الجنائي (التقليدي).

د ـ التفتيش

بعد انتقال المحقق وإجراء المعاينة اللازمة لمسرح جريمة التزوير الإلكتروني، يجب عليه تفتيش المكان، وكذلك تفتيش الموجودين به حسب ما ينص عليه أمر التفتيش الصادر من السلطة المختصة (مرسي، د٠ت، ص٧٤٣)، حيث نصت المادة (٤١) من نظام الإجراءات الجزائية السعودي على ما يلي: «لا يجوز لرجل الضبط الجنائي الدخول في أي محل مسكون أو تفتيشه إلا في الأحوال المنصوص عليها نظاماً، بأمر مسبب من هيئة التحقيق والادعاء العام، وما عدا المساكن فيكتفى في تفتيشها بإذن مسبب من المحقق. وإذا رفض صاحب المسكن أو شاغله تمكين رجل الضبط الجنائي

مـن الدخـول أو قـاوم دخوله، جاز لـه أن يتخذ الوسـائل اللازمة المشروعة لدخول المسـكن بحسـب مـا تقضيه الحال. ويجـوز دخول المسـكن في حالة طلب المساعدة من الداخل، أو حدوث هدم أو غرق أو حريق أو نحو ذلك، أو دخـول معتـد أثناء مطاردتـه للقبض عليه». والاسـتثناء في هذا الصدد في حالة طلب المساعدة فقط من الداخل، كما أوضحت المادة السابقة.

والهـدف مـن التفتيـش في جرائـم التزويـر الإلكتروني هـو البحث عن الأدلـة الماديـة لتحريزها كأسـطوانات وأقـراص الليزر، وتقنيـات الاتصال الملحقة بالحاسـب الآلي، والطابعات والمواسـح الضوئية، وأجهزة التخزين، والأوراق الموجودة في مسرح الجريمة، لاحتمال أن تكون إحداها دليلاً مادياً على اسـتخدامها أو اسـتخدام البرامج الموجـودة عليها في عمليـات التزوير الإلكتروني (الشاذلي وعفيفي، ٢٠٠٣م، ص٣٧٣).

هـ ـ الاستجواب في جرائم التزوير الإلكتروني

ـ مفهوم الاستجواب وخطواته التمهيدية

الاسـتجواب هو توجيه الأسـئلة التفصيلية لمن يشـتبه ارتكابه الجريمة وتوجد أدلة أو قرائن قوية على ارتكابها دون غيره، حيث يهدف الاستجواب إلى إثبات التهمة أو محاولة الإيقاع بالمتهم (سرور، ١٩٨٥م، ص٤٨٠).

والاسـتجواب في جرائـم المعلوماتيـة بصفـة عامـة، وجرائـم التزويـر المعلومـاتي بصفـة خاصة يحتـاج إلى بيوت خـبرة متخصصة في هـذا المجال، وفي ضـوء عدم إمكانية قيام أجهزة العدالة عن دورها في هذا المجال، فيجب الاستعانة بأهل الخبرة أو إعادة تأهيل منسوبي العدالة الجنائية بحيث يتمكنوا من التحقيق في جرائم المعلوماتية (Stephenson 1999: p.73).

وقبل استجواب المتهم في جرائم التزوير الإلكتروني يجب مراعاة الخطوات التالية (United Nations, 1999):

١ـ تبادل المعلومات بين المحقق وخبير الحاسب الآلي، لكي يشرح المحقق للخبير أهمية ترتيب المتهمين وطريقة توجيه الأسئلة إليهم، وفي الوقت نفسه يشرح الخبير للمحقق الأبعاد التقنية والنقاط التي يجب استيضاحها من المتهمين.

٢ ـ حصر النقاط المطلوب استيضاحها من قبل الخبير والمحقق، وترتيبها من قبل المحقق.

٣ ـ تدوين المحقق كافة المصطلحات العلمية مع بيان معانيها للاستفادة منها عند الضرورة.

٤ ـ وضع خطة التحقيق في ضوء المعطيات التي يراها المحقق.

٥ ـ استجواب المتهمين في حضور الخبير، الذي يجوز له توجيه الأسئلة الفرعية أثناء الاتفاق وفق كيفية يتفق عليها مع المحقق، ويفضل أن يكتب الخبير السؤال الفرعي أمام المحقق مع تحديد وقت توجيه السؤال.

٦ ـ مراعاة القوانين الوطنية فيما يتصل بسلطة التحقيق، وتشكيل لجنة تضم في عضويتها الخبرات الفنية في حالة عدم إمكان الاستعانة بخبير من خارج أقسام التحقيقات.

٧ ـ مراعاة التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالمتهم، فالمجرم المتخصص في الحاسب الآلي يحتفظ بمعلوماته وخططه في الحاسب الآلي أو على أقراص.

٨ ـ أهم القواعد التي يجب مراعاتها لضمان نجاح التحقيق مع مرتكبي جرائم التزوير الإلكترونية:

أ ـ تفادي تبديد الوقت في التحقيق حول جرائم الحاسب الآلي التي لا يمكن اكتشافها، أو التي تم تدمير أدلة إثباتها.

ب ـ مراعاة التعامل الجيد بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المتضررة من الجريمة للاستفادة منهم.

جـ ـ التركيز في البحث عن البرامج اللينة اللازمة لكشف البيانات المختزنة ووضع التدابير للمحافظة عليها وحسن استخدامها.

د ـ مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإلكتروني وغير ذلك من الحقوق الخاصة لكي لا تضار البينة التي يحصل عليها المحقق بعدم المشروعية.

هـ ـ العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي وملحقاتها وبرامجها اللينة.

و ـ مراعاة حفظ الأدلة الإلكترونية بالطرق المناسبة لكل حالة حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها، فأي تعديل على الأدلة قد ينهي القضية لصالح المتهم عملاً بمبدأ الشك يفسر لصالح المتهم.

ـ الاستعانة بالقرائن المادية

تسهم القرائن المادية في كشف الغموض، وهي تعتمد على الاستنباط والتحليل الذي يعتمد على أشياء ثابتة من خلال استخلاص معناها ودلالتها، حيث يسعى رجل الضبط الجنائي لجمع القرائن المادية التي تفيد في كشف الحقيقة، وذلك من خلال اتخاذ الإجراءات اللازمة لذلك (سرور،

١٩٨٥م، ص٤٨٠). وغالباً ما يحتاج رجل الضبط الجنائي هنا إلى تدخل المختصين وأهل الخبرة، لكي يتعاملوا مع القرائن المادية بصفة عامة والقرائن المادية في جرائم المعلوماتية بصفة خاصة بالطريقة التي يضمن الاستفادة منها (الردادي، ١٩٨٩م، ص٩٤). وفي هذا الصدد تنص المادة (٢٧) من نظام الإجراءات الجزائية السعودي على أنه: «... ويجب أن ينتقل رجل الضبط الجنائي بنفسه إلى محل الحادث للمحافظة عليه، وضبط كل ما يتعلق بالجريمة، والمحافظة على أدلتها، والقيام بالإجراءات التي تقتضيها الحال، وعليه أن يثبت جميع هذه الإجراءات في المحضر الخاص بذلك».

ـ الاستعانة بالخبراء

يقصد بالخبرة: «مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوفر لديه» (طنطاوي، ١٩٩٧م، ص٢٩٣).

الاستعانة بالخبرة في مرحلة التحقيق أمر تأخذ به غالبية القوانين والأنظمة الإجرائية، بهدف الاستفادة من عنصر الخبرة في تقرير الأدلة ودعم جدية التحريات. وقد نصت المادة (٢٨) من نظام الإجراءات الجزائية على أن: «لرجال الضبط الجنائي في أثناء جمع المعلومات أن يستمعوا إلى أقوال من لديهم معلومات عن الوقائع الجنائية ومرتكبيها، وأن يسألوا من نسب إليه ارتكابها، ويثبتوا ذلك في محاضرهم. ولهم أن يستعينوا بأهل الخبرة من أطباء وغيرهم ويطلبوا رأيهم كتابة». والخبراء بصفة عامة قد يساعدون في تقديم وتفنيد الأدلة المادية التقليدية التي قد تسهم بفاعلية في تحديد الجاني ومستخدم الحاسب الآلي، أما خبراء الحاسب الآلي فيسهمون بفاعلية في تحديد الدليل المادي الخاص بالحاسب الآلي، وكذلك الدليل الرقمي الذي

يـدل على الاختراق والتعدي باسـتخدام تقنيات التتبع، وتقنيات اسـترجاع البرامج والمعلومات المتلفة والمزالة، فضلاً عن إلمامهم بمصطلحات الحاسب الآلي ويحتاج المحقق الجنائي لهم في أعمال التحقيق.

وأهم الخبرات التي يمكن الاستعانة بها خلال مرحلة التحقيق:

١ـ الأطبـاء الشرعيـون: الأطبـاء الشرعيـون فئـة مـن دارسي الطـب تتخصـص في الفحـص الشرعي للجسـم البـشري لتحديد مختلف أنـواع الإصابات البشرية ودرجتها والوقت الـذي مر عليها والآلة المستخدمة في إحداث تلك الإصابات ومن ثم تحديد السبب الفعلي للوفاة أو الإصابة (كامل، ١٩٩٩م، ص٢٩٩).

وهـم يـؤدون دوراً هامـاً في مجـال معاينة مسرح الجريمـة، وفحص المصابـين والمتوفين، وبيان أسـباب ذلـك، من خلال إبـداء الرأي، وتزويـد الجهـات المختصـة بالتقاريـر الفنيـة اللازمـة (الـردادي، ١٩٨٩م، ص٩٦).

والواقع أن عدم الاسـتعانة بالطب الشرعـي يعني عدم القدرة على تزويـد رجـل الضبـط الجنائي بسـبب الوفـاة أو الإصابـة، أو الآلة المسـتخدمة في إحداثها ونوعيـة الإصابات الناجمة عنهـا أو إمكانية تعـدد الجناة، وموقف الضـارب من المضروب، وتحديـد ما إذا كان هنـاك اعتداء جنسي قبل القتـل، أو غير ذلك من النتائج التي يمكن أن يظهرهـا خبراء الطـب الشرعي (مـرسي، ١٩٩٦م، ص٣١٥)، ممـا يحـول دون جدية التحريات الشرطية، وعـدم القدرة على تحديد الاتهام الموجه للمستجوب بدقة.

٢ـ خـبراء الأدلـة الجنائيـة: يتخصص خـبراء الأدلة الجنائيـة في فحص آثـار البصـمات، والأقدام كوسـائل فعَّالة في التحقق من شـخصية

صاحبهـا وتحديد ذاتيته على وجه اليقـين؛ لأن البصمة تحمل الكثير من الصفات المميزة لصاحبها، كما يفيد مكان العثور على البصمة في تحديد تواجد صاحبها بهذا المكان (الدغيدي، ٢٠٠٤م، ص١٦٦).

وأهم مجالات التعـاون التي يقدمها خبراء الأدلة الجنائية لرجل الضبط الجنائي:

أ ـ رفـع آثار بصمات الأصابع والأقدام من مواقع الحوادث ومضاهاتها مع آثار المشتبه فيهم.

ب ـ حفظ أرشـيف لبصمات الأصابع الفردية للخطرين على الأمن بما يمكـن من تحديد شـخصية صاحب الأثر من بصمـة أصبع واحد منه.

جـ ـ تنظيم حفظ أرشيف للسوابق يتيح للقائم بأعمال البحث والتحري التعرف على السـجل الإجرامي لأي شـخص (كامـل، ١٩٩٩م، ص٢٩٩).

ومن هذا يرى الباحث أن اسـتعانة رجـل الضبط الجنائي بخبراء الأدلة الجنائيـة، في الحالات التي تسـتلزم ذلـك خاصةً في قضايا التعـدي والتزوير الإلكتروني تسـاعد على تحديد المشـتبه بـه الذي يجب إجـراء التحريات عنه، وعـدم تبديـد الوقـت والجهـد في عمليات تحـري قـد تخالف الواقـع وتتيح الفرصـة للجاني الحقيقي بالإفلات من العقاب، أو تؤدي إلى تحريات قاصرة ترفضهـا الجهات القضائية لعدم الجدية، ومن ثم تسـهم كذلك في دقة تحديد الأسئلة ومواجهة المتهم بتفاصيل الجريمة التي تساعد في انهياره واعترافه.

ـ المعامل الجنائية

المعامل الجنائية عبارة عن معامل ومختبرات تتضمن أجهزة حساسة قادرة على تحليل العينات بالغة الصغر. وفي الماضي كان التحليل الكيميائي يتطلب حجماً معيناً من المادة المعثور عليها لتحديد نوعيتها ومقارنتها بغيرها؛ ولكن استطاعت المعامل الجنائية بأجهزتها وتقنياتها الحديثة استخدام أجهزة الفصل الكهربائي، واستخدامات أشعة إكس، وأجهزة كشف نوعية العناصر (اليولاروجراف)، وأجهزة قياس القلوية والحموضة، وأجهزة التحليل الطيفي، وأجهزة الامتصاص الذري من تحليل حجم ضئيل من المادة، وتحديد عناصره مثل تحليل ذرات طلاء السيارات أو مساحيق حشو أبواب الخزن الحديدية العالقة بملابس الجاني (كامل، ١٩٩٩م، ص٣٠٦-٣٠٨).

وتساعد الاستعانة بالمعامل الجنائية على تحديد الجاني الذي يجب التحري عنه، بدلاً من توسيع دائرة البحث والتحري وتبديد الوقت والجهد، الذي قد يؤدي إلى الإخفاق في تحديد الجاني الحقيقي، مما يترتب عليه عدم جدية التحريات، حيث إن كثرة عدد المشتبه فيهم يترتب عليه تفتيت وتشتيت الجهود، مما يؤثر سلباً على محصلة النتائج، حيث إن «رفع الآثار والنجاح في تحليلها وفحصها مهما كانت ضئيلة بمساعدة أجهزة المعامل الجنائية تساعد في تحديد الجاني أو على الأقل تحديد الأسلوب الإجرامي المتبع، بمعنى تضييق دائرة الاشتباه وتركيز جهود البحث والتحري» (الدغيدي، ٢٠٠٤م، ص١٨١)، ومن ثم تحديد المتهم المطلوب استجوابه.

ـ تقنية البصمة الوراثية

أطلقت البصمة على البصمة الوراثية تشبيهاً لها ببصمة الأصابع، لأنها تدل على الفرد بعينه (العنزي، ٢٠٠٤م، ص١٠٨). وتعتمد تقنية البصمة الوراثية أو ما يعرف علمياً بتقنية الحمض النووي على وجود الحامض

النووي المعروف باسم الحامض النووي الديوكسي ريبوزي (D.N.A) الذي يظهر على شكل كروموسومات داخل أنوية الخلايا الحية، وكل كروموسوم يحمل عدداً من الجينات التي تحدد الصفات الوراثية لكل فرد، ولذلك يمكن تحديد مدى انتماء بقعة دم أو أي أثر بيولوجي متخلف عن أي فرد من خلال فحص الكروموسومات وعدد الجينات التي تحملها وأشكالها ومقارنتها مع غيرها من كروموسومات وجينات المشتبه به، فهي تحدد بشكل قاطع المشتبه بـه الذي يتم التحري عنه لإثبات مدى علاقته بالجريمة، لأنه من المستحيل أن تتطابق جينات أي فردين (كامل، ١٩٩٩م، ص٣٠٨).

كما تعتبر البصمة الوراثية من الناحية العلمية دليل نفي أو إثبات قاطعة بشرط أن يتم التحليل بطريقة سليمة، حيث تسهم في الفصل في العديد من القضايا المدنية أو الجنائية لمميزاتها التي تفوق كثيراً الأدلة التقليدية كبصمات الأصابع وفصائل الدم، فاحتمال التشابه بين البشر في البصمة الوراثية قد يصل إلى واحد كل عدة بلايين بعكس الفصائل الدموية، حيث تتميز تقنية البصمة الوراثية بما يلي:

أ ـ يمكن تطبيقها على جميع العينات البيولوجية السائلة كالدم والمني واللعاب أو الأنسجة كالشعر والجلد والعظام، وهي ميزة هامة تفيد في حالة عدم وجود بصمات أصابع للمجرم، مما يسهم في التعرف عليه في قضايا القتل والاعتداءات الجنسية والسرقة.

ب ـ يمتاز الحمض النووي بقوة ثبات كبيرة جداً في أقسى الظروف البيئية المختلفة (حرارة، رطوبة، جفاف)، ويقاوم عوامل التحلل والتعفن لفترات طويلة جداً، وبذلك يظل لفترات طويلة في العينات البيولوجية، بينما لا يكون ذلك في الإنزيمات وفصائل الدم، وبذلك

يمكن استخلاصه من العينات البيولوجية الضئيلة جداً والمتحللة سواء السائلة أو الجافة، الحديثة أو القديمة.

جـ ـ يمكن تخزين الحمض النووي DNA بعد استخلاصه من العينات لفترات طويلة.

د ـ تظهر قراءت تقنيات DNA سهولة قراءة نتائجها وعمل الإحصاءات اللازمة وحفظها وتخزينها في الحاسب الآلي لحين طلب المقارنة.

هـ ـ يمكن معرفة جنس العينة بتحديد ما إذا كانت لرجل أو امرأة، مما يفيد في تحديد الدماء في جرائم القتل والسرقة لحصر المشتبه فيهم.

و ـ تسهم تلك التقنية في معرفة العينات المختلطة، خاصةً الآثار المنوية المختلطة بالإفرازات المهبلية في جرائم الاغتصاب، وإرجاع كل عينة إلى مصدرها.

ز ـ قوة التمييز لهذه التقنيات التي تتراوح ما بين ٩٣٪ إلى أكثر من ٩٩,٩٩٩ ٪.

ح ـ يمكن عن طريق هذه التقنية إثبات وقوع الجريمة في حالات اختفاء جسم الجريمة ووجود آثار منها كالدماء أو العظام (الجندي والحصيني، ٢٠٠٢م، ص ١٥٢-١٥٣).

ط ـ تعد البصمة الوراثية دليل إثبات أو نفي لا تقبل الشك.

ي ـ تعد وسيلة هامة في إثبات الأبوة والأمومة بشكل قاطع؛ نظراً لأن الفرد يرث نصف الأنماط الوراثية التي تحددها البصمة الوراثية من والده، ونصفها الآخر من والدته.

ك ـ يمكن عن طريق البصمة الوراثية تحديد هوية الشخص الغائب

سواء أكان مفقوداً، أو هارباً، أو أسيراً، وذلك بمقارنة أي أثر يشتبه أنه عائد له مع البصمات الوراثية لوالديه وأشقائه، ومن ثم التعرف عليه.

ولذلك فإن تقنية البصمة الوراثية لها أهمية قصوى للاستفادة من الآثار البيولوجية المتخلفة بمسرح الجريمة، مما يترتب على إهمالها توسيع دائرة الاشتباه، وقد يقود لعدم جدية التحريات، ويؤكد البعض أهمية الآثار البيولوجية المتحصلة من جسم الإنسان وإفرازاته كدلالة قوية في تحديد المشتبه به (العنزي، ٢٠٠٤م، ص١٦١-١٦٢).

ـ الاستعانة بخبراء الحاسب الآلي

يعد فهم الجوانب التقنية ومصطلحاتها من أكثر الصعوبات التي تواجه رجال التحقيقات في الجرائم المعلوماتية، فالغالبية العظمى من منسوبي أجهزة العدالة الجنائية لا يدركون شيئاً عن الحاسب الآلي وتقنياته المتطورة ولغاته المتنوعة، مما يستدعي الاستعانة بخبراء الحاسب الآلي في التحقيق وإعداد الأسئلة الفرعية لمواجهة مرتكبي جرائم التزوير المعلوماتي والحصول على استنتاجات تسهم في إثبات التهمة أو نفيها، فطبيعة الجريمة استلزمت تدخل خبراء الحاسب الآلي سواء قبل التحقيق بالتنسيق مع المحقق وتزويده بالمصطلحات والأسماء اللازمة لدعم تساؤلاته وتوجيهها، أو أثناء التحقيق لتوجيه الأسئلة الفرعية (البشرى، ٢٠٠٠م، ص ٣٦٥-٣٦٩).

كما أن الاستعانة ببينة الحاسب الآلي في إثبات الحقائق بعمليات حسابية بحتة ضمن تقنية الذكاء الاصطناعي من أساسيات اكتشاف جرائم المعلوماتية بصفة عامة وجرائم التزوير الإلكتروني بصفة خاصة من خلال حصر الحقائق والاحتمالات والأسباب والفرضيات واستنتاج النتائج في

ضـوء معاملات حسـابية وتقنيات تتبـع بهدف تحديد مصـدر الاختراق، مما يعـد بمثابة دليـل رقمي يمكن دعمه بالدليل المكتشـف في حاسـب المشـتبه بـه باسـتخدام تقنيـات اسـترجاع المعلومات والعمليـات، فقد أثبتـت تقنية الحاسبات الآلية نجاحها الفعال في جمع الأدلة الجنائية وصناعة البينة وتحليل القرائن واستنتاج الحقائق (Tillers, 1999: p. 117).

ـ الوسائل غير المشروعة في الاستجواب

التحريض على ارتكاب الجريمة

التحريض هو خلق فكرة الجريمة لدى شخص، ثم تدعيمها كي تتحول إلى تصميم على ارتكابها (حسني، ١٩٨٣م، ص٤٢٠).

وتختلـف وسـائل التحريـض، ولكنهـا تتفـق في التأثير في نفسـية الفرد ودفعه لارتكاب الجريمة سـواء أكان التحريض بالقول، أو بالفعل، كتقديم هدايا ووعود للجاني (عدس، ٢٠٠٤م، ص٢١٣).

فـإذا قام رجل الضبـط الجنائي بتحريض الجاني عـلى ارتكاب الجريمة، بطلـت تحقيقاتـه بها، لأنه أسـهم مسـاهمة أصيلـة بالتحريض عـلى ارتكاب الجريمـة لكـي يسـهل عليه تحديـد مرتكبهـا وتقديمـه للمحاكمـة، وإظهار جهوده للجهات القضائية بطريقة مصطنعة (مرسي، ١٩٩٦م، ص٣٤٧).

إعدام إرادة المستجوب

إعدام إرادة المسـتجوب بأي شكل من الأشـكال يبطل التحقيقات من أساسـها، ويبطل أي إجراء لاحق لها نتيجة الإكراه الذي أجبر الشخص على الفعل (مرسي، ١٩٩٦م، ص٣٤٨)، وأهم وسائل إعدام الإرادة:

أ ـ التهديـد: هو الضغط على المتهم لتوجيهه إلى سـلوك معين (السـبهان،

١٩٩٥م، ص٩٨)، بل إن مجرد الخوف من التهديد يؤدي إلى بطلان الدليل أو القرينة حتى لو كانت ضد شخص من الأشخاص المشبوهين أو أصحاب السوابق الإجرامية (الدغيدي، ٢٠٠٤م، ص٣١٤).

ب ـ الوعد والإغراء: هو بث الأمل لدى المتهم في شيء يتحسن به مركزه مما يؤثر على تصرفاته واختياراته.

جـ ـ استخدام العقاقير المخدرة وجهاز كشف الكذب والتنويم المغناطيسي وغسل المخ: إن استخدام عقار كشف الحقيقة (مصل الحقيقة)، وجهاز كشف الكذب، والتنويم المغناطيسي، وغسل المخ يعد نوعاً من أنواع الإكراه، ويبطل الاستجواب الذي يعتمد عليها نظراً لأن هذه الوسائل تعدم إرادة الفرد.

د ـ استخدام الحيلة والخداع: بإيهام المستجوب بأن لدى القائم بأعمال البحث والتحري أدلة أو شهود ضده، مما يترتب عليه اعترافه، ويكون اعترافه في هذه الحالة باطلاً؛ لأنه وقع تحت تأثير الخداع (السبهان، ١٩٩٥م، ص٢١٣).

هـ ـ التعذيب: يجمع الفقه والقضاء على عدم جواز تعذيب المستجوب للحصول على الاعتراف، فالتعذيب من أكثر صور الإكراه التي تجلب بطلان الاعتراف وما يترتب عليه (حسين، ٢٠٠٢م، ص ٣٣٧-٣٣٨).

وقد نص نظام الإجراءات الجنائية السعودي في المادة الثانية منه على عدم جواز التعذيب بقوله: «... ويحظر إيذاء المقبوض عليه جسدياً، أو معنوياً، كما يحظر تعريضه للتعذيب، أو المعاملة المهينة للكرامة».

اللجوء لأعمال منافية للآداب

إن لجـوء رجل الضبط الجنائي (المحقق) لأعـمال منافية للآداب في جمع الأدلة من شأنه أن يبطلها، لأن فاقد الشيء لا يُعطيه، وهذه القاعدة الأخلاقية يجب أن يلتزم بها رجل الضبط الجنائي، فلا يجب عليه أن يدفع شخصاً معيناً لممارسـة الفحشـاء في منزل مشـبوه بقصد التحقق من إدارتـه للبغاء (مرسي، ١٩٩٦م، ص٣٤٨).

المساس بحرمة الأشخاص والمساكن

إن حرمة الأشخاص والمساكن مصونة بنصوص القرآن الكريم والسنة النبوية الشريفة وبنصوص الدسـاتير الوضعية، ولا يجوز المسـاس بها إلا بناء عـلى إذن من هيئـة التحقيق والادعاء العام، وفي ضـوء توفر دلائل وإمارات قويـة وكافيـة لصـدور هـذا الإذن، ولذلك لا يجـوز لرجل الضبـط الجنائي المساس بهذه الحرمة خلال إجراء تحرياته عن أية جريمة، إلا أن حالة التلبس هـي الاسـتثناء الوحيد التـي تبيـح تفتيش الأشـخاص والأماكـن (مرسي، ١٩٩٦م، ص٣٥٠)، وقـد نصت المادة (٤٠) من نظـام الإجراءات الجزائية السعودي على أن: « للأشخاص ومساكنهم ومكاتبهم ومراكبهم حرمة تجب صيانتها. وحرمة الشـخص تحمي جسـده وملابسه وماله وما يوجد معه من أمتعة. وتشـمل حرمة المسكن كل مكان مسـور أو محاط بأي حاجز، أو معد لاستعماله مأوى».

كما نص نظام الإجراءات الجزائية السعودي في المادة (٣٥) منه على أنه: « في غـير حـالات التلبس، لا يجوز القبض على أي إنسـان أو توقيفه إلا بأمر مـن السـلطة المختصة بذلـك...»، ونص أيضـاً في المادة (٤١) منـه على أنه: «لا يجـوز لرجل الضبط الجنائي الدخول في أي محل مسـكون أو تفتيشـه إلا

في الأحوال المنصوص عليها نظاماً، بأمر مسبب من هيئة التحقيق والادعاء العام، وما عدا المساكن فيكتفى في تفتيشها بإذن مسبب من المحقق. وإذا رفض صاحب المسكن أو شاغله تمكين رجل الضبط الجنائي من الدخول أو قاوم دخوله، جاز له أن يتخذ الوسائل اللازمة المشروعة لدخول المسكن بحسب ما تقتضيه الحال.ويجوز دخول المسكن في حالة طلب المساعدة من الداخل، أو حدوث هدم أو غرق أو حريق أو نحو ذلك، أو دخول معتد أثناء مطاردته للقبض عليه».

يتضح مما سبق أن جريمة التزوير الإلكترونية تستدعي الاستعانة بالخبراء، وهنا دور الخبراء لا يقتصر على تحديد أفعال الجريمة ومدى اكتمال أركانها والتقاط الدليل الإلكتروني سواء من جهاز الشخص أو الجهة التي تعرضت للاختراق والتعدي، أو جهاز المشتبه به، بل يمتد ليشمل تبادل الآراء مع المحقق الجنائي وتبصيره بالمصطلحات العلمية، وكذلك حضور التحقيق وتوجيه بعض الأسئلة الفرعية في ضوء قلة إلمام منسوبي العدالة الجنائية بمصطلحات الجرائم الإلكترونية كجرائم مستحدثة، تستدعي تدريس هذا الفرع من العلم ضمن المعاهد والكليات الشرطية والأمنية بغرض تخريج محققين مؤهلين وملمين بالمصطلحات العلمية لجرائم المعلوماتية.

٢ ـ دور المحقق الفني في إثبات جرائم التزوير الإلكتروني

المحقق الفني هو الخبير المتخصص في جرائم الحاسب الآلي أو الحاسب الجنائي، وقد يكون من العاملين في جهات التحقيق، أو من الخبراء الذين تستعين بهم الجهات القضائية والأمنية عند التحقيق في الجرائم الإلكترونية، من خلال خبرتهم في البحث عن الدليل الإلكتروني، واستخدام تقنيات التتبع لمعرفة مصدر الاختراق والتعدي، أو استخدام تقنيات استرجاع

المعلومـات لتأكيـد الدليـل الرقمي، ومن ثـم تزويد الضابط المحقـق بتقرير مفصـل يشـتمل على الأدلة الرقميـة ومبررات الإدانة، والتعـاون مع ضابط التحقيق في الإعداد لمرحلة المحاكمة للمجرم المعلوماتي.

أ ـ الانتقال فور طلب المساعدة من قبل المحقق

يقوم المحقق الفني بالانتقال إلى مسرح الجريمة بناء على طلب من المحقق في جريمة التزوير الإلكتروني، فهو في هذه الحالة يعد بمثابة خبير سـواء كان يعمل داخل الجهاز الأمني أو خارجه، وهو إجراء صحيح إعمالاً لنص المادة (٢٨) مـن نظـام الإجراءات الجزائيـة التي أفادت: «ولهم أن يسـتعينوا بأهل الخبرة من أطباء وغيرهم ويطلبوا رأيهم كتابة».

ب ـ البحث عن الدليل الرقمي في جرائم التزوير الإلكتروني

وفـور وصـول المحقـق الفنـي إلى مـسرح جريمـة التزويـر الإلكتروني يجـب عليه القيـام بعملية المعاينة الفنية لمسرح الجريمـة من خلال اتخاذ أربعة إجراءات هي:

أ ـ البحـث في جهـاز الحاسـب الآلي المشـتبه بـه وطباعـة محتوياتـه أثناء التحري.

ب ـ البحـث في جهاز الحاسـب الآلي وعمل نسـخ مـن محتويات بعض ملفاته.

جـ ـ عمل نسخة من محتويات الجهاز في موقع الجريمة وبعدها.

د ـ فصل جميع الأجهزة المتصلة بالحاسـب وجمعها لاصطحابها للمختبر الجنائي (الخليفة، ٢٠٠٧م، ص١٠١٥).

إن الهدف من الإجراءات السابقة هو استخلاص وكشف البيانات والاحتفاظ بها، وتحليلها ثم توثيقها وعرضها كأدلة جنائية، والأطراف المكونة لمجال الحاسب الجنائي هي:

أ ـ العلم بمجال الحاسب الآلي والإنترنت وكيفية استخدامهما بكفاءة في التحقيق والتحري واستخلاص الأدلة.

ب ـ الدليل، وذلك بمعرفة ما يمكن استخدامه كدليل يحوز على رضا واقتناع المحكمة.

جـ ـ القانون، ويعني معرفة الخطوات اللازمة لتجريم المشتبه به أو صاحب الحاسب الآلي الذي قام بارتكاب جريمة التزوير المعلوماتية سواء بالتعديل أو الحذف أو الإضافة، أو تزوير التوقيع الإلكتروني بالاستيلاء عليه واستخدامه بغير معرفة صاحبه (G. L. Peter-son, et. al., 2007: pp. 264-265).

والدليل الرقمي عبارة عن: «معلومات يقبلها العقل والمنطق، ويعتمدها العلم، ويتم الحصول عليها بإجراءات علمية وقانونية بترجمة البيانات الحسابية المختزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة، لإثبات حقيقة شيء أو فعل شيء أو نسبة الجريمة إلى شخص له علاقة بجريمة أو جانٍ أو مجني عليه» (يونس، ٢٠٠٦م، ص٢٢).

والأدلة الإلكترونية وسائل إلكترونية غير ملموسة قابلة للتحليل، وتعطي دلالات تصل إلى حد اليقين أو غلبة الظن اللازم لإسناد الجريمة الإلكترونية إلى شخص أو موقع معين (الرشودي، ٢٠٠٨م، ص٢٥١).

وغالباً ما يتم ارتكاب جريمة التزوير الإلكتروني عن طريق التجسس على ملفات البيانات، وتغييرها مباشرةً، أو تزوير التوقيع الإلكتروني من خلال سرقته من منظومته واستخدامه في التوقيع على المحررات بدلاً من صاحبه الأصلي، ويرتكب هذه الجريمة مجرم معلوماتي متخصص، يقوم بطمس دليل جريمته بعد ارتكابها (حجازي، ٢٠٠٥م، ص٣٠).

ولذلك تلحق الأدلة الإلكترونية بالأدلة الفنية العلمية لكونها تحتاج إلى متخصصين في الكشف عنها، فهي مرحلة متقدمة من الأدلة المادية الملموسة، لا يمكن إدراكها بالحواس الطبيعية للإنسان إلا عن طريق الاستعانة بوسائل تقنية كالحاسب الآلي وتحويلها بواسطة الطابعة والفاكس إلى أدلة مادية (البشرى، ٢٠٠٤م، ص ٢٣٤-٢٣٥).

ومن أهم الخصائص التي تجعل الأدلة الإلكترونية من أدلة الإثبات:

أ ـ أنها غير ملموسة ولا محسوسة، فلا يدركها إلا المتخصصون بعد إجراء عدة عمليات من البحث والتنقية.

ب ـ تصل إلى درجة التخيلية في حجمها وشكلها، ولا يمكن العثور عليها في مكان محدد، بل هي منتشرة في الأثير، وتكون مرمزة أو مشفرة، ويصعب فك رموزها وشفرتها إلا عن طريق أجهزة وبرامج علمية متعددة (حجازي، ٢٠٠٥م، ص٣٦).

جـ ـ يمكن الحصول على عدة نسخ منها لها ذات القيمة العلمية التي لا تتوافر للأدلة الأخرى.

د ـ يمكن التعرف على الأدلة الإلكترونية التي تستخدم في التزوير أو التحريف بدقة أكبر من الأدلة المادية الأخرى، حيث أظهرت التقنية أجهزة ووسائل علمية للمضاهاة والتتبع كاستخدام الحاسب الآلي

في التحليل أو تتبع ذبذبات الإرسال للوصول إلى المتهم، حيث تعطي نتائج لا يتطرق إليها الشك بتحديد الموقع الذي تم منه الاختراق (الصغير، ١٩٩٩م، ص١٠٠)، حيث إن لكل جهاز (IP)، وهو عبارة عن عنوان مكون من أربعة أرقام تستخدم لتحديد هوية كل جهاز متصل بالإنترنت، وعندما يتجول أي فرد داخل الإنترنت يترك أرقام الـ (IP) في الأماكن التي تجول خلالها، ومن ثم يمكن الحصول على موقع الجهاز وعنوانه البريدي باستخدام تقنيات التتبع (حجازي، ٢٠٠٥م، ص٦٣).

هـ ـ من الصعب إتلاف الأدلة الجنائية في ظل التطور التقني المعاصر وظهور تقنيات تتبع وبرمجيات قادرة على استرجاع الأدلة الإلكترونية من الحاسب حتى بعد محوها والقضاء عليها وإتلافها، فهذه البرمجيات قادرة على استرجاع الممسوح والتالف من البيانات أو البرامج، ولذلك فإن التخلص من الملفات والبيانات بإزالتها لم يعد مجدياً بسبب توافر برمجيات وتقنيات تتبع قادرة على استرداد الملفات التي تم إلغاؤها أو إتلافها من الحاسوب (يونس، ٢٠٠٦م، ص١١).

و ـ وجود الأدلة والوسائل الإلكترونية كأوعية ووسائل الاتصال الإلكتروني في مسرح الجريمة الإلكترونية.

ز ـ تتميز الأدلة الإلكترونية بسرعة حركتها عبر شبكات الاتصال، وتتميز أيضاً بسعة امتدادها عبر الفضاء دون حدود ولا قيود، فالمجرم المعلوماتي قادر على الوصول لضحاياه عبر مئات الآلاف من الأميال (البشرى، ٢٠٠٤م، ص٢٣٦).

ح ـ يتخذ الدليل الإلكتروني شكلين: الأول صامت وهو ما يمكن الحصول عليه من خلال نسخه بالطباعة أو باستخدام مخرجات الحاسب الآلي كالوثائق والصور والبيانات، والثاني هو المظهر التقني المعلوماتي للدليل الذي يتسم بالحركة والذكاء والقابلية للتحليل كما هو الحال في الملفات التي تساعد على الاختراق والتجسس وإخفاء شخصية المستخدم (الرشودي، ٢٠٠٨م، ص٢٥٦).

يتضح مما سبق أن الدليل الإلكتروني يمكن أن يعد بمثابة دليل مادي قوي في حالة توافر تقنيات التتبع الخاصة التي تحدد موقع الاختراق، ومن ثم إجراء الفحوصات على الجهاز المشتبه به القيام بعملية الاختراق، باستخدام برامج استرجاع الأدلة الإلكترونية المتلفة أو التي تم التخلص منها من الجهاز، مما يعني أن هناك خطوتين لاستنباط الدليل الإلكتروني، الأولى هي: تحديد موقع الاختراق وزمانه، والثانية هي مداهمة الموقع، واستخدام برامج وتقنيات استرجاع الأدلة الإلكترونية لاكتشاف الدليل الإلكتروني.

ج ـ استخدام تقنيات التتبع لمعرفة مصدر الاختراق والتعدي

تنقسم المعاينة التي يقوم بها المحقق الفني في جريمة التزوير الإلكتروني إلى قسمين معاينة الحاسب أو الموقع الذي تعرض للاختراق والتعدي واستغل في تزوير البيانات والمعلومات أو المحررات سواء كان موقع شخصي أو مقر مكتب التصديقات الرقمية (في حالة الاستيلاء على التوقيع الرقمي)، ومعاينة الموقع الذي تم الاختراق والتعدي منه ولكن بعد استصدار إذن الجهات المختصة، فالغرض من معاينة الحاسب الآلي الذي تعرض للاختراق والتعدي واستغل في تزوير البيانات والمعلومات هو استخدام أجهزة وتقنيات التتبع في معرفة الـ (IP) الخاص بالمخترق لتحديد بدقة موقع الجهاز وعنوانه

البريـدي (حجـازي، ٢٠٠٥م، ص٦٣)، ويتـم ذلـك من خـلال الخطوات التالية (إبراهيم، ٢٠٠٨م، ص ١-٧):

ـ التهيئة

هي الخطوة المبدئية في التحقيق في الجرائم الإلكترونية وتتضمن الاتصال بمن تعرض للاختراق والتعدي، واتخاذ الإجراءات التالية:

١ ـ السـيطرة عـلى خادم الملفات لتعطيل حركـة الاتصالات فوراً ومنع استخدامها في إتلاف الأدلة الرقمية.

٢ ـ وأثناء عمل خادم الملفات يمكن الحصول على المعلومات المتحركة.

٣ ـ إجـراء التحليل عـلى جميع عمليات المعالجة، والاتصالات النشـطة بالشبكة.

ـ جمع الدليل الرقمي

وذلك من خلال:

١ ـ نسـخ المعلومات الموجودة على كل وحدة ذاكرة (بايت) لمنع إتلاف النظام الأصلي.

٢ ـ يجـب توخي الحذر أثناء جمـع الدليل الرقمي؛ لأن غالبية المعلومات الرقمية تتغير بسـهولة، وبمجرد تغيرها فمن المستحيل ملاحظة أنها قد تغيرت.

ـ الفحص

تتخذ إجراءات الفحص من خلال:

١ ـ مسح وتحليل قائمة الملفات، والمعالجات، وبرامج بدء التشغيل، وبرامج الخدمات، والحسابات لملاحظة وجود أي ثغرة أو أبواب خلفية، أو ثقوب.

٢ ـ لا يجب إزالة الملفات المهمة، فليس هناك حاجة لإعادة نسخ البيانات.

ـ التحليل:

١ ـ يجب تحليل جميع الأدلة الرقمية لتحديد نوعية المعلومات المخزنة عليها. وتستخدم لذلك برامج مخصوصة يمكنها عرض المعلومات بوضوح بعد فك شفرتها، وهذه البرامج تتضمن بيانات الدخول، والبرامج الإرشادية، والمفاتيح. وهناك العديد من البرمجيات التي تستخدم في تحليل ومعرفة المعلومات المسجلة على الأدلة الرقمية.

٢ ـ بالبحث عن اللوغاريتم الرقمي يمكن الحصول على نقطة البداية.

٣ ـ يمكن تحديد وقت وتاريخ وقوع الاختراق والتعدي والتزوير للبيانات أو المعلومات أو سرقة منظومة التوقيع الإلكتروني واستخدامها في التزوير.

ـ النتائج:

١ ـ اعتماداً على اللوغاريتمات، يمكن اكتشاف مصدر الـ (IP) والأرقام المكونة له، ومن ثم تحديد موقع المخترق وبريده الإلكتروني.

٢ ـ ويمكن أيضاً استخدام الطريقة التي دخلوا بها على خادم الملفات وطوعوه لخدمة أغراضهم.

٣ ـ وتوضح أيضاً اللوغاريتمات ما إذا كان المخترقون قد ارتكبوا أعمالاً أخرى في النظام أم لا.

ـ إعادة النسخ

١ ـ يتم إزالة جميع صفحات الويب المسجلة على الجهاز وإعادة تحديثها من أحدث النسخ والإصدارات بعد فحصها جيداً والتأكد من خلوها من الثقوب.

٢ ـ بعد تحديث الاتصال بالشبكة وتزويد الجهاز بأحدث إصدار، فإن ذلك يمنع المخترق من التحكم في خادم الملفات أو السيطرة عليه مرة أخرى باستخدام نفس طريقة الاختراق.

د ـ استخدام تقنيات استرجاع المعلومات لالتقاط الدليل الرقمي

أما معاينة الأجهزة أو المواقع التي صدر منها الاختراق أو التعدي بعد معرفتها وتحديدها واستصدار إذن الجهات المختصة، فتتم عن طريق برامج وتقنيات تتبع خاصة لجمع الدليل الرقمي الذي يثبت قيام عمليات الاختراق والتعدي بإتلاف البيانات وتزويرها أو سرقة منظومة التوقيع الإلكتروني واستخدامه دون علم صاحبه، فهذه التقنيات والبرمجيات قادرة على استرجاع الممسوح والتالف من البيانات أو البرامج، واسترداد الملفات التي تم إلغاؤها أو إتلافها من الحاسوب لإخفاء الدليل الرقمي لعملية الاختراق والتعدي لارتكاب جريمة التزوير الرقمي (يونس، ٢٠٠٦م، ص١١)، كذاكرة بيانات «هكس دمب» التي تسمح بالوصول إلى المحتوى المحذوف أو المحمي، وفك شفرة الذاكرة الآلي لمحتويات الذاكرة من خلال إعادة بناء هياكل البيانات المنطقية، وإعادة بناء البيانات المحذوفة،ـ وجلب البيانات المصدرية، وعرض البيانات مرة أخرى (قصيباتي، ٢٠٠٨م، ص٣).

ويرى الباحث أن التطور التقني المعاصر سوف يسهم بإذن الله في القضاء على جرائم المعلوماتية أو على الأقل الحد منها، في ضوء تطور

وسـائل وتقنيات التتبـع لمعرفة مصدر الاختراق، وتحديـده، ومن ثم مهاجمة الموقع المخترق، واسـتخدام تقنيات اسـترجاع المعلومـات المحذوفة والمتلفة كدليـل قوي يثبت ارتكاب جرائم المعلوماتية بصفة عامة وجرائم التزوير أو الاسـتيلاء على منظومة التوقيع الإلكتروني واسـتخدامه في تزوير المحررات بصفة خاصة، ولكن ذلك يتطلب تعاوناً دولياً، لأن طابع جريمة المعلوماتية أحيانـاً طابـع دولي، فيمكن ارتكابها من على بعـد مئات الآلاف من الأميال، وهذا يستدعي الاستعانة بالأقمار الاصطناعية لتحديد موقع الاختراق، ومن ثـم الاتصال بالسـلطات في موقع الاختراق الذي قد يكـون في قارة أخرى، ولذلك فبدون التعاون الدولي لا يمكن معاينة الجهاز الذي تم منه الاختراق ولاسـتخدام تقنيات اسـترجاع المعلومـات المحذوفة والمتلفـة كدليل مادي يثبت ارتكاب الاختراق والتعدي.

هـ ـ تزويد المحقق الجنائي بتقرير مفصل يشتمل على الأدلة الرقمية ومبررات الإدانة

بعـد أن ينتهـي المحقـق الفنـي مـن اسـتخلاص الأدلـة الرقميـة التـي تثبـت الاخـتراق والتعـدي وارتـكاب جريمـة التزوير من خلال اكتشـاف الأدلـة الرقميـة التي تثبت ارتـكاب جريمة الاخـتراق والتعـدي والتزوير، كالفيروسات، أو برامج الاختراق، أو الملفات التي تستخدم في انتحال صفة المواقـع وتغيـير محتوياتها، فإنه يقوم بحفظ هذه الأدلـة على أقراص، ومن ثم كتابة تقرير مفصل يشير فيها إلى إدانة الموقع أو الجهاز المستخدم في الاختراق مـن خـلال اسـتخدام الأدلـة الرقمية التـي تثبت قيـام الاخـتراق والتعدي والتغيير في المحررات باسـتخدام تقنية اسـترجاع المعلومات السـابق ذكرها (إبراهيم، ٢٠٠٨م، ص٧).

ويـرى الباحـث أن مـبررات الإدانة قد لا تشـير بالـضرورة إلى الفاعل الأصلي إذا كان هناك تعدد للمستخدمين لجهاز الحاسب الآلي، ولكنها تحصر الاشتباه في أقل عدد ممكن من الأفراد الذين استخدموا الجهاز في ذلك اليوم، ومن ثم التحقيق معهم جميعاً للتعرف على الفاعل الأصلي.

ويعـد المحقـق الفني بمثابـة الخبير، فالاسـتعانة بالخـبرة في مرحلة جمع الاسـتدلالات أمـر تأخـذ بـه غالبيـة القوانين والأنظمـة الإجرائيـة، بهدف الاسـتفادة مـن عنصر الخبرة في تقرير الأدلة من خـلال كتابة تقارير تفصيلية تتضمن تحديد المشتبه به وأدلة الإدانة (طنطاوي، ١٩٩٧م: ٢٩٥). وقد نصت المادة (٢٨) من نظام الإجراءات الجزائية السعودي على أن: «لرجال الضبط الجنائـي في أثناء جمع المعلومات أن يسـتمعوا إلى أقوال مـن لديهم معلومات عن الوقائع الجنائية ومرتكبيها، وأن يسـألوا من نسـب إليه ارتكابها، ويثبتوا ذلك في محاضرهم· ولهم أن يستعينوا بأهل الخبرة من أطباء وغيرهم ويطلبوا رأيهم كتابة».

و ـ الإعداد لمرحلة المحاكمة بالتعاون مع المحقق الجنائي

يشـكل تقديم الأدلة الرقمية في جرائم التزوير الإلكتروني صعوبة بالغة في ضـوء الحاجة لشرح المصطلحات التقنيـة للقضاة وأعضاء النيابة وهيئات التحقيق والادعاء العام، وهذا بالطبع يسـتدعي التعاون بين المحقق الجنائي والمحقـق الفنـي (الخبـير) في تقديـم الأدلـة وتفسـيراتها للجهـات القضائية والنيابيـة، لأن تـرك المحقق الفنـي (الخبير إذا كان من خـارج أجهزة العدالة الجنائية) يفقد القضية الجنائية عناصرها القانونية، ومن ثمَّ لا تتمكن المحكمة من الوقوف على الحقائق المكونة لأركان الفعل الإجرامي والتيقن من الأدلة التـي تثبـت تلـك الأركان، لذلك يجب التحضـير لإجـراءات المحاكمة من

خلال الخطوات التالية (البشرى، ٢٠٠٠م، ص ٣٧٤-٣٧٦):

أ ـ الخطوة الأولى: يقوم بها المحقق الجنائي التقليدي من خلال كتابة إجراءات تلخيص القضية وتعبئة النماذج والاستمارات الخاصة بملف القضية، وإعداد ورقة حصر التهم وصياغة سيناريو الجريمة كما كشفتها التحريات والأدلة المتوافرة.

ب ـ الخطوة الثانية: تتضمن اللقاء بين المحقق الجنائي التقليدي والمحقق الفني لحصر الأدلة المتوافرة وترتيبها وفقاً لأهميتها، ويقوم المحقق التقليدي بشرح الجوانب القانونية للمحقق الفني، وتأكيد ربط الأدلة والخبرة الفنية بعناصر وأركان الجريمة التي سيتم محاكمة المتهم بموجبها.

جـ ـ الخطوة الثالثة: يلتقي المحقق الجنائي التقليدي بممثل الاتهام أو وكيل النيابة، لشرح أبعاد الفعل الإجرامي وتمكين ممثل الادعاء من صياغة التهمة المناسبة والاتفاق حول عناصر وأركان الجريمة وترتيب الأدلة لإثبات كل ركن أو عنصر من عناصر جريمة التزوير، ويجب خلال هذه الخطوة التأكد من مدى إلمام ممثل الاتهام بالتقنيات والبرامج ذات العلاقة بالحاسب الآلي موضوع القضية.

د ـ الخطوة الرابعة: يتم خلال هذه الخطوة اللقاء بين المحقق التقليدي والمحقق الفني (الخبير) وممثل الادعاء لترتيب المصطلحات الفنية المستخدمة أثناء إجراء المحاكمات، مع ضرورة الاتفاق حول تلك المصطلحات وكيفية استخدامها والمرادفات التي قد ترد أثناء الاستجواب لكي تطمئن الأطراف الثلاثة على وجود لغة موحدة لا تقبل الشك أو الخطأ، فأي خلاف ينشأ بين المحقق التقليدي

والمحقـق الفني وممثل الادعـاء قد يطيح بالأدلـة الرقمية التي تقوم عليها التهمة، عملاً بالقاعدة القانونية (الشك يفسر لصالح المتهم).

هـ ـ الخطوة الخامسـة: هـي مرحلة وضع سـيناريو المحاكمة عن طريق ممثل الاتهام من خلال ترتيب الأحداث والوقائع الفنية التي تشكل الجريمـة مـع توافر عناصر القصـد الجنائي وإظهار مـبررات علاقة المتهم بارتكاب التزوير.

ثانياً: المحرر الإلكتروني

المحرر المعلوماتي عبارة عن مستند أو وثيقة تحتوي على معلومات، وهذه المعلومات قد تكون خاصة بفرد أو شركة أو جهة أمنية، أو أية منظمة، وهذه المحررات هي محل جريمة التزوير المعلوماتي، من خلال الاختراق والتعدي على مواقع وجود هذه المحررات، ومن ثم العمل على تعديلها أو إتلافها، أو تزويرهـا بالحذف أو الإضافـة أو التقليد أو الاصطنـاع أو غيرها من الطرق التي تسـتخدم في التزوير بأشـكاله كافة، فالتزوير في المحرر المعلوماتي أبسط وأسهل بكثير من التزوير في المحررات العادية، لأنه لا يحتاج إلا إلى التعديل المبـاشر، أو الدخول على قاعدة البيانات وتعديـل بيانات المحرر الإلكتروني تزويـراً، ومـن ثـم إصدار نسـخ منـه باسـتخدام أدوات الإخـراج كالطابعة والماسح الضوئي (حجازي، ٢٠٠٥م، ص ١٨٩-١٩٠).

١ ـ التصديق في المحرر الإلكتروني

التصديـق عمليـة تتضمن اعتـماد التصديـق الإلكـتروني بحيث تسري صحتـه عـلى جميـع الأوراق والمعامـلات التي يتـم وضعه عليهـا من خلال شـهادة تثبت صحتـه، وهي شـهادة من إحـدى الهيئات المعروفـة والمعترف

بها دولياً كهيئة التصديقات الرقمية الدولية «Version and Digital Signature Trust» التي تصادق على صحة التوقيع الإلكتروني وتمنح الفرد شهادة بالتوقيع الإلكتروني مقابل رسوم معينة، ويأخذ طالب التوقيع مع هذه الشهادة ما يسمى بالمفتاح العام (شفرة يعرفها المرسل والمستقبل) والخاص (شفرة خاصة بالموقع فقط)، فعند إرسال الرسالة الإلكترونية، يتم تشفيرها باستخدام المفتاح العام الذي يعرفه المرسل والمستقبل، مع إرفاق التوقيع الإلكتروني داخل الرسالة، ومن ثمَّ يقوم البرنامج الخاص بالمستقبل بإرسال نسخة من الوثيقة الموقعة إلكترونياً إلى الهيئة المعتمدة التي أصدرت الشهادة للتأكد من صحة التوقيع وسلامة الرسالة، وبعد إثبات صحة التوقيع يقرؤها المستقبل بمفتاحه الخاص، ويجيب على المرسل بالطريقة نفسها، وتتم هذه العملية خلال دقائق (اليوسف، ٢٠٠٨م، ص ٢٨٥-٢٨٦).

وفي المملكة العربية السعودي يتولى المركز الوطني للتصديق الرقمي تصديق التوقيعات الإلكترونية، حيث تم إنشاؤه وفقا لقرار اللجنة الدائمة للتجارة الالكترونية بتاريخ ١٠/ ١/ ١٤٢٢هـ الذي أناط مهمة إنشاء وتشغيل البنية التحتية للمفاتيح العامة لمدينة الملك عبد العزيز للعلوم والتقنية، وتمت الموافقة السامية على ذلك بتاريخ ١٧/ ٥/ ١٤٢٢ هـ بموجب الأمر السامي رقم٧/ ب/ ٩٣٧٨، وقد تم نقل مهام المركز الوطني للتصديق الرقمي من مدينة الملك عبد العزيز للعلوم والتقنية إلى وزارة الاتصالات وتقنية المعلومات في مطلع عام ١٤٢٦هـ. ويقدم المركز الوطني للتصديق الرقمي منظومة متكاملة لإدارة البنية التحتية للمفاتيح العامة (Public Key Infrastructure) والتي هي عبارة عن منظومة أمنية متكاملة لإدارة المفاتيح الرقمية المستخدمة في الحفاظ على سرية المعلومات والتثبت من هوية المتعاملين، إلى جانب الحفاظ على سلامة البيانات من

العبث والتغيير، والقيام بإجراء التوقيعات الرقمية. وهذه الخصائص تقوم عليها كافة الأعمال الإلكترونية كالتعاملات الإلكترونية الحكومية والتجارة الالكترونية، وغيرها من التطبيقات الالكترونية الشبكية. وتمكّن هذه البنية الأمنية المتعاملين عن طريق شبكة الإنترنت بمختلف فئاتهم من إجراء الأعمال والعمليات الإلكترونية بأمن وموثوقية وسلامة تامة. ويتمثل دور المركز الوطني للتصديق الرقمي في المصادقة على مراكز التصديق المنتشرة في قطاعات الدولة والقطاع الخاص وإضفاء صبغة قانونية لها ولتعاملاتها وذلك من خلال إصدار أنظمة وسياسات الشهادة الرقمية وإجراءات التصديق الرقمي وكذلك التحقق من سلامة الإجراءات المتبعة في إصدار الشهادات الرقمية وحقوق المستخدمين وخصوصيتهم. كما أن عدم وجود المركز الوطني يؤدي إلى الاعتماد على عمليات التصديق المتبادل (Cross Certification) الذي يعد بالغ التعقيد ويحتاج إلى تنسيق متواصل بين الجهات المصدرة للشهادات الرقمية (المركز الوطني للتصديق الرقمي، ٢٠٠٨م).

ويتولى المركز الوطني للتصديق الرقمي اعتماد شهادات التصديق الرقمي الصادرة من الجهات الأجنبية، حيث نصت المادة السابعة عشرة من نظام التعاملات الإلكترونية الذي تم إقراره في جلسة مجلس الوزراء السعودي التي انعقدت في ٧/ ٣/ ١٤٢٨هـ لضبط التعاملات والتوقيعات الالكترونية وتنظيمها وتوفير الإطار النظامي لها على ما يلي: «يختص المركز باعتماد شهادات التصديق الرقمي الصادرة من الجهات الأجنبية خارج المملكة، وتعامل هذه الشهادات معاملة نظيراتها بداخل المملكة، وذلك وفقاً للضوابط والإجراءات التي تحددها اللائحة».

٢ ـ التوقيع الإلكتروني

أ ـ مفهوم التوقيع الإلكتروني وأسلوب تزويره

التوقيع الإلكتروني عبارة عن: «طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الإنترنت، فالفكرة الكامنة وراء التوقيعات الإلكترونية هي نفسها كما في التوقيع المكتوب بخط اليد، فهي تستخدم للتصديق ويلتصق بهوية الموقع على معاملة ما» (المسعودي والحلبي، ٢٠٠٧م، ص٦٤١).

وهو «شهادة رقمية تحتوي على بصمة إلكترونية للشخص الموقع توضع على وثيقة تؤكد منشأها وهوية من وقع عليها» (اليوسف، ٢٠٠٧م، ص٢٨٥).

والتوقيع الإلكتروني عبارة عن ملف رقمي صغير تصدره إحدى الهيئات المتخصصة المعترف بها من الحكومات، وتتضمن تخزين اسم صاحب التوقيع وهويته، وتاريخ انتهاء الشهادة ومصدرها (حجازي، ٢٠٠٧م، ص٢٣١).

ويتم تزوير التوقيع الإلكتروني بطريقة مختلفة تماماً، فالتوقيع الإلكتروني المزور مطابق تماماً للتوقيع الأصلي، ولكن يتم التزوير من خلال سرقة منظومة التوقيع الإلكتروني من خلال التجسس الإلكتروني والتلصص، ومن ثم الحصول على التوقيع الإلكتروني وتوقيع الأوراق والمحررات به، فالتوقيع الإلكتروني توقيع سليم إذا تمت مضاهاته، ولكنه ليس صادراً من مالك منظومة التوقيع الإلكتروني، أي أنه صادر عن شخص آخر تمكن من سرقة منظومة التوقيع الإلكتروني للمالك الأصلي (الجنيبهي والجنيبهي، ٢٠٠٥م، ص١١٥).

ب ـ أنواع التوقيع الإلكتروني

هناك نوعان شائعان من التوقيعات الإلكترونية:

أ ـ المفتاحي: وفيه يتم تزويد الوثيقة الإلكترونية بتوقيع مشفر مميز يحدد الشخص الذي قام بتوقيع الوثيقة ووقتها، ومعلومات عن صاحب التوقيع.

ب ـ البيومتري: يعتمد على تحديد نمط حركة يد الشخص أثناء التوقيع، حيث يتم توصيل قلم إلكتروني بجهاز الحاسب الآلي ليستخدمه الشخص في التوقيع، ويقوم الحاسب الآلي بتسجيل حركات يد الشخص أثناء التوقيع كسمة مميزة لهذا الشخص، حيث إن لكل شخص أسلوب توقيع معين يأخذ حركات مختلفة، وكذلك بضغطة مختلفة على القلم، كما يدخل في التوقيع البيومتري البصمة الإلكترونية، ويتم التأكد من هذا النوع من التوقيعات من خلال الهيئة التي أصدرته (اليوسف، ٢٠٠٧م، ص٢٨٦).

جـ ـ مميزات التوقيع الإلكتروني

من أهم مميزات التوقيع الرقمي:

أ ـ يقر المعلومات التي يتضمنها السند أو يهدف إليها صاحب التوقيع، فعن طريق بطاقة الائتمان وعن طريق اتباع الإجراءات المتفق عليها بين حامل البطاقة والبنك يحصل الأول على المبلغ الذي يريده بدلاً من انتظار الدور عند اللجوء للسحب اليدوي.

ب ـ يدل على الحقيقة بدرجة أكثر من التوقيع التقليدي.

جـ ـ يسمح بإبرام الصفقات عن بعد، دون حضور المتعاقدين

بأشخاصهم، ومن ثمَّ يساعد في تنمية وضمان التجارة الإلكترونية.

د ـ وسيلة مأمونة لتحديد هوية الشخص الذي قام بالتوقيع (حجازي، ٢٠٠٧م، ص٢٤٠).

هـ ـ يصعب تزويره، نتيجة تشفير أجزاء من الوثيقة المرسلة ذاتها عن طريق برنامج الحاسب الآلي وليس المرسل أو المستقبل.

و ـ لا يمكن اقتطاع الوثيقة عن التوقيع الوارد عنها، فالتوقيع الإلكتروني لا يثبت الشخص منظم الوثيقة فقط، بل يثبت بشكل محدد الوثيقة محل هذا التوقيع، فعند فك التشفير يتعين أن ينطبق التوقيع ذاته على الوثيقة.

ز ـ المساهمة في توسيع التجارة الإلكترونية.

ح ـ تأمين المعاملات الإلكترونية، والحفاظ على سرية المعلومات أو الرسالة، مع عدم قدرة أي شخص آخر على الاطلاع أو تعديل أو تحريف محتواها.

ط ـ يمكن تحديد هوية المرسل والمستقبل إلكترونياً، والتأكد من مصداقية هذه الشخصيات بالكشف عن أي تلاعب أو تحايل (اليوسف، ٢٠٠٧م، ص ٢٨٧-٢٨٨).

د ـ عيوب التوقيع الإلكتروني

بالرغم من مميزات التوقيع الإلكتروني إلا أن له عدة سلبيات من أهمها:

أ ـ احتمال تعرضه للسرقة والضياع، إذا تمكن أحد المخترقين من سرقة منظومته، واستخدامها في توقيع محرر معلوماتي.

ب ـ إمكانية تقليد الشريط الممغنط الموجود على البطاقة الائتمانية.

جـ ـ لا يعبر عن شخصية صاحبه مثل التوقيع التقليدي (حجازي، ٢٠٠٧م، ص ٢٤١-٢٤٢).

د ـ إمكانية نشر فيروسات تضر عن طريق البريد الإلكتروني، مما يضر بالمراسلات الحكومية، أو يعرضها لعملية تنصت شامل من الخارج في ظل ما يسمى بالفرز الأوتوماتيكي للمراسلات الإلكترونية داخل المركز الرئيس للشبكة، كما يحدث في الولايات المتحدة، حيث يمكن إعداد تقارير عن المعلومات التي تتضمنها المراسلات الحكومية لأي دولة تضع شبكة معلوماتها داخل الإنترنت بما فيها الحكومية والشخصية (اليوسف، ٢٠٠٧م، ص٢٨٩).

يتضح مما سبق أن التوقيع الإلكتروني وسيلة آمنة، وفعالة في دعم التعاملات الإلكترونية، والمساعدة على انتشار التجارة الإلكترونية بما توفره من نسبة أمان مرتفعة نسبياً، في ضوء إمكانية اكتشاف حالات الاختراق والتعدي، ومتابعتها واكتشاف المخترقين بواسطة تقنيات التتبع، وتقنيات استرجاع المعلومات، ولكن ذلك قد يواجه بمعوقات أخرى كبعد المسافة أو الاختلافات السياسية والقانونية، كما أن الوقاية خير من العلاج، فمازالت حتى التوقيعات الإلكترونية عرضةً للسرقة،ومن يستطيع الاستيلاء على منظومتها بالتجسس على المعلومات يمكنه استخدامها في تزوير المحررات، مما يشير إلى أن تأمين نظم المعلومات ومنع الاختراق والتعدي من خلال ابتكار طرق وتقنيات تمنع الاختراق والتعدي هو وسيلة ضمان أمن التعاملات الإلكترونية وحمايتها من عمليات الغش والنصب والاحتيال المعلوماتي وكذلك التزوير المعلوماتي.

٢ . ١ . ٤ مواجهة جرائم التزوير الإلكتروني

يتطلب مواجهة جرائم التزوير الإلكتروني تمتع المحققين بمهارات علمية فنية لإثبات عمليات التزوير المعلوماتي عند اكتشافها، واستخلاص الأدلة الرقمية التي تقنع القضاة بالإدانة- ونسبة الجريمة لشخص محدد، حيث تسهم المهارات الفنية بدرجات متباينة في زيادة قدرة المحققين على مكافحة جرائم التزوير المعلوماتي، واختصار الوقت والجهد، فضلاً عن تقليل الخسائر إلى أدنى قدر ممكن (أبو شامة، ١٩٩٢م، ص٤٢).

وبما أن المواجهة تتطلب تشريعات وقوانين لمواجهة هذه الجرائم المستحدثة، والتي لا يمكن لتشريعات وأنظمة مكافحة التزوير الحالية كنظام مكافحة التزوير الصادر بالمرسوم الملكي رقم (١١٤) وتاريخ ٢٦/ ١١/ ١٣٨٠هـ، ونظام مكافحة التزوير الصادر بناء على تعميم وزير العدل رقم ١٣/ ت/ ٢٧٠٥ في ٢٤/ ٧/ ١٤٢٦هـ والمرسوم الملكي رقم م/ ١٦ في ٨/ ٧/ ١٤٢٦هـ وقرار مجلس الوزراء رقم ١٦٧ في ٣/ ٧/ ١٤٢٦هـ المتضمن إضافة مادتين إلى نظام مكافحة التزوير الصادر بالمرسوم الملكي رقم (١١٤) في ٢٦/ ١١/ ١٣٨٠هـ التصدي لها، لذا فقد أصدر المنظم السعودي مؤخراً نظام مكافحة جرائم المعلوماتية، ونظام التعاملات الإلكترونية.

وقد أقر مجلس الوزراء السعودي الموقر في جلسته يوم الاثنين ٧ ربيع الأول ١٤٢٨هـ نظام مكافحة جرائم المعلوماتية للحد من جرائم المعلوماتية وآثارها السلبية، حيث يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

١ ـ المساعدة على تحقيق الأمن المعلوماتي.

٢ ـ حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

٣ ـ حماية المصلحة العامة، والأخلاق، والآداب العامة.

٤ ـ حماية الاقتصاد الوطني (المادة الثانية من نظام مكافحة جرائم المعلوماتية، ٢٠٠٧م: ص٢).

كما تم إقرار نظام التعاملات الإلكترونية في المملكة العربية السعودية في جلسة مجلس الوزراء السعودي التي انعقدت في ٧/ ٣/ ١٤٢٨هـ لضبط التعاملات والتوقيعات الالكترونية وتنظيمها وتوفير الإطار النظامي لها (نظام التعاملات الإلكترونية، ٢٠٠٧م)، حيث يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها، وتوفير إطار نظامي بما يؤدي إلى تحقيق ما يلي:

١ـ إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بوساطة سجلات إلكترونية يعول عليها.

٢ـ إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.

٣ ـ تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي، للاستفادة منها في جميع المجالات، كالإجراءات الحكومية، والتجارة، والطب والتعليم، والدفع المالي الإلكتروني.

٤ ـ إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية.

٥ ـ منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات

الإلكترونية (المادة الثانية من نظام التعاملات الإلكترونية،٢٠٠٧م: ص٣).

إن الهدف من صدور هذين النظامين هو زيادة القدرة على مواجهة جرائم المعلوماتية، وإلزام الدوائر الجزائية القضائية بديوان المظالم باتباعها عند النظر في هذه القضايا، وبذلك تساير المملكة العربية السعودية سبل المكافحة الدولية والعربية من خلال الاستفادة منها في مجال التعاون الأمني، وفي مجال تسليم المجرمين، وإمكانية تتبع مثل هذه القضايا، ومن أهم المعاهدات والاتفاقيات الدولية في هذا الصدد (الجنبيهي والجنبيهي، ٢٠٠٥م، ص ١٨٠-٢٠٢٥):

١ ـ معاهدة بودابست لمكافحة جرائم الإنترنت: تم التوقيع على هذه المعاهدة في ٢٣ نوفمبر عام ٢٠٠١م في العاصمة المجرية بودابست بهدف توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت.

٢ ـ المعاهدة الأوروبية لمكافحة جرائم الإنترنت: هي معاهدة شاملة وقعتها اللجنة الخاصة بمكافحة الجريمة بتكليف من المجلس الأوروبي عام ٢٠٠٢م بهدف مساعدة الدول على مكافحة جرائم الإنترنت.

٣ ـ اتحاد الشركات والكيانات الاقتصادية الكبرى في مجال حماية أمن المعلومات: سعت لتوفير الحماية لنظم معلوماتها من خلال إيجاد أطر مناسبة من التعاون بينها لصد هذه الجرائم ومحاولات القرصنة.

٤ ـ المعاهدات والقوانين الخاصة بحق الملكية الفكرية: من أهم تلك المعاهدات: معاهدة برن، ومعاهدة تريبس، ومعاهدة الويبو:

أ ـ معاهدة برن: تم التوقيع عليها في سويسرا عام ١٩٧١م لوضع حجر الأساس في مجال الحماية الدولية لحق المؤلف، وقد وقعت عليها (١٢٠) دولة من بينها مصر.

ب ـ معاهدة تريبس: تم التوقيع عليها من قبل الدول الأعضاء عام ١٩٩٤م بهدف حماية الملكية الفكرية (العريان، ٢٠٠٤م، ص١٦٥).

جـ ـ معاهدات الويبو: تنقسم معاهدات الويبو إلى ثلاثة معاهدات: تتناول الأولى حق المؤلف، وتتناول الثانية الأداء والتسجيل الصوتي، بينما تتناول الثالثة الحماية الدولية لحق المؤلف والحقوق المجاورة، وتم التوقيع عليها جميعاً عام ١٩٩٦م (الجنبيهي والجنبيهي، ٢٠٠٥م، ص ٢٠٢-٢٠٥).

أولاً: الدور القضائي في مواجهة جرائم التزوير الإلكتروني

القضاء هو وسيلة استعادة الحقوق المسلوبة، ومواجهة الظواهر الإجرامية من خلال تطبيق القوانين وتفسيرها وتوقيع العقوبات حسب ملابسات كل قضية،وفي هذا الصدد يتولى القاضي عملية تقدير الأدلة المادية بحسب أهميتها وقيمتها في الإثبات.

ويتم تقييم أدلة الجرائم المعلوماتية من قبل القضاء من خلال ثلاثة نظم رئيسة للإثبات هي: نظام الأدلة القانونية أو النظام المقيد، ونظام حرية الإثبات أو نظام الاقتناع الذاتي للقاضي، ونظام الإثبات المختلط.

١ ـ تقييم أدلة جرائم التزوير من قبل القاضي في النظام المقيد

يحظر على القاضي بمقتضى هذا النظام تقييم حكمه في الدعوى إلا بناء على أدلة محددة سلفاً من قبل المنظم، ومن ثم لا يحكم القاضي في الدعوى

المطروحة أمامه إلا بناء على توافر أدلة مقيدة ومحددة، فلا يترك له سلطة تقديره للأدلة المادية، فلا يمكن قبول الأدلة المادية إلا بناء على شرطين هما:

١ ـ أن يكون الدليل متعلقاً بالواقعة التي ينظرها القضاء.

٢ ـ أن يكون للدليل أهمية بحيث يكون متجاوزاً أو يفوق بوضوح تأثيره الضار على الدعوى (الشاذلي وعفيفي، ٢٠٠٣م، ص ٣٨٥-١٨٦).

ومن هذا المنطلق يجب أن تكون الأدلة المقدمة ملموسة وأساسية وأصلية وليست بديلة، بمعنى عدم صلاحية الدليل الإلكتروني مطلقاً كدليل إثبات؛ لأن الإشارات الإلكترونية والنبضات الممغنطة التي تعتمد عليها الحاسبات ليست مرئية للعين البشرية، فلا يمكن للقضاة الاطلاع عليها، ويمكن أن يعد بمثابة دليل ثانوي وليس أصلياً (فريد، ١٩٩٤م، ص ١٧٤-١٧٥).

٢ ـ تقييم أدلة جرائم التزوير من قبل القاضي في نظام الاقتناع الذاتي للقاضي

يمنح هذا النظام القاضي سلطة تقديرية واسعة في تقييم الأدلة المادية التي يستند إليها في إصدار حكمه، سواء من حيث قبول الأدلة ذاتها، وعددها، أو من حيث تقديره الشخصي لكل دليل، باعتبار أن الإثبات يستدعي استعانة القضاء بكافة الوسائل المتاحة والممكنة لتقصي الحقيقة. ومن هذا المنطلق يجوز قبول الأدلة الرقمية كأدلة إثبات إذا اقتنع القاضي بها، فلا يوجد ما يحول دون قبول الأدلة الرقمية كأدلة إثبات أمام القضاء الجنائي (الشاذلي وعفيفي، ٢٠٠٣م، ص ٣٨٩-٣٩٢).

٣ ـ تقييم أدلة جرائم التزوير من قبل القاضي في نظام الإثبات المختلط

نظـام الإثبـات المختلط عبارة عـن مزج بين نظام حريـة الإثبات ونظام الإثبات المقيد لجمع مزاياهما، وتلافي عيوبهما، حيث يقوم المنظم بتحديد أدلة الإثبـات التـي يجوز للقاضي الاسـتناد إليهـا عند إصدار حكمـه في الدعوى التـي ينظرهـا، مـع منحه الحـق في تقييـم ووزن كل دليل على حـدة، وتقرير مـدى كفايته للحكم بالإدانـة. وبمقتضى هذا النظـام لا يوجد ما يحول دون قبـول الدليل الإلكـتروني في جرائم التزوير إذا دعم هذا الدليل تقرير الخبير، بمعنى إمكانية قبول الدليل الرقمي كدليل إدانة في جرائم التزوير عن طريق المعاينـة التي تقوم بهـا جهات التحقيق أو المحكمة بمسـاعدة الخبراء، ولكن ذلك لا يغطي كافة الأدلة التي يمكن التقاطها من الحاسبات الآلية، ويترتب عليـه تجنـب أو طرح أدلة أخرى بالرغم من أهميتها إذا لم تأت بطرق معينة أو بمعرفة الخبراء (فريد، ١٩٩٤م، ص ١٦١-١٦٤).

ثانياً: موقف الشريعة الإسلامية من جرائم التزوير الإلكتروني

جميـع الجرائـم الحديثة التي لم تكـن معهودة في السـابق تدخل ضمن ما يسـميه الفقهاء «الجرائم التعزيرية»، وهـذا يؤكد أن خصائص وصفات هذه الجرائم هي التي تحكم طريقة ووسـائل إثباتها، فمادامت الجرائم الإلكترونية تتصـف بالدقـة، والخياليـة، والسرعة، والتعقيـد، والعلميـة، والتخصصية، والتقنية، فالشريعة الإسـلامية بمبادئها وأصولها وقواعدها الشرعية في مجال الإثبـات الجنائـي لا تمنع من اسـتخدام نفس هذه الخصائص وتسـخيرها في مجـال الإثبـات، فاسـتخدام التقنية في الإثبـات عامل مهم، بل قـد يكون هو الأسـلوب الوحيـد الفاعل في مكافحـة تطور وتنامي الإجـرام الإلكتروني، فالشريعـة الإسـلامية لا تنظـر لمسـمى ونوعيـة وسـائل الإثبـات، بـل تنظر

إلى النتائج التي تحققها في كشف الحقيقة، فمن الصعب إثبات جريمة التزوير الإلكتروني باستخدام وسائل وطرق تقليدية لا تتناسب مع طبيعة وخصائص هذه الجريمة (الرشودي، ٢٠٠٨م، ص٢٨٠).

وقد اختلف الفقهاء في التكييف الشرعي لجرائم التزوير الإلكتروني، حسب ما يترتب عليه هذا التزوير، وقد يتضمن هذا التزوير انتحال شخصية فرد أو موقع وتوجيه إهانات أو سباب أو قذف الآخرين، أو ارتكاب عمليات سرقة لمنظومة التوقيع الإلكتروني، أو التقدم بمعلومات مزورة واستخدامها في البيع والشراء بمعنى سرقة أموال آخرين أو اختلاسها، وبصفة عامة تستوجب جريمة التزوير عقوبة تعزيرية، بجانب العقوبات الأخرى التي تترتب على التزوير من سرقة أو اختلاس أو قذف، وبصفة عامة اختلف العلماء فقط في تحديد عقوبة السرقة، فالبعض اعتبرها اختلاساً؛ لأن المعلومات شيء غير ملموس، والدليل الإلكتروني لا يرقى إلى حجية الأدلة المادية، واعتبرها البعض الآخر سرقة تستحق حد السرقة، ولكن في حالة استخدام وسائل تقنية تثبت باليقين غير القابل للشك ارتكاب الجريمة وإثباتها إلى مرتكبها الحقيقي (الرشودي، ٢٠٠٨م، ص٢٨١).

وقد جرمت الشريعة الإسلامية التزوير، لأنه يتضمن الغش وأكل أموال الناس بالباطل، وتغيير الحقيقة، ونشر الكذب والباطل، وما إلى ذلك من الجرائم الأخرى التي تؤدي إلى الفساد في الأرض، حيث تقوم سياسة التجريم في الشريعة الإسلامية على أساس حماية الجماعة وصيانة نظامها، ودفع الشرور والآثام والأخطاء والأضرار والمفاسد من جهة، ومن جهة أخرى إصلاح الأفراد وتهذيبهم ورعاية حقوقهم، وتذكيرهم بما لهم من

حقـوق وما عليهـم من التزامـات، واسـتنقاذهم من الضلالـة، وكفهم عن المعـاصي والجرائـم والمخالفـات، وهدايتهم نحو الطريق السـوي والصراط المستقيم (بوساق، ٢٠٠٢م، ص٨٢).

لذلك شرعت لها الشريعة الإسـلامية بعض العقوبات التعزيرية التالية للحد منها ومن آثارها السلبية:

١ ـ اللعن: تلعن الشريعة الإسلامية المزورين، لأن التزوير يعد من قبيل الإثم والعدوان على حقوق الآخرين.

٢ ـ نقـض عهـد الذمـي إذا سـاعد مـزوراً أو تسـتر عليـه (ابـن مفلح، ١٩٨٨م، ج٦: ص٢٥٧).

٣ ـ أدنـى درجـات التزوير ومـا يلحق به من جرائم أنـه معصية يعاقب عليها الشارع بعقوبة تعزيرية.

وينحصر دور السياسة الشرعية في تجريم التزوير الإلكتروني فيما يلي:

١ ـ النهي عن الاعتداء على حرمة الحياة الخاصة والأموال

يسهم التزوير الإلكتروني وما يلحق به من جرائم في انتهاك حرمة الحياة الخاصة لبعض الأفراد.

٢ ـ النهي عن الفساد في الأرض

يترتـب على ارتـكاب جرائـم التزوير الإلكـتروني والجرائـم الملحقة به المسـاعدة على الإفسـاد في الأرض سـواء بالتشـهير بالأفراد، أو تهديدهم أو ابتزازهـم وإتـلاف أموالهـم أو إخافتهـم وترويعهـم (العمـيري، ٢٠٠٤م: ص٣٣٠).

٣ ـ النهي عن الظلم والبغي

يعـد التزويـر الإلكتروني واسـتغلال المعرفة والإلمـام بالتقنية الحديثة في القيام بعمليات التزوير وما يلحق بها من جرائم اختلاس الأموال، والقذف والتشـهير بالآخريـن، وكشـف عوراتهـم، والبغـي والخـروج عن السـلطة الرسـمية، من أشـد المنكرات لأن خطره يعم المجتمع ويصيب الأبرياء، وبه تعم الفتنة (العميري، ٢٠٠٤م: ص٣٣٣).

٢. ٢ الدراسات السابقة والتعقيب عليها

يقصد بالدراسـات السـابقة الجهود البحثيـة التطبيقيـة أو الميدانية التي تتعلق بمشـكلة البحث تحت الدراسة ـ سواء أكانت رسائل أم أبحاث علمية منشـورة في مجـلات علمية محكمـة، حيث تهتم الدراسـات السـابقة بالطرق العلميـة التـي يتـم من خلالها دراسـة المشـكلات مـن قبل باحثـين آخرين، وذلـك بالتركيز على المنهجية العلمية المتبعة والنتائج والتوصيات (القحطاني وآخرون، ٢٠٠٠م، ص١٣٤).

وتحقيقاً لهدف الدراسة استعرض الباحث بعض الدراسات والبحوث والمؤلفـات العربية والأجنبيـة التي تناولت التحقيـق في الجرائم الإلكترونية بصفة عامة، وجرائم التزوير الإلكتروني بصفة خاصة، من خلال استعراض الجرائـم الإلكترونيـة، وأسـاليب التحقيـق ومعوقاتـه، ومكافحـة الجرائـم الإلكترونيـة، حيـث اختار الباحث مجموعة من الدراسـات السـابقة العربية والأجنبيـة التـي تناولت بشـكل مباشر أو غـير مباشر الجرائـم الإلكترونية، والتزوير الإلكتروني وصوره، والأسـاليب والوسـائل اللازمـة للتحقيق في الجرائم الإلكترونية. وتم تناول كل من هذه المراجع والوثائق بناء على محاور الدراسـة لتكتمل الصورة بـين الجانب النظري للدراسـة والجانب التطبيقي

للخروج بنتائج علمية وموضوعية. والمحاور التي استعرضت الدراسات السابقة، تبعاً لتسلسلها هي:

١ ـ التحقيق في الجرائم الإلكترونية.

٢ ـ معوقات التحقيق في الجرائم الإلكترونية.

٣ ـ مكافحة الجرائم الإلكترونية.

٢ . ٢ . ١ الدراسات التي تناولت التحقيق في الجرائم الإلكترونية

قام(Erdonmez 2002) بدراسة عن فحص واكتشاف جرائم الكمبيوتر بهدف التعرف على أساليب فحص واكتشاف جرائم الكمبيوتر. وقد أجريت الدراسة على العاملين في أمن المعلومات بشركات الحاسب الآلي، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وتوصلت نتائج الدراسة إلى أن فحص واكتشاف جرائم الكمبيوتر يتطلب معارف ومهارات تتجاوز تلك التي يحوزها المحققون، ولهذا السبب ينبغي تكوين فريق خاص من المحققين للتحقيق في هذا النوع من الجرائم ويكون لديهم الخبرة والدراية بهذا النوع، كما أن الطبيعة الخاصة بجرائم الحاسوب تتطلب مهارات خاصة للتصدي لها.

لذلك يؤكد الباحث أهمية إلمام المحققين بأنظمة التشغيل المختلفة بالإضافة إلى القدرة على التعرف على العتاد والبرمجيات خصوصاً العاملين في الدوريات من رجال الشرطة لأنهم أول من يصل إلى موقع الجريمة.

وقد أوصت الدراسة بإعداد الكوادر الشرطية المدربة تدريباً جيداً يؤهلهم لامتلاك خبرات ومهارات توازي إن لم تتفوق على تلك الموجودة لدى مرتكبي هذه الجرائم.

وأجرى العنزي (٢٠٠٣م) دراسة عن «وسائل التحقيق في جرائم نظم المعلومات»، التي هدفت إلى وضع إطار عام للسياسة الأمنية الشاملة لحماية نظم المعلومات، وتحديد الإجراءات الأمنية الفنية والإدارية لتحقيق أمن نظم المعلومات، وتحديد أنماط جرائم نظم المعلومات ومدى وقوعها وأضرارها ودوافعها، والأساليب المستخدمة في ارتكاب جرائم نظم المعلومات ومنافذها، والأدوات المستخدمة من قبل مجرمي نظم المعلومات وكيفية الحصول عليها، ومعرفة وسائل التحقيق في جرائم نظم المعلومات، والمعوقات التي تحول دون استخدام تلك الوسائل، وأنواع الأدلة المثبتة لارتكاب جرائم نظم المعلومات. وقد أجريت الدراسة على المحققين بأقسام الشرطة في مدينة الرياض والشؤون الفنية بوزارة الداخلية، والعاملين بمجال نظم المعلومات بالقطاع العام، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

توصلت الدراسة إلى أن وجود تقصير في اتباع إجراءات أمن المعلومات، وعدم وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات، وأن أهم العناصر الواجب توافرها بالسياسة الأمنية على الترتيب هي: وجود سياسة معينة للتحقيق مع من يرتكب الجرائم المعلوماتية، وإلزام الموظفين باتباع إجراءات السياسة الأمنية، ووضع عقوبات للمخالفين، وإعلان السياسة الأمنية للموظفين بشكل عام، وتقيد الرؤساء بالسياسة الأمنية عند إعطاء التعليمات.

وقد توصلت الدراسة إلى مجموعة من التوصيات من أهمها: ضرورة تلافي القصور والنقص في مهارات التحقيق في جرائم نظم المعلومات لدى المحققين بالأجهزة الأمنية وإيجاد آليات للاستفادة من خبرات الجهات المتخصصة في مجال التحقيق في جرائم الحاسوب والإنترنت والاهتمام

بتدريب المحققين في معاهد متخصصة لإكسابهم المهارات اللازمة للتحقيق بفاعلية في جرائم نظم المعلومات وينبغي توفير الأجهزة الحديثة والبرمجيات المتخصصة للجهات الأمنية للقيام بمهام التحقيق في هذه الجرائم.

كما أجرى الكركي (٢٠٠٣م) دراسة عن «التحقيق في جرائم الحاسوب» والتي هدفت إلى إثبات الأدلة الجنائية الرقمية وسلامتها وكيفية التعامل معها؛ لأن منها ما يتطلب مهارات خاصة لا تتوفر لدى كل المحققين، لذلك يجب على المحقق كخطوة أولى أن يميز بين المعلومات التي لها علاقة بالجريمة أو التي ليس لها علاقة بالجريمة وذلك من خلال معرفته بجهاز الحاسب الآلي ووسائط تخزين البيانات وكوابل الشبكات وغيرها والتي تعد وعاءً للمعلومات الرقمية. وقد أجريت الدراسة على المحققين في شرطة منطقة الرياض، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وكان من نتائج هذه الدراسة سلسلة الوصاية وهي قائمة من البيانات الشخصية الخاصة بكل من تعامل مع الدليل من أجل الحفاظ عليه من التلاعب أو الإهمال، وأصالة الأدلة وعدم تغيير حالتها الأصلية من أهم متطلبات القانون لقبول هذه الأدلة لإثبات الجرائم كما أن تصنيف ومقارنة وإفراد الدليل الرقمي من خلال إيجاد الخصائص التي ينفرد بها الدليل ويتميز بها عن غيره بهدف التمكن من ربطه بحاسوب معين لتحديد الجاني أو على الأقل تضيق نطاق المشتبه بهم لذلك أوصت الدراسة بضرورة أن يتم رفع وتحريز الأدلة الجنائية الرقمية بحالتها الأصلية تماشياً مع القانون الذي يطلب أصالة الأدلة وعدم تغيير حالتها الأصلية. وضمان القدرة على التفريق بين الدليل الأصلي والنسخة المأخوذة عنه وذلك عن طريق التوثيق كإجراء مهم أثناء التعامل مع الأدلة.

وقام البشرى (٢٠٠٣م) بدراسة عن «الأدلة الجنائية الرقمية: مفهومها ودورها بالإثبات» بهدف التعرف على مفهوم الأدلة الرقمية، ودورها في إثبات جرائم التعدي والاختراق. وقد أجريت الدراسة على المحققين بأقسام الشرطة في مدينة الرياض والشؤون الفنية بوزارة الداخلية، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وقد توصلت الدراسة إلى نتائج من أهمها: اختلاف الأدلة الرقمية باختلاف الأسلوب الإجرامي، وطرق جمعها، ومن يقوم بها، وتصنيفها، وأن الأدلة الرقمية أكثر الأدلة وفرةً وثباتاً، وأنها نالت مصداقية أمام المحاكم الشرعية المدنية، وأن الأجهزة الرقمية التي تفحص الأدلة المادية كالبصمات الوراثية أولى بفحص الأدلة الرقمية.

وأوصت الدراسة بجملة توصيات من أهمها: ضرورة اعتماد الأدلة الرقمية كأدلة لإثبات يقينية في القضاء الشرعي والمدني، وتدريب العاملين في أجهزة العدالة الجنائية على اكتشاف والتقاط الأدلة الرقمية، وإكساب العاملين في أجهزة العدالة الجنائية مهارات التحقيق الأساسية في الجرائم الإلكترونية.

٢. ٢. ٢ الدراسات التي تناولت معوقات التحقيق في الجرائم الإلكترونية

أجرى رستم (١٩٩٤م) دراسة عن «الجوانب الإجرائية للجرائم المعلوماتية» بهدف التعرف على التحقيق في الجرائم المعلوماتية والصعوبات التي تواجه المحقق فيها. وهي دراسة وصفية مكتبية، وقد استخدم الباحث المنهج الوصفي.

توصلت الدراسة إلى نتائج من أهمها: أن أهم المعوقات التي تواجه المحققين في جرائم المعلوماتية هي نقص خبرة وتدريب الشرطة لمواجهة تلك الجرائم، وأنه لابد من توافر المعرفة العلمية والقدرات الذهنية والنفسية لمن يتولى التحقيق في هذه الجرائم.

وأوصت الدراسة بجملة توصيات من أهمها: تدريب العاملين في الشرطة تدريباً تخصصياً متقدماً على التحقيق في جرائم المعلوماتية، وتزويدهم بالخبرات اللازمة للتحقيق في هذه الجرائم.

كما أجرى(Goodman 1997) دراسة عن «أسباب عدم اهتمام الشرطة بجرائم الكمبيوتر» بهدف التعرف على أسباب عدم اهتمام رجال الشرطة بجرائم الحاسب الآلي، ووسائل مواجهة تلك الجرائم، في ضوء التطور التقني المتسارع الذي أضفى صعوبة على مرتكب هذه الجريمة وأوجد معوقات أمام المحققين بها. وقد أجريت الدراسة على المحققين في جرائم الحاسب الآلي بالشرطة الفيدرالية، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وقد توصلت إلى نتائج أهمها: أن أهم أسباب عدم اهتمام رجال الشرطة بجرائم الحاسب الآلي هو افتقادهم للمهارات الأساسية في التعامل مع الحاسوب، وربما الخوف المرضي من التقنية بشكل عام، نتيجة النقص الواضح في التدريب الذي يتلقاه منسوبو الشرطة سواء في استخدام الحاسوب بشكل عام أو في التعامل مع جرائم الحاسوب، حيث لا تهتم إدارات الشرطة بتدريب حديثي التخرج في المسائل المتعلقة بالتقنية العالية، وينحصر التدريب في كيفية استخراج معلومات عن أنظمة قواعد البيانات

الخاصة بالمشبوهين والسيارات المسروقة ونحو ذلك، وهو ما يقدم للضباط بيانات أولية لا تساعد على إعدادهم لمكافحة جرائم الحاسوب.

لذلك أوصت بضرورة تدريب منسوبي الشرطة على استخدام العتاد والبرمجيات، والعمل على تطوير مهاراتهم في استخدام الحاسب الآلي لزيادة قدراتهم على مواجهة جرائم الحاسب الآلي.

وأجرى (Wahbler 1998) دراسة عن «جرائم الحاسب الآلي» هدفت إلى التعرف على جرائم الحاسب الآلي وكيفية إثباتها بالأدلة الإلكترونية. وقد أجريت الدراسة على المحققين في جرائم الحاسب الآلي في قطاع الشرطة في ميلبورن باستراليا، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وكان من أهم نتائجها، صعوبة إثبات جرائم الحاسب الآلي، وأنها من أكبر التحديات التي تواجه أجهزة التحقيق والقضاء في استراليا، وأن قطاعاً كبيراً من المحققين قليلي الخبرة يواجهون صعوبات فنية وعملية للحصول على أدلة كافية للإدانة في هذه الجرائم، وأن أغلب المدانين في جرائم الحاسب الآلي من أصحاب المهارات الفنية في استخدامه.

لذلك أوصت الدراسة بضرورة عقد دورات تدريبية متقدمة في مجال جرائم الحاسب الآلي للمسؤولين عن التحقيق في تلك الجرائم.

كما أجرى بحر (١٩٩٩م) عن «معوقات التحقيق في جرائم الإنترنت» هدفت إلى التعرف على معوقات التحقيق في جرائم الإنترنت عند ضباط الشرطة في البحرين. وقد أجريت الدراسة على المحققين بأقسام الشرطة بالبحرين، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وكان مـن أهم نتائجها: أن نقص الخـبرة والتدريب في مجال التحقيق في هذه الجرائم أدى إلى فشل العديد من أجهزة الشرطة في مكافحتها كما أشارت الدراسـة إلى أن أكثر من ثلثي عينتها وهم من ضباط الشرطة يعتقدون أنه لا يوجـد لديهم المهارات الفنية التي ينبغي توافرهـا لإتمام عمليات التحقيق في جرائم الحاسـوب والإنترنت وقلة الدورات التخصصية للتحقيق في جرائم الإنترنت من قبل جهة العمل وعدم كفاءة هذه الدورات إن وجدت، لذلك أوصـت الدراسـة بـضرورة تكثيف الـدورات التدريبية بكافة مسـتوياتها في مجال الحاسب الآلي والإنترنت وإنشاء موقع على الإنترنت يهدف إلى الارتقاء بمسـتوى العاملين في جهاز الأمن على أن يتولى الإشراف عليه متخصصون وخبراء في المجال الأمني والتدريب، وإدخال تعديلات جوهرية على مناهج المعاهد والكليات الأمنية لتواكب تطورات تقنية المعلومات والجرائم المرتكبة بواسطتها.

كما أجرى(Smith 2001) دراسـة عن المشكلات التي تواجه المحققين في جرائم الحاسـوب، بهدف التعرف على المشكلات التي تواجه المحققين في جرائم الحاسـوب التي من أهمهـا البعد الدولي، حيـث إن الملاحقة القضائية قـد تتطلـب توجيه اتهام أو رفـع دعوى على أشـخاص أو جهات موجودين في دول أخـرى، وهذا الأمر يؤخر إجراءات التحقيق ويرفع كلفته ويزيد من أعبائه. وهي دراسة وصفية مكتبية، وقد استخدم الباحث المنهج الوصفي.

وقـد توصلت إلى نتائـج منها أن جرائم الحاسـوب خلقت إشـكاليات محددة تتركز بشـكل رئيـسي في كون الكثير من هذه الجرائـم يمكن أن تكون غير قارية، وهذا يبرز مشـكلات حق إقامة الدعوى والاختصاص القضائي

ويزيـد من صعوبات التصدي لهذه الجرائم، كما أن مستوى الخبرة والتمويل المـالي المتوفـرة لدى أجهزة الشرطة تعـد غير ملائمة للتعامل مـع العديد من حوادث وجرائم الحاسوب التي لا تتمثل في مدى صعوبة التحقيق فيها، وإنما قـدرة أجهزة الشرطة عـلى توفير الكفاءات المتخصصة في هـذا المجال لتتولى القيـام بهذه المهمـة وفي قدرتها على المحافظة عليهـم وتطوير قدراتهم. لذلك أوصـت بضرورة تطوير أدوات وأسـاليب التحقيق بحيـث تتيح للمحققين وخبراء الأدلة الجنائية الرقمية، تحريز ونقل هذه البيانات بشكل جيد وسليم تقنيـاً وقضائياً. والعمل على زيادة قـدرة رجال الشرطة والعدالة على فحص وتحليل هذه البيانات بحثاً عن أية أدلة جنائية.

وقام الشـهري (٢٠٠٢م) بدراسـة عن «المعوقـات الإدارية في التعامل الأمنـي مـع جرائم الحاسـب الآلي» بهدف التعـرف على أهـم المعوقات التي تواجـه اسـتخدام الحاسـب الآلي، وبصفة خاصة أثنـاء التحقيـق في الجرائم الإلكترونيـة. وقـد أجريت الدراسـة عـلى العاملـين في الأمن العـام بمدينة الرياض، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

توصلـت الدراسـة إلى نتائـج مـن أهمهـا: أن جرائم الحاسـب الآلي من أخطر الجرائم التي تقع على نظم المعلومات، وأنها في تزايد مستمر، وأن هناك إلماماً ومعرفة بجرائم الحاسب الآلي من قبل العاملين بالأجهزة الأمنية، وقلة انتشار جرائم الحاسـب الآلي بمدينة الرياض، وأن أهم المعوقات في التعامل الأمنـي مع جرائم الحاسـب الآلي هي نقص المعرفة بالحاسـب الآلي، ونقص مهـارات التعامل مع الإنترنت، وعدم كفاية التدريب، وعدم توفير الاتصال بالإنترنـت، وعـدم توافـر أجهـزة حاسـب آلي، وقلـة الخـبراء المختصين في التحقيـق في جرائم الحاسـب الآلي، بالإضافة إلى عـدم إبلاغ الجهات المجني عليها عن الجريمة، ونقص الأنظمة المجرمة لها.

وأوصت الدراسة بجملة توصيات من أهمها: تأهيل العاملين في مجال التحقيق على التحقيق في الجرائم الإلكترونية، والاستعانة بخبراء الحاسب الآلي في التحقيق في تلك الجرائم، وحث الجهات التي تتعرض للضرر والاختراق إلى الإبلاغ عن تلك الجرائم.

وأجرى حجازي (٢٠٠٢م) دراسة عن «الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت» بهدف التعرف على كيفية التقاط الدليل الإلكتروني في جرائم التزوير باستخدام الكمبيوتر والإنترنت. وهي دراسة وصفية مكتبية، وقد استخدم الباحث المنهج الوصفي.

توصلت الدراسة إلى نتائج من أهمها: وجود صعوبات تواجه عملية استخلاص الدليل الإلكتروني في الجريمة المعلوماتية من أهمها: نقص خبرة أجهزة العدالة بصفة عامة، ونقصها لدى الأجهزة الأمنية بصفة خاصة، فيما يتعلق بثقافة الحاسب الآلي وتقنياته في مختلف مناحي الحياة قياساً بالدول الغربية، حيث إن امتلاك رجال الأمن للمهارات الشرطية في التحقيق التي طالما أسعفتهم في التصدي للجرائم التقليدية لن تكون ذات فائدة تذكر عندما يتعلق الأمر بالتحقيق في جرائم الحاسب الآلي والإنترنت؛ لأن الأخيرة تتصف بطابع تقني خاص يميز أدلتها، وطرق الكشف عن مرتكبيها، تمييزاً كبيراً عن مثيلاتها في الجرائم التقليدية.

وأوصت الدراسة بجملة توصيات من أهمها منح المختصين بالتحقيق في الجرائم الإلكترونية دورات تدريبية تخصصية لتمكينهم من استيعاب تقنيات الحاسب الآلي وبرامجه وأنظمته، والتعرف على طبيعة الجريمة الإلكترونية وطرق ارتكابها، وأساليبها، وأدواتها.

٢ . ٢ . ٣ الدراسات التي تناولت مكافحة الجرائم الإلكترونية

أجرى (Thompson1991) دراسة عن «المهارات التحقيقية في التسعينيات وما بعدها» بهدف التعرف على دور المهارات التحقيقية في مكافحة الجرائم الإلكترونية، من خلال الكشف عن دور الفهم الصحيح لتقنية الحاسب الآلي في التعرف على الأدلة الإلكترونية وجمعها. وقد أجريت الدراسة على المحققين في كانبيرا باستراليا، وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وقد توصلت إلى نتائج من أهمها: أهمية امتلاك محققي الجرائم ذات الطابع التجاري مهارات خاصة تتمثل في الفهم الصحيح لتقنية الحاسوب وأنظمة المعلومات الخاصة بالأعمال التجارية ليتمكنوا من التقاط الأدلة الإلكترونية وجمعها أثناء التحقيقات، وأهمية إلمام رجال الشرطة بأصول التعامل مع الحاسوب بما يكفي لتفتيش وضبط الأجهزة وأنظمة المعلومات الحاسوبية المستخدمة في ارتكاب الجرائم الإلكترونية.

وقد أوصت الدراسة بضرورة منح الضباط دورات تدريبية تخصصية في أصول التعامل مع الحاسوب، وكيفية تفتيش وضبط الأجهزة، والعمل على رفع مهاراتهم في مجال التحقيق، وكيفية استخلاص الأدلة الرقمية ذات القيمة في الإثبات من سجلات العمل العادية المسجلة في الحاسب الآلي.

وأجرى (Kelly 1995) دراسة عن «جرائم الكمبيوتر» بهدف التعرف على التطور المتوقع لجرائم الحاسب الآلي كماً وكيفاً، وأسباب عدم اهتمام رجال العدالة بهذه الجرائم التي ترتفع وتزداد آثارها السلبية يوماً بعد يوم، وأسباب عدم إدراجها كتصنيف مستقل ضمن الإحصائيات الخاصة بأنواع الجرائم المختلف، وأسباب عدم الإبلاغ عن التعرض لهذه الجرائم. وقد أجريت

الدراسة على العاملين في أقسام التحقيق الفيدرالية، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

توصلت الدراسة إلى نتائج من أهمها: يرجع عدم اهتمام رجال العدالة بالجرائم الإلكترونية إلى قلة إلمامهم بأساليب التحقيق في هذه الجرائم، فضلاً عن اعتبارها عبئاً إضافياً عليهم بجانب الجرائم التقليدية، مما يجعلهم مطالبين بالتدريب على هذه الجرائم التقنية التي تتطلب تخصصاً دقيقاً وقدرة متطورة على استخدام الحاسب الآلي والإلمام بتفاصيل إساءة استخدامه لاستخلاص الأدلة الرقمية وتكوين قناعة بها أمام الجهات القضائية، وأفضل الطرق والأساليب للتعامل مع الأدلة الرقمية، حيث إن التعامل الخاطىء قد يترتب عليه فقدانها أو إتلافها.

وأوصت الدراسة بجملة توصيات من أهمها: تنمية ثقافة الحاسوب لدى رجال الشرطة، والحاجة لتزويدهم بتدريب متخصص للإلمام بتفاصيل الحاسب الآلي وكيفية استخدامه في ارتكاب الجرائم الإلكترونية، وكيفية استخدام تقنيات التتبع واسترجاع المعلومات لالتقاط الدليل الرقمي.

وأجرى(Groover 1996) دراسة عن «مواجهة الصعوبات بالإعداد لمواجهة جرائم الكمبيوتر» بهدف التعرف على الصعوبات التي تواجه المحققين ورجال الشرطة عند التصدي لجرائم الحاسب الآلي. وقد أجريت الدراسة على العاملين في المركز الوطني للجرائم البيضاء بالولايات المتحدة الامريكية، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وقد توصلت إلى نتائج من أهمها: يشكل تزايد استخدام الحاسب الآلي في إنجاز الأعمال الرسمية عبئاً على جهات إنفاذ العدالة في ظل قصور

تدريب وفاعلية المحققين في مجال الحاسب الآلي، حتى إن أبسط استخدامات الحاسب الآلي في أية جريمة قد يعد عائقاً للتحقيق إذا كان رجال الشرطة يجهلون التعامل معه، فالكثير من الأدلة قد يضيع أو يتبدد عند إساءة التعامل مع الحاسبات الآلية الموجودة في مسرح الجريمة.

وقد أوصت الدراسة بضرورة إيجاد الكوادر البشرية المؤهلة على التحقيق في جرائم الحاسوب، من خلال التدريب اللازم لإكسابهم المهارات الخاصة بالتحقيق في تلك الجرائم، فضلاً عن ضرورة إلمام رجال الشرطة بجرائم الحاسب الآلي فيما يتعلق بتحريز الأدلة أو على الأقل حماية مسرح الجريمة ومنع يد العبث من الامتداد إليه، بجانب زيادة أعداد العاملين في مجال الحاسب الجنائي لكي يتمكنوا من التصدي لمشكلة الجرائم الإلكترونية، والعمل على دمج الحاسوب في التدريب الأساسي لضباط الشرطة، وتفعيل دور الحاسوب في العمل الشرطي، وأتمتة المكاتب وإدراج المعلومات المتعلقة بالقضايا في أنظمة حاسوبية خاصة، وأن التطوير يجب أن يكون مسؤولية الإدارات الرسمية، وضرورة توفير الدعم المالي المناسب لتطوير أداء الضباط فيما يتعلق بالتحقيق في جرائم الحاسب الآلي.

وأجرى (Tim 1998) دراسة عن «جرائم الحاسب الآلي» بهدف التعرف على جرائم الحاسب الآلي، والآثار المترتبة عليها. وقد أجريت الدراسة على الشركات الأمريكية العاملة في مجال أمن المعلومات، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وتوصلت الدراسة إلى نتائج من أهمها: أن (٥٢٠) شركة أمريكية أبلغت عن فقدان ما قيمته (١٢٠) مليون دولار بسبب جرائم الحاسب الآلي عام

١٩٩٧م، بزيادة قدرها (٠,٣٦٪) عن عام ١٩٩٦م، وأن (٠,٥٤٪) من المشمولين بالدراسة يرون أن مؤسساتهم قد تعرضت للاختراق والتعدي.

وقد أوصت الدراسة بضرورة استخدام نظم أمن المعلومات، وجدران الحماية التي تحد من الاختراق والتعدي، وضرورة إبلاغ الشرطة عن أي حالة اختراق أو تعد.

وقام كل من المسند والمهيني (٢٠٠١م) بدراسة عن «جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات» بهدف التعرف على جرائم الحاسب الآلي، وأنواعها، وأثرها على المجتمع وأساليب مكافحتها. وهي دراسة وصفية مكتبية، واستخدم الباحث المنهج الوصفي.

توصلت الدراسة إلى نتائج من أهمها: تشكل جرائم الحاسب الآلي في ضوء دعم الإنترنت وانتشارها السريع تهديداً مباشراً وخطيراً للأمن الوطني والاقتصاد المحلي والعالمي، وأنها تعد بمثابة انتهاك لحقوق الأفراد والمؤسسات على اختلاف أنواعها، وأن المتسللين والمتطفلين قد وجدوا ضالتهم في الشبكة العالمية لممارسة جرائم التزوير واختلاس الأموال والقرصنة المعلوماتية والتجسس، وصعوبة اكتشاف جرائم الحاسب الآلي لعدم وجود شهود، ولصعوبة استخلاص الأدلة الرقمية التي تشير إلى الجاني، وأن أكثر المنشآت التي تتعرض للتعدي والاختراق تتكتم على ما يحدث لنظم معلوماتها من اختراق وتعد، وأن جرائم الحاسب الآلي تعطل نشاطات المؤسسات بشكل كلي أو جزئي.

وأوصت الدراسة بجملة توصيات من أهمها: تعزيز التعاون الدولي والإقليمي في جرائم الحاسب الآلي، وإنشاء أقسام متخصصة للتحقيق في

جرائم الحاسب الآلي، وإنشاء قاعدة بيانات لوصف جرائم الحاسب الآلي.

وأجرت(Etter 2001) دراسة عن جرائم الحاسوب المستحدثة وطرق التصدي لها بهدف التعرف على أهم المهارات والمعارف الجديدة التي يمكن من خلالها التصدي لجرائم الحاسوب المستحدثة. وقد أجريت الدراسة على المحققين بأقسام الشرطة في مدينة استراليا، واستخدمت الباحثة المنهج الوصفي بأسلوب المسح الاجتماعي.

وتوصلت الدراسة إلى نتائج من أهمها: امتلاك المهارات بشكل عام والمهارات التخصصية بشكل خاص لكوادر الأدلة الجنائية لن يكون هدفاً سهلاً. كما أن المهارات المطلوبة لا تنحصر فقط في القدرة على التعامل مع الجرائم ذات الطابع التقني البحت. لأن الشرطة يجب أن تكون قادرة على القيام بعملها في مسرح الجريمة الذي يحتوي على حواسيب أو تقنيات حديثة بنفس الكفاءة التي تتعامل فيها مع مسرح الجريمة من أية أبعاد تقنية.

وقد أوصت الدراسة إلى ضرورة أن يفهم الجميع أن الشرطة لن تستطيع بإمكاناتها أن تتصدى لجميع الجرائم ذات الصلة بالحاسوب، وأنه يجب تحديد أبعاد واضحة في طبيعة التعاون المشترك بين جميع الجهات في ذلك ينبغي وضع برامج تدريبية لرجال الشرطة تمكنهم من اكتساب مهارات وتقنيات وأساليب تحقيقية جديدة تساعدهم في كشف وإثبات جرائم الحاسوب.

كما أجرى(Hollis et. al 2001) دراسة عن «احتياجات ومتطلبات رجال العدالة لمكافحة الجرائم الإلكترونية» بهدف تقدير احتياجات ومتطلبات رجال العدالة لمكافحة الجرائم الإلكترونية. والتعرف على نوعية الخبرات التي ينبغي على فريق التحقيق في وحدات الجرائم الإلكترونية الإلمام بها. وقد أجريت الدراسة على العاملين في المعهد الوطني للعدالة

التابع لوزارة العدل الأمريكية، واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

وتوصلت إلى نتائج من أهمها: حاجة رجال العدالة إلى الدعم لإنشاء وتطوير وحدات تحقيق في جرائم الحاسوب. وإنشاء وحدات للفحص والتحليل قابلة للتطوير في مجال الأدلة الجنائية الرقمية.

وأوصت الدراسة بضرورة التعاون بين الجهات الحكومية والقطاع الخاص في مجال مكافحة الجرائم الإلكترونية وذلك بالإبلاغ عن الجرائم التي تقع على مؤسسات القطاع الخاص والمساعدة في دعم وتدريب رجال الشرطة لذلك أوصت الدراسة بحاجة منسوبي الشرطة إلى المساعدة في وضع تصور لأفضل الإجراءات والدروس المستفادة من وحدات التحقيق الناجحة والقائمة حالياً مع العمل على دعم التوجه إلى إنشاء وحدات قوة مهام على مستوى المناطق لمباشرة التحقيق في الجرائم الإلكترونية ذات الطابع التقني الشديد التعقيد. وأهمية إيجاد آليات فعالة للاتصال والتعاون وتبادل الخبرات والمشاركة في الموارد بين العاملين بالتحقيق في جرائم الحاسوب في كافة المواقع والتخصصات.

وأجرى(Rapalus 2002) دراسة عن «جنايات أمن المعلومات» بهدف التعرف على جرائم نظم المعلومات وأنواعها، وأسبابها، وآثارها، وأساليب مكافحتها. وقد أجريت الدراسة على العاملين في معهد أمن الحاسب الآلي والعاملين في مراكز أمن المعلومات بالولايات المتحدة الأمريكية. واستخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

توصلت الدراسة إلى نتائج من أهمها: تكبد مؤسسات الأعمال الأمريكية خسائر مالية متزايدة نتيجة التعرض لجرائم أمن المعلومات، وبلغ متوسط

الخسائر السنوية على مدى ثلاث سنوات قبل عام ٢٠٠٠م نحو ١٣٠ مليون دولار، وأن غالبية من يسيئون استخدام الشبكة من الموظفين في المؤسسات، وأن أهم أوجه الإساءة تتمثل في الاتصال بمواقع لصور إباحية، ولبرمجيات قرصنة وطباعة محتوياتها، أو استخدام غير لائق لنظم البريد الإلكتروني، وأن نسبة قليلة تقوم بالإبلاغ عن سرقة المعلومات أو البيانات التي تتعلق بمعاملات تجارية، وأن هناك زيادة مستمرة في جرائم نظم المعلومات، وأن جرائم الفيروسات تأتي في المرتبة الأولى، تليها جرائم التخريب، وأخيراً جرائم التزوير والاحتيال المالي.

وأوصت الدراسة بجملة توصيات من أهمها: تعزيز التعاون الدولي لمواجهة جرائم الحاسب الآلي، وإنشاء هيئة عليا للتحقيق في جرائم الحاسب الآلي، وزيادة العقوبات المقررة على مرتكبي جرائم الحاسب الآلي.

كما أجرى(Cert 2002) دراسة عن «منظمة طوارىء الحاسب الآلي» بهدف التعرف على المخالفات التي ترتكب باستخدام الحاسب الآلي عبر شبكة الإنترنت، وأساليب مكافحة جرائم الإنترنت. وقد أجريت الدراسة على العاملين في منظمة طوارىء الحاسب الآلي بالولايات المتحدة الأمريكية. وقد استخدم الباحث المنهج الوصفي بأسلوب المسح الاجتماعي.

توصلت الدراسة إلى نتائج من أهمها: كلما زادت الحاجة لاستخدام نظم المعلومات، زاد عدد مستخدمي الإنترنت، وترافق مع ذلك زيادة في معدلات ارتكاب الجرائم عن طريقها.

وأوصت الدراسة بجملة توصيات من أهمها: استخدام برامج الحماية التي تقي من الاختراق والتعدي، وتعديل التشريعات العقابية لكي تتواكب مع الجرائم الإلكترونية المستحدثة.

٢. ٢. ٤ التعقيب على الدراسات السابقة

اهتمت هذه الدراسات والبحوث من حيث التحقيق في جرائم الحاسوب، كدليل على خطورة هذه الجرائم سواء على المستوى الدولي أو المستوى المحلي وأن العمل على إثبات هذه الجرائم ومعاقبة مرتكبيها هدف أساسي من أهداف رجال الشرطة والعدالة على حد سواء. وانطلقت بعض هذه الدراسات من منظور تحديد الأدلة الجنائية في جرائم الكمبيوتر والإنترنت، ووسائل التحقيق فيها والمعوقات التي تعوق إثباتها، وأهم الجرائم المستحدثة منها، والمشكلات التي تواجه المحققين فيها، واحتياجات رجال العدالة لمكافحة هذه الجرائم. كما ركزت الدراسات السابقة على بعض المعوقات التي تعوق إثبات الأدلة في الجرائم المعلوماتية مثل قلة خبرة رجال الأمن والعدالة بهذه الجرائم، نقص المهارات اللازمة للتحقيق في هذه الجرائم، وأن جرائم الحاسوب غير قارية، (عبر وطنية) وهذا يزيد من صعوبة التصدي لها. والدراسات السابقة تدور حول الصعوبات التي تواجه التحقيق في جرائم الكمبيوتر وقد استفاد الباحث من تحليل البحوث والدراسات السابقة في التعرف على أهم الصعوبات التي تواجه اكتشاف جرائم الكمبيوتر، وأن للخبرة دوراً أساسياً في كشف جرائم الكمبيوتر لذلك عني الباحث أن تكون عينة الدراسة من المعنيين بالتحقيق مباشرة بهذه الجرائم وكيفية التصدي لها.

وبصفة عامة فقد حاول الباحث الاستفادة من إجراءات ونتائج وتوصيات الدراسات السابقة فيما يتفق مع دراسته إلا أن الدراسة الحالية تهدف إلى التعرف على فاعلية الأساليب المستخدمة في إثبات جريمة التزوير

الإلكتروني والتي تمكن المحققين في أقسام المكافحة من التصدي لهذه الجرائم وهذا. ما لم تتطرق له الدراسات السابقة.

وقد تناولت الدراسات السابقة التحقيق في الجرائم الإلكترونية، ومعوقات التحقيق في الجرائم الإلكترونية، ومكافحة الجرائم الإلكترونية بدرجات متباينة، فقد ركزت دراسة الكركي على الأسس الفنية الدقيقة لرفع وتحريز الأدلة الرقمية بصفة عامة، أما دراسة حجازي فتناولت الدليل الجنائي الرقمي وكيفية التعامل معه من قبل المحققين الجنائيين، والجوانب التشريعية المتعلقة به والتي قد تؤثر على مصداقية الدليل الرقمي أمام الجهات القضائية، بينما ركزت دراسة البشرى على عدم جدوى المهارات التقليدية التي يتمتع بها ضباط الشرطة في مواجهة الجرائم الإلكترونية باعتبارها ذات طبيعة متباينة، وتتطلب توافر مهارات فنية وخبرة متخصصة، وأكدت دراسة رستم أهمية إيجاد آلية تدريب واحدة لتنمية مهارات منسوبي التحقيق وزيادة قدرتهم على التحقيق في الجرائم الإلكترونية والتقاط الأدلة الرقمية.

وتميزت دراسة العنزي بتناول وسائل التحقيق التي من أهمها الوسائل العلمية في التحقيق في الجرائم الإلكترونية، والمهارات المطلوب توافرها في المحقق الفني للتحقيق في الجرائم الإلكترونية، لكنها تناولت الجرائم الإلكترونية بصفة عامة ولم تنفرد بالتركيز على جريمة التزوير كإحدى الجرائم ذات التأثيرات السلبية التي يمكن ارتكابها سواء من قبل المخترقين، أو من قبل المصرح لهم بالاستخدام ممن يسيئون استغلال الثقة من العاملين في المنظمات الحكومية والخاصة. أما دراسة بحر فقد ركزت على جرائم الإنترنت، وهدفت إلى الوقوف على المعوقات التي تحد من قدرة ضباط الشرطة على التحقيق في هذه الجرائم.

ويتضح من خلال تتبع جميع الدراسات العربية أنها لم تتناول جرائم

التزوير الإلكتروني أو سرقة منظومة التوقيع الإلكتروني بتوسع، وكان لتشعب مجالات الدراسة من خلال دراسة أنواع الجرائم الإلكترونية كافة دورها في عدم تركيز الاهتمام على جريمة التزوير بعينها، بالرغم من أن جرائم التزوير تتضمن في طياتها تغيير المحررات، والتقليد، والاصطناع، والتحريف، فضلاً عن سرقة منظومة التوقيع الإلكتروني وما يترتب على ذلك من مخالفات، أو التزوير من قبل المصرح لهم باستخدام النظام والدخول عليه، أو انتحال شخصية المواقع أو الأشخاص واستخدامها، وهو ما تتميز به هذه الدراسة فجريمة التزوير متشعبة بحيث لا يمكن إضافة جرائم أخرى معها.

أما الدراسات الأجنبية فقد ركزت غالبيتها على التحقيق في جرائم الحاسوب، والمهارات الواجب توافرها للتحقيق في جرائم الحاسوب، والمعوقات التي تواجه المحققين والتي من أهمها عدم الإلمام بتقنية المعلومات، أو ضعف القدرة على استخدام الحاسب الآلي أو معرفة مصطلحاته ومفاهيمه، ومن ثم عدم الاهتمام بالجرائم الإلكترونية، وعدم الرغبة في التحقيق فيها، مما ينعكس سلباً على أمن المعلومات نتيجة انتشار هذه الجرائم يوماً بعد يوم وصعوبة اكتشافها،ونقص المتخصصين في مجال الحاسب الجنائي،وارتفاع تكلفة إعداد الكوادر البشرية القادرة على التحقيق في جرائم الحاسب الآلي.

وتتميز الدراسة الحالية عن جميع الدراسات السابقة في تركيزها على التعرف على فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني وقدرتها على كشف غموض هذه الجرائم، وإيجاد العلاقة بين الجاني والمجني عليه، وتحديد المواقع التي يتم منها الاختراق والتعدي على نظم المعلومات وقواعد البيانات وتغيير مضمونها بما يغاير الحقيقية للحصول على مخرجات إلكترونية مزورة تحقق له أو لمن يعمل لحسابه مصالح. ولذلك تكتسب هذه الدراسة أهمية خاصة في ضوء انتشار هذه الظاهرة، واستغلالها في ارتكاب

جرائم تنعكس سلباً على أمن الوطن والمواطن في ضوء انتشار التعاملات الإلكترونية في الجهات الحكومية، ومكمن الخطورة ليس في عمليات الاختراق والتعدي، ولكن في استغلال بعض المصرح لهم بالدخول على نظم المعلومات ومنحهم هذه الثقة في ارتكاب عمليات تزوير بغرض الكسب غير المشروع (الرشوة)، ومن ثم تبديد الأمن المعلوماتي الذي تتميز به التعاملات الإلكترونية وفقدان الثقة في مصداقيتها، مما يلفت النظر لأهمية اتخاذ إجراءات تحول دون تغيير البيانات الموجودة إلا في إطار تعديلات محددة، والتحكم في قواعد البيانات من خلال غرفة تحكم مركزية للتعرف على ارتكاب أية تعديلات ومن قام بارتكابها، ومدى مشروعيتها، فضلاً عن سعي هذه الدراسة خلال جانبها النظري والعملي لإبراز فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني وصور جرائم التزوير الإلكتروني ووسائل ارتكابها وبيان سمات المجرم والمجني عليه في جرائم التزوير الإلكتروني وفاعلية الأساليب التي يتبعها المحقق الجنائي والفني في التحقيق في جرائم التزوير الإلكتروني والتعرف على المعوقات التي تؤدي إلى عدم فاعليتها في إثبات الجريمة في محاولة للفت نظر المختصين بأهمية إكساب العاملين في مجال التحقيق للمهارات الفنية اللازمة للتحقيق الجنائي والفني في جرائم المعلوماتية بصفة عامة، وجرائم التزوير الإلكتروني بصفة خاصة ودعم فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني والعمل على رفع كفاءتها وتحديثها باستمرار لتواكب الثورة المعلوماتية الإلكترونية.

الفصل الثالث

الإجراءات المنهجية للدراسة

٣. الإجراءات المنهجية للدراسة

٣. ١ منهج الدراسة

استخدم الباحث المنهج الوصفي الذي يعتمد على دراسة الظاهرة كما هي في الواقع، بوصفها وصفاً دقيقاً، والتعبير عنها كيفياً وكمياً، حيث يصف التعبير الكيفي الظاهرة ويوضح خصائصها، بينما يعطي التعبير الكمي وصفاً رقمياً يوضح مقدار الظاهرة أو حجمها (عبيدات، ٢٠٠٦م: ص٣٠٧)، كما لا يتوقف هذا المنهج عند جمع المعلومات الخاصة بالظاهرة لاستقصاء مظاهرها وعلاقاتها المختلفة، بل يمتد ليشمل التحليل والربط والتفسير للوصول إلى استنتاجات يبنى عليها التصور المقترح (العساف، ٢٠٠٠م: ص١٨٦).

كما استخدم الباحث منهج تحليل المضمون الذي يعني تحليل الظاهرة وفقاً لفئات محددة يعتمد عليها للوصول إلى وصف كمي هادف ومنظم (العساف، ٢٠٠٠م، ص٢٣٥)، من خلال الرجوع إلى عشرين حكماً صادراً عن الدوائر الجزائية المختلفة بديوان المظالم تضمنت قرارات عن ارتكاب جريمة التزوير الإلكتروني بهدف تحليلها وتوضيح هذه المخالفات، وتطبيقاتها، والعقوبات المترتبة عليها، والإجابة عن التساؤل السادس والسابع والعاشر التي سعت للتعرف على فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والأساليب الأساليب الإجرائية والتقليدية والمادية المستخدمة في إثبات جرائم التزوير الإلكتروني.

٣. ٢ مجتمع الدراسة

يتشكل مجتمع الدراسة من المحققين الجنائيين والفنيين العاملين في مكافحة التزوير في الأمن العام وعددهم (٨٠) محققاً جنائياً، و(٧٥) محققاً فنياً من خلال الحصر الشامل لهم، والمحققين الجنائيين والفنيين العاملين في مكافحة التزوير بالجوازات وعددهم (٥٦) محققاً جنائياً، و(٤٢) محققاً فنياً من خلال الحصر الشامل لهم، وبذلك يبلغ العدد الإجمالي لمجتمع الدراسة (٢٥٣) محققاً. وقد وقع اختيار الباحث على العاملين في مكافحة التزوير في الأمن العام والجوازات لأنهم المختصون بمكافحة جرائم التزوير بحكم الاختصاص، وكان اختيار الباحث للمحققين الجنائيين والفنيين لاستقصاء آرائهم نحو فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني في ضوء الخبرات الذاتية العلمية والفنية لكل منهم واكتشافهم لعمليات التزوير خلال ممارستهم العملية في مدن المملكة العربية السعودية حسبما ورد في التنظيم الإداري للمناطق حيث وزعت أداة الدراسة على (١٣) منطقة إدارية.

ونظراً لمحدودية حجم مجتمع الدراسة، فقد قام الباحث بحصر شامل لجميع مفردات مجتمع الدراسة، لضمان توفر أغلب الخبرات العملية لدى مفردات مجتمع الدراسة، وتم توزيع الاستبانات عليهم واسترجاعها بطريقة مباشرة من قبل الباحث، وكان عدد الاستبانات المستردة (٢٤٥) استبانة، من بينها (٤) استبانات غير مكتملة الإجابة، وبذلك أصبح عدد الاستبانات الصالحة للتحليل (٢٤١) استبانة بنسبة (٩٥,٣ ٪) من الاستبانات الموزعة على مفردات مجتمع الدراسة، كما يتضح من الجدول رقم (١)، والتي يمكن اعتبارها عينة عشوائية كبيرة ممثلة لمجتمع الدراسة.

وهـذا المجتمع أعني بـه المعنيين بمكافحـة جريمة التزويـر الإلكتروني مـن المحققـين الجنائيين والفنيـين، وذلك بالتعـرف على آرائهم نحـو فاعلية الأساليب المسـتخدمة في إثبات هذه الجريمة، لأنهم المسؤولون عن مكافحة هذه الجريمة في المملكة.

٣. ٣ أداة الدراسة

قام الباحث بجمع بيانات هذه الدراسة باستخدام الأدوات التالية:

البيانات المكتبية

هـي البيانات الأساسـية (الأوليـة) والثانوية التي تمثـل الخلفية النظرية التي بنيت عليها هذه الدراسة بالاعتماد على التالي:

١ ـ الكتب العلمية.

٢ ـ البحوث والدراسات العلمية التي بحثت في موضوع الدراسة.

٣ ـ البحـوث والدراسـات العلميـة التـي بحثت في موضوع الدراسـة المنشورة في الدوريات العلمية المُحكَّمة.

٤ ـ الدراسات السابقة المتعلقة بموضوع الدراسة.

٣. ٤ إجراءات التطبيق واختبارات الصدق والثبات

البيانات الميدانية

قام الباحث بجمعها عن طريق الاستبانة لخدمة أغراض الدراسة، وقد صمّم الباحث الاستبانة وفق أسئلة الدراسة على النحو التالي:

٣ . ٤ . ١ بناء أداة الدراسة

لتحديد آراء المحققين الجنائيين والفنيين العاملين في مكافحة التزوير في الأمن العام والجوازات نحو فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني من خلال الكشف عن خصائص جريمة التزوير الإلكتروني، وصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني قام الباحث بإعداد استبانة لجمع البيانات والمعلومات من مفردات مجتمع الدراسة، وجاء البناء على النحو التالي:

١ ـ البيانات الأولية

اشتملت على الخصائص الديموجرافية لمفردات مجتمع الدراسة وتكونت من تسع فقرات هي: العمر، المؤهل التعليمي، جهة العمل، منطقة العمل، الرتبة العسكرية، طبيعة العمل، سنوات الخبرة في مجال العمل، الدورات التدريبية في مجال جرائم التزوير المعلوماتية.

٢ ـ محاور أداة الدراسة

اشتملت الدراسة على ثمانية محاور رئيسة تضمنت (١٢٠) عبارة بواقع (١٥) عبارة لكل محور، وسوف يستخدم الباحث مقياس (ليكرت) الخماسي حسب التنوع (موافق بشدة، موافق، محايد، غير موافق، غير موافق مطلقاً)، حيث يعبر الرقم (٥) عن أكبر درجة (موافق بشدة) ويعبر الرقم (١) عن أصغر درجة (غير موافق مطلقاً).

وقد جاءت المحاور على النحو التالي:

ـ المحور الأول: خصائص جريمة التزوير الإلكتروني.

ـ المحور الثاني: صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

ـ المحور الثالث: الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني.

ـ المحور الرابع: سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني.

ـ المحور الخامس: سمات المجني عليه في جرائم التزوير الإلكتروني.

ـ المحـور السـادس: فاعلية الأسـاليب التـي يتبعها المحقـق الجنائي في إثبات جرائم التزوير الإلكتروني.

ـ المحور السـابع: فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني.

ـ المحـور الثـامن: المعوقـات التـي تـؤدي إلى عـدم فاعليـة الأسـاليب المسـتخدمة مـن المحقـق الجنائـي والفنـي في إثبـات جرائـم التزوير الإلكتروني.

والجدول رقم (١) يوضح توزيع أداة الدراسة.

الجدول رقم (١) توزيع أداة الدراسة

عدد الاستبانات	التوزيع	العائد	الفاقد	المستبعد	النهائي
المجموع	٣٥٢	٢٤٥	٨	٤	٢٤١
النسبة	١٠٠	٩٦,٨	٣,١	١,٦	٩٥,٣

٣ .٤ .٢ التحقق من مدى صدق أداة الدراسة

تعـد الأداة صادقـة إذا تمكنت من قياس ما صُممت لقياسـه، وحددت مدى صلاحية درجاته للقيام بتفسـيرات مرتبطة بالمجال المقاس (العسـاف، ٢٠٠٠م)، وقد تم التحقق من صدق الأداة من ثلاثة جوانب كما يلي:

١ ـ التحقق من مدى الصدق الظاهري لأداة الدراسة

تكـون أداة الدراسـة صادقـة إذا كان مظهرهـا يـدل على أنهـا تقيس ما وضعـت لقياسـه، وقـد تم التحقـق من مدى صـدق أداة الدراسـة بعرضها

على سبعة عشر محكماً، تم اختيارهم من ذوي الخبرة والمعرفة والكفاءة من الأساتذة في مجالات البحث العلمي (ملحق رقم ٢: قائمة بأسماء المحكمين ووظائفهم)، لإبداء مرئياتهم حيالها وفقاً للنقاط التالية:

- مدى مناسبة، وشمولية متغيرات البيانات الأولية.
- مدى أهمية ووضوح الصياغة اللغوية للعبارات.
- مدى انتماء كل عبارة لمحورها، ومدى قياسها لما وضعت من أجله.
- مدى ملاءمة ودقة تسمية كل محور، وتدرجات مقياسه.

وفي ضوء الملاحظات التي سوف يبديها المُحكِّمون، سيقوم الباحث بإجراء التعديلات التي اتفق عليها المُحكِّمون بحذف وتعديل صياغة بعض العبارات حتى تزداد أداة الدراسة وضوحاً، وملاءمةً لقياس ما وضعت من أجله.

٢ ـ التحقق من مدى الصدق البنائي لأداة الدراسة

قام الباحث بعد التأكد من الصدق الظاهري لأداة الدراسة بتحديد مدى التجانس الداخلي لأداة الدراسة من خلال حساب معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الذي تنتمي إليه، ثم حساب الارتباط المصحح بالمحور في حالة حذف العنصر من المحور، وحساب معامل إلفا إذا حذف العنصر. والجدول رقم (٢) يوضح معاملات صدق وثبات جميع عبارات الاستبانة بالدرجة الكلية لجميع عبارات المحور الذي تنتمي إليه.

الجدول رقم (٢) التحليل السيكومتري للاستبانة

م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط	م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط
المحور الأول				المحور الثالث			
١	٠,٦٩٥٧	٠,٢٣**	٠,٣٣٣**	١	٠,٩١٧٥	٠,٥٦**	٠,٦٣٣**
٢	٠,٦٩٤٣	٠,٢٥**	٠,٣٦٢**	٢	٠,٩١٤٢	٠,٦٦**	٠,٧١١**
٣	٠,٦٨٤١	٠,٣٥**	٠,٤٦٢**	٣	٠,٩١٤٥	٠,٦٥**	٠,٧٠١**
٤	٠,٦٩١٢	٠,٢٨**	٠,٤٠٠**	٤	٠,٩١٣٩	٠,٦٧**	٠,٧١٩**
٥	٠,٦٧٦٦	٠,٤٠**	٠,٥٢٦**	٥	٠,٩١٢٧	٠,٧١**	٠,٧٥٤**
٦	٠,٦٩٦٤	٠,٢٣**	٠,٣٥٣**	٦	٠,٩١٢٥	٠,٧٠**	٠,٧٥٦**
٧	٠,٦٧٢٣	٠,٤٢**	٠,٥٦٢**	٧	٠,٩١٣٢	٠,٦٩**	٠,٧٤٠**
٨	٠,٦٧٩٠	٠,٣٩**	٠,٥٠٦**	٨	٠,٩١٢٨	٠,٧٠**	٠,٧٤٨**
٩	٠,٦٧٩٦	٠,٣٩**	٠,٥٠٢**	٩	٠,٩١٦٤	٠,٥٩**	٠,٦٦٨**
١٠	٠,٦٩٢٠	٠,٣١**	٠,٤٩٠**	١٠	٠,٩١٣٤	٠,٦٨**	٠,٧٣٢**
١١	٠,٦٨٠٧	٠,٣٦**	٠,٥١٢**	١١	٠,٩١٢٧	٠,٧٠**	٠,٧٥٢**
١٢	٠,٦٨٦٦	٠,٣٢**	٠,٤٤٦**	١٢	٠,٩١٦٤	٠,٥٩**	٠,٦٥٦**
١٣	٠,٦٩٢٧	٠,٢٩**	٠,٤٧٠**	١٣	٠,٩١٨٦	٠,٥٠**	٠,٥٦٢**
١٤	٠,٧٠٢٦	٠,١٧**	٠,٣٠٥**	١٤	٠,٩١٦٩	٠,٥٧**	٠,٦٢٤**
١٥	٠,٦٩٨٠	٢١,٧٠	٠,٣٣٨**	١٥	٠,٩١٨٩	٠,٤٩**	٠,٥٥٥**
قيمة معامل ألفا كرونباخ للمحور الأول = ٠,٧٠٣٠				قيمة معامل ألفا كرونباخ للمحور الثالث = ٠,٩٢٠٢			

م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط	م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط
المحور الثاني				المحور الرابع			
١	٠,٨٤١١	٠,١٩**	٠,٣١٠**	١	٠,٧٩٥١	٠,٣٩**	٠,٤٨٨**
٢	٠,٨٣٣١	٠,٣٢**	٠,٤١٦**	٢	٠,٨٠٣٥	٠,٣٢**	٠,٤٦٠**
٣	٠,٨٢٠٩	٠,٥٣**	٠,٦١٧**	٣	٠,٧٩٦٨	٠,٣٨**	٠,٤٥٨**
٤	٠,٨٢٢٢	٠,٥٢**	٠,٥٩٨**	٤	٠,٧٩٣٢	٠,٤٢**	٠,٥٤٢**
٥	٠,٨٢٩٧	٠,٣٩**	٠,٤٩١**	٥	٠,٨٠٤٥	٠,٣١**	٠,٤٤٨**
٦	٠,٨٢٥٢	٠,٤٧**	٠,٥٦٦**	٦	٠,٨٠٠٠	٠,٣٢**	٠,٤١٤**
٧	٠,٨١٦٩	٠,٥٩**	٠,٦٧٠**	٧	٠,٨٠١٢	٠,٣٣**	٠,٤٥٣**
٨	٠,٨٣٤٩	٠,٣١**	٠,٤١٦**	٨	٠,٧٩٠١	٠,٤٧**	٠,٥٥٩**
٩	٠,٨٢٠٥	٠,٥٤**	٠,٦٢٣**	٩	٠,٧٨٩٦	٠,٤٧**	٠,٥٧٠**
١٠	٠,٨١٦٤	٠,٦٠**	٠,٦٧٨**	١٠	٠,٧٩١٢	٠,٤٥**	٠,٥٥٥**
١١	٠,٨٢١٤	٠,٥٣**	٠,٦١١**	١١	٠,٧٨٣٧	٠,٥٥**	٠,٦٣٥**
١٢	٠,٨٢٠٥	٠,٥٣**	٠,٦٢٧**	١٢	٠,٧٨٥١	٠,٥٤**	٠,٦٢٢**
١٣	٠,٨٢٥٩	٠,٤٥**	٠,٥٥٣**	١٣	٠,٧٨٤٦	٠,٥٧**	٠,٦٤١**
١٤	٠,٨٢١٢	٠,٥٣**	٠,٦١٣**	١٤	٠,٧٩١٤	٠,٤٥**	٠,٥٤٥**
١٥	٠,٨٣١٥	٠,٣٥**	٠,٤٣٨**	١٥	٠,٧٩٥٢	٠,٣٩**	٠,٤٩٣**
قيمة معامل ألفا كرونباخ للمحور الثاني = ٠,٨٣٥٣				قيمة معامل ألفا كرونباخ للمحور الرابع = ٠,٨٠٤٨			

م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط	م	معامل ألفا لكرونباخ إذا حذف العنصر	معامل الارتباط المصحح	معامل الارتباط
المحور الخامس				المحور السابع			
١	٠,٨٢٧٢	٠,٤٣**	٠,٥١٤**	١	٠,٨٩٨٣	٠,٥١**	٠,٥٦٩**
٢	٠,٨٢٥٠	٠,٤٦**	٠,٥٥٤**	٢	٠,٨٩٧٣	٠,٥٤**	٠,٥٩٩**
٣	٠,٨٢٧١	٠,٤٣**	٠,٥٢٧**	٣	٠,٩٠٠٥	٠,٤٦**	٠,٥٤١**
٤	٠,٨٢٣٨	٠,٤٩**	٠,٥٨٣**	٤	٠,٩٠٠٤	٠,٤٤**	٠,٥٠٨**
٥	٠,٨٢٨٢	٠,٤١**	٠,٥٠٦**	٥	٠,٨٩٧٤	٠,٥٣**	٠,٥٩٧**
٦	٠,٨٢٧١	٠,٤٣**	٠,٥٢٠**	٦	٠,٨٩٣٧	٠,٦٤**	٠,٦٩٥**
٧	٠,٨٢١٠	٠,٥٣**	٠,٦٢٠**	٧	٠,٨٩٦٤	٠,٥٧**	٠,٦٥٣**
٨	٠,٨٢١٩	٠,٥٢**	٠,٦٠١**	٨	٠,٨٩٤٧	٠,٦١**	٠,٦٧٨**
٩	٠,٨٢٥٠	٠,٤٧**	٠,٥٥٣**	٩	٠,٨٩٢٢	٠,٦٨**	٠,٧٣٠**
١٠	٠,٨٢١١	٠,٥٣**	٠,٦١٤**	١٠	٠,٨٩٦٠	٠,٥٧**	٠,٦٤٧**
١١	٠,٨٣٢٨	٠,٣٣**	٠,٤٢٤**	١١	٠,٨٩٣٩	٠,٦٣**	٠,٦٨٩**
١٢	٠,٨٣١٧	٠,٣٩**	٠,٥١٥**	١٢	٠,٨٩٠٥	٠,٧١**	٠,٧٦٣**
١٣	٠,٨٢١٨	٠,٥٢**	٠,٦١٦**	١٣	٠,٨٩٠٥	٠,٧١**	٠,٧٦٣**
١٤	٠,٨٢٤٦	٠,٤٧**	٠,٥٦٣**	١٤	٠,٨٩٢٨	٠,٦٥**	٠,٧١٥**
١٥	٠,٨٢٤٨	٠,٤٧**	٠,٥٥٩**	١٥	٠,٨٩٨٣	٠,٥١**	٠,٥٨٦**
قيمة معامل ألفا كرونباخ للمحور الخامس = ٠,٨٣٥٣				قيمة معامل ألفا كرونباخ للمحور السابع = ٠,٩٠١٩			

المحور السادس				المحور الثامن			
١	٠,٨٤٨٨	٠,٣٩**	٠,٤٨٦**	١	٠,٨٤٨٣	٠,٤١**	٧٠,٤٩٩
٢	٠,٨٤٧٣	٠,٤٢**	٠,٥٠٧**	٢	٠,٨٤٧١	٠,٤٥**	٠,٥٦١**
٣	٠,٨٤٥٠	٠,٤٧**	٠,٥٤٨**	٣	٠,٨٤٤٥	٠,٤٩**	٠,٥٨٧**
٤	٠,٨٤٨٤	٠,٣٩**	٠,٤٨٨**	٤	٠,٨٤٨٠	٠,٤٢**	٠,٥٠٢**
٥	٠,٨٤٠٧	٠,٥٦**	٠,٦٢٧**	٥	٠,٨٤٠٧	٠,٥٧**	٠,٦٣٨**
٦	٠,٨٤١٣	٠,٥٤**	٠,٦١٧**	٦	٠,٨٤٤٠	٠,٥٠**	٠,٦٠٣**
٧	٠,٨٤١٤	٠,٥٣**	٠,٦١٧**	٧	٠,٨٤٧٥	٠,٤٤**	٠,٥٣٧**
٨	٠,٨٤٣٠	٠,٥٠**	٠,٥٩٤**	٨	٠,٨٤٠٧	٠,٥٥**	٠,٦٣٧**
٩	٠,٨٤٠٨	٠,٥٤**	٠,٦٣٢**	٩	٠,٨٤٤٥	٠,٤٩**	٠,٥٧٧**
١٠	٠,٨٤٤٩	٠,٤٨**	٠,٥٧٧**	١٠	٠,٨٤٣٢	٠,٥١**	٠,٥٩١**
١١	٠,٨٤٧٣	٠,٤٤**	٠,٥٤٦**	١١	٠,٨٤٢٦	٠,٥٤**	٠,٦٠٤**
١٢	٠,٨٤٣٤	٠,٤٩**	٠,٥٨٠**	١٢	٠,٨٤٤٨	٠,٤٨**	٠,٥٧٤**
١٣	٠,٨٤٧٠	٠,٤٣**	٠,٥١٧**	١٣	٠,٨٤٣٧	٠,٥٠**	٠,٥٨٣**
١٤	٠,٨٣٧٧	٠,٦٠**	٠,٦٧٣**	١٤	٠,٨٤١٨	٠,٥٤**	٠,٦١٥**
١٥	٠,٨٤٣٢	٠,٥٠**	٠,٥٨٢**	١٥	٠,٨٤٦٤	٠,٤٦**	٠,٥٢٩**
قيمة معامل ألفا كرونباخ للمحور السادس = ٠,٨٥٢٩				قيمة معامل ألفا كرونباخ للمحور الثامن = ٠,٨٥٣٤			

** دال عند مستوى معنوية (٠١ , ٠).

وقد أظهرت مستويات الاختبار بالنسبة لجميع محاور الاستبانة أن جميع عباراتها مرتبطة ارتباطاً دالاً إحصائياً مع جميع عبارات المحاور التي تنتمي إليها عند مستوى معنوية (٠١ , ٠).

كما اتضح من الجدول رقم (٢) أن جميع العناصر (في جميع المحاور) كان معامل الثبات (ألفا) في حالة حذفها أقل من قيمة ألفا للمحور للكل، مما يعني أن جميع العناصر (داخل المحاور المختلفة) مهمة وغيابها عن المحور

يؤثـر سـلباً على مقيـاس المحور، أي أنه عنـصر ثابت ويؤثـر في ثبات المحور ككل ومن ثم الاستبانة ككل، فيما عدا العبارة رقم (١) من المحور الثاني، إلا أن معاملات الثبات الخاص بهذه العبارة ليس بالكبير بالقدر الذي يستدعي حذفها، خصوصاً أن معاملات الثبات للمحاور هي بالفعل عالية ولا تحتاج إلى زيـادة، وخصوصـاً وأن هـذه الزيادة تتطلـب التضحية ببعـض العناصر التي أثبتت أدبيات الدراسـة (الإطار النظري للدراسة والدراسات السابقة) حـول الموضوع أهمية أخذها في الحسـبان، لـذا رأى الباحث الاحتفاظ بها في الدراسة، حتى لا يخل بالإطار النظري والدراسات السابقة.

ويتضـح مـن الجدول رقـم (٢) أن معامـلات الارتباط بـين درجة كل عبارة والدرجة الكلية لجميع العبارات التي يتضمنها المحور تتمثل فيما يلي:

١ـ تراوحت معاملات الارتبـاط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الأول ما بين (٠,٣٠٥، ٠,٥٦٢) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠,٠١).

٢ ـ تراوحت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الثاني ما بين (٠,٣١٠، ٠,٦٧٨) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠,٠١).

٣ـ تراوحـت معامـلات الارتبـاط بـين درجـة كل عبـارة والدرجـة الكلية لعبارات المحـور الثالث ما بين(٠,٥٥٥، ٠,٧٥٦) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠,٠١).

٤ ـ تراوحـت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الرابع ما بين (٠,٤١٤، ٠,٦٤١) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠,٠١).

٥ ـ تراوحت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الخامس ما بين (٤٢٤ , ٠، ٦٢٠ , ٠) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠١ , ٠).

٦ ـ تراوحت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور السادس ما بين (٤٨٦ , ٠، ٦٧٣ , ٠) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠١ , ٠).

٧ ـ تراوحت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور السابع ما بين (٥٠٨ , ٠، ٧٦٣ , ٠) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠١ , ٠).

٨ ـ تراوحت معاملات الارتباط بين درجة كل عبارة والدرجة الكلية لعبارات المحور الثامن ما بين (٤٩٩ , ٠، ٦٣٨ , ٠) وهي معاملات ارتباط دالة إحصائياً عند مستوى معنوية (٠١ , ٠).

٣ .٤ .٣ فحص ثبات الاستبانة (ثبات أداة الدراسة)

قام الباحث بالتأكد من ثبات أداة الدراسة لاختبار معامل الثبات باستخدام طريقة الاتساق الذاتي، وهي طريقة ألفا كرونباخ، وكانت النتائج كما في الجدول التالي:

الجدول رقم (٣) معامل ثبات أداة الدراسة

م	المحور	عدد العبارات	عدد الحالات	معامل الثبات
١	المحور الأول	١٥	٢٤١	٠,٧٠
٢	المحور الثاني	١٥	٢٤١	٠,٨٣
٣	المحور الثالث	١٥	٢٤١	٠,٩٢
٤	المحور الرابع	١٥	٢٤١	٠,٨٠
٥	المحور الخامس	١٥	٢٤١	٠,٨٤
٦	المحور السادس	١٥	٢٤١	٠,٨٥
٧	المحورالسابع	١٥	٢٤١	٠,٩٠
٨	المحور الثامن	١٥	٢٤١	٠,٨٥

وقد أظهر حساب ثبات الاستبانة باستخدام طريقة ألفا كرونباخ (Cronbach's Alpha) أن قيمة الثبات للمحور الأول (خصائص جريمة التزوير الإلكتروني) (٠,٧٠)، وقيمة الثبات للمحور الثاني (صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية) (٠,٨٣)، وقيمة الثبات للمحور الثالث (الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني) (٠,٩٢)، وقيمة الثبات للمحور الرابع (سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني) (٠,٨٠)، وقيمة الثبات للمحور الخامس (سمات المجني عليه في جرائم التزوير الإلكتروني) (٠,٨٤)، وقيمة الثبات للمحور السادس (فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني)(٠,٨٥)، وقيمة الثبات للمحور السابع (فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني) (٠,٩٠)، وقيمة الثبات للمحور الثامن (المعوقات التي تؤدي

إلى عـدم فاعلية الأسـاليب المسـتخدمة من المحقق الجنائـي والفني في إثبات جرائـم التزوير الإلكـتروني) (٨٥ , ٠)، وهذا يعنـي أن جميع هذه المعاملات ذات قيمـة عاليـة، وهـذه القيمة مؤشر لصلاحية أداة الدراسـة (الاسـتبانة) بغرض تحقيق أهدافها من خلال الإجابة على أسـئلتها، مما يشـير إلى إمكانية ثبات النتائج التي يمكن أن تسفر عنها عند تطبيقها.

والملحق رقم (١) يوضح أداة الدراسة في صيغتها النهائية.

٣. ٥ الأساليب الإحصائية

تم الاسـتفادة من خدمـات مركز المعلومـات والحاسـب الآلي بجامعة نايـف العربية للعلوم الأمنية في معالجة البيانات إحصائياً باسـتخدام برنامج الحزمـة الإحصائيـة الاجتماعية «SPSS»، حيث تضمنت المعالجة الأسـاليب الإحصائية التالية، بعد حساب كل من:

١ ـ معامل ارتباط بيرسون (Pearson) بين درجة العبارة والدرجة الكلية للمحـور الذي تنتمي إليه لتحديد مدى الصدق البنائي والاتسـاق الداخلي لأداة الدراسة.

٢ ـ معامـل ارتباط كرونباخ ألفـا (Cronbach's Alpha) لتحديد معامل ثبات أداة الدراسة.

وبعد ذلك تم حساب كل من المقاييس الإحصائية التالية:

أ ـ التكـرارات والنسـب المئوية لوصـف خصائص مفردات الدراسـة، ولتحديد الاسـتجابة تجاه محاور وأبعاد الدراسـة التي تضمنتها أداة الدراسة.

ب ـ حساب المتوسط الحسابي، والانحراف المعياري، لتحديد استجابات مفردات الدراسة نحو محاور وأبعاد الدراسة المختلفة.

جـ ـ متوسط الوزن النسبي الفارق لتحديد الأهمية النسبية التي تقيس فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، وذلك بضرب استجابات (موافق بشدة)×٥، واستجابات (موافق)×٤، واستجابات (محايد)×٣، واستجابات (غيرموافق)×٢، واستجابات (غير موافق مطلقاً) × ١.

د ـ اختبار (T-Test) ; لدلالة الفروق في استجابات أفراد عينة الدراسة وفقاً لمتغير طبيعة العمل (محقق جنائي، محقق فني).

هـ ـ اختبار (كا٢) لحسن المطابقة لاختبار ما إذا كان أفراد العينة توزع بالتساوي على الاستجابات الخمسة المختلفة (موافق بشدة، موافق، محايد، غير موافق، غير موافق مطلقاً).

و ـ تحليل التباين أحادي الاتجاه (ANOVA)؛ لمعرفة دلالة الفروق في استجابات مفردات عينة الدراسة نحو محاور الدراسة باختلاف الخصائص الديموجرافية لمفردات عينة الدراسة.

ز ـ اختبار (LSD)؛ لتوضيح مقارنة الفروق ذات الدلالة الإحصائية المتصلة بتلك الخصائص في حالة وجود فروق.

يمكن الحصول على المتوسطات النسبية الفارقة التالية:

ـ متوسط من ٤,٢١ إلى ٥,٠ يشير إلى موافق بشدة، أو مهمة جداً.

ـ متوسط من ٣,٤١ إلى ٤,٢٠ يشير إلى موافق أو مهمة.

ـ متوسط من ٢,٦١ إلى ٣,٤٠ يشير إلى محايد، أو متوسطة الأهمية.

ـ متوسط من ١,٨١ إلى ٢,٦٠ يشير إلى غير موافق، أو غير مهمة.

ـ متوسط من ١,٠ إلى ١,٨٠ يشير إلى غير موافق مطلقاً، أو غير مهمة مطلقاً.

الفصل الرابع

عرض وتحليل بيانات الدراسة ومناقشة نتائجها

٤ .عرض وتحليل بيانات الدراسة ومناقشة نتائجها

تمهيد

تحقيقاً لأهداف الدراسة في الكشف عن فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، قام الباحث بإجراء هذه الدراسة المسحية لاستطلاع آراء منسوبي الجهات المختصة بمكافحة جرائم التزوير بالأمن العام والجوازات في مناطق المملكة كافة، ويختص هذا الفصل بعرض النتائج التي توصلت إليها هذه الدراسة المسحية وتحليلها وتفسيرها.

ويتضمن هذا الفصل عشرة عناصر توضح خصائص مجتمع الدراسة بجانب الإجابة عن أسئلة الدراسة وهي: خصائص جريمة التزوير الإلكتروني، وصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، ومدى الاختلاف في وجهات نظر المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية. ويقوم الباحث في كل عنصر من تلك

العناصر بعرض وتحليل الإجابة عنه، ثم الوصول الى استنتاجات ترتبط به، ثم تفسير تلك النتائج، وذلك بعد عرض الجداول التي توضح الخصائص الأساسية لمجتمع الدراسة.

٤ . ١ خصائص مفردات الدراسة

تتسم عينة الدراسة بعدد من الخصائص حددتها نوعية المتغيرات الديموجرافية التي تناولتها الدراسة، ويمكن توضيحها فيما يلي :

١ ـ العمر

يوضح الجدول رقم (٤) توزيع مفردات الدراسة وفقاً للعمر.

الجدول رقم (٤) توزيع مفردات الدراسة وفقاً للعمر

العمر	التكرار	النسبة المئوية
٢٥ سنة	١٢	٥,٠
من ٢٦ إلى أقل من ٣٠ سنة	٥١	٢١,٢
من ٣٠ إلى أقل من ٣٥ سنة	٧١	٢٩,٥
من ٣٥ سنة فاكثر	١٠٧	٤٤,٤
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (٤) أن أعلى نسبة من مفردات الدراسة (٤٤,٤ ٪) تبلغ أعمارهم (٣٥ سنة فأكثر)، وأن (٢٩,٥ ٪) تتراوح أعمارهم ما بين (٣٠ إلى أقل من ٣٥ سنة)، وأن (٢١,٢ ٪) تتراوح أعمارهم ما بين (٢٦ إلى أقل من ٣٠ سنة)، وأخيراً الذين تبلغ أعمارهم (٢٥ سنة) بنسبة (٥,٠ ٪).

وتـدل النتيجة السـابقة عـلى التنـوع في أعمـار مفردات الدراسـة، مع ارتفاع الأعمار نسـبياً، مما يعكس تنوع عامل الخبرة، ويخدم أهداف الدراسة، حيـث يضمن التعـرف على آراء المسـتويات العمريـة المختلفة بـما تحمله من خـبرات متراكمة نحو تحديد فاعلية الأسـاليب المسـتخدمة في إثبات جرائم التزوير الإلكتروني.

٢ ـ المؤهل التعليمي

يوضـح الجـدول رقـم (٥) توزيـع مفـردات الدراسـة وفقـاً للمؤهـل التعليمي.

الجدول رقم (٥) توزيع مفردات الدراسة وفقاً للمؤهل التعليمي

المؤهل التعليمي	التكرار	النسبة المئوية
الثانوية العامة	٩٩	٤١,١
بكالوريوس	١٢٨	٥٣,١
دراسات عليا	١٤	٥,٨
المجموع	٢٤١	١٠٠

يبين اسـتعراض بيانات الجـدول رقم (٥) أن غالبية مفردات الدراسـة (١,٥٣ ٪) حاصلـون على درجة البكالوريوس، وأن (١,٤١ ٪) حاصلون على الثانوية العامة، بينما الأقلية حاصلون على دراسات عليا بنسبة (٨,٥٪).

والنتيجة السـابقة تدل على تنوع المسـتوى التعليمي لمفردات الدراسـة، ممـا يعنـي أن تحديـد فاعلية الأسـاليب المسـتخدمة في إثبات جرائـم التزوير الإلكـتروني سـيتأثر إلى حـد مـا بخلفيتهـم العلميـة، أي أنه لن يكـون تقييماً عشـوائياً، نظراً لتأثير المسـتوى الدراسي في اتجاهات المفردات نحو الأشياء،

لأن العلم يكسب المفردات قيماً وخبرات تسهم إلى حد كبير في تكوين اتجاهات إيجابية أو سلبية نحو موضوع معين.

٣ـ جهة العمل

يوضح الجدول رقم (٦) توزيع مفردات الدراسة وفقاً لجهة العمل.

الجدول رقم (٦) توزيع مفردات الدراسة وفقاً لجهة العمل

جهة العمل	التكرار	النسبة المئوية
مكافحة التزوير بالأمن العام	٧٥	٣١,١
أبحاث التزوير بالأمن العام	٧١	٢٩,٥
مكافحة التزوير بالجوازات	٥٤	٢٢,٤
أبحاث التزوير بالجوازات	٤١	١٧,٠
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (٦) أن غالبية مفردات الدراسة بنسبة (٣١,١٪) يعملون بمكافحة التزوير بالأمن العام، وأن (٢٩,٥ ٪) يعملون في أبحاث التزوير بالأمن العام، وأن (٢٢,٤ ٪) يعملون في مكافحة التزوير بالجوازات، بينما الأقلية يعملون في أبحاث التزوير بالجوازات بنسبة (١٧,٠٪).

وتدل النتيجة السابقة على أن هناك تنوعاً في جهات العمل بين مفردات الدراسة، مما يعني تحديد آراء غالبية الجهات المشاركة في مكافحة التزوير، فضلاً عن دراسة تأثير إجراءات المكافحة التي تتبعها كل جهة في مواجهة عمليات التزوير التقليدي والإلكتروني، ومن ثمَّ إمكانية الاستفادة في التحديد الدقيق لكل من خصائص جريمة التزوير الإلكتروني، وصور

جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

٤ ـ طبيعة العمل

يوضح الجدول رقم (٧) توزيع مفردات الدراسة وفقاً لطبيعة العمل.

الجدول رقم (٧) توزيع مفردات الدراسة وفقاً لطبيعة العمل

طبيعة العمل	التكرار	النسبة المئوية
محقق جنائي	١٢٩	٥٣,٥
محقق فني	١١٢	٤٦,٥
المجموع	٢٤١	١٠٠

يبين استعراض بيانات الجدول رقم (٧) أن غالبية مفردات الدراسة (٥٣,٥ ٪) من المحققين الجنائيين، بينما (٤٦,٥ ٪) من المحققين الفنيين.

والنتيجة السابقة تخدم أهداف الدراسة، حيث تضمن التعرف على آراء المحققين الجنائيين والفنيين في تحديد فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني.

٥ ـ منطقة العمل

يوضح الجدول رقم (٨) توزيع مفردات الدراسة وفقاً لمنطقة العمل.

الجدول رقم (٨) توزيع مفردات الدراسة وفقاً لمنطقة العمل

منطقة العمل	التكرار	النسبة المئوية
الرياض	٤٩	٢٠,٣
مكة المكرمة	٣٤	١٤,١
المدينة المنورة	١٨	٧,٥
القصيم	٩	٣,٧
عسير	١٣	٥,٤
المنطقة الشرقية	١٤	٥,٨
تبوك	٢٠	٨,٣
حائل	١٣	٥,٤
جازان	١٦	٦,٦
الحدود الشمالية	٥	٢,١
نجران	٢٠	٨,٣
الباحة	١٧	٧,١
الجوف	١٣	٥,٤
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (٨) أن غالبية مفردات الدراسة بنسبة (٢٠,٣٪) يعملون في منطقة الرياض، وأن (١٤,١ ٪) يعملون في مكة المكرمة، وأن (٨,٣ ٪) يعملون في كل من تبوك ونجران، وأن (٧,٥ ٪) يعملون في المدينة المنورة، وأن (٧,١ ٪) يعملون في الباحة، وأن (٦,٦ ٪) يعملون في جازان، وأن (٥,٨ ٪) يعملون في المنطقة الشرقية، وأن

(٤ , ٥٪) يعملون في كل من عسير وحائل والجوف، وأن (٧ , ٣٪) يعملون في القصيم، بينما الأقلية يعملون في الحدود الشمالية بنسبة (١ , ٢٪).

وتدل النتيجة السابقة على أن هناك تنـوعاً في مناطق العمل بين مفردات الدراسة، فضلاً عن شمول مكافحة التزوير في جميع المناطق الإدارية للمملكة، مما يعني تحديد آراء العاملين في المناطق المختلفة، وعمليات التزوير التقليدي والإلكتروني التي تواجهها كل منطقة في ضوء انتشار التعاملات الإلكترونية والسعي للربط بين مناطق المملكة كافة بهذه التقنية لتيسير إجراءات العمل.

٦ ـ الرتبة العسكرية

نظـراً لأن الرتبـة العسـكرية تسـهم إلى حـد كبـير في تكويـن اتجاهـات إيجابيـة أو سـلبية، فقد حرصـــت هذه الدراسـة على التعـرف على دور هذا المتغير بالتفصيل نحو فاعلية الأسـاليب المسـتخدمة في إثبات جرائم التزوير الإلكتروني، والجدول رقم (٩) يوضح توزيع مفردات الدراسـة وفقاً للرتبة العسكرية.

الجدول رقم (٩) توزيع مفردات الدراسة وفقاً للرتبة العسكرية

الرتبة العسكرية	التكرار	النسبة المئوية
صف ضابط	١٠٠	٤١,٥
ملازم	٢٥	١٠,٤
ملازم أول	٣١	١٢,٩
نقيب	٣١	١٢,٩
رائد	٢٣	٩,٥
مقدم فما فوق	٣١	١٢,٩
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (٩) أن غالبية مفردات الدراسة بنسبة (٥ , ٤١ ٪) من صف الضباط، وأن (٩ , ١٢ ٪) برتبة مازم أول، وأن (٩ , ١٢ ٪) برتبة نقيب، وأن (٩ , ١٢ ٪) برتبة مقدم فما فوق، وأن ٤ , ١٠ ٪) برتبة ملازم، بينما الأقلية برتبة رائد بنسبة (٥ , ٩ ٪).

وتدل النتيجة السابقة على أن هناك تنوعاً في الرتب العسكرية بين مفردات الدراسة، مما يعني الاستفادة من آراء غالبية الرتب العسكرية المختلفة بما تحمله من خبرات متراكمة في تحديد فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني.

٧ ـ عدد سنوات الخبرة في مجال العمل

يوضح الجدول رقم (١٠) توزيع مفردات الدراسة وفقاً لعدد سنوات الخبرة في مجال العمل.

الجدول رقم (١٠) توزيع مفردات الدراسة وفقاً لعدد سنوات الخبرة في مجال العمل

عدد سنوات الخبرة	التكرار	النسبة المئوية
أقل من ٥ سنوات	٥١	٢١,٢
من ٥ سنوات إلى أقل من ١٠ سنوات	٦٨	٢٨,٢
من ١٠ سنوات إلى أقل من ١٥ سنة	٥٥	٢٢,٨
من ١٥ سنة إلى أقل من ٢٠ سنة	٢٧	١١,٢
من ٢٠ سنة فأكثر	٣١	١٢,٩
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (١٠) أن أعلى نسبة من مفردات الدراسة (٢ , ٢٨ ٪) تتراوح خبراتهم العملية في مجال العمل ما بين (٥ إلى أقل من

١٠ سنوات)، وأن (٨ , ٢٢ ٪) تتراوح خبراتهم العملية ما بين (١٠ إلى أقل من ١٥٦ سنة)، وأن (٢ , ٢١ ٪) تقل خبراتهم العملية عن (٥ سنوات)، وأن (٩ , ١٢ ٪) تبلغ خبراتهم العملية (٢٠ سنة فأكثر)، بينما الأقلون تتراوح خبراتهم العملية ما بين (١٥ إلى أقل من ٢٠ سنة بنسبة (٢ , ١١ ٪).

تدل النتيجة السابقة على تنوع الخبرات العملية لمفردات الدراسة، مما يجعلهم قادرين على تكوين آراء إيجابية أو سلبية أكثر دقة تجاه فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني، حيث تعد الخبرة من أكثر العوامل المؤثرة في آراء الأفراد نحو الأشياء، لأن الخبرات المتراكمة عبر التجارب تسهم إلى حد كبير في تكوين اتجاهات إيجابية أو سلبية نحو موضوع معين.

٨ ـ عدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية

يوضح الجدول رقم (١١) توزيع مفردات الدراسة وفقاً لعدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية.

الجدول رقم (١١) توزيع مفردات الدراسة وفقاً لعدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية

عدد الدورات التدريبية	التكرار	النسبة المئوية
لم ألتحق بأية دورة	١١٠	٤٥,٦
دورة واحدة	٦٣	٢٦,١
التحقت بدورتين	٢٨	١١,٦
ثلاث دورات فأكثر	٤٠	١٦,٦
المجموع	٢٤١	١٠٠

يتضح من الجدول رقم (١١) أن غالبية مفردات الدراسة (٦ , ٤٥ ٪) لم يلتحقوا بأية دورة في مجال جرائم التزوير الإلكترونية، وأن (١ , ٢٦ ٪) التحقوا بدورة واحدة، وأن (٦ , ١٦ ٪) التحقوا بثلاث دورات فأكثر، بينما الأقلية بنسبة (٦ , ١١ ٪) التحقوا بدورتين.

والنتيجة السابقة تشير إلى اهتمام الجهات المشاركة في مكافحة التزوير بإلحاق منسوبيها بالدورات التدريبية بدرجة متوسطة، مما يخدم أهداف الدراسة، ويجعلهم أكثر قدرة على الإجابة عن فقرات الاستبانة.

٤ .٢ خصائص جريمة التزوير الإلكتروني

للإجابة عن السؤال الأول من أسئلة الدراسة وهو : ما خصائص جريمة التزوير الإلكتروني؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد خصائص جريمة التزوير الإلكتروني من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت الذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٢) استجابات جميع مفردات الدراسة لتحديد خصائص جريمة التزوير الإلكتروني.

الجدول رقم (١٢) خصائص جريمة التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
٢	يتوافر فيها القصد الجنائي الخاص (التزوير).	ت	١١٩	١٠٩	١٢	١	–	٤,٤٤	٠,٦١	١٩٣,٦	٠,٠**	الأول
		٪	٤٩,٤	٤٥,٢	٥,٢	٠,٤	–					
٤	تشكل اعتداء على النظام المعلوماتي.	ت	١٢٣	١٠١	١٥	١	١	٤,٤٣	٠,٦٧	٢٨٩,٢	٠,٠**	الثاني
		٪	٥١,٠	٤١,٩	٦,٢	٠,٤	٠,٤					
٩	تعتد من الجرائم العابرة للحدود الجغرافية.	ت	١١١	١١٣	١٢	٥	–	٤,٤٣	٠,٦٩	٢٨٠,٦	٠,٠**	الثالث
		٪	٤٦,١	٤٦,٩	٥,٠	٢,١	–					
١٢	لا تحتاج لعنف جسدي أو مقاومة كالجرائم التقليدية.	ت	١١٩	١٠٥	١٢	٣	٢	٤,٣٩	٠,٧٢	٢٨٤,٨	٠,٠**	الرابع
		٪	٤٩,٤	٤٣,٦	٥,٠	١,٢	٠,٨					
٨	تتطلب حرفية وإتقاناً في التنفيذ.	ت	١١١	١١٣	١٢	٥	–	٤,٣٧	٠,٦٨	١٧٨,٢	٠,٠**	الخامس
		٪	٤٦,١	٤٦,٩	٥,٠	٢,١	–					
١٤	تهدف في الغالب إلى تحقيق أرباح مالية.	ت	١١٤	١٠٢	٢٢	٣	–	٤,٣٦	٠,٦٩	١٥٥,٦	٠,٠**	السادس
		٪	٤٧,٣	٤٢,٣	٩,١	١,٢	–					
١	يتوافر فيها القصد الجنائي العام.	ت	١٠٦	١٢٠	١٠	٣	٢	٤,٣٥	٠,٦٩	٢٩٣,٢	٠,٠**	السابع
		٪	٤٤,٠	٤٩,٨	٤,١	١,٢	٠,٨					
٣	تحتاج لخبرة وتخطيط علمي مدروس لارتكابها.	ت	٩٩	١٢٦	١٣	٣	–	٤,٣٣	٠,٦٤	١٨٨,١	٠,٠**	الثامن
		٪	٤١,١	٥٢,٣	٥,٤	١,٢	–					
١٥	تؤدي إلى فقد الثقة في التعاملات المالية الإلكترونية.	ت	١٠٠	١١٧	٢٢	٢	–	٤,٣١	٠,٦٧	١٦٠,٣	٠,٠**	التاسع
		٪	٤١,٥	٤٨,٥	٩,١	٠,٨	–					

تابع .... جدول رقم (١٢) خصائص جريمة التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غيرموافق مطلقاً					
٦	إمكانية ارتكابها بطرق التزوير المعنوي (جعل واقعة مزورة في صورة واقعة صحيحة).	ت	٩٧	١٢٠	٢٢	٢	–	٤,٢٩	٠,٦٧	١٦٢,٣	٠,٠**	العاشر
		٪	٤٠,٢	٤٩,٨	٩,١	٠,٨	–					
٧	قد يرتكبها في الغالب خبراء على درجة عالية من الكفاءة في استخدام الحاسب الآلي.	ت	١١٤	٩١	٢٠	١٥	١	٤,٢٥	٠,٨٨	٢١٣,٤	٠,٠**	الحادي عشر
		٪	٤٧,٣	٣٧,٨	٨,٣	٦,٢	٠,٤					
٥	تتطلب استخدام تقنيات الاختراق والتعدي.	ت	٨٣	١٢٠	٣٠	٧	١	٤,١٥	٠,٧٨	٢٢٠,٤	٠,٠**	الثاني عشر
		٪	٣٤,٤	٤٩,٨	١٢,٤	٢,٩	٠,٤					
١١	سهولة إتلاف الأدلة الإلكترونية التي تشير لمرتكبها.	ت	٥١	١٠٧	٦١	٢١	١	٣,٧٧	٠,٨٩	١٣٦,٩	٠,٠**	الثالث عشر
		٪	٢١,٢	٤٤,٤	٢٥,٣	٨,٧	٠,٤					
١٠	لا يوجد لها أثر مادي ظاهر.	ت	٥٦	١٠٦	٣٨	٣٣	٨	٣,٧٠	١,٠٧	١١١,١	٠,٠**	الرابع عشر
		٪	٢٣,٢	٤٤,٠	١٥,٨	١٣,٧	٣,٣					
١٣	يصعب تتبع مرتكبيها والقبض عليهم.	ت	٤٥	١٠٥	٥١	٣٥	٥	٣,٦٢	١,٠١	١٠٩,٦	٠,٠**	الخامس عشر
		٪	١٨,٧	٤٣,٦	٢١,٢	١٤,٥	٢,١					
متوسط استجابات مفردات الدراسة على محورخصائص جريمة التزوير الإلكتروني								٤,٢١	٠,٣٤			

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بخصائص جريمة التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٢) أن المتوسط الحسابي العام لمحور خصائص جريمة التزوير الإلكتروني قد بلغ (٢١ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود خصائص مهمة جداً لجريمة التزوير الإلكتروني.

كما كشف الجدول أن هناك إحدى عشرة خاصية تمثل (٣ , ٧٣٪) من الخصائص التي تضمنها محور خصائص جريمة التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢٥ , ٤ ـ ٤٤ , ٤)، مما يشير إلى شدة أهميتها، فهي من الخصائص المهمة جداً لجريمة التزوير الإلكتروني.

وتبين من الجدول أن هناك أربع خصائص تمثل (٧ , ٢٦٪) من الخصائص التي تضمنها محور خصائص جريمة التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٦٢ , ٣ـ ١٥ , ٤)، مما يشير إلى أهميتها، فهي من الخصائص المهمة لجريمة التزوير الإلكتروني.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة الكركي (٢٠٠٣م) في أن الجرائم الإلكترونية جرائم عابرة للحدود، كما تتفق جزئياً مع ما توصلت إليه دراسة البشرى (٢٠٠٣م) ودراسة (Erdonmez 2002) في عدم حاجة الجرائم الإلكترونية إلى العنف الجسدي، بل تتطلب حرفية وإتقاناً، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة (Wahbler 1988) في صعوبة إثبات الجرائم الإلكترونية.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال خصائص جريمة التزوير الإلكتروني، بأن الطابع التقني لهذه الجريمة يضفي عليها عدة

خصائص يأتي في مقدمتها توافر القصد الجنائي الخاص (التزوير) سواء في المحرر المعلوماتي أو سجلات الحاسب الآلي عن طريق إدخال بيانات غير صحيحة بسجلات الحاسب، أو سرقة منظومة التوقيع الإلكتروني واستخدامه بدلاً من صاحبه الأصلي، مما يشكل اعتداءاً على النظام المعلوماتي؛ لأن القيام بذلك يتطلب الاختراق والتعدي والدخول على المواقع دون تصريح، أو استغلال التصريح في ارتكاب جريمة التزوير بإساءة استغلال الثقة، كما تعد جريمة التزوير الإلكتروني من الجرائم العابرة للحدود الجغرافية التي لا تحتاج لعنف جسدي أو مقاومة كما في الجرائم التقليدية، بل تتطلب حرفية وإتقاناً في التنفيذ، وهدفها الرئيس هو تحقيق الربح المالي، ولذلك يترتب عليها إيقاع الضرر بأفراد المجتمع، ولذلك يتوافر فيها القصد الجنائي العام. ويشير الشهري والعطوي (٢٠٠٧م، ص١٢٨) إلى أن جرائم التزوير تحتاج إلى التخطيط والدقة في التنفيذ، والمعرفة الفنية باختراق الحواجز الأمنية وتدميرها، والوصول إلى المعلومات والبيانات الخاصة بالأفراد أو المنظمات، وتغييرها لتحقيق أرباح ومكاسب مادية أو معنوية لصالح مرتكب الجريمة أو لصالح شخص آخر، أما الصغير (١٩٩٩م، ص٣٥) فيرى أن جريمة التزوير الإلكتروني جريمة عابرة للحدود، فلا يوجد لها حدود معينة، بل يمكن ارتكابها من أي مكان في العالم.

كما تؤدي جريمة التزوير الإلكتروني إلى فقدان الثقة بالتعاملات الإلكترونية، وبصفة خاصة عند قيام البعض بالاستيلاء على أرقام بطاقات الائتمان أو تحويل المبالغ المالية من أرصدة بعض العملاء إلى أرصدتهم أو الشراء والتسديد من حساباتهم بعد اختراق نظم معلومات البنوك، مما يفقد العديد الثقة من التعاملات الإلكترونية، ويجعلهم يحذرون منها، فهي لا تقتصر على التزوير المادي، بل يمكن ارتكابها بطرق التزوير المعنوي (جعل

واقعة مزورة في صورة واقعة صحيحة) كما في حالة تغيير الغرض من القدوم لأحد القادمين إلى المملكة من قادم إلى الزيارة إلى قادم عمل، أو تغيير مسمى الوظيفة من عسكري إلى متسبب لكي يستطيع السفر بها خارج المملكة دون الحصول على إذن من مرجعه. وهذه الجرائم يتم ارتكابها من قبل المصرح لهم بالدخول على النظام الذين يسيئون استغلال تلك الثقة، أو من قبل خبراء على درجة عالية من الكفاءة في استخدام الحاسب الآلي ولهم خبرة طويلة في استخدام تقنيات الاختراق والتعدي، ويتمتعون بقدرات فائقة على إتلاف الأدلة المادية التي تدينهم بعد ارتكاب جرائمهم، وهذا ما يجعل من أهم خصائص جريمة التزوير الإلكتروني عدم وجود أثر مادي ظاهر يشير إلى مرتكبها، فطبيعة هذه الجريمة التي تتكون من ذبذبات ونبضات كهربائية غير مرئية تجعل من الصعب اكتشافها، كما أن سهولة إتلاف الأدلة الإلكترونية يجعل من الصعب تتبع مرتكبيها والقبض عليهم. ولذلك يشير مدني (٢٠٠٧م، ص٤٨) إلى أن ارتكاب جريمة التزوير الإلكتروني يتطلب الإلمام بمعارف ومهارات فنية متقدمة في مجال الحاسب الآلي والإنترنت، أما العريان (٢٠٠٤م، ص٤٩) فيشير إلى أن صعوبة تتبع مرتكب الجريمة الإلكترونية يعزى إلى سهولة تدمير الإدلة المادية وإتلافها بعد ارتكاب الجريمة.

وبهذا يتحقق الهدف الأول من أهداف الدراسة وهو معرفة خصائص جريمة التزوير الإلكتروني.

٤ . ٣ الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني

للإجابة عن السؤال الثاني من أسئلة الدراسة وهو: ما الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت الذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٣) استجابات جميع مفردات الدراسة لتحديد الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني.

الجدول رقم (١٣) الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
١٥	تتم من خلال أدوات كسر كلمات السر Password Crackers.	ت	٩٤	١٢٦	١٩	٢	–	٤,٢٩	٠,٦٥	١٧٥,٢	٠,٠**	الأول
		٪	٣٩,٠	٥٢,٣	٧,٩	٠,٨	–					
٨	تتم عن طريق إفشاء الرقم السري من قبل الموظفين لزملاء العمل بحسن نية.	ت	١٠٠	١١٤	٢٠	٤	٣	٤,٢٦	٠,٧٨	٢٤٤,٩	٠,٠**	الثاني
		٪	٤١,٥	٤٧,٣	٨,٣	١,٧	١,٢					
٢	تتم باستخدام برامج فك التشفير.	ت	٧٨	١٣٢	٢٨	٣	–	٤,١٨	٠,٦٨	١٦٢,٣	٠,٠**	الثالث
		٪	٣٢,٤	٥٤,٨	١١,٦	١,٢	–					
١	تتم عن طريق المحاولة المتكررة من خلال استخدام لوحة المفاتيح.	ت	٦٤	١٣٩	٢٩	٧	٢	٤,٠٦	٠,٧٦	٢٦٣,٤	٠,٠**	الرابع
		٪	٢٦,٦	٥٧,٧	١٢,٠	٢,٩	٠,٨					
١٣	يتم عن طريق مولدات أرقام البطاقة الائتمانية C.CNumbers Generators.	ت	٧٥	١٠٥	٥٥	٥	١	٤,٠٣	٠,٨١	١٦٧,٧	٠,٠**	الخامس
		٪	٣١,١	٤٣,٦	٢٢,٨	٢,١	٠,٤					
٥	تتم عن طريق الأجهزة ومحركات الأقراص المرنة والليزر.	ت	٤٥	١٣٢	٥٤	٩	١	٣,٨٨	٠,٧٦	٢٢٤,٧	٠,٠**	السادس
		٪	١٨,٧	٥٤,٨	٢٢,٤	٣,٧	٠,٤					
١٤	تتم عن طريق أدوات التجسس على رزم البيانات Paacket Sniffers.	ت	٤٢	١٣٣	٥٨	٦	٢	٣,٨٦	٠,٧٦	٢٣٣,٢	٠,٠**	السابع
		٪	١٧,٤	٥٥,٢	٢٤,١	٢,٥	٠,٨					

١١	تتم عن طريق الثقوب التي تتخلل بعض البرامج Programs Holes .	ت	٣٨	١٣٣	٦٤	٥	١	٣,٨٤	٠,٧٢	٢٤١,٥	٠,٠**	الثامن
		٪	١٥,٨	٥٥,٢	٢٦,٦	٢,١	٠,٤					
٤	تتم عن طريق الشبكة الواسعة WAN والبرامج المرتبطة بها.	ت	٣٥	١٤٠	٥٩	٥	٢	٣,٨٣	٠,٧٢	٢٦٣,٩	٠,٠**	التاسع
		٪	١٤,٥	٥٨,١	٢٤,٥	٢,١	٠,٨					
٣	تتم عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد.	ت	٣١	١٤٠	٥٨	٩	٣	٣,٧٨	٠٧٦	٢٥٧,٢	٠,٠**	العاشر
		٪	١٢,٩	٥٨,١	٢٤,١	٣,٧	١,٢					
٩	تتم عن طريق التخفي الشبكي Anonymity.	ت	٣٣	١٣٣	٦٥	٧	٣	٣,٧٧	٠,٧٧	٢٣٧,٤	٠,٠**	الحادي عشر
		٪	١٣,٧	٥٥,٢	٢٧,٠	٢,٩	١,٢					
١٠	تتم عن طريق تمويه العنوان الشبكي IP Spoofing.	ت	٣٥	١١٤	٨٤	٦	٢	٣,٧٢	٠,٧٧	٢٠١,٣	٠,٠**	الثاني عشر
		٪	١٤,٥	٤٧,٣	٣٤,٩	٢,٥	٠,٨					
١٢	تتم عن طريق لواقط ضربات لوحة المفاتيح Key Loggers.	ت	٣٧	٩٩	٨٩	١٤	٢	٣,٦٤	٠,٨٤	١٥٩,٢	٠,٠**	الثالث عشر
		٪	١٥,٤	٤١,١	٣٦,٩	٥,٨	٠,٨					
٧	تتم عن طريق شبكة VPN والبرامج التي تعمل عليها.	ت	٣٢	٩٧	٩٧	١٣	٢	٣,٦٠	٠,٨٢	١٧٤,٢	٠,٠**	الرابع عشر
		٪	١٣,٣	٤٠,٢	٤٠,٢	٥,٤	٠,٨					
٦	تتم عن طريق التقاط الأشعة المنبعثة من الحاسب الآلي.	ت	٢٨	٩٠	١٠٣	١٧	٣	٣,٥١	٠,٨٤	١٦٩,٦	٠,٠**	الخامس عشر
		٪	١١,٦	٣٧,٣	٤٢,٧	٧,١	١,٢					
متوسط استجابات مفردات الدراسة على محور الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني								٣,٨٨	٠,٤٢			

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بالوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٣) أن المتوسط الحسابي العام لمحور الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني قد بلغ (٨٨ , ٣) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود وسائل مهمة لارتكاب جريمة التزوير الإلكتروني.

كما كشف الجدول أن هناك وسيلتين تمثلان (٣ , ١٣ ٪) من الوسائل التي تضمنها محور الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني قد تراوحت متوسطاتهما الحسابية ما بين (٢٦ , ٤ـ ٢٩ , ٤)، مما يشير إلى شدة أهميتهما، فهما من الوسائل المهمة جداً لارتكاب جريمة التزوير الإلكتروني.

وتبين من الجدول أن هناك ثلاثة عشر وسيلة تمثل (٧ , ٨٧ ٪) من الوسائل التي تضمنها محور الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٥١ , ٣ـ ١٨ , ٤)، مما يشير إلى أهميتها، فهي من الوسائل المهمة لارتكاب جريمة التزوير الإلكتروني.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه (Erdonmez 2002) في أن أهم وسائل ارتكاب الجريمة الإلكترونية هي استخدام أدوات كسر كلمة السر، وبرامج فك التشفير، كما تتفق جزئياً مع ما توصلت إليه دراسة حجازي (٢٠٠٥م) في أن أدوات التجسس على رزم البيانات والشبكة الواسعة والبرامج المرتبطة بها من أهم وسائل ارتكاب الجريمة الإلكترونية، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة(Goodman 1997) في أن تمويه العنوان الشبكي والتخفي الشبكي من أهم وسائل ارتكاب الجريمة الإلكترونية.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، بأن هناك وسائل متعددة تتواكب مع التطور التقني المعاصر، وتسهم في ارتكاب جريمة التزوير الإلكتروني بطرق مبتكرة أحياناً وتقليدية أحياناً، ويأتي في مقدمة هذه الوسائل استخدام أدوات كسر كلمات السر، أو برامج فك التشفير، وهي عبارة عن أقراص وبرامج تحتوي على لوغاريتمات تقوم بعمليات تباديل وتوافيق بسرعات مهولة حتى الحصول على الرقم السري الخاص بالنظام، وإمكانية الدخول عليه واستخدامه، ومن ثم ارتكاب جريمة التزوير الإلكتروني. ومن أشهر الطرق التقليدية التي تستخدم في ارتكاب جريمة التزوير الإلكتروني إفشاء الرقم السري من قبل الموظف لزملاء العمل بحسن النية، أو عن طريق المحاولة المتكررة من خلال لوحة المفاتيح، حيث يمكن أن تثمر إحدى هذه المحاولات عن الرقم السري الصحيح الذي يمكن المستخدم من الدخول على النظام والعبث به، وكذلك ارتكاب جريمة التزوير الإلكتروني. ويشير الحميد ونينو (٢٠٠٧م، ص٥٤) إلى أن استخدام أدوات كسر كلمات السر، أو برامج فك التشفير من أهم وسائل ارتكاب الجريمة الإلكترونية، بينما يؤكد عبد المطلب (٢٠٠١م، ص٢٢٠) أهمية تلك البرامج وقدرتها الفائقة على فك أية شفرة.

كما يمكن ارتكاب جريمة التزوير الإلكتروني عن طريق مولدات أرقام البطاقات الائتمانية، حيث تمكن من الحصول على أرقام بطاقات الائتمان الخاصة بأي مودع، ومن ثم القيام بعمليات الشراء باستخدام رصيده بالبنك، بالإضافة إلى إمكانية ارتكاب هذه الجريمة باستخدام الأجهزة ومحركات الأقراص المرنة والليزر بعد اختراق المواقع والعمل على تعديل محتوياتها، أو سرقة منظومة التوقيع الإلكتروني. ويشير العريان (٢٠٠٤م،

ص٤٥) إلى أن التزوير لا يقتصر على التغيير في سجلات الحاسب الآلي، ولكنه يمتد ليشمل سرقة منظومة التوقيع الإلكتروني.

ولا تقتصر وسائل ارتكاب جريمة التزوير الإلكتروني على الطرق السابقة، بل تشمل وسائل متنوعة من أهمها أدوات التجسس على رزم البيانات أثناء مرورها عبر الشبكة، ومن خلال الثقوب التي تتخلل بعض البرامج، وبصفة خاصة البرامج التي يتم تحميلها من شبكة الإنترنت، حيث يتعمد المخترقون ترك بعض الثقوب بهذه البرامج، واستخدامها كوسيلة للنفاذ إلى نظم المعلومات والعبث بها، أو ارتكاب جرائم التزوير، وكذلك يمكن استخدام الشبكة الواسعة WAN والبرامج المرتبطة بها التي تتيح الفرصة للدخول على بعض المواقع وفك الشفرات الخاصة بها، وكذلك الشبكة المحلية LAN وبرامج التشارك في الموارد التي يمكن استخدامها كثغرات للنفاذ إلى بعض المواقع وارتكاب الجرائم الإلكترونية بها. ويشير حجازي (٢٠٠٥م، ص١٢٢) إلى تعدد وسائل وأساليب ارتكاب التزوير الإلكتروني باستغلال الشبكات وبعض البرامج المساعدة في اختراق انظم المعلومات والتعدي عليها.

كما أنه يمكن استخدام التخفي الشبكي كوسيلة للاختراق والتعدي وارتكاب جريمة التزوير الإلكترونية، أو من خلال تمويه العنوان الشبكي، للهروب من المسؤولية عند استخدام تقنيات التتبع واسترجاع المعلومات لمعرفة الموقع الذي تم منه الاختراق والتعدي، بجانب لجوء البعض إلى استخدام لواقط ضربات لوحة المفاتيح التي قد تفتح بالمصادفة بعض المواقع المحجوبة وتمكن المخترقين من ارتكاب جرائم التزوير بهذه المواقع، وأيضاً يمكن استخدام شبكة VPN التي تمنح إمكانات واسعة للدخول على

المواقـع من خلال برامجها التي تسـتطيع فك تشـفير بعض المواقـع وإتاحتها للمسـتخدمين دون قيـود، ممـا يعنـي أن الانضـمام لهـذه الشـبكة كفيل بحل مشـكلة التشـفير والمواقـع المحجوبـة. ويشـير سـعد (٢٠٠٨م، ص٥) إلى إمكانية اسـتخدام الشبكات الخاصة في عمليات الاختراق والتعدي في ضوء ارتباطهـا بمنظومـات خاصـة تتغلب على كلـمات المرور وتكسرهـا، وتفك الشفرات، وتوفر وقت وجهد المخترقين أثناء محالات الدخول العشوائي.

كـما أن هناك وسـيلة يمكن أن تسـتخدم في ارتـكاب جريمة التزوير الإلكـتروني، وهـي التقاط الأشـعة المنبثعة من الحاسـب الآلي، والتي يمكن من خلال هذه الأشـعة سرقة محتويات الحاسـب الآلي بأكمله وبدون تشفير، ومن ثمَّ إمكانية اسـتغلال المعلومات الموجودة في الحاسب وإجراء عمليات التبديـل والتعديل عليها. ويشـير محمـود (٢٠٠٧م، ص١٣٣٢) إلى إمكانية اسـتخدام جهاز الاسـتقبال والهوائي المناسـب مـع بعض الأجهـزة المعاونة لالتقـاط المعلومـات التـي يحتـوي عليها أي جهاز حاسـب آلي عـن بعد من خـلال الإشـعاعات الكهرومغناطيسـية المنبعثـة مـن الجهـاز، ويـرى محمد (٢٠٠٧م، ص١٤٧٧) أن مكمـن الخطورة يكمن في أن المعلومات المسروقة بهـذه الطريقة تكون غير مشـفرة أو مخفـاة، لأن الإشـعاعات الصادرة تحمل المعلومـات بنفس مواصفاتها الأصلية، ولا تمر خلال شـبكة تقوم بتشـفيرها مـن خلال برامـج الحماية، مما يمكـن من الحصول عـلى المعلومات بوضوح، ويتيح إمكانية تقليدها أو اصطناعها أو تزويرها بحرية تامة.

وبهذا يتحقق الهدف الثاني من أهداف الدراسـة وهو معرفة الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني.

٤ . ٤ صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية

للإجابة عن السؤال الثالث من أسئلة الدراسة وهو : ما صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية ؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٤) استجابات جميع مفردات الدراسة لتحديد صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

الجدول رقم (١٣) الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
٥	استخراج رخص سير إلكترونية مزورة للمركبات.	ت	٧٠	١٥٤	١٦	١	–	٤,٢٢	٠,٥٧	٢٣٨,٢	٠,٠**	الثامن
		٪	٢٩,٠	٦٣,٩	٦,٦	٠,٤	–					
١	استخراج جواز سفر إلكتروني مزور.	ت	٧٥	١٤٤	١٥	٦	١	٤,١٩	٠,٦٩	٣١١,٣	٠,٠**	التاسع
		٪	٣١,١	٥٩,٨	٦,٢	٢,٥	٠,٤					
٨	استخراج رخص بناء إلكترونية مزورة.	ت	٦٨	١٤٩	٢٢	٢	–	٤,١٧	٠,٦١٥	٢١٢,٣	٠,٠**	العاشر
		٪	٢٨,٢	٦١,٨	٩,١	٠,٨	–					
١١	استخراج ضمانات بنكية إلكترونية مزورة.	ت	٧٢	١٤٣	٢٠	٦	–	٤,١٧	٠,٦٨	١٩١,٧	٠,٠**	الحادي عشر
		٪	٢٩,٩	٥٩,٣	٨,٣	٢,٥	–					
١٠	استخراج شهادة إلكترونية مزورة للزكاة والدخل.	ت	٦٧	١٤٩	٢٢	٣	–	٤,١٦	٠,٦٣	٢١٠,٢	٠,٠**	الثاني عشر
		٪	٢٧,٨	٦١,٨	٩,١	١,٢	–					
٧	تزوير محررات استخراج السجل المدني إلكترونياً.	ت	٧١	١٤٣	٢١	٦	–	٤,١٦	٠,٦٨	١٨٩,٩	٠,٠**	الثالث عشر
		٪	٢٩,٥	٥٩,٣	٨,٧	٢,٥	–					
٦	استخراج بطاقات أحوال إلكترونية مزورة.	ت	٧٠	١٤٣	٢٢	٦	–	٤,١٥	٠,٦٨	١٨٨,٤	٠,٠**	الرابع عشر
		٪	٢٩,٠	٥٩,٣	٩,١	٢,٥	–					
٩	استخراج وكالات الشرعية إلكترونية مزورة.	ت	٧٠	١٣٨	٢٦	٦	١	٤,١٢	٠,٧٢	٢٧٠,٦	٠,٠**	الخامس عشر
		٪	٢٩,٠	٥٧,٣	١٠,٨	٢,٥	٠,٤					
	متوسط استجابات مفردات الدراسة على محور صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية							٤,٢٦	٠,٤٣			

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بالوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٤) أن المتوسط الحسابي العام لمحور صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية قد بلغ (٢٦ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود صور مهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

كما كشف الجدول أن هناك ثماني صور تمثل (٣ , ٥٣٪) من الصور التي تضمنها محور صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية قد تراوحت متوسطاتها الحسابية ما بين (٢٢ , ٤ـ ٤٩ , ٤)، مما يشير إلى شدة أهميتها، فهي من الصور المهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وهي على النحو التالي :

١ ـ قيام صاحب الصلاحية بتغيير بيانات أجنبي من قادم للعمرة إلى قادم للعمل، وجاءت هذه الصورة في المركز الأول لترتيب الأهمية النسبية بمتوسط (٤٩ , ٤)، حيث وافق على أهميتها (٦ , ٩٩ ٪).

٢ ـ تغيير مهنة مقيم إلكترونياً تزويراً لتيسير إجراءات استقدام أسرته، وجاءت هذه الصورة في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٤٢ , ٤)، حيث وافق على أهميتها (٤ , ٩٨٪) مقابل (٤ , ٠ ٪) اعترضوا على أهميتها.

٣ ـ دخول صاحب صلاحية بطريقة عير مشروعة على النظام لرفع المخالفات المرورية عن سيارة لحين نقل ملكيتها إلكترونياً، وجاءت هذه الصورة في المركز الثالث لترتيب الأهمية النسبية

بمتوسط (٣٨ , ٤)، حيث وافق على أهميتها (٥ , ٩٧ ٪) مقابل (٤ , ٠ ٪) اعترضوا على أهميتها.

٤ ـ استخراج تأشيرات إلكترونية مزورة للحج والعمرة، وجاءت هذه الصورة في المركز الرابع لترتيب الأهمية النسبية بمتوسط (٣٧ , ٤)، حيث وافق على أهميتها (٧ , ٩٦ ٪) مقابل (٨ , ٠ ٪) اعترضوا على أهميتها.

٥ ـ استخراج تأشيرات إلكترونية مزورة لاستقدام العمالة، وجاءت هذه الصورة في المركز الخامس لترتيب الأهمية النسبية بمتوسط (٣٣ , ٤)، حيث وافق على أهميتها (٤ , ٩٥ ٪) مقابل (٦ , ١ ٪) اعترضوا على أهميتها.

٦ ـ استخراج بطاقات الائتمان البنكية (فيزا ـ ماستركارد) مزورة، وجاءت هذه الصورة في المركز السادس لترتيب الأهمية النسبية بمتوسط (٢٩ , ٤)، حيث وافق على أهميتها (٩ , ٩٠٪) مقابل (٧ , ١ ٪) اعترضوا على أهميتها.

٧ ـ استخراج رخص قيادة إلكترونية عامة وخاصة مزورة، وجاءت هذه الصورة في المركز السابع لترتيب الأهمية النسبية بمتوسط (٢٧ , ٤)، حيث وافق على أهميتها (٠ , ٩٣ ٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

٨ ـ استخراج رخص سير إلكترونية مزورة للمركبات، وجاءت هذه الصورة في المركز الثامن لترتيب الأهمية النسبية بمتوسط (٢٢ , ٤)، حيث وافق على أهميتها (٩ , ٩٢ ٪) مقابل (٤ , ٠ ٪) اعترضوا على أهميتها.

وتبين من الجدول أن هناك سبع صور تمثل (٧ , ٤٦ ٪) من الصور التي تضمنها محور صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية قد تراوحت متوسطاتها الحسابية ما بين (١٢ , ٤ـ ١٩ , ٤)، مما يشير إلى أهميتها، فهي من الصور المهمة للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وهي على النحو التالي :

١ ـ استخراج جواز سفر إلكتروني مزور، وجاءت هذه الصورة في المركز التاسع لترتيب الأهمية النسبية بمتوسط (١٩ , ٤)، حيث وافق على أهميتها (٩ , ٩٠ ٪) مقابل (٩ , ٢ ٪) اعترضوا على أهميتها.

٢ ـ استخراج رخص بناء إلكترونية مزورة، وجاءت هذه الصورة في المركز العاشر لترتيب الأهمية النسبية بمتوسط (١٧ , ٤)، حيث وافق على أهميتها (٠ , ٩٠ ٪) مقابل (٨ , ٠ ٪) اعترضوا على أهميتها.

٣ ـ استخراج ضمانات بنكية إلكترونية مزورة، وجاءت هذه الصورة في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (١٧ , ٤)، حيث وافق على أهميتها (٢ , ٨٩ ٪) مقابل (٥ , ٢ ٪) اعترضوا على أهميتها.

٤ ـ استخراج شهادة إلكترونية مزورة للزكاة والدخل، وجاءت هذه الصورة في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (١٦ , ٤)، حيث وافق على أهميتها (٦ , ٨٩ ٪) مقابل (٢ , ١٪) اعترضوا على أهميتها.

٥ ـ تزوير محررات استخراج السجل المدني إلكترونياً، وجاءت هذه الصورة في المركز الثالث عشر لترتيب الأهمية النسبية بمتوسط

(١٦ , ٤)، حيث وافق على أهميتها (٨ , ٨٨ ٪) مقابل (٥ , ٢ ٪) اعترضوا على أهميتها.

٦ ـ استخراج بطاقات أحوال إلكترونية مزورة، وجاءت هذه الصورة في المركز الرابع عشر لترتيب الأهمية النسبية بمتوسط (١٥ , ٤)، حيث وافق على أهميتها (٣ , ٨٨ ٪) مقابل (٥ , ٢ ٪) اعترضوا على أهميتها.

٧ ـ استخراج وكالات شرعية إلكترونية مزورة، وجاءت هذه الصورة في المركز الخامس عشر لترتيب الأهمية النسبية بمتوسط (١٢ , ٤)، حيث وافق على أهميتها (٣ , ٨٦ ٪) مقابل (٩ , ٢ ٪) اعترضوا على أهميتها.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ توجد صور مهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

٢ ـ إن الصور المهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية هي :

أ ـ قيام صاحب الصلاحية بتغيير بيانات أجنبي من قادم للعمرة إلى قادم للعمل.

ب ـ تغيير مهنة مقيم إلكترونياً تزويراً لتيسير إجراءات استقدام أسرته.

جـ ـ دخول صاحب صلاحية بطريقة عير مشروعة على النظام لرفع المخالفات المرورية عن سيارة لحين نقل ملكيتها إلكترونياً.

د ـ استخراج تأشيرات إلكترونية مزورة للحج والعمرة.

هـ ـ استخراج تأشيرات إلكترونية مزورة لاستقدام العمالة.

و ـ استخراج بطاقات الائتمان البنكية (فيزا ـ ماستركارد) مزورة.

ز ـ استخراج رخص قيادة إلكترونية عامة وخاصة مزورة.

ح ـ استخراج رخص سير إلكترونية مزورة للمركبات.

٣ـ إن الصور المهمة للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية هي :

أ ـ استخراج جواز سفر إلكتروني مزور.

ب ـ استخراج رخص بناء إلكترونية مزورة.

جـ ـ استخراج ضمانات بنكية إلكترونية مزورة.

د ـ استخراج شهادة إلكترونية مزورة للزكاة والدخل.

هـ ـ تزوير محررات استخراج السجل المدني إلكترونياً.

و ـ استخراج بطاقات أحوال إلكترونية مزورة.

ز ـ استخراج وكالات شرعية إلكترونية مزورة.

وتتفق هذه النتائج جزئياً مع ما توصل إليه الكركي (٢٠٠٣م) في أن استخراج وثائق مزورة من أهم صور جريمة التزوير الإلكتروني، كما تتفق جزئياً مع ما توصلت إليه دراسة حجازي (٢٠٠٥م) في أن إساءة استخدام صاحب الصلاحية موقعه من أهم أسباب ارتكاب صور التزوير الإلكتروني المختلفة، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة (Goodman 1997) في أن التغيير في سجلات الحاسب بإدخال بيانات غير صحيحة من أهم صور جريمة التزوير الإلكتروني.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، بأن هناك عدة صور لارتكاب جريمة التزوير الإلكتروني، وهذه الصور تبدأ من اختراق وتعد من خارج المنظمة باستخدام أدوات ووسائل وتقنيات الاختراق والتعدي، أو من خلال قيام صاحب الصلاحية بتغيير البيانات في سجلات الحاسب الآلي دون مسوغات نظامية لهذا التغيير. وتتعدد الأمثلة والصور على ذلك، وهي إما تكون مباشرة بالتغيير في السجلات اللازمة كتغيير بيانات أجنبي من قادم لأداء العمرة إلى قادم للعمل، أو تغيير مهنة مقيم تزويراً لتيسير إجراءات استقدام أسرته، أو رفع المخالفات المرورية عن سيارة بنقل ملكيتها مؤقتاً إلى شخص آخر، لتجديدها نظامياً، ومن ثمَّ إعادة ملكيتها إلى مالكها الأصلي، وإما تكون صوراً غير مباشرة من خلال استخراج بطاقة أحوال مزورة لأشخاص غير سعوديين على أنهم سعوديون، ومن ثم استخدامها في استخراج جواز سفر أو سجل تجاري مزور وفقاً لقاعدة (ما بني على باطل فهو باطل)، أو تغيير المهنة في حفيظة النفوس من عسكري إلى متسبب لكي يتسنى له استخراج جواز سفر بالمهنة الجديد والسفر للخارج دون الحصول على إذن من مرجعه. ويشير حجازي (٢٠٠٥م، ص١٢٤) إلى تعدد صور التزوير الإلكتروني، واشتمال غالبيتها على تغيير في سجلات الحاسب الآلي دون مسوغات نظامية.

كما أن هناك العديد من صور التزوير الإلكتروني التي تتضمن التغيير في سجلات الحاسب دون مسوغات نظامية لهذا التغيير من خلال استخراج تأشيرات إلكترونية مزورة للحج والعمرة، واستخراج بطاقات الائتمان البنكية (فيزا ـ ماستركارد المزورة)، واستخراج رخص قيادة إلكترونية عامة وخاصة مزورة، واستخراج رخص سير إلكترونية مزورة، واستخراج رخص بناء

إلكترونية مزورة، واستخراج ضمانات بنكية إلكترونية مزورة، واستخراج شهادة إلكترونية مزورة للزكاة والدخل، وتزوير محررات استخراج السجل المدني إلكترونياً، واستخراد بطاقة أحوال إلكترونية مزورة، واستخراج وكالات شرعية إلكترونية مزورة. ويقع التزوير الإلكتروني بمجرد إدخال البيانات المزورة إلى سجلات الحاسب الآلي، بينما يقع التزوير التقليدي عند استخراج المستندات من الحاسب واستخدامها، كاستخراج بطاقة أحوال مزورة أو تم تعديل المهنة بها تزويراً، واستخدامها في استخراج جواز سفر واستعماله أيضاً في السفر، وعنصر الضرر الذي يترتب على التغيير لا حصر له، ففي حالة استخدام أجنبي التزوير لاستخراج بطاقة أحوال مزورة، واستخدامها في استخراج سجل تجاري يكون قد أوقع الضرر بالمواطنين وشاركهم في فرص الرزق وخالف القوانين، وكذلك يتحقق عنصر الضرر في حالة تغيير مهنة مواطن سعودي من عسكري إلى متسبب لتيسير استخراج جواز سفر واستخدامه في السفر للخارج من خلال مخالفة الأوامر والسفر دون تصريح من مرجعه، ويشير العريان (٢٠٠٤م، ص١٣٧) إلى أن التزوير هو تغيير الحقيقة في محرر بإحدى الطرق التي وضحها القانون تغييراً من شأنه أن يسبب ضرراً. أما خضر (١٩٨٨م، ص٢٥) فيضيف القصد الجنائي الخاص من التزوير كركن من أركان وقوعه وهو تغيير الحقيقة في بيانات محرر ما، بإحدى الطرق المحددة نظاماً، مع ترتيب ضرر للغير، ومع توافر نية استعمال المحرر للحصول على منفعة أو قضاء مصلحة من أجلها تمت عملية التزوير. ويفصل الهيتي (٢٠٠٥م، ص٧٦) الفرق بين التزوير التقليدي والتزوير الإلكتروني فيشير إلى أن التزوير الإلكتروني إتلاف المعلومات أو تشويهها أو تحريفها بالتعديل سواء بالحذف أو الإضافة، بالإضافة إلى أنه قد يتعلق بالكيان المادي للحاسب الآلي، أو البرامج ذاتها، وهو يندرج بصفة

عامـة تحـت نطاق التزويـر الإلكتروني كسـلوك غير مشروع يتعلـق بمعالجة المعلومات ونقلها، فهو سـلوك غير قانوني وغير مسـموح به يتعلق بالتعامل الفوري مع المعلومات والبيانات أو انتقالها.

وبهـذا يتحقـق الهـدف الثالث مـن أهداف الدراسـة وهـو معرفة صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

٤ . ٥ سـمات المجرم الإلكتروني فـي جرائم التزوير الإلكتروني

للإجابة عن السـؤال الرابع من أسـئلة الدراسـة وهو : ما سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني ؟ قام الباحث بتحليل اسـتجابات مفردات الدراسـة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربيـة السـعودية، وتنـاول التحليـل تحديـد سـمات المجـرم الإلكتروني في جرائم التزوير الإلكتروني من خلال المتوسـط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٥) استجابات جميع مفردات الدراسة لتحديد سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني.

الجدول رقم (١٥) سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
٨	يتمتع بالمهارة في استخدام الحاسب الآلي.	ت	١١٩	١٠٨	١٠	٤	–	٤,٤٢	٠,٦٥	١٨٩,٦	٠,٠**	الأول
		٪	٤٩,٤	٤٤,٨	٤,١	١,٧	–					
٣	يهدف في الغالب من ارتكاب جريمة التزوير المعلوماتي إلى الحصول على منفعة.	ت	١٠٢	١٣٦	٣	–	–	٤,٤١	٠,٥٢	١١٨,٩	٠,٠**	الثاني
		٪	٤٢,٣	٥٦,٤	١,٢	–	–					
١	يتمتع بالاحترافية بذكاء.	ت	١٠٨	١١٨	١٣	٢	–	٤,٣٨	٠,٦٣	١٨٦,٦	٠,٠**	الثالث
		٪	٤٤,٨	٤٩,٠	٥,٤	٠,٨	–					
٦	يرتكب جريمة التزوير لمصلحته الخاصة.	ت	٨٥	١٣٥	٢٠	١	–	٤,٣٨	٠,٦٣	١٨٨,١	٠,٠**	الرابع
		٪	٣٥,٣	٥٦,٠	٨,٣	٠,٤	–					
٩	يتمتع بالقدرة على اختراق نظم المعلومات وتحييد جدران الحماية وبرامج مكافحة الفيروسات.	ت	١٠٠	١٠٩	٢٦	٤	٢	٤,٢٥	٠,٧٨	٢٢٧,٤	٠,٠**	الخامس
		٪	٤١,٥	٤٥,٢	١٠,٨	١,٧	٠,٨					
١٥	يثابر في محاولات متكررة لاختراق المواقع.	ت	٨٠	١٣٦	٢٢	١	٢	٤,٢١	٠,٦٩	٢٨٥,٧	٠,٠**	السادس
		٪	٣٣,٢	٥٦,٤	٩,١	٠,٤	٠,٨					
١٣	يستخدم أساليب متطورة لسرقة منظومة التوقيع الإلكتروني.	ت	٦٥	١٤٦	٣٠	–	–	٤,١٥	٠,٦١	٨٨,١	٠,٠**	السابع
		٪	٢٧,٠	٦٠,٦	١٢,٤	–	–					
١٢	يبتكر أساليب جديدة لتزوير المحررات الإلكترونية.	ت	٦٥	١٣٩	٣٣	٤	–	٤,١٠	٠,٦٨	١٦٨,١	٠,٠**	الثامن
		٪	٢٧,٠	٥٧,٧	١٣,٧	١,٧	–					

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٥) أن المتوسط الحسابي العام لمحور سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني قد بلغ (١١ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود سمات مهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني.

كما كشف الجدول أن هناك ست سمات تمثل (٠ , ٤٠ ٪) من السمات التي تضمنها محور سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢١ , ٤ـ ٤٢ , ٤)، مما يشير إلى شدة أهميتها، فهي من السمات المهمة جداً للمجرم الإلكتروني في جرائم التزوير الإلكتروني ، وهي على النحو التالي :

١ ـ يتمتع بالمهارة في استخدام الحاسب الآلي، وجاءت هذه السمة في المركز الأول لترتيب الأهمية النسبية بمتوسط (٤٢ , ٤)، حيث وافق على أهميتها (٢ , ٩٤ ٪) مقابل (٧ , ١ ٪) اعترضوا على أهميتها.

٢ـ يهدف في الغالب من ارتكاب جريمة التزوير المعلوماتي إلى الحصول على منفعة، وجاءت هذه السمة في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٤١ , ٤)، حيث وافق على أهميتها (٧ , ٩٨ ٪).

٣ـ يتمتع بالاحترافية بذكاء، وجاءت هذه السمة في المركز الثالث لترتيب الأهمية النسبية بمتوسط (٣٨ , ٤)، حيث وافق على أهميتها (٨ , ٩٤٪) مقابل (٨ , ٠ ٪) اعترضوا على أهميتها.

٤ ـ يرتكب جريمة التزوير لمصلحته الخاصة، وجاءت هذه السمة في المركز الرابع لترتيب الأهمية النسبية بمتوسط (٣٨ , ٤)، حيث وافق على أهميتها (٣ , ٩١ ٪) مقابل (٤ , ٠ ٪) اعترضوا على أهميتها.

٥ ـ يتمتع بالقدرة على اختراق نظم المعلومات وتحييد جدران الحماية وبرامج مكافحة الفيروسات، وجاءت هذه السمة في المركز الخامس لترتيب الأهمية النسبية بمتوسط (٢٥ , ٤)، حيث وافق على أهميتها (٧ , ٨٦ ٪) مقابل (٥ , ٢ ٪) اعترضوا على أهميتها.

٦ ـ يثابر في محاولات متكررة لاختراق المواقع، وجاءت هذه السمة في المركز السادس لترتيب الأهمية النسبية بمتوسط (٢١ , ٤)، حيث وافق على أهميتها (٦ , ٨٩ ٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

وتبين من الجدول أن هناك تسع سمات تمثل (٠ , ٦٠ ٪) من السمات التي تضمنها محور سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٧٢ , ٣ـ ١٥ , ٤)، مما يشير إلى أهميتها، فهي من السمات المهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني ، وهي على النحو التالي :

١ ـ يستخدم أساليب متطورة لسرقة منظومة التوقيع الإلكتروني، وجاءت هذه السمة في المركز السابع لترتيب الأهمية النسبية بمتوسط (١٥ , ٤)، حيث وافق على أهميتها (٦ , ٨٧ ٪).

٢ ـ يبتكر أساليب جديدة لتزوير المحررات الإلكترونية، وجاءت هذه السمة في المركز الثامن لترتيب الأهمية النسبية بمتوسط (١٠ , ٤)،

حيث وافق على أهميتها (٧ , ٨٤ ٪) مقابل (٧ , ١ ٪) اعترضوا على أهميتها.

٣ ـ لديه قدرة فائقة على المعالجة الإلكترونية للنصوص والكلمات، وجاءت هذه السمة في المركز التاسع لترتيب الأهمية النسبية بمتوسط (٠٩ , ٤)، حيث وافق على أهميتها (٢ , ٨٢ ٪) مقابل (٥ , ٢ ٪) اعترضوا على أهميتها.

٤ ـ يسرع في تدمير الأدلة الرقمية التي استخدمها في ارتكاب جريمة التزوير المعلوماتي، وجاءت هذه السمة في المركز العاشر لترتيب الأهمية النسبية بمتوسط (٠٧ , ٤)، حيث وافق على أهميتها (٣ , ٨١ ٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

٥ ـ يرتكب جريمة التزوير لمصلحة الآخرين، وجاءت هذه السمة في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (٩٨ , ٣)، حيث وافق على أهميتها (١ , ٨٨ ٪) مقابل (٩ , ٤ ٪) اعترضوا على أهميتها.

٦ ـ يعمل غالبيتهم في المنظمات التي يقع عليها التزوير في مجال نظم المعلومات، وجاءت هذه السمة في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (٩٦ , ٣)، حيث وافق على أهميتها (٧ , ٧٤ ٪) مقابل (٧ , ٣ ٪) اعترضوا على أهميتها.

٧ ـ يمتلك علاقات إنسانية جيدة مع الآخرين، وجاءت هذه السمة في المركز الثالث عشر لترتيب الأهمية النسبية بمتوسط (٨١ , ٣)، حيث وافق على أهميتها (٢ , ٧٢ ٪) مقابل (٠ , ١٢ ٪) اعترضوا على أهميتها.

٨ ـ يرتكب التزوير لإثبات قدراته على الاختراق والتعدي، وجاءت هذه السمة في المركز الرابع عشر لترتيب الأهمية النسبية بمتوسط (٣,٧٩)، حيث وافق على أهميتها (٣,٦٩ ٪) مقابل (٩,٧ ٪) اعترضوا على أهميتها.

٩ ـ يرتكب جريمة التزوير رداً على الاستغناء عن خدماته، وجاءت هذه السمة في المركز الخامس عشر لترتيب الأهمية النسبية بمتوسط (٣,٧٢)، حيث وافق على أهميتها (٨,٥٩ ٪) مقابل (٣,٨ ٪) اعترضوا على أهميتها.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ توجد سمات مهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني.

٢ ـ إن السمات المهمة جداً للمجرم الإلكتروني في جرائم التزوير الإلكتروني هي :

أ ـ يتمتع بالمهارة في استخدام الحاسب الآلي.

ب ـ يهدف في الغالب من ارتكاب جريمة التزوير المعلوماتي إلى الحصول على منفعة.

جـ ـ يتمتع بالاحترافية بذكاء.

د ـ يرتكب جريمة التزوير لمصلحته الخاصة.

هـ ـ يتمتع بالقدرة على اختراق نظم المعلومات وتحييد جدران الحماية وبرامج مكافحة الفيروسات.

و ـ يثابر في محاولات متكررة لاختراق المواقع.

٣ ـ إن السمات المهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني هي :

أ ـ يستخدم أساليب متطورة لسرقة منظومة التوقيع الإلكتروني.

ب ـ يبتكر أساليب جديدة لتزوير المحررات الإلكترونية.

جـ ـ لديه قدرة فائقة على المعالجة الإلكترونية للنصوص والكلمات.

د ـ يسرع في تدمير الأدلة الرقمية التي استخدمها في ارتكاب جريمة التزوير المعلوماتي.

هـ ـ يرتكب جريمة التزوير لمصلحة الآخرين.

و ـ يعمل غالبيتهم في المنظمات التي يقع عليها التزوير في مجال نظم المعلومات.

ز ـ يمتلك علاقات إنسانية جيدة مع الآخرين.

ح ـ يرتكب التزوير لإثبات قدراته على الاختراق والتعدي.

ط ـ يرتكب جريمة التزوير رداً على الاستغناء عن خدماته.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة حجازي (٢٠٠٥م) في تمتع المجرم الإلكتروني بسمات تؤهلة لارتكاب الجرائم الإلكترونية بصفة عامة وجرائم التزوير الإلكتروني بصفة خاصة من أهمها المهارة في استخدام الحاسب الآلي، والاحترافية والذكاء، والقدرة على اختراق نظم المعلومات، كما تتفق جزئياً مع ما توصلت إليه دراسة(Erdonmez, 2002) في أن من أهم سمات المجرم الإلكتروني استخدام أساليب متطورة في الاختراق والتعدي والتزوير، في ضوء قدرته الفائقة على معالجة النصوص والكلمات، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة المسند والهيتي (٢٠٠١م) في أن من أهم سمات المجرم الإلكتروني السرعة في تدمير الأدلة الرقمية التي استخدمها في ارتكاب الجريمة الإلكترونية.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، بأن هناك عدة سمات يجب توافرها في المجرم الإلكتروني يأتي في مقدمتها تمتعه بالمهارة في استخدام الحاسب الآلي، حيث تمكنه تلك المهارات من القيام بعمليات الاختراق والتعدي ومعرفة أساليب كسر كلمات المرور واختراق المواقع والحصول على ما يريد من المعلومات والبيانات، وتغيير ما يريد وتزوير ما يرغب به، وهو في هذا الصدد يرتكب جريمة التزوير المعلوماتي للحصول على منفعة سواء كانت له أو للغير، ولذلك قد يرتكب جريمة التزوير الإلكتروني لمصلحته الشخصية أو لمصلحة الغير، وهو يتمتع بالاحترافية والذكاء والمثابرة في محاولات الاختراق والتعدي لحين تحقيق هدفه في اختراق نظم المعلومات وتحييد جدران الحماية وبرامج مكافحة الفيروسات؛ حيث يستخدم برامج مضادة أو فيروسات غير معروفة لتمكينه من الدخول على الأنظمة واستخدامها كما لو كان مصرح له باستخدامها. ويشير العريان (٢٠٠٤م، ص٦٢) إلى أن المجرم المعلوماتي يتمتع بالاحترافية والذكاء، ويستخدم تقنيات التدمير الناعمة التي تساعده على التلاعب ببيانات وبرامج الحاسب الآلي لمحو البيانات أو تعطيل استخدام البرامج.

كما يستخدم المجرم المعلوماتي أساليب متطورة لسرقة منظومة التوقيع الإلكتروني كاستخدام الشبكة الشبح ذات القدرات العالية على الاختراق والتعدي، والتي تمنح مستخدمها الفرصة للدخول إلى كافة المواقع المحجوبة والمشفرة من خلال قدرتها العالية جداً على كسر كلمات السر وفك الشفرات. ويشير مؤنس محب الدين (٢٠٠٦م، ص١٥) إلى أن الشبكة الشبح تمثل الجديد في عالم الاختراق؛ ويصعب الكشف عنها لأنها تمتاز بسرعة الاختفاء، وعدم إمكان رصدها وتحديد موقعها. وتدور الشبهات حالياً حول أربعة

مواقع لها، ثلاثة منها في الصين، والرابع في شمال كاليفورنيا. وقد تمكنت من اختراق القارات الأمريكية وأجهزة الـ FBI ، وبعض البنوك في كل من سويسرا والهند وإيران.

ومن أهم سمات المجرم الإلكتروني أنه يبتكر أساليب جديدة لتزوير المحررات الإلكترونية جزئياً أو كلياً، فضلاً عن قدرته على معالجة النصوص والكلمات إلكترونياً لإصدار وثائق ومحررات مزورة أو مصطنعة، مع الإسراع في تدمير الأدلة الرقمية التي استخدمها في ارتكاب جريمة التزوير المعلوماتي لكي لا يمكن الكشف عن موقعه باستخدام تقنيات التتبع وتقنيات استرجاع المعلومات. ويشير حجازي (٢٠٠٥م، ص٦٣) إلى أن وسيلة تقنيات التتبع واسترجاع المعلومات في الكشف عن عمليات الاختراق والتعدي وتزوير المعلومات هي التعرف على الـ IP الذي يتركه المخترق أثناء تجواله في الشبكة، وعند اختراقه لأي موقع.

واللافت للنظر أن المجرم المعلوماتي يعمل غالباً في المنظمات التي يقع عليها التزوير في مجال نظم المعلومات، حيث يستغل طبيعة عمله في ارتكاب جرائم التزوير سواء بالاختراق أو التعدي، أو استغلال وضعه كمصرح له بالدخول على النظام، إلا أن هذا الدخول في الجهات الحكومية مشروط ومقيد، فيمكن من خلال مركز المعلومات الوطني تحديد الموظف الذي دخل على النظام وغير البيانات والمعلومات من خلال البرنت الصادر من المكان الذي تم به التزوير، ويحدد مركز المعلومات الوطني رقم المستخدم ووقت دخوله على النظام والتغيير الذي قام به، فيكون بمثابة دليل إدانة مباشر يحدد المجرم الذي قام بعملية التزوير دون غيره.

ويمتلك المجرم المعلوماتي علاقات إنسانية جيدة مع الآخرين، بل ويعتبر أن عمله فيه مساعدة للناس على قضاء مصالحها، وأنه يرغب في تيسير

مهمة الناس ومساعدتهم على إنجاز أعمالهم في مقابل مبلغ مالي بسيط، أو مقابل الصداقة، ومن ثمَّ لا يبالي بارتكاب التزوير، بل يترتب على قيامه بتلك الأعمال تشعب علاقاته الإنسانية، كما قد يرتكب التزوير لإثبات قدراته على الاختراق والتعدي، أو رداً على الاستغناء عن خدماته بفصله من العمل. ويشير العريان (٢٠٠٤م، ص٦٢) إلى حرص المجرم المعلوماتي على تدعيم علاقاته الإنسانية، وتطبيقاً لذلك ترتكب كثير من جرائم المعلوماتية بدافع الكبرياء، أو للرد على تعرضه للفصل من العمل أو الاستغناء عن خدماته، أو بدافع النصب أو الحسد أو بدافع اللهو، أو لإظهار ما يتمتع به من مهارات تبرز تفوقه في مواجهة أنظمة أمن المعلومات، أو لمجرد الحصول على منفعة مالية.

وبهذا يتحقق الهدف الرابع من أهداف الدراسة وهو معرفة سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني.

٤ . ٦ سمات المجني عليه في جرائم التزوير الإلكتروني

للإجابة عن السؤال الخامس من أسئلة الدراسة وهو : ما سمات المجني عليه في جرائم التزوير الإلكتروني ؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد سمات المجني عليه في جرائم التزوير الإلكتروني من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٦) استجابات جميع مفردات الدراسة لتحديد سمات المجني عليه في جرائم التزوير الإلكتروني.

الجدول رقم (١٦) سمات المجني عليه في جرائم التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
١١	تخفي الجهات (البنوك والمؤسسات المالية) خبر تعرضها للتزوير خوفاً من فقدان ثقة العملاء بها.	ت	١١٧	١٠٣	١٨	٣	–	٤,٣٩	٠,٦٨	١٦٧,٨	٠,٠**	الأول
		٪	٤٨,٥	٤٢,٧	٧,٥	١,٢	–					
١	المعاناة من ضعف نظم الحماية الخاصة بالحاسب الآلي.	ت	٨٨	١٣٠	٢١	٢	–	٤,٢٦	٠,٦٥	١٧٥,٤	٠,٠**	الثاني
		٪	٣٦,٥	٥٣,٩	٨,٧	٠,٨	–					
٣	قلة الخبرة اللازمة لاكتشاف الفيروسات المستخدمة في ارتكاب التزوير.	ت	٨٩	١٢٣	٢١	٧	١	٤,٢١	٠,٧٥	٢٤٧,٤	٠,٠**	الثالث
		٪	٣٦,٩	٥١,٠	٨,٧	٢,٩	٠,٤					
٨	الانخداع بالعروض التجارية الوهمية.	ت	٧٧	١٢٨	٣٢	٤	–	٤,١٥	٠,٧١	١٤٦,٦	٠,٠**	الرابع
		٪	٣٢,٠	٥٣,١	١٣,٣	١,٧	–					
٩	الخسارة المالية نتيجة عدم الاحتراز في الإدلاء ببيانات البطاقات الائتمانية.	ت	٦٩	١٤١	٢٨	٣	–	٤,١٥	٠,٦٦	١٨١,٢	٠,٠**	الخامس
		٪	٢٨,٦	٥٨,٥	١١,٦	١,٢	–					

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
٥	المعاناة من العشوائية في استقبال البريد الإلكتروني.	ت	٧٠	١٣١	٣٥	٥	–	٤,١٠	٠,٧١	١٤٥,٩	٠,٠**	الثامن
		٪	٢٩,٠	٥٤,٤	١٤,٥	٢,١	–					
٢	الانخداع بإغراءات التخفيضات الوهمية من قبل الجناة.	ت	٥٥	١٥٧	٢٢	٥	٢	٤,٠٧	٠,٦٩	٣٤٣,٨	٠,٠**	التاسع
		٪	٢٢,٨	٦٥,١	٩,١	٢,١	٠,٨					
١٤	تتعرض المنظمات للاختراق والتعدي لارتكاب التزوير أكثر من الأفراد.	ت	٦٢	١٣٢	٤٠	٦	١	٤,٠٣	٠,٧٥	٢٣٤,٢	٠,٠**	العاشر
		٪	٢٥,٧	٥٤,٨	١٦,٦	٢,٥	٠,٤					
٤	التنقل بين صفحات الإنترنت دون هدف واضح.	ت	٦٥	١١٩	٤٤	١٣	–	٣,٩٨	٠,٨٢	٩٩,١	٠,٠**	الحادي عشر
		٪	٢٧,٠	٤٩,٤	١٨,٣	٥,٤	–					
٧	التعرض للابتزاز من قبل المواقع المشبوهة.	ت	٥٩	١١٥	٥٤	١٢	١	٣,٩١	٠,٨٤	١٦٩,١	٠,٠**	الثاني عشر
		٪	٢٤,٥	٤٧,٧	٢٢,٤	٥,٠	٠,٤					
١٠	يتعرض للحرج عند استخدام المسمى في المواقع المشبوهة.	ت	٥٠	١٢٤	٥٩	٨	–	٣,٩٠	٠,٧٦	١١٤,٥	٠,٠**	الثالث عشر
		٪	٢٠,٧	٥١,٥	٢٤,٥	٣,٣	–					
١٢	تقوم المؤسسات المالية المجني عليها في الغالب بتعويض عملائها المتضررين من جرائم التزوير الإلكتروني.	ت	٦٠	١٠١	٥٧	٢٠	٣	٣,٨١	٠,٩٥	١٢١,٢	٠,٠**	الرابع عشر
		٪	٢٤,٩	٤١,٩	٢٣,٧	٨,٣	١,٢					
١٣	تستجيب بعض الجهات المجني عليها لطلبات المبتزين.	ت	٤٧	١٠٠	٧١	٢٣	–	٣,٧١	٠,٨٩	٥٤,١	٠,٠**	الخامس عشر
		٪	١٩,٥	٤١,٥	٢٩,٥	٩,٥	–					
متوسط استجابات مفردات الدراسة على محور سمات المجني عليه في جرائم التزوير الإلكتروني								٤,٠٦	٠,٤٢			

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بسمات المجني عليه في جرائم التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٦) أن المتوسط الحسابي العام لمحور سمات المجني عليه في جرائم التزوير الإلكتروني قد بلغ (٠٦ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود سمات مهمة للمجني عليه في جرائم التزوير الإلكتروني.

كما كشف الجدول أن هناك ثلاث سمات تمثل (٠ , ٢٠ ٪) من السمات التي تضمنها محور سمات المجني عليه في جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢١ , ٤ـ ٣٩ , ٤)، مما يشير إلى شدة أهميتها، فهي من السمات المهمة جداً للمجني عليه في جرائم التزوير الإلكتروني، وهي على النحو التالي :

١ ـ تخفي الجهات (البنوك والمؤسسات المالية) خبر تعرضها للتزوير خوفاً من فقدان ثقة العملاء بها، وجاءت هذه السمة في المركز الأول لترتيب الأهمية النسبية بمتوسط (٣٩ , ٤)، حيث وافق على أهميتها (٢ , ٩١ ٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

٢ ـ المعاناة من ضعف نظم الحماية الخاصة بالحاسب الآلي، وجاءت هذه السمة في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٢٦ , ٤)، حيث وافق على أهميتها (٤ , ٩٠ ٪) مقابل (٨ , ٠ ٪) اعترضوا على أهميتها.

٣ ـ قلة الخبرة اللازمة لاكتشاف الفيروسات المستخدمة في ارتكاب التزوير، وجاءت هذه السمة في المركز الثالث لترتيب الأهمية

النسبية بمتوسط (٢١ , ٤)، حيث وافق على أهميتها (٩ , ٨٧ ٪) مقابل (٣ , ٣ ٪) اعترضوا على أهميتها.

وتبين من الجدول أن هناك اثنتى عشرة سمة تمثل (٠ , ٨٠ ٪) من السمات التي تضمنها محور سمات المجني عليه في جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٧١ , ٣ـ ١٥ , ٤)، مما يشير إلى أهميتها، فهي من السمات المهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني ، وهي على النحو التالي :

١ ـ الانخداع بالعروض التجارية الوهمية، وجاءت هذه السمة في المركز الرابع لترتيب الأهمية النسبية بمتوسط (١٥ , ٤)، حيث وافق على أهميتها (١ , ٨٧ ٪) مقابل (٧ , ١ ٪) اعترضوا على أهميتها.

٢ ـ الخسارة المالية نتيجة عدم الاحتراز في الإدلاء ببيانات البطاقات الائتمانية، وجاءت هذه السمة في المركز الخامس لترتيب الأهمية النسبية بمتوسط (١٥ , ٤)، حيث وافق على أهميتها (١ , ٨٧٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

٣ ـ مساهمة قلة الخبرة في استخدام الشبكة في سهولة الاستيلاء على البيانات المهمة، وجاءت هذه السمة في المركز السادس لترتيب الأهمية النسبية بمتوسط (١٥ , ٤)، حيث وافق على أهميتها (٦ , ٨٤ ٪) مقابل (٢ , ١ ٪) اعترضوا على أهميتها.

٤ ـ المنظمات المالية أكثر تعرضاً للاختراق والتعدي والتزوير من المنظمات الأخرى، وجاءت هذه السمة في المركز السابع لترتيب الأهمية النسبية بمتوسط (١٤ , ٤)، حيث وافق على أهميتها (٦ , ٨٤ ٪) مقابل (١ , ٢ ٪) اعترضوا على أهميتها.

٥ ـ المعاناة من العشوائية في استقبال البريد الإلكتروني، وجاءت هذه السمة في المركز الثامن لترتيب الأهمية النسبية بمتوسط (١٠ , ٤)، حيث وافق على أهميتها (٤ , ٨١ ٪) مقابل (١ , ٢ ٪) اعترضوا على أهميتها.

٦ ـ الانخداع بإغراءات التخفيضات الوهمية من قبل الجناة، وجاءت هذه السمة في المركز التاسع لترتيب الأهمية النسبية بمتوسط (٠٧ , ٤)، حيث وافق على أهميتها (٩ , ٨٧ ٪) مقابل (٩ , ٢٪) اعترضوا على أهميتها.

٧ ـ تتعرض المنظمات للاختراق والتعدي لارتكاب التزوير أكثر من الأفراد، وجاءت هذه السمة في المركز العاشر لترتيب الأهمية النسبية بمتوسط (٠٣ , ٤)، حيث وافق على أهميتها (٥ , ٨٠ ٪) مقابل (٩ , ٢ ٪) اعترضوا على أهميتها.

٨ ـ التنقل بين صفحات الإنترنت دون هدف واضح، وجاءت هذه السمة في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (٩٨ , ٣)، حيث وافق على أهميتها (٤ , ٧٦ ٪) مقابل (٤ , ٥ ٪) اعترضوا على أهميتها.

٩ ـ التعرض للابتزاز من قبل المواقع المشبوهة، وجاءت هذه السمة في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (٩١ , ٣)، حيث وافق على أهميتها (٢ , ٧٢ ٪) مقابل (٤ , ٥ ٪) اعترضوا على أهميتها.

١٠ ـ يتعرض للحرج عند استخدام المسمى في المواقع المشبوهة، وجاءت هذه السمة في المركز الثالث عشر لترتيب الأهمية النسبية

بمتوسط (٣,٩٠)، حيث وافق على أهميتها (٢,٧٢٪) مقابل (٣,٣٪) اعترضوا على أهميتها.

١١ ـ تقوم المؤسسات المالية المجني عليها في الغالب بتعويض عملائها المتضررين من جرائم التزوير الإلكتروني، وجاءت هذه السمة في المركز الرابع عشر لترتيب الأهمية النسبية بمتوسط (٣,٨١)، حيث وافق على أهميتها (٨,٦٦٪) مقابل (٥,٩٪) اعترضوا على أهميتها.

١٢ ـ تستجيب بعض الجهات المجني عليها لطلبات المبتزين، وجاءت هذه السمة في المركز الخامس عشر لترتيب الأهمية النسبية بمتوسط (٣,٧١)، حيث وافق على أهميتها (٠,٦١٪) مقابل (٥,٩٪) اعترضوا على أهميتها.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ توجد سمات مهمة للمجني عليه في جرائم التزوير الإلكتروني.

٢ ـ إن السمات المهمة جداً للمجني عليه في جرائم التزوير الإلكتروني هي :

أ ـ تخفي الجهات (البنوك والمؤسسات المالية) خبر تعرضها للتزوير خوفاً من فقدان ثقة العملاء بها.

ب ـ المعاناة من ضعف نظم الحماية الخاصة بالحاسب الآلي.

جـ ـ قلة الخبرة اللازمة لاكتشاف الفيروسات المستخدمة في ارتكاب التزوير.

٣ ـ إن السمات المهمة للمجني عليه في جرائم التزوير الإلكتروني هي :

أ ـ الانخداع بالعروض التجارية الوهمية.

ب ـ الخسارة المالية نتيجة عدم الاحتراز في الإدلاء ببيانات البطاقات الائتمانية.

جـ ـ مساهمة قلة الخبرة في استخدام الشبكة في سهولة الاستيلاء على البيانات المهمة.

د ـ المنظمات المالية أكثر تعرضاً للاختراق والتعدي والتزوير من المنظمات الأخرى.

هـ ـ المعاناة من العشوائية في استقبال البريد الإلكتروني.

و ـ الانخداع بإغراءات التخفيضات الوهمية من قبل الجناة.

ز ـ تتعرض المنظمات للاختراق والتعدي لارتكاب التزوير أكثر من الأفراد.

ح ـ التنقل بين صفحات الإنترنت دون هدف واضح.

ط ـ التعرض للابتزاز من قبل المواقع المشبوهة.

ي ـ يتعرض للحرج عند استخدام المسمى في المواقع المشبوهة.

ك ـ تقوم المؤسسات المالية المجني عليها في الغالب بتعويض عملائها المتضررين من جرائم التزوير الإلكتروني.

ل ـ تستجيب بعض الجهات المجني عليها لطلبات المبتزين.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة حجازي (٢٠٠٥م) في أن تمتع المجني عليه بسمات تجعله عرضه للجرائم الإلكترونية بصفة عامة وجرائم التزوير الإلكتروني بصفة خاصة من أهمها قلة الخبرة في استخدام الشبكة، مما يترتب عليه سهولة الاستيلاء على بياناته المهمة، والعشوائية في استقبال البريد الإلكتروني، والتنقل بين صفحات الإنترنت دون هدف

واضـح، كما تتفـق جزئياً مع ما توصلت إليه دراسـة (Erdonmez 2002) في أن المنظـمات المالية أكثر تعرضـاً للاختراق والتعدي مـن المنظمات الأخرى، وأيضـاً تتفق جزئياً مع ما توصلت إليه دراسـة المسـند والهيتي (٢٠٠١م) في تعرض المجني عليه للابتزاز من قبل المواقع المشبوهة.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال سمات المجني عليـه في جرائم التزوير الإلكتروني، بأن هناك عدة سـمات للمجني عليه يأتي في مقدمتها إخفاء الجهات (البنوك والمؤسسات المالية) خبر تعرضها للتزوير خوفـاً من فقدان ثقة عملائها بها؛ لأن التزوير في الغالب يتضمن الاسـتيلاء عـلى أموال من أحـد الحسـابات الخاصة بأحـد العملاء بالبنك أو المؤسسـة الماليـة سـواء بتحويله إلى حسـاب آخـر، أو بإجراء عمليـات شراء من ذلك الحسـاب، وهـذا ينـشر الهلع بـين العملاء من تعرضهـم لتبديـد أموالهم، مما يجعلهم يسارعون إلى سحب مدخراتهم من تلك البنوك أو المؤسسات المالية، ممـا يجبر تلك الجهات على التكتم خوفاً من وقـوع ذلك وفقدان ثقة عملائها بهـا، ويزداد الأمر سـوءاً في حالة ضعف نظم الحماية الخاصة بالحاسـب الآلي وقلة الخبرة اللازمة لاكتشـاف الفيروسـات المسـتخدمة في ارتكاب التزوير والتي قد يطلقها المزور للاسـتعانة بها في اختراق النظام والعبث بها. ويشـير الهيتـي (٢٠٠٥م، ص٢١٨) إلى أن الجهات المجني عليها تخفي خبر تعرضها للتزوير خوفاً من فقدان ثقة عملائها بها. .

كـما ينخـدع كثـير مـن المجنـي عليهـم في جرائـم التزويـر الإلكـتروني بالعروض التجارية الوهمية، حيث ينتحل بعض الأشـخاص مواقع لمنظمات تجارية مشـهورة، ويقدمون سلعاً وخدمات بأسـعار زهيدة، مما يجعل المجني عليهـم ينجذبون لها ويقومون بملء النمـوذج الإلكتروني للشراء، ويتضمن هـذا النموذج أرقام بطاقـات الائتمان، والبنك الذي أصدرهـا، فيقوم الجناة

بالدخول على أنظمة البنك والتعامل بأرقام البطاقة واستخدامها في عمليات الشراء أو التحويل من حساب لآخر، فالإدلاء ببيانات البطاقة الائتمانية يجب ان يكون في أضيق الحدود، وللمنظمات المعروفة جيداً لتجنب الخسارة المالية التي تنتج من عدم الاحتراز في الإدلاء ببيانات البطاقة الائتمانية. ويشير الشوابكة (٢٠٠٤م، ص١٩) إلى خطورة الإدلاء ببيانات بطاقة الائتمان أو البطاقات البنكية، نتيجة عمليات التغرير التي تتضمن الحصول على أرقام البطاقة واستغلالها في عمليات الشراء، فضلاً عن إمكانية تحويل الأموال من حساب المودع الأصلي إلى حساب الجاني أو ذويه.

إن قلة الخبرة التي يعاني منها بعض مستخدمي الشبكة تجعلهم صيداً سهلاً للجناة من خلال منحهم الفرصة للاستيلاء على البيانات المهمة بسهولة، ويرجع ذلك إلى عدة عوامل من أهمها العشوائية في استقبال البريد الإلكتروني الذي قد يتضمن فيروسات تسيطر على الحاسب الآلي للمجني عليه وتمكن المخترقين من الدخول وقتما شاءوا، فضلاً عن الانخداع بالتخفيضات الوهمية من قبل الجناة الذين يستخدمون هذه التخفيضات كوسيلة لإغراء المجني عليهم لطلب الشراء، ومن ثم معرفة بياناتهم، أو تتبع الـ IP الخاص بهم واختراق مواقعهم والاستيلاء على أموالهم.

ولما كانت المنظمات تمتلك إمكانات مالية أكثر بكثير من الأفراد، لذلك يوجه المخترقون نشاطاتهم إلى تلك المنظمات بهدف الحصول على صيد ثمين من خلال تحويل المبالغ المالية الضخمة من حسابات تلك المنظمات إلى حساباتهم الخاصة، أو إصدار أوامر شراء لمقتنيات وأغراض خاصة بهم والتسديد من حسابات تلك المنظمات، حيث تتعرض المنظمات للاختراق والتعدي لارتكاب التزوير أكثر من الأفراد، وكذلك الحال بالنسبة للمنظمات الأمنية والخدمية التي يزداد الوضع فيها خطورة نتيجة إمكانية الاطلاع على

أسرار أمنية، أو القيام بعمليات تزوير في سجلات الحاسب الآلي لتغيير مهنة أو تغيير وثائق رسمية كبطاقات الأحوال وجوازات السفر واستخدامها، مما يترتب عليه وقوع جريمة التزوير الإلكتروني بالتزوير في سجلات الحاسب الآلي، والتزوير التقليدي نتيجة التوقيع على مستندات بها بيانات وهمية غير صحيحة لاستخراج تلك المحررات، وبصفة عامة تعد المؤسسات المالية أكثر تعرضاً للاختراق والتعدي وارتكاب عمليات التزوير من المنظمات الأخرى، لأن الهدف الرئيس من الاختراق والتعدي وارتكاب التزوير هو الحصول على المال سواء من أرصدة المؤسسة المالية أو من حسابات عملائها بتحويل الأرصدة أو استغلال أرقام بطاقات الائتمان في عمليات شراء، بالإضافة إلى معرفة أسرار المؤسسة المالية وتعريض سمعتها للخطر بإفشاء أسرار عملائها، ولذلك فبالرغم من قيام المؤسسات المالية بتحمل الخسائر وتعويض عملائها المتضررين من جرائم التزوير الإلكتروني، إلا أنها تضطر أحياناً إلى الاستجابة لطلبات المبتزين خوفاً من تعرضها لطلب تعويضات من قبل العملاء نتيجة إفشاء أسرارهم وعدم الحفاظ عليها، فالتعرض للابتزاز من قبل المواقع المشبوهة من الجرائم الأخرى التي يرتكبها بعض المخترقين ويستغلونها في ابتزاز المؤسسات المالية وغير المالية. ويشير العريان (٢٠٠٤م، ص٦٦) إلى استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية على (٢٢) شريطاً تحوي معلومات تخص عملاء الشركة، وهدد ببيعها للشركات المنافسة إذا لم يحصل على فدية مقدارها ٢٠٠,٠٠٠ دولار، واضطرت الشركة لدفع المبلغ لاسترداد الشرائط المغنطة المسروقة، لأن الخسائر المترتبة على إفشائها تفوق بكثير المبلغ المطلوب.

كما أن من أهم سمات المجني عليه التي يترتب عليها تعرضه لعمليات التزوير بعد الاختراق والتعدي على بياناته وجهازه تنقله بين صفحات

الإنترنت دون هدف واضح، ودخوله على المواقع المشبوهة، والتي تدعو أحياناً الزائرين إلى أن يكونوا من أعضائها، وتطلب منهم ملء بيانات العضوية، ومن ثم تستغل تلك البيانات في عمليات الاختراق والتعدي وارتكاب جريمة التزوير، أو تقوم بابتزازه بتهديده بنشر ما يسيء إليه إذا لم يدفع المبالغ المالية المطلوبة، ولكي لا يتعرض للحرج عند استخدام اسمه في تلك المواقع المشبوهة.

وبهذا يتحقق الهدف الخامس من أهداف الدراسة وهو معرفة سمات المجني عليه في جرائم التزوير الإلكتروني.

٤ . ٧ فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

للإجابة عن السؤال السادس من أسئلة الدراسة وهو : ما فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٧) استجابات جميع مفردات الدراسة لتحديد فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني.

الجدول رقم (١٧) فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
١	الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات.	ت	١٣٧	٩٥	٨	١	-	٤,٥٣	٠,٥٩	٢٢١,٤	٠,٠**	الأول
		٪	٥٦,٨	٣٩,٤	٣,٣	٠,٤	-					
٢	الاستفادة من علم الحاسب الجنائي في إثبات جريمة التزوير الإلكتروني.	ت	١٣٢	١٠٢	٧	-	-	٤,٥٢	٠,٥٦	١٠٦,٠	٠,٠**	الثاني
		٪	٥٤,٨	٤٢,٣	٢,٩	-	-					
٤	الإسراع في إجراء المعاينة للأجهزة المشتبه في ارتكابها جرائم التعدي والاختراق.	ت	١٣٣	١٠٠	٨	-	-	٤,٥٢	٠,٥٦	١٠٤,٥	٠,٠**	الثالث
		٪	٥٥,٢	٤١,٥	٣,٣	-	-					
٣	الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي.	ت	١٢٩	١٠٨	٤	-	-	٤,٥٢	٠,٥٣	١١١,٥	٠,٠**	الرابع
		٪	٥٣,٥	٤٤,٨	١,٧	-	-					

تابع ... الجدول رقم (١٧) فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

١٣	تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة.	ت	١٠٩	١٢٠	١٢	–	–	٤,٤٠	٠,٥٨	٨٧,٩	٠,٠**	الثامن
		٪	٤٥,٢	٤٩,٨	٥,٠	–	–					
١٠	التحفظ على الأجهزة المشتبه بها وملحقاتها.	ت	١١٣	١١٤	١٠	١	٣	٤,٣٨	٠,٧٠	٢٩٥,٩	٠,٠**	التاسع
		٪	٤٦,٩	٤٧,٣	٤,١	٠,٤	١,٢					
١٢	أخذ إفادات المتواجدين في المكان.	ت	١٠١	١٣٠	٩	١	–	٤,٣٧	٠,٥٨	٢١٠,٢	٠,٠**	العاشر
		٪	٤١,٩	٥٣,٩	٣,٧	٠,٤	–					
٨	تمكين خبراء الحاسب الآلي من توجيه الأسئلة الفرعية اللازمة لإثبات التهمة.	ت	١٠٣	١٢٥	٩	٣	١	٤,٣٥	٠,٦٦	٣٠٥,٢	٠,٠**	الحادي عشر
		٪	٤٢,٧	٥١,٩	٣,٧	١,٢	٠,٤					
٦	إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين.	ت	١٠١	١٢٥	١٣	٢	–	٤,٣٥	٠,٦٢	١٩٠,٥	٠,٠**	الثاني عشر
		٪	٤١,٩	٥١,٩	٥,٤	٠,٨	–					

تابع ... الجدول رقم (١٧) فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

٧	طلب خبراء الحاسب الآلي حضور التحقيق إذا تطلب ذلك.	ت	٩٧	١٢١	٢٢	١	–	٤,٣٠	٠,٦٥	١٦٦,٢	٠,٠**	الثالث عشر
		٪	٤٠,٢	٥٠,٢	٩,١	٠,٤	–					
١١	وقف خدمة الاتصال بالحاسب من خلال خادمات الملفات حتى لا تتسبب الاتصالات بإتلاف الأدلة.	ت	١٠٠	١١٧	٢١	١	٢	٤,٢٩	٠,٧١	١٥٩,٤	٠,٠**	الرابع عشر
		٪	٤١,٥	٤٨,٥	٨,٧	٠,٤	٠,٨					
٩	ترتيب استجواب المتهمين حسب توجيهات خبراء الحاسب الآلي.	ت	٩١	١٢٤	٢١	٥	–	٤,٢٥	٠,٦٩	١٥٩,٤	٠,٠**	الخامس عشر
		٪	٣٧,٨	٥١,٥	٨,٧	٢,١	–					
متوسط استجابات مفردات الدراسة على محور فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني							٤,٤١	٠,٣٥				

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٧) أن المتوسط الحسابي العام لمحور فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني قد بلغ (٤١ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى أن الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني فعالة جداً.

كما كشف الجدول أن جميع الأساليب وتمثل (٠ , ١٠٠ ٪) من الأساليب التي تضمنها محور فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢٥ , ٤ـ ٥٣ , ٤)، مما يشير إلى شدة فاعليتها، فهي من الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني ، وهي على النحو التالي :

١ ـ الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات، وجاء هذا الأسلوب في المركز الأول لترتيب الأهمية النسبية بمتوسط (٥٣ , ٤)، حيث وافق على فاعليته (٢ , ٩٦ ٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

٢ ـ الاستفادة من علم الحاسب الجنائي في إثبات جريمة التزوير الإلكتروني، وجاء هذا الأسلوب في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٥٢ , ٤)، حيث وافق على فاعليته (١ , ٩٧٪).

٣ ـ الإسراع في إجراء المعاينة للأجهزة المشتبه في ارتكابها جرائم التعدي

والاختراق، وجاء هذا الأسلوب في المركز الثالث لترتيب الأهمية النسبية بمتوسط (٥٢ , ٤)، حيث وافق على فاعليته (٧ , ٩٦٪).

٤ ـ الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي، وجاء هذا الأسلوب في المركز الرابع لترتيب الأهمية النسبية بمتوسط (٥٢ , ٤)، حيث وافق على فاعليته (٣ , ٩٨ ٪).

٥ ـ تحديد دور كل فرد أثناء مداهمة المكان المشتبه بوجود الأجهزة به، وجاء هذا الأسلوب في المركز الخامس لترتيب الأهمية النسبية بمتوسط (٤٨ , ٤)، حيث وافق على فاعليته (٥ , ٩٧٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

٦ ـ إجراء التحريات اللازمة عن موقع الأجهزة المشتبه بها، وجاء هذا الأسلوب في المركز السادس لترتيب الأهمية النسبية بمتوسط (٤٨ , ٤)، حيث وافق على فاعليته (٩ , ٩٧ ٪).

٧ ـ التحفظ على تقنيات الاتصال المرتبطة بالحاسب الآلي، وجاء هذا الأسلوب في المركز السابع لترتيب الأهمية النسبية بمتوسط (٤١ , ٤)، حيث وافق على فاعليته (٣ , ٩٦ ٪) مقابل (٨ , ٠ ٪) اعترضوا على فاعليته.

٨ ـ تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة، وجاء هذا الأسلوب في المركز الثامن لترتيب الأهمية النسبية بمتوسط (٤٠ , ٤)، حيث وافق على فاعليته (٠ , ٩٥ ٪).

٩ ـ التحفظ على الأجهزة المشتبه بها وملحقاتها، وجاء هذا الأسلوب في المركز التاسع لترتيب الأهمية النسبية بمتوسط (٣٨ , ٤)، حيث وافق على فاعليته (٢ , ٩٤٪) مقابل (٦ , ١٪) اعترضوا على فاعليته.

١٠ ـ أخذ إفادات المتواجدين في المكان، وجاء هذا الأسلوب في المركز العاشر لترتيب الأهمية النسبية بمتوسط (٣٧, ٤)، حيث وافق على فاعليته (٨, ٩٥ ٪) مقابل (٤, ٠ ٪) اعترضوا على فاعليته.

١١ ـ تمكين خبراء الحاسب الآلي من توجيه الأسئلة الفرعية اللازمة لإثبات التهمة، وجاء هذا الأسلوب في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (٣٥, ٤)، حيث وافق على فاعليته (٦, ٩٤ ٪) مقابل (٦, ١ ٪) اعترضوا على فاعليته.

١٢ ـ إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين، وجاء هذا الأسلوب في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (٣٥, ٤)، حيث وافق على فاعليته (٨, ٩٣ ٪) مقابل (٨, ٠ ٪) اعترضوا على فاعليته.

١٣ ـ طلب خبراء الحاسب الآلي حضور التحقيق إذا تطلب ذلك، وجاء هذا الأسلوب في المركز الثالث عشر لترتيب الأهمية النسبية بمتوسط (٣٠, ٤)، حيث وافق على فاعليته (٤, ٩٠ ٪) مقابل (٤, ٠ ٪) اعترضوا على فاعليته.

١٤ ـ وقف خدمة الاتصال بالحاسب من خلال خادمات الملفات حتى لا تسبب الاتصالات إتلاف الأدلة، وجاء هذا الأسلوب في المركز الرابع عشر لترتيب الأهمية النسبية بمتوسط (٢٩, ٤)، حيث وافق على فاعليته (٠, ٩٠ ٪) مقابل (٢, ١٪) اعترضوا على فاعليته.

١٥ ـ ترتيب استجواب المتهمين حسب توجيهات خبراء الحاسب الآلي، وجاء هذا الأسلوب في المركز الخامس عشر لترتيب الأهمية

النسبية بمتوسط (٢٥ , ٤)، حيث وافــق على فاعليته (٣ , ٨٩ ٪) مقابل (١ , ٢ ٪) اعترضوا على فاعليته.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ يتبـع المحقـق الجنائي أسـاليب فعالة جداً في إثبـات جرائم التزوير الإلكتروني.

٢ ـ إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني هي:

أ ـ الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات.

ب ـ الاسـتفادة من علم الحاسـب الجنائي في إثبات جريمة التزوير الإلكتروني.

جـ ـ الإسراع في إجـراء المعاينة للأجهزة المشـتبه في ارتكابها جرائم التعدي والاختراق.

د ـ الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي.

هـ ـ تحديد دور كل فرد أثناء مداهمة المكان المشـتبه بوجود الأجهزة به.

و ـ إجراء التحريات اللازمة عن موقع الأجهزة المشتبه بها.

ز ـ التحفظ على تقنيات الاتصال المرتبطة بالحاسب الآلي.

ح ـ تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة.

ط ـ التحفظ على الأجهزة المشتبه بها وملحقاتها.

ي ـ أخذ إفادات المتواجدين في المكان.

ك ـ تمكين خبراء الحاسب الآلي من توجيه الأسئلة الفرعية اللازمة لإثبات التهمة.

ل ـ إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين.

م ـ طلب خبراء الحاسب الآلي حضور التحقيق إذا تطلب ذلك.

ن ـ وقف خدمة الاتصال بالحاسب من خلال خادمات الملفات حتى لا تسبب الاتصالات إتلاف الأدلة.

س ـ ترتيب استجواب المتهمين حسب توجيهات خبراء الحاسب الآلي.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة رستم (١٩٩٤م) في أن إجراء التحريات اللازمة عن موقع الأجهزة المشتبه بها وتحديد دور كل فرد أثناء مداهمة المكان المشتبه بوجود الأجهزة به من أهم الأساليب التي يتبعها المحقق الجنائي في إثبات الجرائم الإلكترونية، كما تتفق جزئياً مع ما توصلت إليه دراسة (Erdonmez, 2002) في أن التحفظ على الأجهزة المشتبه بها وملحقاتها من الأساليب الفعالة لإثبات الجرائم الإلكترونية، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة (Thompson, 1991) في أن إيقاف الاتصال بالحاسب الآلي لضمان عدم إتلاف الأدلة المادية بالاتصال الخارجي وإعداد الأسئلة بالاتفاق مع خبراء الحاسب الجنائي قبل توجيهها للمتهمين من الأساليب الفعالة لإثبات الجريمة الإلكترونية، كما تتفق مع ما توصلت إليه دراسة (Kelly, 1995) في أن أخذ إفادات المتواجدين في المكان وطلب حضور خبراء الحاسب الآلي التحقيق من الأساليب الفعالة لإثبات الجريمة الإلكترونية.

ويمكـن تفسـير النتائـج التـي توصلـت إليها الدراسـة في مجـال فاعلية الأسـاليب التي يتبعها المحقق الجنائي في إثبات جرائـم التزوير الإلكتروني، بأن هناك عدة أساليب فعالة جداً يأتي في مقدمتها الاستعانة بخبراء الحاسب الآلي في فهم المصطلحـــات في ضوء صعوبة المصطلحات وعدم إلمام غالبية المحققين الجنائيين بها، والاستفادة من علم الحاسب الجنائي في إثبات جريمة التزويـر الإلكتروني، حيث يسـاعد هـذا العمل على التقـاط الدليل الرقمي، ونسـبة الجريمة إلى موقع معين، بمعنى تحديد الجهاز المسـتخدم في الاختراق والتعدي والتزوير، وهذا يستدعي الإسراع في إجراء المعاينة للأجهزة المشتبه بها بعد الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي لكي يتمكن المحقق من إثبات حالة الأجهزة، وقطع اتصالها بالشـبكات الخارجية أو الداخلية لكي لا يتم إتلاف الأدلة المادية أو الأدلة الرقمية من خلال الجناة، وهـذا أيضاً يتطلب إجراء التحريات اللازمة عن موقع الأجهزة المشـتبه بها، وتحديـد دور كل فرد أثناء مداهمة المكان المشـتبه بوجود الأجهزة به، بجانب التحفظ على تقنيات الاتصال المرتبطة بالحاسب الآلي والتحفظ على الأجهزة المشـتبه بها وملحقاتها كأدلة مادية تثبت القيام بعمليات الاختراق والتعدي. ويشـير كامل (١٩٩٩م، ص٣١٤) إلى ضرورة اتباع القواعد الفنية للمعاينة مـن خلال الإسراع في إجـراء المعاينة والتحفظ على الموجـودات التي يمكن أن تسـتخدم كأدلـة مادية. أما العريـان (٢٠٠٤م، ص١٣٥) فيؤكد ضرورة التحفـظ عـلى الأجهـزة المشـتبه بها، وكذلـك تقنيـات الاتصـال المرتبطة بها التي يشـك المحقق في اسـتخدامها في عمليات الاخـتراق والتعدي والتزوير الإلكتروني، لكي لا يقوم الجاني بتدميرها أو إتلافها، مع ضرورة تحريز جميع المضبوطات بعد إجراء الفحص عليها وتدوين ذلك في محضر الضبط،وتحريز مـا يجب تحريزه من الأجهزة والتقنيات، والبدء بفحص الأجهزة التي يمكن

حفظها في المكان أو نقلها إلى مكان الفحص بعد تحريزها، بينما يشير الحبشي (١٩٩٠م، ص١٢) إلى ضرورة الاستعانة بخبراء الحاسب الآلي لتأمين الحاسب الآلي والحفاظ على الأدلة الموجودة به من التلف أو تعطيلها من قبل مرتكب الجرائم التزوير الإلكتروني.

ولضمان فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني يجب تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة، لتحديد المشتبه بهم وحصرهم في أضيق نطاق ممكن، مع أخذ إفادات المتواجدين في المكان، وتمكين خبراء الحاسب الآلي من توجيه الأسئلة اللازمة لإثبات التهمة، وهذا يستدعي إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين، ومن ثم طلب خبراء الحاسب الآلي لحضور التحقيق إذا تطلب الأمر ذلك لأنه أقدر على تحديد وسائل ارتكاب الجريمة الإلكترونية وخطوات ارتكابها، وكذلك تمنحهم خبراتهم في استخدام الحاسب الآلي تحديد الخطوات الإجرائية لعملية الاختراق والتعدي والتزوير، مما يمكنهم من ترتيب استجواب المتهمين بما يضمن عدم التضارب في الأقوال، وسرعة تحديد مرتكب جريمة التزوير الإلكتروني. ويشير البشرى (٢٠٠٠م، ص ص٣٦٦-٣٦٧) إلى ضرورة ترتيب استجواب المتهمين حسب طبيعة جريمة التزوير المرتكبة، وحسب مرئيات خبير الحاسب الآلي الذي يجب أن يشارك في وضع الأسئلة مع المحقق، وترتيبها وفقاً للخطوات الإجرائية، وكذلك ترتيب المتهمين إذا كان هناك أكثر من متهم حسب توجيهات خبير الحاسب الآلي ، وبهذا يتحقق الهدف السادس من أهداف الدراسة وهو معرفة فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني.

٤ . ٨ فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني

للإجابة عن السؤال السابع من أسئلة الدراسة وهو: ما فاعلية الأساليب التـي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني ؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد فاعلية الأساليب التـي يتبعهـا المحقـق الفنـي في إثبات جرائـم التزوير الإلكـتروني من خلال المتوسط الحسـابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسـط الحسابي وحسـب أقل قيم للتشـتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضـح الجـدول رقـم (١٨) اسـتجابات جميـع مفـردات الدراسـة لتحديد فاعلية الأسـاليب التي يتبعهـا المحقق الفني في إثبات جرائم التزوير الإلكتروني.

الجدول رقم (١٨) فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
٤	الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية التزوير من الموظفين في الإدارات الإلكترونية التابعة لها.	ت	١٣٩	٩٧	٥	-	-	٤,٦٥	٠,٥٤	١١٦,٩	٠,٠**	الأول
		٪	٥٧,٧	٤٠,٢	٢,١	-	-					
١	عمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي.	ت	١٣٢	١٠٥	٤	-	-	٤,٥٣	٠,٥٣	١١٣,٣	٠,٠**	الثاني
		٪	٥٤,٨	٤٣,٦	١,٧	-	-					
١١	توثيق البيانات التي استخدمت في جرائم تزوير المحررات الإلكترونية.	ت	١٢٢	١١٠	٧	٢	-	٤,٤٦	٠,٥٩	٢٠٧,٧	٠,٠**	الثالث
		٪	٥٠,٦	٤٥,٦	٢,٩	٠,٨	-					
٢	استخدام تقنيات التتبع للعثور على البريد الإلكتروني للمخترق.	ت	١١٧	١١٦	٨	-	-	٤,٤٥	٠,٥٦	٩٧,٧	٠,٠**	الرابع
		٪	٤٨,٥	٤٨,١	٣,٣	-	-					

تابع .... الجدول رقم (١٨) فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني

٥	استخدام تقنيات استرجاع المعلومات لاسترجاع الملفات والبيانات المحذوفة التي استخدمت في الاختراق والتعدي.	ت	١١٣	١٢١	٦	١	-	٤,٤٤	٠,٥٧	٢١٤,٦	٠,٠**	الخامس
		٪	٤٦,٩	٥٠,٢	٢,٥	٠,٤	-					
١٥	استخدام برامج إزالة الإخفاء لتحديد عناصر الدليل الرقمي المخبأة.	ت	١١٢	١١٧	٩	٢	١	٤,٤٠	٠,٦٥	٣٠٥,٠	٠,٠**	السادس
		٪	٤٦,٥	٤٨,٥	٣,٧	٠,٨	٠,٤					
٦	استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة.	ت	١١١	١١٥	١٥	-	-	٤,٤٠	٠,٦١	٧٩,٨	٠,٠**	السابع
		٪	٤٦,١	٤٧,٧	٦,٢	-	-					
٣	الاستعانة بتقنيات تتبع الذبذبات لتحديد موقع الجهاز الذي استخدام في الاختراق والتعدي.	ت	١١٧	١٠١	٢٢	١	-	٤,٣٩	٠,٦٧	١٦٣,٦	٠,٠**	الثامن
		٪	٤٨,٥	٤١,٩	٩,١	٠,٤	-					
٩	استخدام برامج البحث عن المفردات النصية للعثور على المحرر المعلوماتي المزور.	ت	٨٩	١٣٤	١٧	١	-	٤,٢٩	٠,٦١	١٩٣,٣	٠,٠**	التاسع
		٪	٣٦,٩	٥٥,٦	٧,١	٠,٤	-					
١٢	نسخ الدليل الرقمي.	ت	٩٤	١١٩	٢٦	٢	-	٤,٢٧	٠,٦٨	١٥١,٩	٠,٠**	العاشر
		٪	٣٩,٠	٤٩,٤	١٠,٨	٠,٨	-					

تابع .... الجدول رقم (١٨) فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني

١٣	تحليل الدليل الرقمي.	ت	٨٩	١٢٨	٢١	٣	–	٤,٢٦	٠,٦٧	١٦٩,٩	٠,٠**	الحادي عشر
		٪	٣٦,٩	٥٣,١	٨,٧	١,٢	–					
١٤	عرض الدليل الرقمي.	ت	٩٣	١٢١	٢٤	٣	–	٤,٢٦	٠,٦٩	١٥٥,٣	٠,٠**	الثاني عشر
		٪	٣٨,٦	٥٠,٢	١٠,٠	١,٢	–					
١٠	استخدام مضادات الفيروسات لاكتشاف الفيروسات المستخدمة في الاختراق والتعدي.	ت	٨٨	١٣٣	١٦	٢	٢	٤,٢٦	٠,٦٩	٢٩٢,١	٠,٠**	الثالث عشر
		٪	٣٦,٥	٥٥,٢	٦,٦	٠,٨	٠,٨					
٧	استخدام أقراص فك كلمة المرور للدخول على المواقع المحجوبة.	ت	٩٤	١٠٧	٣٦	٤	–	٤,٢١	٠,٧٥	١١٧,٥	٠,٠**	الرابع عشر
		٪	٣٩,٠	٤٤,٤	١٤,٩	١,٧	–					
٨	استخدام برامج الاستنساخ الجنائي للأقراص الضوئية.	ت	٨٢	١٢٢	٣٤	٣	–	٤,١٧	٠,٧١	١٣٦,٩	٠,٠**	الخامس عشر
		٪	٣٤,٠	٥٠,٦	١٤,١	١,٢	–					
متوسط استجابات مفردات الدراسة على محور فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني								٤,٣٦	٠,٤١			

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٨) أن المتوسط الحسابي العام لمحور فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني قد بلغ (٣٦ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى أن الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني فعالة جداً.

كما كشف الجدول أن هناك أربعة عشر أسلوباً تمثل (٣ , ٩٣ ٪) من الأساليب التي تضمنها محور فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢١ , ٤ـ٥٦ , ٤)، مما يشير إلى شدة فاعليتها، فهي من الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني، وهي على النحو التالي :

١ـ الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية التزوير من الموظفين في الإدارات الإلكترونية التابعة لها، وجاء هذا الأسلوب في المركز الأول لترتيب الأهمية النسبية بمتوسط (٦٥ , ٤)، حيث وافق على فاعليته (٩ , ٩٧ ٪).

٢ ـ عمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي، وجاء هذا الأسلوب في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٥٣ , ٤)، حيث وافق على فاعليته (٤ , ٩٨ ٪).

٣ـ توثيق البيانات التي استخدمت في جرائم تزوير المحررات الإلكترونية، وجاء هذا الأسلوب في المركز الثالث لترتيب الأهمية

النسبية بمتوسط (٤٦ , ٤)، حيث وافق على فاعليته (٢ , ٩٦٪) مقابل (٨ , ٠ ٪) اعترضوا على فاعليته.

٤ ـ استخدام تقنيات التتبع للعثور على البريد الإلكتروني للمخترق، وجاء هذا الأسلوب في المركز الرابع لترتيب الأهمية النسبية بمتوسط (٤٥ , ٤)، حيث وافق على فاعليته (١ , ٩٧٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

٥ ـ استخدام تقنيات استرجاع المعلومات لاسترجاع الملفات والبيانات المحذوفة التي استخدمت في الاختراق والتعدي، وجاء هذا الأسلوب في المركز الخامس لترتيب الأهمية النسبية بمتوسط (٤٤ , ٤)، حيث وافق على فاعليته (١ , ٩٧ ٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

٦ ـ استخدام برامج إزالة الإخفاء لتحديد عناصر الدليل الرقمي المخبأة، وجاء هذا الأسلوب في المركز السادس لترتيب الأهمية النسبية بمتوسط (٤٠ , ٤)، حيث وافق على فاعليته (٠ , ٩٥ ٪) مقابل (٢ , ١ ٪) اعترضوا على فاعليته.

٧ ـ استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة، وجاء هذا الأسلوب في المركز السابع لترتيب الأهمية النسبية بمتوسط (٤٠ , ٤)، حيث وافق على فاعليته (٨ , ٩٣ ٪).

٨ ـ الاستعانة بتقنيات تتبع الذبذبات لتحديد موقع الجهاز الذي استخدام في الاختراق والتعدي، وجاء هذا الأسلوب في المركز الثامن لترتيب الأهمية النسبية بمتوسط (٣٩ , ٤)، حيث وافق على فاعليته (٤ , ٩٠ ٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

٩ ـ استخدام برامج البحث عن المفردات النصية للعثور على المحرر المعلوماتي المزور، وجاء هذا الأسلوب في المركز التاسع لترتيب الأهمية النسبية بمتوسط (٢٩ , ٤)، حيث وافق على فاعليته (٥ , ٩٢ ٪) مقابل (٤ , ٠ ٪) اعترضوا على فاعليته.

١٠ ـ نسخ الدليل الرقمي، وجاء هذا الأسلوب في المركز العاشر لترتيب الأهمية النسبية بمتوسط (٢٧ , ٤)، حيث وافق على فاعليته (٤ , ٨٨ ٪) مقابل (٨ , ٠ ٪) اعترضوا على فاعليته.

١١ ـ تحليل الدليل الرقمي، وجاء هذا الأسلوب في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (٢٦ , ٤)، حيث وافق على فاعليته (٠ , ٩٠ ٪) مقابل (٢ , ١ ٪) اعترضوا على فاعليته.

١٢ ـ عرض الدليل الرقمي، وجاء هذا الأسلوب في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (٢٦ , ٤)، حيث وافق على فاعليته (٨ , ٨٨ ٪) مقابل (٢ , ١ ٪) اعترضوا على فاعليته.

١٣ ـ استخدام مضادات الفيروسات لاكتشاف الفيروسات المستخدمة في الاختراق والتعدي، وجاء هذا الأسلوب في المركز الثالث عشر لترتيب الأهمية النسبية بمتوسط (٢٦ , ٤)، حيث وافق على فاعليته (٧ , ٩١ ٪) مقابل (٦ , ١ ٪) اعترضوا على فاعليته.

١٤ ـ استخدام أقراص فك كلمة المرور للدخول على المواقع المحجوبة، وجاء هذا الأسلوب في المركز الرابع عشر لترتيب الأهمية النسبية بمتوسط (٢١ , ٤)، حيث وافق على فاعليته (٤ , ٨٣ ٪) مقابل (٧ , ١ ٪) اعترضوا على فاعليته.

وتبين من الجدول أن هناك أسلوباً وحيداً يمثل (٧ , ٦ ٪) من الأساليب التي تضمنها محور فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم

التزوير الإلكتروني قد بلغ متوسطه الحسابي (١٧ , ٤)، مما يشير إلى فاعليته، فهو من الأساليب الفعالة في إثبات جرائم التزوير الإلكتروني، وهو على النحو التالي :

استخدام برامج الاستنساخ الجنائي للأقراص الضوئية، وجاء هذا الأسلوب في المركز الخامس عشر لترتيب الأهمية النسبية، حيث وافق على فاعليته (٦ , ٨٤ ٪) مقابل (٢ , ١٪) اعترضوا على فاعليته.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ يتبع المحقق الفني أساليب فعالة جداً في إثبات جرائم التزوير الإلكتروني.

٢ ـ إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني هي:

أ ـ الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية التزوير من الموظفين في الإدارات الإلكترونية التابعة لها.

ب ـ عمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي.

جـ ـ توثيق البيانات التي استخدمت في جرائم تزوير المحررات الإلكترونية.

د ـ استخدام تقنيات التتبع للعثور على البريد الإلكتروني للمخترق.

هـ ـ استخدام تقنيات استرجاع المعلومات لاسترجاع الملفات والبيانات المحذوفة التي استخدمت في الاختراق والتعدي.

و ـ استخدام برامج إزالة الإخفاء لتحديد عناصر الدليل الرقمي المخبأة.

ز ـ استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة.

ح ـ الاستعانة بتقنيات تتبع الذبذبات لتحديد موقع الجهاز الذي استخدام في الاختراق والتعدي.

ط ـ استخدام برامج البحث عن المفردات النصية للعثور على المحرر المعلوماتي المزور.

ي ـ نسخ الدليل الرقمي.

ك ـ تحليل الدليل الرقمي.

ل ـ عرض الدليل الرقمي.

م ـ استخدام أقراص فك كلمة المرور للدخول على المواقع المحجوبة.

٣ ـ إن الأسلوب الفعال في إثبات جرائم التزوير الإلكتروني هو: استخدام برامج الاستنساخ الجنائي للأقراص الضوئية.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة رستم (١٩٩٤م) في أن توثيق البيانات التي استخدمت في جرائم التزوير من أهم الأساليب التي يتبعها المحقق الفني في إثبات الجرائم الإلكترونية، كما تتفق جزئياً مع ما توصلت إليه دراسة (Erdonmez, 2002) في أن عمل نسخة كاملة من البيانات الموجودة على الحاسب الذي تعرض للاختراق والتعدي من الأساليب الفعالة لإثبات الجرائم الإلكترونية، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة (Thompson, 1991) في أن استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة من الأساليب الفعالة لإثبات الجريمة الإلكترونية، كما تتفق مع ما توصلت إليه دراسة (Kelly, 1995) في استخدام مضادات الفيروسات لاكتشاف الفيروسات المستخدمة في الاختراق والتعدي من الأساليب الفعالة لإثبات الجريمة الإلكترونية.

ويمكـن تفسـير النتائـج التـي توصلـت إليها الدراسـة في مجـال فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، بأن هناك عدة أسـاليب فعالة جـداً يأتي في مقدمتها الاسـتعانة بمركز المعلومات لمعرفـة المسـتخدم الـذي قـام بعمليـة التزويـر مـن الموظفـين في الإدارات الإلكترونية التابعة لها، لأن النظام في المملكة يمنح كل مفوض بالدخول على النظـام رقماً سرياً خاصاً به لا يسـتخدمه غيره، ولذلـك فعند إجراء أي تغيير يتم الرجوع لمركز المعلومات لتحديد من قام بإجراء التغيير ويظهر ذلك على البرنـت الخاص بالجهاز، حيث يحدد وقت التغيير وزمنه والموظف الذي قام بإجرائه حسب رقمه السري الذي دخل به على النظام.

كـما أن عمـل نسـخة كاملة مـن البيانـات الموجودة على الحاسـب الآلي الـذي تعـرض للاخـتراق والتعـدي يقـي مـن إمكانية إتـلاف البيانـات أو محوهـا، وتحتفظ داخلهـا بالـ (IP) الخـاص بالمخترق الـذي يمكن الحصول عليه باسـتخدام تقنيات التتبع وتقنيات اسـترجاع المعلومـات، حيث يؤدي في النهاية إلى معرفة البريد الإلكتروني الخاص بالمخترق، بالإضافة إلى معرفة نوعيـة الملفـات والبيانات التي اسـتخدمت في الاخـتراق والتعدي، ولذلك يجـب أيضـاً توثيـق البيانات التـي اسـتخدمت في جرائـم تزويـر المحررات الإلكترونية، لإمكانية استخدامها كدليل عند الحاجة.

ومن الأسـاليب الفعالـة جداً التي يسـتخدمها المحقق الفنـي في إثبات جرائـم التزويـر الإلكتروني اسـتخدام برامج إزالة الإخفـاء لتحديد عناصر الدليـل الرقمـي المخبأة، فهـذه البرامج لها قـدرة على إزالة العنـاصر المخفاة وتحديدهـا، ومـن ثـمَّ تحديـد عنـاصر الدليـل الرقمـي التي اسـتخدمت في الاختراق والتعدي والتزوير، وأيضاً يسـهم اسـتخدام برامج فك التشفير في اكتشاف الأدلة المشفرة التي يستعين بها المخترق في القيام بعمليات الاختراق

والتعـدي لتحديـد هـذه الأدلة ومن ثـمَّ الاسـتعانة بتقنيات تتبـع الذبذبات لتحديـد موقـع الجهـاز الـذي اسـتخدم في الاخـتراق والتعـدي، بجانـب اسـتخدام برامج البحث عن المفردات النصية للعثـور على المحرر المعلوماتي المزور، ومن ثمَّ تحديد أسـاليب الدخول إليه ووسـائل تزويره وتتبع الـ (IP) الخاص بالمخترقين، فضلاً عن استخدام برامج فك التشفير لاكتشاف الأدلة المشـفرة. ويشـير حجازي (٢٠٠٥م، ص٦٣) إلى أن من أهم الوسائل الفنية لإثبات جرائم التزوير الإلكترونية البحث عن عنوان الـ (IP) للجهاز مصدر الجريمـة، ومن ثم العثور عليـه وتحديد موقع الجهاز وتاريـخ الاختراق، أما عبد المطلب (٢٠٠١م، ص٢١٩) فيرى أن أهم الوسائل الفنية هي استخدام البروكسي الذي يحتفظ بالعمليات التي تمت عليه، مما يمكن من اسـتخدامها كدليـل إثبات قـوي، خاصـةً وأن المعلومـات لا توجد لدى المسـتخدم، بل توجد لدى مقدم الخدمة.

ويسـهم نسـخ وتحليل وعرض الدليل الرقمي في إثبـات وقوع جريمة التزويـر الإلكتروني بقـوة، فالدليل الرقمي هو دليـل الإدانة لمرتكب جريمة التزوير الإلكتروني، سواء بتحديد الأدوات والبرامج المستخدمة في الاختراق والتعدي والتزوير، أو تحديد الفيروسات والطرق التي استخدمت في ذلك، وتسـهم أيضاً مضادات الفيروسـات في اكتشـاف الفيروسـات المسـتخدمة في الاخـتراق والتعـدي، وكذلـك الحال بالنسـبة لأقراص فـك كلمة المرور للدخـول عـلى المواقع المحجوبـة. وتشـير (Arabiat, 2002, p.12) إلى أهمية برامج التتبع واسترجاع المعلومات في نسخ وتحليل وعرض الدليل الرقمي، أمـا العنـزي (٢٠٠٣م، ص١٠٢) فيشـير إلى أهميـة أدوات فحـص ومراقبة الشبكة والأدوات المساعدة بالتحقيق حيث تستطيع الدخول على الشبكات، وتلمس برامج السرقة والتلصص، وكذلك الفيروسـات التي استخدمت في عمليات الاختراق والتعدي والتزوير، وتحديد مصدرها بدقة.

أما استخدام برامج الاستنساخ الجنائي للأقراص الضوئية فتستخدم كدليل مادي، من خلال البحث في محتوى هذه الأقراص عن برامج التعدي والاختراق أو الفيروسات التي تساعد على ذلك، فوجود هذه البرامج أو الفيروسات يشير إلى استخدامها في الاختراق والتعدي والتزوير المعلوماتي.

وبهذا يتحقق الهدف السابع من أهداف الدراسة وهو معرفة فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني.

٤ . ٩ المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني

للإجابة عن السؤال الثامن من أسئلة الدراسة وهو : ما المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني ؟ قام الباحث بتحليل استجابات مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية، وتناول التحليل تحديد المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني من خلال المتوسط الحسابي والانحراف المعياري وبترتيب تلك العبارات حسب أعلى قيم للمتوسط الحسابي وحسب أقل قيم للتشتت والذي يمثله الانحراف المعياري عند تساوي قيم المتوسط الحسابي.

ويوضح الجدول رقم (١٩) استجابات جميع مفردات الدراسة لتحديد المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

الجدول رقم (١٩) المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني

رقم	العبارة		الاستجابة					المتوسط الحسابي	الانحراف المعياري	قيمة مربع كاي	مستوى الدلالة	الترتيب
			موافق بشدة	موافق	محايد	غير موافق	غير موافق مطلقاً					
١٥	ندرة البرامج التدريبية اللازمة لتأهيل المحققين لإثبات جرائم التزوير الإلكتروني.	ت	١٦٤	٧٦	١	–	–	٤,٦٨	٠,٤٨	١٦٥,٧	٠,٠**	الأول
		٪	٦٨,٠	٣١,٥	٠,٤	–	–					
١١	قلة إلمام بعض المحققين بالبرامج الخاصة بالتعدي والاختراق والتزوير.	ت	١٤٣	٩١	٧	–	–	٤,٥٦	٠,٥٥	١١٧,٢	٠,٠**	الثاني
		٪	٥٩,٣	٣٧,٨	٢,٩	–	–					
١٠	قلة إلمام المحققين بمجال الحاسب الجنائي في إثبات الجريمة.	ت	١٥٠	٧٩	١٠	٢	–	٤,٥٦	٠,٦٢	٢٣٧,٨	٠,٠**	الثالث
		٪	٦٢,٢	٣٢,٨	٤,١	٠,٨	–					
٥	قلة الإمكانات الفنية اللازمة لإثبات جرائم التزوير المعلوماتي.	ت	١٣٠	١٠٦	٤	١	–	٤,٥١	٠,٥٦	٢٢٦,٣	٠,٠**	الرابع
		٪	٥٣,٩	٤٤,٠	١,٧	٠,٤	–					
٩	قلة خبرات السلطات المسؤولة عن ضبط وإثبات جرائم التزوير الإلكتروني والتحقيق فيها.	ت	١٣٧	٩٠	٩	٥	–	٤,٤٩	٠,٦٧	٢٠٦,٧	٠,٠**	الخامس
		٪	٥٦,٨	٣٧,٣	٣,٧	٢,١	–					

تابع ... الجدول رقم (١٩) المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني

١٣	قصور التعاون الدولي في مجال مكافحة جرائم التزوير المعلوماتي.	ت	١٢١	١٠٧	١١	٢	–	٤,٤٤	٠,٦٢	١٩٤,١	٠,٠**	السادس
		٪	٥٠,٢	٤٤,٤	٤,٦	٠,٨	–					
١٤	ثقة الجهات القضائية في الدليل الإلكتروني قاصرة نظراً لإمكانية تزويره.	ت	١٠٦	١١٩	١٥	١	–	٤,٣٧	٠,٦٢	١٨٤,٣	٠,٠**	السابع
		٪	٤٤,٠	٤٩,٤	٦,٢	٠,٤	–					
١٢	تكتم الجهات المجني عليها عن البلاغ خوفاً من فقدان الثقة بتعاملاتها (المنظمات المالية).	ت	١١٢	١١٠	١٦	٢	١	٤,٣٧	٠,٦٨	٢٧٥,٧	٠,٠**	الثامن
		٪	٤٦,٥	٤٥,٦	٦,٦	٠,٨	٠,٤					
٤	محاكاة المحرر الإلكتروني المزور للأصل تماماً، فلا يوجد به شطب أو كشط يدل على تزويره ترتكب بسببه جرائم أخرى.	ت	٩٨	١٣٣	٩	١	–	٤,٣٦	٠,٥٨	٢١٣,٤	٠,٠**	التاسع
		٪	٤٠,٧	٥٥,٢	٣,٧	٠,٤	–					
٨	إمكانية ارتكابها من مسافات بعيدة تتعدى إقليم الدولة (غير قارية).	ت	١١٣	١٠٦	١٨	٤	–	٤,٣٦	٠,٦٩	١٦٣,١	٠,٠**	العاشر
		٪	٤٦,٩	٤٤,٠	٧,٥	١,٧	–					
٧	إمكانية التخلص من الأجهزة المستخدمة في التزوير الإلكتروني بحرقها أو تدميرها.	ت	١١٢	١٠٩	١٦	٣	١	٤,٣٦	٠,٧	٢٧١,٣	٠,٠**	الحادي عشر
		٪	٤٦,٥	٤٥,٢	٦,٦	١,٢	٠,٤					

تابع ... الجدول رقم (١٩) المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني

١	عدم كفاية الأدلة للإدانة في جرائم التزوير المعلوماتي.	ت	٩٤	١٣٤	١٢	١	–	٤,٣٣	٠,٥٩	٢٠٦,١	٠,٠**	الثاني عشر
		٪	٣٩,٠	٥٥,٦	٥,٠	٠,٤	–					
٦	إمكانية تزوير الأدلة الإلكترونية لإلحاق التهمة بشخص آخر بريء.	ت	٩٨	١٠٥	٣٢	٦	–	٤,٢٢	٠,٧٧	١١٨,٩	٠,٠**	الثالث عشر
		٪	٤٠,٧	٤٣,٦	١٣,٣	٢,٥	–					
٣	عدم تخلف الآثار المادية الملموسة كما في حالة الجرائم التقليدية.	ت	٨٦	١٢٨	١٩	٨	–	٤,٢١	٠,٧٣	١٦٠,٧	٠,٠**	الرابع عشر
		٪	٣٥,٧	٥٣,١	٧,٩	٣,٣	–					
٢	سهولة التخلص من الأدلة الإلكترونية بمحوها.	ت	٨٤	١٢١	٢٨	٧	١	٤,١٦	٠,٧٧	٢٢٦,٤	٠,٠**	الخامس عشر
		٪	٣٤,٩	٥٠,٢	١١,٦	٢,٩	٠,٤					
متوسط استجابات مفردات الدراسة على محور المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني								٤,٤٠	٠,٣٧			

** دالة إحصائياً عند مستوى معنوية (٠,٠١) أو أقل.

يوضح اختبار كا٢ عدم التطابق في استجابات أفراد مجتمع الدراسة في جميع الفقرات والعبارات الخاصة بالمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني وذلك عند مستوى دلالة (٠١ , ٠) فأقل.

ويتضح من الجدول رقم (١٩) أن المتوسط الحسابي العام لمحور المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني قد بلغ (١٦ , ٤) من خمس نقاط، مما يشير في ضوء متوسط الوزن النسبي الفارق (٢١ , ٤) إلى وجود معوقات مهمة جداً تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية جداً.

كما كشف الجدول أن هناك أربعة عشر معوقاً تمثل (٣ , ٩٣ ٪) من المعوقات التي تضمنها محور المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني قد تراوحت متوسطاتها الحسابية ما بين (٢١ , ٤ـ ٦٨ , ٤)، مما يشير إلى شدة أهميتها، فهي من المعوقات المهمة جداً التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية جداً، وهي على النحو التالي :

١ـ ندرة البرامج التدريبية اللازمة لتأهيل المحققين لإثبات جرائم التزوير الإلكتروني، وجاء هذا المعوق في المركز الأول لترتيب الأهمية النسبية بمتوسط (٦٨ , ٤)، حيث وافق على وجوده(٥ , ٩٩ ٪).

٢ ـ قلة إلمام بعض المحققين بالبرامج الخاصة بالتعدي والاختراق والتزوير، وجاء هذا المعوق في المركز الثاني لترتيب الأهمية النسبية بمتوسط (٥٦ , ٤)، حيث وافق على وجوده (١ , ٩٧ ٪).

٣ ـ قلة إلمام المحققين بمجال الحاسب الجنائي في إثبات الجريمة، وجاء هذا المعوق في المركز الثالث لترتيب الأهمية النسبية بمتوسط (٥٦ , ٤)، حيث وافق على وجوده (٠ , ٩٥ ٪) مقابل (٨ , ٠ ٪) اعترضوا على وجوده.

٤ ـ قلة الإمكانات الفنية اللازمة لإثبات جرائم التزوير المعلوماتي، وجاء هذا المعوق في المركز الرابع لترتيب الأهمية النسبية بمتوسط (٥١ , ٤)، حيث وافق على وجوده (٩ , ٩٧ ٪) مقابل (٤ , ٠ ٪) اعترضوا على وجوده.

٥ ـ قلة خبرات السلطات المسؤولة عن ضبط وإثبات جرائم التزوير الإلكتروني والتحقيق فيها، وجاء هذا المعوق في المركز الخامس لترتيب الأهمية النسبية بمتوسط (٤٩ , ٤)، حيث وافق على وجوده (١ , ٩٤ ٪) مقابل (١ , ٢ ٪) اعترضوا على وجوده.

٦ ـ قصور التعاون الدولي في مجال مكافحة جرائم التزوير المعلوماتي، وجاء هذا المعوق في المركز السادس لترتيب الأهمية النسبية بمتوسط (٤٤ , ٤)، حيث وافق على وجوده (٦ , ٩٤ ٪) مقابل (٨ , ٠ ٪) اعترضوا على وجوده.

٧ ـ ثقة الجهات القضائية في الدليل الإلكتروني قاصرة نظراً لإمكانية تزويره، وجاء هذا المعوق في المركز السابع لترتيب الأهمية النسبية بمتوسط (٣٧ , ٤)، حيث وافق على وجوده (٤ , ٩٣ ٪) مقابل (٤ , ٠ ٪) اعترضوا على وجوده.

٨ ـ تكتم الجهات المجني عليها عن البلاغ خوفاً من فقدان الثقة بتعاملاتها (المنظمات المالية، وجاء هذا المعوق في المركز الثامن لترتيب الأهمية

النسبية بمتوسط (٣٧, ٤)، حيث وافق على وجوده (١, ٩٢ ٪) مقابل (٢, ١ ٪) اعترضوا على وجوده.

٩ ـ محاكاة المحرر الإلكتروني المزور للأصل تماماً، فلا يوجد به شطب أو كشط يدل على تزويره ترتكب بسببه جرائم أخرى، وجاء هذا المعوق في المركز التاسع لترتيب الأهمية النسبية بمتوسط (٣٦, ٤)، حيث وافق على وجوده (٩, ٩٥ ٪) مقابل (٤, ٠ ٪) اعترضوا على وجوده.

١٠ ـ إمكانية ارتكابها من مسافات بعيدة تتعدى إقليم الدولة (غير قارية، وجاء هذا المعوق في المركز العاشر لترتيب الأهمية النسبية بمتوسط (٣٦, ٤)، حيث وافق على وجوده (٩, ٩٠ ٪) مقابل (٧, ١ ٪) اعترضوا على وجوده.

١١ ـ إمكانية التخلص من الأجهزة المستخدمة في التزوير الإلكتروني بحرقها أو تدميرها، وجاء هذا المعوق في المركز الحادي عشر لترتيب الأهمية النسبية بمتوسط (٣٦, ٤)، حيث وافق على وجوده (٧, ٩١ ٪) مقابل (٦, ١ ٪) اعترضوا على وجوده.

١٢ ـ عدم كفاية الأدلة للإدانة في جرائم التزوير المعلوماتي، وجاء هذا المعوق في المركز الثاني عشر لترتيب الأهمية النسبية بمتوسط (٣٣, ٤)، حيث وافق على وجوده (٦, ٩٤ ٪) مقابل (٤, ٠ ٪) اعترضوا على وجوده.

١٣ ـ إمكانية تزوير الأدلة الإلكترونية لإلحاق التهمة بشخص آخر بريء، وجاء هذا المعوق في المركز الثالث عشر لترتيب الأهمية النسبية بمتوسط (٢٢, ٤)، حيث وافق على وجوده (٣, ٨٤ ٪) مقابل (٥, ٢ ٪) اعترضوا على وجوده.

١٤ ـ عـدم تخلف الآثار المادية الملموسـة كما في حالـة الجرائم التقليدية، وجـاء هـذا المعوق في المركـز الرابع عـشر لترتيب الأهمية النسـبية بمتوسـط (٢١ , ٤)، حيث وافـــق على وجوده (٨ , ٨٨٪) مقابل (٣ , ٣ ٪) اعترضوا على وجوده.

وتبـين من الجدول أن هناك معوقاً وحيداً يمثل (٧ , ٦ ٪) من المعوقات التي تضمنها محور المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة مـن المحقـق الجنائـي والفنـي في إثبات جرائـم التزويـر الإلكـتروني قد بلغ متوسـطه الحسـابي (١٦ , ٤)، مما يشـير إلى أهميتـه، فهو من المعوقـات المهمة التي تؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقق الجنائي والفني في إثبـات جرائم التزوير الإلكـتروني بدرجة قوية، وهو عـلى النحـو التالي : سهولة التخلص من الأدلة الإلكترونية بمحوها، وجاء هذا المعوق في المركز الخامس عشر لترتيب الأهمية النسـبية، حيث وافـق على وجوده (١ , ٨٥ ٪) مقابل (٣ , ٣ ٪) اعترضوا على وجوده.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ توجد معوقات مهمة جداً تؤدي إلى عدم فاعلية الأساليب المستخدمة مـن المحقق الجنائـي والفني في إثبـات جرائم التزويـر الإلكتروني بدرجة قوية جداً.

٢ ـ إن المعوقـات المهمـة جـداً التـي تـؤدي إلى عـدم فاعلية الأسـاليب المسـتخدمة من المحقـق الجنائي والفنـي في إثبات جرائـم التزوير الإلكتروني بدرجة قوية جداً هي :

أ ـ نـدرة البرامـج التدريبية اللازمة لتأهيل المحققـين لإثبات جرائم التزوير الإلكتروني.

ب ـ قلـة إلمام بعض المحققين بالبرامج الخاصة بالتعدي والاختراق والتزوير.

جـ ـ قلة إلمام المحققين بمجال الحاسب الجنائي في إثبات الجريمة.

د ـ قلة الإمكانات الفنية اللازمة لإثبات جرائم التزوير المعلوماتي.

هـ ـ قلـة خبرات السـلطات المسـؤولة عن ضبـط وإثبـات جرائم التزوير الإلكتروني والتحقيق فيها.

و ـ قصور التعاون الدولي في مجال مكافحة جرائم التزوير المعلوماتي.

ز ـ ثقة الجهات القضائية في الدليل الإلكتروني قاصرة نظراً لإمكانية تزويره.

ح ـ تكتـم الجهـات المجني عليها عـن البلاغ خوفاً مـن فقدان الثقة بتعاملاتها (المنظمات المالية).

ط ـ محـاكاة المحـرر الإلكـتروني المـزور للأصل تماماً، فـلا يوجد به شطب أو كشط يدل على تزويره ترتكب بسببه جرائم أخرى.

ي ـ إمكانية ارتكابها من مسـافات بعيـدة تتعدى إقليم الدولة (غير قارية).

ك ـ إمكانية التخلص من الأجهزة المستخدمة في التزوير الإلكتروني بحرقها أو تدميرها.

ل ـ عدم كفاية الأدلة للإدانة في جرائم التزوير المعلوماتي.

م ـ إمكانية التخلص من الأجهزة المسـتخدمة في التزوير الإلكتروني بحرقها أو تدميرها.

ن ـ عدم تخلف الآثار المادية الملموسة كما في حالة الجرائم التقليدية.

٣ ـ إن المعوق المهم الذي يؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية هو : سهولة التخلص من الأدلة الإلكترونية بمحوها.

وتتفق هذه النتائج جزئياً مع ما توصلت إليه دراسة (Wahbler, 1998) في أن من أهم المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جريمة التزوير الإلكتروني صعوبة إثبات جرائم الحاسب الآلي، كما تتفق جزئياً مع ما توصلت إليه دراسة (Smith, 2001) في أن هذه الجرائم عابرة للقارات ويمكن ارتكابها من مسافات بعيدة تجلب صعوبة في تحديد مرتكبها في ظل الاختلافات القانونية والسياسية والمذهبية، وأيضاً تتفق جزئياً مع ما توصلت إليه دراسة رستم (١٩٩٤م) ودراسة بحر (١٩٩٩م) في أن أهم المعوقات التي تواجه المحققين في جرائم المعلوماتية هي نقص الخبرة والتدريب اللازمين لمواجهة تلك الجرائم ، كما تتفق مع ما توصلت إليه دراسة الشهري (٢٠٠٢م) ودراسة حجازي (٢٠٠٢م) ودراسة (Goodman, 1997) في أن أهم معوقات إثبات جريمة التزوير الإلكتروني هي نقص الخبرة والمعرفة بالحاسب الآلي، ونقص مهارات التعامل مع الإنترنت، وعدم كفاية التدريب، بالإضافة إلى عدم إبلاغ الجهات المجني عليها عن الجريمة.

ويمكن تفسير النتائج التي توصلت إليها الدراسة في مجال المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، بأن هناك عدة معوقات قوية جداً يأتي في مقدمتها ندرة البرامج التدريبية اللازمة لتأهيل المحققين لإثبات جرائم التزوير الإلكتروني، وقلة إلمام بعض المحققين بالبرامج الخاصة

بالتعـدي والاختراق والتزوير، وقلة إلمام المحققين بمجال الحاسـب الجنائي في إثبـات الجريمـة في ضـوء حداثـة تخصـص مجال الحاسـب الجنائـي، وقلة خبرات السـلطات المسـؤولة عن ضبـط وإثبات جرائم التزويـر الإلكتروني والتحقيق فيها، والحاجة الماسـة لتدريب العاملـين في أجهزة العدالة الجنائية على إتقان التحقيق فيها، لتزويدهم بالقدرة والخبرة العملية اللازمة للتحقيق واسـتخدام المصطلحـات العلمية وتوجيه الأسـئلة وبنائها وفـق طبيعة هذه الجرائم التقنية المسـتحدثة. ويشـير البشرى (٢٠٠٠م، ص ص٣٦١ـ٣٦٤) إلى أن ندرة البرامج التدريبية وقلة إلمام المحققين بالبرامج الخاصة بالاختراق والتزويـر وكذلـك قلة إلمامهـم بمجال الحاسـب الجنائي في إثبـات الجريمة مـن أهم المعوقـات التي تحول دون إثبـات الجريمة الإلكترونيـة بصفة عامة وجريمة التزوير الإلكتروني بصفة خاصة.

كما أن هناك معوقـات قوية جداً من أهمها قلة الإمكانات الفنية اللازمة لإثبـات جرائـم التزويـر الإلكتروني، حيث يحتاج اكتشـاف جريمـة التزوير الإلكتروني تقنيات تتبع وتقنيات اسـترجاع المعلومات وغيرها من التقنيات التـي تهـدف إلى تتبـع مصـدر الاخـتراق والتعدي، ويحتـاج اسـتخدام هذه التقنيات بدقة ومثابرة إلى خبرة فنية متقدمة. ويشير(Tillers, 1999, p. 117) إلى حاجة إثبات جرائم التزوير إلى مسـتويات تقنية من خلال حصر الحقائق والاحتمالات والأسـباب والفرضيات واسـتنتاج النتائج في ضوء معاملات حسـابية وتقنيـات تتبع بهدف تحديد مصـدر الاختراق، مما يعـد بمثابة دليل رقمي يمكن دعمه بالدليل المكتشف في حاسب المشتبه به باستخدام تقنيات اسـترجاع المعلومات والعمليات، فقد أثبتت تقنية الحاسبات الآلية نجاحها الفعال في جمع الأدلة الجنائية وصناعة البينة وتحليل القرائن واستنتاج الحقائق.

ومـن أهم المعوقات التي تواجه إثبات الجرائـم الإلكترونية بصفة عامة وجرائم التزوير الإلكتروني بصفة خاصة عدم ثقة الجهات القضائية في الدليل الإلكـتروني لإمكانيـة تزويـره في ضـوء تعدد المسـتخدمين وانتشـار تقنيات الاخـتراق والتعـدي، فعـدم قناعة الجهـات القضائيـة بالدليـل الإلكتروني تحـول دون التعويـل عليـه كدليل إدانة في ضـوء منح بعض القوانين المشـتبه بهـم أو المتهمـين حـق الصمت وعـدم الحديث عما يترتـب عليـه إدانتهم أو إدانـة أقاربهم، بالإضافة إلى إمكانيـة تزوير الدليل الإلكتروني لإلحاق التهمة بشخص بريء، في ضوء صعوبة التوصل للآثار المادية الملموسة كما في الجرائم التقليديـة، وسـهولة التخلـص من الإدلـة الإلكترونيـة بمحوهـا، وكذلك إمكانيـة التخلص من الأجهزة المسـتخدمة في التزوير الإلكتروني بحرقها أو تدميرها في ضوء المكاسـب التي يحصل عليها الفرد التي تتعدى سـعر الجهاز الـذي تم منـه الاختراق والتعدي، مما يترتب عليه عـدم كفاية الأدلة اللازمة للإثبات، كما أن مبررات الإدانة قد لا تشير بالضرورة إلى الفاعل الأصلي إذا كان هناك تعدد للمسـتخدمين لجهاز الحاسـب الآلي، ولكنها تحصر الاشتباه في أقل عدد ممكن من الأفراد الذين استخدموا الجهاز في ذلك اليوم، ومن ثم التحقيق معهم جميعاً للتعرف على الفاعل الأصلي.

ويسـهم تكتـم الجهات المجني عليها عـن البلاغ خوفاً مـن فقدان الثقة بتعاملاتهـا في صعوبة إثبات جرائـم التزوير الإلكتروني، حيث تفضل بعض الجهـات الصمت ودفع تعويضـات لعملائها المتضررين مـن قبل الاختراق والتعـدي والتزوير الإلكتروني خوفاً من فقدان الثقة من قبل عملائها؛ ولأن الخسـائر التـي تتعرض لهـا في حالة فقـدان الثقة تفوق بكثـير قيمة التعويض المالي للضحايا، ويكثر ذلك في المؤسسات المالية والبنوك التي تقوم بتعويض ضحاياهـا من العمـلاء بدفع النقـود أو القيمة التي تم الاسـتيلاء عليها من

حسـاباتهم. ويشـير الهيتي (٢٠٠٥م، ص٢١٨) إلى أن تكتم الجهات المجني عليها من أهم المعوقات التي تحول دون إثبات الجريمة الإلكترونية.

إن طبيعـة الجريمة الإلكترونية العابـرة للقارات تجعلها ذات طابع دولي يحتـم التعاون مـن قبل المجتمع الـدولي لمواجهة هذه الجرائـم؛ ولكن يترتب عـلى قصور التعاون الدولي في مواجهة هذه الجرائم ضعف القدرة على إثباتها في ضوء الاختلافات القانونية والسياسية والمذهبية بين الدول، وعدم وجود نـص قانوني يلزمها بالتعاون لمواجهة جرائـم المعلوماتية بصفة عامة وجرائم التزوير الإلكتروني بصفة خاصة.

كـما أن محـاكاة المحـرر الإلكتروني المـزور للأصل تماماً، سـواء بنسـخه وإخراجـه بأدوات الإخراج كالطابع أو الماسـح الضوئـي، وعدم وجود أي شطب أو كشط يدل على تزويره يسهم في ارتكاب جرائم أخرى أو الاستفادة من المحرر الإلكتروني المزور في اسـتخراج أوراق ثبوتية ومسـتندات أخرى مـزورة لاحتوائهـا على معلومـات غير صحيحة، كما هو الحال في اسـتخراج بطاقـة أحـوال سـعودية مـزورة يترتب عليهـا اسـتخراج جواز سـفر مزور ورخصة قيادة مزورة واستخدامها، مما يترتب عليه وقوع التزوير الإلكتروني والتقليـدي، فالتزوير الإلكـتروني يقع بمجرد إدخـال المعلومات المزورة إلى سـجلات الحاسـب الآلي دون توافر المسـوغ النظامي لها، (كاستخراج بطاقة أحوال سـعودية لأجنبي دون حصول على الجنسـية، أو تغيير مهنة سـعودي من عسـكري إلى متسبب لاسـتخراج جواز سـفر يمكنه من السفر للخارج دون الحصـول عـلى إذن من مرجعـه، أو إضافة زوجة إلى إقامـة زوجها على أنهـا قادمـة للإقامة مـع زوجها، بالرغم مـن قدومها لأداء فريضـة العمرة). أمـا التزوير التقليدي فيقع نتيجة التوقيع على الأوراق والمسـتندات والنماذج الخاصة باستخراج الأوراق الثبوتية المزورة مع العلم بعدم صحتها.

وبهذا يتحقق الهدف الثامن من أهداف الدراسة وهو معرفة المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني.

١٠.٤ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية

للإجابة عن السؤال التاسع من تساؤلات الدراسة وهو : هل هناك فروق ذات دلالة إحصائية في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية ؟

قام الباحث بتحليل مفردات الدراسة من منسوبي الجهات المختصة بمكافحة التزوير في المملكة العربية السعودية لتحديد الدلالة الإحصائية للفروق في رؤيتهم نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيرات : العمر، والمؤهل التعليمي، وجهة العمل، ومنطقة العمل، والرتبة العسكرية، وطبيعة العمل، وعدد سنوات الخبرة في مجال العمل، وعدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية، وذلك من خلال حساب اختبار (T-test)، وتحليل التباين الأحادي (ANOVA).

١ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل:

أ ـ اختلاف رؤية المبحوثين نحو خصائص جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٠) نتائج اختبار (T_Test) لدلالة الفروق في رؤية المبحوثين لخصائص جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٠) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لخصائص جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
خصائص جريمة التزوير الإلكتروني	محقق جنائي	١٢٩	٤,٢٤	٠,٣٤	١,١٢٧	٢٣٩	٠,٢٦١
	محقق فني	١١٢	٤,١٩	٠,٣٣			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (١,١٢٧) وهي غير دالة إحصائياً عند مستوى دلالة (٠,٢٦١) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو خصائص جريمة التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لخصائص جريمة التزوير الإلكتروني، فهم جميعاً يدركون خصائص جريمة التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد خصائص

جريمـة التزوير الإلكـتروني، فالخصائص معروفة للجميـع بغض النظر عن طبيعة عملهم.

ب ـ اختـلاف رؤية المبحوثين نحو الوسـائل المسـتخدمة في ارتكاب جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل :

يوضـح الجـدول رقم (٢١) نتائـج اختبار (t_test) لدلالـة الفروق في رؤية المبحوثين للوسـائل المسـتخدمة في ارتكاب جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢١) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين للوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
وسائل ارتكاب جريمة التزوير الإلكتروني	محقق جنائي	١٢٩	٢,٩٠	٠,٤٤	٠,٧٣٣	٢٣٩	٠,٤٦٤
	محقق فني	١١٢	٣,٨٦	٠,٣٩			

توضـح البيانـات مـن جـدول اختبـار (T_Test) أن قيمة (T) تسـاوي (٠,٧٣٣) وهـى غـير دالة إحصائياً عند مسـتوى دلالـة (٠,٤٦٤) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسـة من أصحاب طبيعة العمل المختلفة (محقـق جنائـي ـ محقـق فني) نحو الوسـائل المسـتخدمة في ارتـكاب جريمة التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم للوسائل المستخدمة في

ارتكاب جريمة التزوير الإلكتروني، فهم جميعاً يدركون الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، فالوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

جـ ـ اختلاف رؤية المبحوثين نحو صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٢) نتائج اختبار (T_Test) لدلالة الفروق في رؤية المبحوثين لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية باختلاف متغير طبيعة العمل.

الجدول رقم (٢٢) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
صور جريمة التزوير الإلكتروني	محقق جنائي	١٢٩	٤,٣١	٠,٤٤	٢,١٠٤	٢٣٩	٠,٠٣٦*
	محقق فني	١١٢	٤,١٩	٠,٤٢			

* دال عند مستوى دلالة (٠,٠٥) فأقل.

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (٢,١٠٤) وهي دالة إحصائياً عند مستوى دلالة (٠,٠٣٦) بمعنى أن

هنـاك تبايناً في آراء مفردات الدراسـة مـن أصحاب طبيعة العمـل المختلفة (محقـق جنائي ـ محقق فني) نحو صـور جريمة التزوير الإلكتروني في الدوائر الحكوميـة الإلكترونية، أي أنه توجد فروق في رؤيتهم لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وكان اتجاه الفروق بالمتوسطات لصالـح المحققـين الجنائيـين الذين بلغ متوسـطهم (٣١ , ٤)، أمـا المحققون الفنيون فجاءت متوسـطاتهم أقل وتسـاوي (١٩ , ٤) ، مما يعني أن المحققين الجنائيـين أكثر إدراكاً لصور جريمـة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وقد يعزى هذا إلى أن المحققين الجنائيين يهتمون بصور وأشكال جريمـة التزويـر سـواء كانت تغيـير بيانات في سـجلات الحاسـب الآلي، أو سرقـة منظومـة التوقيـع الإلكـتروني، أو تغيـير مهنـة واسـتخدامها إصدار وثائـق ثبوتيـة مزورة، فهم أكثـر إلماماً بتصنيفات جرائـم التزوير الإلكتروني وتكييفهـا القانـوني، بخلاف المحققـين الفنيين الذين يركـزون على الجوانب الفنيـة لارتكاب ووقوع جريمـة التزوير الإلكترونية، وكيفيـة التقاط الأدلة الإلكترونية اللازمة لإثباتها بالطرق والتقنيات الفنية.

د ـ اختلاف رؤية المبحوثين نحو سـمات المجرم الإلكتروني في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٣) نتائج اختبار (test_t) لدلالة الفروق في رؤية المبحوثين لسـمات المجرم الإلكتروني في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٣) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
سمات المجرم الإلكتروني في جرائم التزوير	محقق جنائي	١٢٩	٤,١٠	٠,٤١	-٠,٠٩	٢٣٩	٠,٩٢٩
	محقق فني	١١٢	٤,١١	٠,٣٦			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (-٠,٠٩) وهي غير دالة إحصائياً عند مستوى دلالة (٠,٩٢٩) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي - محقق فني) نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، فهم جميعاً يدركون سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، فسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

هـ ـ اختلاف رؤية المبحوثين نحو سمات المجني عليه في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل :

يوضح الجدول رقم (٢٤) نتائج اختبار (t_test) لدلالة الفروق في رؤية المبحوثين لسمات المجني عليه في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٤) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لسمات المجني عليه في جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
سمات المجني عليه في جرائم التزوير الإلكتروني	محقق جنائي	١٢٩	٤,٠٧	٠,٤٢	٠,٤٧٥	٢٣٩	٠,٦٣٥
	محقق فني	١١٢	٤,٠٤	٠,٤٢			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (٠,٤٧٥) وهي غير دالة إحصائياً عند مستوى دلالة (٠,٦٣٥) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو سمات المجني عليه في جرائم التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لسمات المجني عليه في جرائم التزوير الإلكتروني، فهم جميعاً يدركون سمات المجني عليه في جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد سمات المجني عليه في جرائم التزوير الإلكتروني،

فسمات المجني عليه في جرائم التزوير الإلكتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

و ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٥) نتائج اختبار (t_test) لدلالة الفروق في رؤية المبحوثين لفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٥) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
فاعلية أساليب الإثبات التي يتبعها المحقق الجنائي	محقق جنائي	١٢٩	٤,٤٢	٠,٣٩	٠,٦٥١	٢٣٩	٠,٥١٥
	محقق فني	١١٢	٤,٣٩	٠,٣٠			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (٠,٦٥١) وهى غير دالة إحصائياً عند مستوى دلالة (٠,٥١٥) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، فهم جميعاً يدركون فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ففاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

ز ـ اختلاف رؤية المبحوثين نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

للإجابة عن التساؤل: هل توجد فروق في فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل ؟ استخدم الباحث اختبار (t_test)، ويوضح الجدول رقم (٢٦) نتائج اختبار (t_test) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٦) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	رقم	العبارة	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)	الترتيب
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	١	الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات.	محقق جنائي	١٢٩	٤,٤٨	٠,٦١	-١,٣٢	٢٣٩	٠,١٩	الأول
			محقق فني	١١٢	٤,٥٨	٠,٥٥				
	٢	الاستفادة من علم الحاسب الجنائي في إثبات جريمة التزوير الإلكتروني.	محقق جنائي	١٢٩	٤,٥٢	٠,٥٣	٠,٢١	٢٣٩	٠,٩٨	الثاني
			محقق فني	١١٢	٤,٥٢	٠,٥٩				
	٤	الإسراع في إجراء المعاينة للأجهزة المشتبه في ارتكابها جرائم التعدي والاختراق.	محقق جنائي	١٢٩	٤,٥٧	٠,٥٧	١,٣٩	٢٣٩	٠,١٦	الثالث
			محقق فني	١١٢	٤,٤٦	٠,٥٥				
	٣	الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي.	محقق جنائي	١٢٩	٤,٥٠	٠,٥٥	-٠,٧٠	٢٣٩	٠,٤٨	الرابع
			محقق فني	١١٢	٤,٥٤	٠,٥٢				
	١٥	تحديد دور كل فرد أثناء مداهمة المكان المشتبه بوجود الأجهزة به.	محقق جنائي	١٢٩	٤,٤٩	٠,٥٩	٠,٢١	٢٣٩	٠,٨٤	الخامس
			محقق فني	١١٢	٤,٤٧	٠,٥٤				
	٥	إجراء التحريات اللازمة عن موقع الأجهزة المشتبه بها.	محقق جنائي	١٢٩	٤,٤٧	٠,٥٣	-٠,٢٦	٢٣٩	٠,٧٩	السادس
			محقق فني	١١٢	٤,٤٩	٠,٥٥				
	١٤	التحفظ على تقنيات الاتصال المرتبطة بالحاسب الآلي.	محقق جنائي	١٢٩	٤,٤٦	٠,٦٦	١,٢٧	٢٣٩	٠,٢١	السابع
			محقق فني	١١٢	٤,٣٦	٠,٥٥				
	١٣	تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة.	محقق جنائي	١٢٩	٤,٤٠	٠,٦١	-٠,٢٠	٢٣٩	٠,٨٤	الثامن
			محقق فني	١١٢	٤,٤١	٠,٥٦				
	١٠	التحفظ على الأجهزة المشتبه بها وملحقاتها.	محقق جنائي	١٢٩	٤,٣٨	٠,٧٩	-٠,٠٥	٢٣٩	٠,٩٦	التاسع
			محقق فني	١١٢	٤,٣٨	٠,٥٩				
	١٢	أخذ إفادات المتواجدين في المكان.	محقق جنائي	١٢٩	٤,٣٧	٠,٦٠	-٠,٠٤	٢٣٩	٠,٩٧	العاشر
			محقق فني	١١٢	٤,٣٨	٠,٥٥				

تابع ... الجدول رقم (٢٦) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	رقم	العبارة	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)	الترتيب
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	٨	تمكين خبراء الحاسب الآلي من توجيه الأسئلة الفرعية اللازمة لإثبات التهمة.	محقق جنائي	١٢٩	٤,٤٢	٠,٦٩	١,٦٩	٢٣٩	٠,٠٩١	الحادي عشر
			محقق فني	١١٢	٤,٢٨	٠,٦٠				
	٦	إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين.	محقق جنائي	١٢٩	٤,٣٦	٠,٦٥	٠,٢٢	٢٣٩	٠,٨٣	الثاني عشر
			محقق فني	١١٢	٤,٣٤	٠,٥٩				
	٧	طلب خبراء الحاسب الآلي حضور التحقيق إذا تطلب ذلك.	محقق جنائي	١٢٩	٤,٣٥	٠,٦٧	١,١٨	٢٣٩	٠,٢٤	الثالث عشر
			محقق فني	١١٢	٤,٢٥	٠,٦٢				
	١١	وقف خدمة الاتصال بالحاسب من خلال خادمات الملفات حتى لا تسبب الاتصالات بإتلاف الأدلة.	محقق جنائي	١٢٩	٤,٣٣	٠,٧٧	٠,٩٠	٢٣٩	٠,٣٧	الرابع عشر
			محقق فني	١١٢	٤,٢٥	٠,٦٤				
	٩	ترتيب استجواب المتهمين حسب توجيهات خبراء الحاسب الآلي.	محقق جنائي	١٢٩	٤,٢٨	٠,٧٥	٠,٧٢	٢٣٩	٠,٤٧	الخامس عشر
			محقق فني	١١٢	٤,٢١	٠,٦٤				

توضح البيانات من جدول اختبار (T_Test) أن قيم (T) لجميع العبارات غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جريمة التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، فهم جميعاً يدركون فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، فضلاً عن طبيعة عملهم التي تحتم تبادل الآراء والخبرات ومن ثمَّ اكتساب القدرة على تحديد فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، فهي معروفة للجميع بغض النظر عن طبيعة عملهم.

ح ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٧) نتائج اختبار (t_test) لدلالة الفروق في رؤية المبحوثين لفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٧) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
فاعلية أساليب الإثبات التي يتبعها المحقق الفني	محقق جنائي	١٢٩	٤,٣٥	٠,٤٤	٠,٢٥ –	٢٣٩	٠,٨١
	محقق فني	١١٢	٤,٣٦	٠,٣٨			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (ـ ٠,٢٥) وهي غير دالة إحصائياً عند مستوى دلالة (٠,٨١) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، فهم جميعاً يدركون فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، ففاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

ط ـ اختلاف رؤية المبحوثين نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

للإجابة عن التساؤل : هل توجد فروق في فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل ؟ استخدم الباحث اختبار (T_Test)، ويوضح الجدول رقم (٢٨) نتائج اختبار (T_Test) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٨) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	رقم	العبارة	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (tailed-٢)	الترتيب
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	٤	الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية التزوير من الموظفين في الإدارات الإلكترونية التابعة لها.	محقق جنائي	١٢٩	٤,٥٧	٠,٥٤	٠,٥٥	٢٣٩	٠,٥٩	الأول
			محقق فني	١١٢	٤,٥٤	٠,٥٣				
	١	عمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي.	محقق جنائي	١٢٩	٤,٤٨	٠,٥٣	-١,٥٩	٢٣٩	٠,١١	الثاني
			محقق فني	١١٢	٤,٥٩	٠,٥٢				
	١١	توثيق البيانات التي استخدمت في جرائم تزوير المحررات الإلكترونية.	محقق جنائي	١٢٩	٤,٤٠	٠,٦٣	-١,٨٣	٢٣٩	٠,٠٦٩	الثالث
			محقق فني	١١٢	٤,٥٤	٠,٥٥				
	٢	استخدام تقنيات التتبع للعثور على البريد الإلكتروني للمخترق.	محقق جنائي	١٢٩	٤,٤٧	٠,٥٦	٠,٣٨	٢٣٩	٠,٧٠	الرابع
			محقق فني	١١٢	٤,٤٤	٠,٥٧				
	٥	استخدام تقنيات استرجاع المعلومات لاسترجاع الملفات والبيانات المحذوفة التي استخدمت في الاختراق والتعدي.	محقق جنائي	١٢٩	٤,٤٣	٠,٥٦	-٠,٢٧	٢٣٩	٠,٧٩	الخامس
			محقق فني	١١٢	٤,٤٥	٠,٥٨				
	١٥	استخدام برامج إزالة الإخفاء لتحديد عناصر الدليل الرقمي المخبأة.	محقق جنائي	١٢٩	٤,٤٣	٠,٦٨	٠,٧٢	٢٣٩	٠,٤٧	السادس
			محقق فني	١١٢	٤,٣٧	٠,٦٠				

تابع... الجدول رقم (٢٨) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	رقم	العبارة	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2_tailed)	الترتيب
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	٦	استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة.	محقق جنائي	١٢٩	٤,٤٠	٠,٥٩	٠,١٣	٢٣٩	٠,٨٩	السابع
			محقق فني	١١٢	٤,٣٩	٠,٦٢				
	٣	الاستعانة بتقنيات تتبع الذبذبات لتحديد موقع الجهاز الذي استخدام في الاختراق والتعدي.	محقق جنائي	١٢٩	٤,٤٠	٠,٦٦	٠,٤٣	٢٣٩	٠,٦٧	الثامن
			محقق فني	١١٢	٤,٣٧	٠,٦٧				
	٩	استخدام برامج البحث عن المفردات النصية للعثور على المحرر المعلوماتي المزور.	محقق جنائي	١٢٩	٤,٢٧	٠,٦٣	٠,٥٢_	٢٣٩	٠,٦٠	التاسع
			محقق فني	١١٢	٤,٣١	٠,٥٩				
	١٢	نسخ الدليل الرقمي.	محقق جنائي	١٢٩	٤,٢٢	٠,٧٢	١,١٩_	٢٣٩	٠,٢٤	العاشر
			محقق فني	١١٢	٤,٣٢	٠,٦٣				
	١٣	تحليل الدليل الرقمي.	محقق جنائي	١٢٩	٤,٢٦	٠,٦٩	٠,٠٣_	٢٣٩	٠,٩٧	الحادي عشر
			محقق فني	١١٢	٤,٢٦	٠,٦٣				
	١٤	عرض الدليل الرقمي.	محقق جنائي	١٢٩	٤,٢٧	٠,٧٢	٠,٢٤	٢٣٩	٠,٨١	الثاني عشر
			محقق فني	١١٢	٤,٢٥	٠,٦٥				
	١٠	استخدام مضادات الفيروسات لاكتشاف الفيروسات المستخدمة في الاختراق والتعدي.	محقق جنائي	١٢٩	٤,٢٦	٠,٦٧	٠,١٥	٢٣٩	٠,٨٨	الثالث عشر
			محقق فني	١١٢	٤,٢٥	٠,٧٢				
	٧	استخدام أقراص فك كلمة المرور للدخول على المواقع المحجوبة.	محقق جنائي	١٢٩	٤,١٦	٠,٧٩	٠,٩٩_	٢٣٩	٠,٣٢	الرابع عشر
			محقق فني	١١٢	٤,٢٦	٠,٧١				
	٨	استخدام برامج الاستنساخ الجنائي للأقراص الضوئية.	محقق جنائي	١٢٩	٤,٢٢	٠,٧١	١,١٩	٢٣٩	٠,٢٤	الخامس عشر
			محقق فني	١١٢	٤,١٢	٠,٧٠				

توضح البيانات من جدول اختبار (T_Test) أن قيم (T) لجميع العبارات غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جريمة التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم لفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، فهم جميعاً يدركون فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، فضلاً عن طبيعة عملهم التي تحتم تبادل الآراء والخبرات ومن ثمَّ اكتساب القدرة على تحديد فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، فهي معروفة للجميع بغض النظر عن طبيعة عملهم.

ي ـ اختلاف رؤية المبحوثين نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

يوضح الجدول رقم (٢٩) نتائج اختبار (T_Test) لدلالة الفروق في رؤية المبحوثين للمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل.

الجدول رقم (٢٩) نتائج اختبار (ت) لدلالة الفروق في رؤية المبحوثين المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني باختلاف متغير طبيعة العمل

المحور	طبيعة العمل	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة (ت) T	درجات الحرية	الدلالة Sig (2-tailed)
معوقات أساليب إثبات جرائم التزوير الإلكتروني	محقق جنائي	١٢٩	٤,٤٣	٠,٣٨	١,٥٢	٢٣٩	٠,١٣
	محقق فني	١١٢	٤,٣٦	٠,٣٦			

توضح البيانات من جدول اختبار (T_Test) أن قيمة (T) تساوي (١,٥٢) وهي غير دالة إحصائياً عند مستوى دلالة (١٣ , ٠) بمعنى أن هناك اتفاقاً في آراء مفردات الدراسة من أصحاب طبيعة العمل المختلفة (محقق جنائي ـ محقق فني) نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، أي أنه لا توجد فروق في رؤيتهم للمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، فهم جميعاً يدركون المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بنفس الدرجة في ضوء عملهم في ثقافة تنظيمية متشابهة تكسبهم قدرة متماثلة على تحديد المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، فالمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق

الجنائـي والفني في إثبات جرائم التزوير الإلكـتروني معروفة للجميع بغض النظر عن طبيعة عملهم.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٢ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو الوسـائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٣ ـ توجد فروق ذات دلالة إحصائية بين رؤية مفردات الدراسة لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية تعزى إلى متغـير طبيعة العمل، وكانـت الفروق الدالـة إحصائياً لصالح المحققـين الجنائيـين، أي أن المحققين الجنائيين أكثـر إدراكاً لصور جريمـة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، نظراً لأن المحققـين الجنائيـين يهتمون بصور وأشـكال جريمـة التزوير سـواء كانـت تغيـير بيانات في سـجلات الحاسـب الآلي، أو سرقة منظومة التوقيع الإلكتروني، أو تغيير مهنة واستخدامها في إصدار وثائـق ثبوتيـة مزورة، فهـم أكثر إلمامـاً بتصنيفات جرائـم التزوير الإلكـتروني وتكييفهـا القانوني، بخـلاف المحققـين الفنيين الذين يركـزون عـلى الجوانب الفنيـة لارتـكاب ووقوع جريمـة التزوير الإلكترونيـة، وكيفيـة التقاط الأدلـة الإلكترونية اللازمـة لإثباتها بالطرق والتقنيات الفنية.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٥ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٧ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٨ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٩ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

١٠ ـ لدى مفردات الدراسة رؤية متشابهة نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٢ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير العمر

يوضح الجدول رقم (٣٠) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير العمر.

الجدول رقم (٣٠) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير العمر

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,٦٦	٣	٠,٠٢٢	٠,١٨٨	٠,٩٠٤
	داخل المجموعات	٢٧,٥٥٨	٢٣٧	٠,١١٦		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٣٧١	٣	٠,١٢٤	٠,٦٩٧	٠,٥٥٥
	داخل المجموعات	٤٢,٠١٢	٢٣٧	٠,١٧٧		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	٠,٢٥٠	٣	٠,٠٨٣	٠,٤٤٢	٠,٧٢٣
	داخل المجموعات	٤٤,٦٦٩	٢٣٧	٠,١٨٨		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,١٠٣	٣	٠,٠٣٤	٠,٢٢٩	٠,٨٧٦
	داخل المجموعات	٣٥,٤١٩	٢٣٧	٠,١٤٩		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	٠,٧٣٦	٣	٠,٢٤٥	١,٤٣٠	٠,٢٣٥
	داخل المجموعات	٤٠,٦٦١	٢٣٧	٠,١٧٢		
	المجموع	٤١,٣٩٧	٢٤٠			

فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٥٦٦	٣	٠,١٨٩	١,٥٤٥	٠,٢٠٤
	داخل المجموعات	٢٨,٩٤٨	٢٣٧	٠,١٢٢		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٠٦٩	٣	٠,٠٢٣	٠,١٣٣	٠,٩٤٠
	داخل المجموعات	٤٠,٩٥١	٢٣٧	٠,١٧٣		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٥٦٨	٣	٠,١٨٩	١,٣٨٩	٠,٢٤٧
	داخل المجموعات	٣٢,٣٢٩	٢٣٧	٠,١٣٦		
	المجموع	٣٢,٨٩٨	٢٤٠			

يوضح الجدول رقم (٣٠) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن العمر لا يؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم

التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني بغض النظر عن أعمارهم.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت أعمارهم.

٢ ـ لدى مفردات الدراسة رؤية متشابهة نحو الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني مهما اختلفت أعمارهم.

٣ ـ لدى مفردات الدراسة رؤية متشابهة نحو صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية مهما اختلفت أعمارهم.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٥ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٧ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٨ ـ لدى مفردات الدراسة رؤية متشابهة نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٣ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير المؤهل التعليمي

يوضح الجدول رقم (٣١) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير المؤهل التعليمي.

الجدول رقم (٣١) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير المؤهل التعليمي

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,٠٣٣	٢	٠,٠١٦	٠,١٤١	٠,٨٦٨
	داخل المجموعات	٢٧,٥٩٠	٢٣٨	٠,١١٦		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٦٧٨	٢	٠,٣٣٩	١,٩٣٤	٠,١٤٧
	داخل المجموعات	٤١,٧٠٥	٢٣٨	٠,١٧٥		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	٠,٠٥٦	٢	٠,٠٢٨	٠,١٤٨	٠,٨٦٢
	داخل المجموعات	٤٤,٨٦٣	٢٣٨	٠,١٨٨		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,٨٢٨	٢	٠,٤١٤	٢,٨٣٩	٠,٠٦٠
	داخل المجموعات	٣٤,٦٩٤	٢٣٨	٠,١٤٦		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	١,٢٨٠	٢	٠,٦٤٠	٣,٧٩٦	٠,٠٢٤*
	داخل المجموعات	٤٠,١١٧	٢٣٨	٠,١٦٩		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,١٤٤	٢	٠,٠٧٢	٠,٥٨٣	٠,٥٥٩
	داخل المجموعات	٢٩,٣٧٠	٢٣٨	٠,١٢٣		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٢٠٢	٢	٠,١٠١	٠,٥٨٨	٠,٥٥٦
	داخل المجموعات	٤٠,٨١٨	٢٣٨	٠,١٧٢		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,١٤٥	٢	٠,٠٧٢	٠,٥٢٦	٠,٥٩٢
	داخل المجموعات	٣٢,٧٥٣	٢٣٨	٠,١٣٨		
	المجموع	٣٢,٨٩٨	٢٤٠			

* دال عند مستوى دلالة (٠,٠٥) أو أقل.

يوضح الجدول رقم (٣١) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، باستثناء محور سمات المجني عليه في جرائم التزوير الإلكتروني، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن المؤهل التعليمي لا يؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد خصائص جريمة التزوير الإلكتروني، وصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي

في إثبـات جرائم التزوير الإلكتروني، وفاعلية الأسـاليب التي يتبعها المحقق الفنـي في إثبات جرائـم التزوير الإلكتروني، والمعوقـات التي تؤدي إلى عدم فاعليـة الأسـاليب المسـتخدمة من المحقق الجنائـي والفني في إثبـات جرائم التزوير الإلكتروني بغض النظر عن مؤهلاتهم التعليمية.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت مؤهلاتهم التعليمية.

٢ ـ لـدى مفردات الدراسـة رؤية متشـابهة نحو الوسـائل المسـتخدمة في ارتـكاب جريمـة التزويـر الإلكتروني مهما اختلفـت مؤهلاتهم التعليمية.

٣ ـ لـدى مفردات الدراسـة رؤية متشـابهة نحو صور جريمـة التزوير الإلكـتروني في الدوائـر الحكوميـة الإلكترونيـة مهـما اختلفـت مؤهلاتهم التعليمية.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلفت مؤهلاتهم التعليمية.

٥ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو فاعلية الأسـاليب التي يتبعهـا المحقـق الجنائي في إثبـات جرائم التزويـر الإلكتروني مهما اختلفت مؤهلاتهم التعليمية.

٦ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو فاعلية الأسـاليب التي يتبعهـا المحقـق الفنـي في إثبـات جرائـم التزوير الإلكـتروني مهما اختلفت مؤهلاتهم التعليمية.

٧ ـ لـدى مفـردات الدراسـة رؤية متشـابهة نحو المعوقـات التي تؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقـق الجنائي والفني في إثبـات جرائـم التزويـر الإلكـتروني مهـما اختلفـت مؤهلاتهم التعليمية.

٤ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير جهة العمل

يوضـح الجـدول رقـم (٣٢) نتائـج تحليـل التبايـن في رؤيـة المبحوثين لفاعلية الأسـاليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير جهة العمل.

الجدول رقم (٣٢) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير جهة العمل

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,٧١٠	٣	٠,٢٣٧	٢,٠٨٤	٠,١٠٣
	داخل المجموعات	٢٦,٩١٣	٢٣٧	٠,١١٤		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٣٦٩	٣	٠,١٢٣	٠,٦٩٣	٠,٥٥٧
	داخل المجموعات	٤٢,٠١٤	٢٣٧	٠,١٧٧		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	١,٧٧٠	٣	٠,٥٩٠	٣,٢٤٠	٠,٠٢٣*
	داخل المجموعات	٤٣,١٤٩	٢٣٧	٠,١٨٢		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,١٤٢	٣	٠,٠٤٧	٠,٣١٦	٠,٨١٤
	داخل المجموعات	٣٥,٣٨٠	٢٣٧	٠,١٤٩		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	١,٢٦٤	٣	٠,٤٢١	٢,٤٨٩	٠,٠٦١
	داخل المجموعات	٤٠,١٣٢	٢٣٧	٠,١٦٩		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٢٤٥	٣	٠,٠٨٢	٠,٦٦٠	٠,٥٧٧
	داخل المجموعات	٢٩,٢٧٠	٢٣٧	٠,١٢٤		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٩٧٧	٣	٠,٣٢٦	١,٩٢٧	٠,١٢٦
	داخل المجموعات	٤٠,٠٤٣	٢٣٧	٠,١٦٩		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٥٠١	٣	٠,١٦٧	١,٢٢٢	٠,٣٠٢
	داخل المجموعات	٣٢,٣٩٧	٢٣٧	٠,١٣٧		
	المجموع	٣٢,٨٩٨	٢٤٠			

* دال عند مستوى دلالة (٠,٠٥) أو أقل.

يوضح الجدول رقم (٣٢) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، باستثناء محور صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن جهة العمل لا تؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم

التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بغض النظر عن جهات أعمالهم.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٢ ـ لدى مفردات الدراسة رؤية متشابهة نحو الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٣ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٥ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٧ ـ لـدى مفـردات الدراسـة رؤية متشـابهة نحو المعوقـات التي تؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقـق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت جهات أعمالهم.

٥ ـ اختـلاف رؤيـة المبحوثين نحـو فاعلية الأسـاليـب المستخدمـة في إثبـات جرائـم التزويـر الإلكتـروني باختـلاف متغير منطقة العمل

يوضـح الجـدول رقـم (٣٣) نتائـج تحليـل التبايـن في رؤيـة المبحوثين لفاعلية الأسـاليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير منطقة العمل.

الجدول رقم (٣٣) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير منطقة العمل

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	١,٨٥٦	١٢	٠,١٥٥	١,٣٦٨	٠,١٨٢
	داخل المجموعات	٢٥,٧٦٨	٢٢٨	٠,١١٣		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٤,١٥٦	١٢	٠,٣٤٦	٢,٠٦٦	*٠,٠٢٠
	داخل المجموعات	٣٨,٢٢٦	٢٢٨	٠,١٦٨		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	٥,٥٣٤	١٢	٠,٤٦١	٢,٦٧٠	**٠,٠٠٢
	داخل المجموعات	٣٩,٣٨٥	٢٢٨	٠,١٧٣		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٣,٤٥٩	١٢	٠,٢٨٨	٢,٠٥٠	*٠,٠٢١
	داخل المجموعات	٣٢,٠٦٢	٢٢٨	٠,١٤١		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	٢,٥١٣	١٢	٠,٢٠٩	١,٢٢٨	٠,٢٦٥
	داخل المجموعات	٣٨,٨٨٤	٢٢٨	٠,١٧١		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	١,٩٧١	١٢	٠,١٦٤	١,٣٥٩	٠,١٨٧
	داخل المجموعات	٢٧,٥٤٤	٢٢٨	٠,١٢١		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٢,٩٥٦	١٢	٠,٢٤٦	١,٤٧٦	٠,١٣٤
	داخل المجموعات	٣٨,٠٦٣	٢٢٨	٠,١٦٧		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٥,١٥٩	١٢	٠,٤٣٠	٣,٥٣٣	**٠,٠٠٠
	داخل المجموعات	٢٧,٧٣٩	٢٢٨	٠,١٢٢		
	المجموع	٣٢,٨٩٨	٢٤٠			

* دال عند مستوى دلالة (٠,٠٥) أو أقل.

** دال عند مستوى دلالة (٠,٠١) أو أقل.

يوضح الجدول رقم (٣٣) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام محاور : خصائص جريمة التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن منطقة العمل لا تؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد خصائص جريمة التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني بغض النظر عن المنطقة التي يعملون بها.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت المنطقة التي يعملون بها.

٢ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفت المنطقة التي يعملون بها.

٣ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلفت المنطقة التي يعملون بها.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت المنطقة التي يعملون بها.

٦ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير الرتبة العسكرية

يوضح الجدول رقم (٣٤) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير الرتبة العسكرية.

الجدول رقم (٣٤) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير الرتبة العسكرية

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,٢٠٥	٥	٠,٠٤١	٠,٣٥١	٠,٨٨١
	داخل المجموعات	٢٧,٤١٩	٢٣٥	٠,١١٧		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٢٠١	٥	٠,٠٤٠	٠,٢٢٤	٠,٩٥٢
	داخل المجموعات	٤٢,١٨٢	٢٣٥	٠,١٧٩		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	٠,١٩٥	٥	٠,٠٣٩	٠,٢٠٥	٠,٩٦٠
	داخل المجموعات	٤٤,٧٢٤	٢٣٥	٠,١٩٠		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,٦١٤	٥	٠,١٢٣	٠,٨٢٧	٠,٥٣١
	داخل المجموعات	٣٤,٩٠٧	٢٣٥	٠,١٤٩		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	٠,٦٢٩	٥	٠,١٢٦	٠,٧٢٦	٠,٦٠٥
	داخل المجموعات	٤٠,٧٦٨	٢٣٥	٠,١٧٣		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	١,٣٧٧	٥	٠,٢٧٥	٢,٣٠٠	٠,٠٤٦*
	داخل المجموعات	٢٨,١٣٧	٢٣٥	٠,١٢٠		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٤٩٦	٥	٠,٠٩٩	٠,٥٧٦	٠,٧١٩
	داخل المجموعات	٤٠,٥٢٤	٢٣٥	٠,١٧٢		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٤٧٩	٥	٠,٠٩٦	٠,٦٩٤	٠,٦٢٨
	داخل المجموعات	٣٢,٤١٩	٢٣٥	٠,١٣٨		
	المجموع	٣٢,٨٩٨	٢٤٠			

* دال عند مستوى دلالة (٠,٠٥) أو أقل.

يوضح الجدول رقم (٣٤) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، باستثناء محور فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن الرتبة العسكرية لا تؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية

الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بغض النظر عن رتبهم العسكرية.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٢ ـ لدى مفردات الدراسة رؤية متشابهة نحو الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٣ ـ لدى مفردات الدراسة رؤية متشابهة نحو صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية مهما اختلفت رتبهم العسكرية.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٥ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٧ ـ لدى مفردات الدراسة رؤية متشابهة نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٧ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد سنوات الخبرة في مجال العمل

يوضح الجدول رقم (٣٥) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد سنوات الخبرة في مجال العمل.

الجدول رقم (٣٥) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد سنوات الخبرة في مجال العمل

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,١٦٠	٤	٠,٠٤٠	٠,٣٤٤	٠,٨٤٨
	داخل المجموعات	٢٧,٤٦٣	٢٣٦	٠,١١٦		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٣٦٢	٤	٠,٠٩١	٠,٥٠٨	٠,٧٣٠
	داخل المجموعات	٤٢,٠٢٠	٢٣٦	٠,١٧٨		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	٠,١٠٧	٤	٠,٠٢٧	٠,١٤١	٠,٩٦٧
	داخل المجموعات	٤٤,٨١٢	٢٣٦	٠,١٩٠		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,٢٩٠	٤	٠,٠٧٣	٠,٤٨٦	٠,٧٤٦
	داخل المجموعات	٣٥,٢٣١	٢٣٦	٠,١٤٩		
	المجموع	٣٥,٥٢١	٢٤٠			

سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	٠,٦٤٦	٤	٠,١٦٢	٠,٩٣٦	٠,٤٤٤
	داخل المجموعات	٤٠,٧٥٠	٢٣٦	٠,١٧٣		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٤١٣	٤	٠,١٠٣	٠,٨٣٨	٠,٥٠٢
	داخل المجموعات	٢٩,١٠١	٢٣٦	٠,١٢٣		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	١,٠٣٢	٤	٠,٢٥٨	١,٥٢٣	٠,١٩٦
	داخل المجموعات	٣٩,٩٨٧	٢٣٦	٠,١٦٩		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	١,٠٥٠	٤	٠,٢٦٢	١,٩٤٥	٠,١٠٤
	داخل المجموعات	٣١,٨٤٨	٢٣٦	٠,١٣٥		
	المجموع	٣٢,٨٩٨	٢٤٠			

يوضح الجدول رقم (٣٥) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، ولصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي

تـؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقـق الجنائي والفني في إثبـات جرائم التزويـر الإلكتروني، وهذا مؤشر على أن عدد سـنوات الخبرة في مجـال العمـل لا يؤثر في رؤية مفردات الدراسـة لخصائص جريمة التزوير الإلكـتروني، ولصـور جريمـة التزويـر الإلكـتروني في الدوائـر الحكوميـة الإلكترونية، وللوسـائل المسـتخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسـمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسـمات المجني عليـه في جرائم التزوير الإلكتروني، ولفاعلية الأسـاليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، ولفاعلية الأسـاليب التي يتبعها المحقـق الفني في إثبات جرائم التزوير الإلكـتروني، وللمعوقات التي تؤدي إلى عـدم فاعلية الأسـاليب المسـتخدمة من المحقق الجنائـي والفني في إثبات جرائـم التزويـر الإلكـتروني، نظـراً لأن الجميـع يعملـون في ثقافـة تنظيمية واحدة، تكسـبهم قدرات متشـابهة على تحديد فاعلية الأسـاليب المستخدمة في إثبـات جرائم التزوير الإلكتروني بغض النظر عن عدد سـنوات خبراتهم العملية في مجال العمل.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لـدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكـتروني مهـما اختلف عدد سـنوات خبراتهـم العملية في مجال العمل.

٢ ـ لـدى مفردات الدراسـة رؤية متشـابهة نحو الوسـائل المسـتخدمة في ارتـكاب جريمة التزوير الإلكتروني مهما اختلف عدد سـنوات خبراتهم العملية في مجال العمل.

٣ ـ لـدى مفردات الدراسـة رؤية متشـابهة نحو صور جريمـة التزوير

الإلكتروني في الدوائر الحكومية الإلكترونية مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٥ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٧ ـ لدى مفردات الدراسة رؤية متشابهة نحو فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٨ ـ لدى مفردات الدراسة رؤية متشابهة نحو المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلف عدد سنوات خبراتهم العملية في مجال العمل.

٨ ـ اختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية

يوضح الجدول رقم (٣٦) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية.

الجدول رقم (٣٦) نتائج تحليل التباين في رؤية المبحوثين لفاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغير عدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية

المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة قيمة (p)
خصائص جريمة التزوير الإلكتروني	بين المجموعات	٠,٠١٨	٣	٠,٠٠٦	٠,٠٥٣	٠,٩٨٤
	داخل المجموعات	٢٧,٦٠٥	٢٣٧	٠,١١٦		
	المجموع	٢٧,٦٢٣	٢٤٠			
الوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني	بين المجموعات	٠,٤٨٦	٣	٠,١٦٢	٠,٩١٧	٠,٤٣٣
	داخل المجموعات	٤١,٨٩٦	٢٣٧	٠,١٧٧		
	المجموع	٤٢,٣٨٢	٢٤٠			
صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية	بين المجموعات	١,٤٧٣	٣	٠,٤٩١	٢,٦٧٨	*٠,٠٤٨
	داخل المجموعات	٤٣,٤٤٦	٢٣٧	٠,١٨٣		
	المجموع	٤٤,٩١٩	٢٤٠			
سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني	بين المجموعات	٠,٢٦٨	٣	٠,٠٨٩	٠,٦٠١	٠,٦١٥
	داخل المجموعات	٣٥,٢٥٣	٢٣٧	٠,١٤٩		
	المجموع	٣٥,٥٢١	٢٤٠			
سمات المجني عليه في جرائم التزوير الإلكتروني	بين المجموعات	٠,٣٧٨	٣	٠,١٢٦	٠,٧٢٨	٠,٥٣٦
	داخل المجموعات	٤١,٠١٩	٢٣٧	٠,١٧٣		
	المجموع	٤١,٣٩٧	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٩٧٨	٣	٠,٣٢٦	٢,٧٠٨	*٠,٠٤٦
	داخل المجموعات	٢٨,٥٣٦	٢٣٧	٠,١٢٠		
	المجموع	٢٩,٥١٤	٢٤٠			
فاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني	بين المجموعات	١,١٥١	٣	٠,٣٢٦	٢,٧٠٨	٠,٠٤٦
	داخل المجموعات	٣٩,٨٦٨	٢٣٧	٠,١٢٠		
	المجموع	٤١,٠٢٠	٢٤٠			
المعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني	بين المجموعات	٠,٦٦٠	٣	٠,٢٢٠	١,٦١٧	٠,١٨٦
	داخل المجموعات	٣٢,٢٣٨	٢٣٧	٠,١٣٦		
	المجموع	٣٢,٨٩٨	٢٤٠			

* دال عند مستوى دلالة (٠,٠٥) أو أقل.

يوضح الجدول رقم (٣٦) أن قيمة ف غير دالة إحصائياً عند مستوى دلالة (٠,٠٥) أمام جميع المحاور، باستثناء محوري صور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، مما يشير إلى عدم وجود فروق دالة إحصائياً بين مفردات الدراسة في رؤيتهم لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، وهذا مؤشر على أن عدد الدورات التدريبية في مجال جرائم التزوير الإلكترونية لا يؤثر في رؤية مفردات الدراسة لخصائص جريمة التزوير الإلكتروني، وللوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، ولسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، ولسمات المجني عليه في جرائم التزوير الإلكتروني، ولفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وللمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني، نظراً لأن الجميع يعملون في ثقافة تنظيمية واحدة، تكسبهم قدرات متشابهة على تحديد خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم

التزويـر الإلكتروني بغض النظر عـن عدد الدورات التدريبيـة التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

وفي ضوء ذلك يمكن استنتاج ما يلي :

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكـتروني مهـما اختلف عـدد الـدورات التدريبية التـي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٢ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو الوسـائل المستخدمة في ارتـكاب جريمة التزويـر الإلكتروني مهما اختلف عـدد الدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٣ ـ لدى مفردات الدراسة رؤية متشابهة نحو سمات المجرم الإلكتروني في جرائم التزوير الإلكتروني مهما اختلف عدد الدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٤ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو سـمات المجني عليه في جرائـم التزوير الإلكـتروني مهما اختلف عدد الـدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٥ ـ لدى مفردات الدراسـة رؤية متشـابهة نحو فاعلية الأسـاليب التي يتبعهـا المحقـق الفنـي في إثبـات جرائـم التزوير الإلكـتروني مهما اختلف عدد الدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٦ ـ لـدى مفـردات الدراسـة رؤية متشـابهة نحو المعوقـات التي تؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقـق الجنائي والفني في إثبـات جرائم التزويـر الإلكتروني مهما اختلـف عدد الدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٤ . ١١ تحليل بعض القضايا الخاصة بالتزوير

تمهيد وتقسيم

يعد الجانب التطبيقي ثمرة الدراسة النظرية ، وذلك لما له من أهمية بالغة في بيـان مدى اهتـمام الجهات المختصـة بتطبيق الأنظمة المرعيـة ابتغاء تحقيق العدل الذي ينشده المنظم في المملكة العربية السعودية.

وعلى الرغم من الصعوبات التي واجهت الباحث في دراسـته التطبيقية والتـي كانـت من أهمها رفض بعض الجهات تسـليم الأوراق التي تشـير إلى قضايا التزوير، أو الأحكام الصادرة بشـأنها، إلا أن الباحث اسـتطاع بفضل الله عز وجل الحصول على بعض قضايا التزوير وقرارات أحكام صادرة عن الدوائر الجزائية بديوان المظالم في مختلف مناطق المملكة شملت جل البحث.

وقد اتبع الباحث في عرض هذه القضايا لدراستها المنهج التالي:

١ ـ إعطـاء كل قضيـة رقماً عـلى النحو التـالي : القضيـة الأولى، القضية الثانية.

٢ ـ كتابة عنوان لكل قضية بحسب ملابساتها.

٣ ـ كتابة الأسماء في شكل رموز حرصاً على السرية.

٤ ـ ذكر وقائع القضية، وبيان العقوبة المقررة.

٥ ـ تحليـل وقائـع القضيـة وذلك ببيـان أركانهـا، وفقاً لنظـام مكافحة التزوير بالمملكة.

وقد حرص الباحث على بيان صور التزوير الإلكتروني أثناء التحليل، وفاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني التي جرى

إيرادها في الإطار النظري المتمثلة في الأساليب التقليدية والإجرائية والمادية والصعوبات التي تواجه الإثبات.

كما حرص الباحث على سرد المواد التي توضح صور التجريم والعقاب على صور جريمة التزوير التقليدي والإلكتروني، حيث نصت المادة الخامسة على ما يلي : «كل موظف ارتكب أثناء وظيفته تزويراً ... أو بإثباته وقائع كاذبة على أنها وقائع صحيحة، أو بتغيير الأسماء المدونة في الأوراق الرسمية والسجلات، ووضع أسماء غير صحيحة بدلاً عنها، عوقب بالحبس من سنة إلى خمس سنوات» (المادة ٥ من نظام مكافحة التزوير السعودي الصادر بالمرسوم الملكي رقم (١١٤) وتاريخ ٢٦/ ١١/ ١٣٨٠هـ)، ونصت المادة السادسة على ما يلي : «يعاقب الأشخاص العاديون الذين يرتكبون الجرائم المنصوص عليها في المادة السابقة أو الذين يستعملون الوثائق والأوراق المزورة والأوراق المنصوص عليها في المادة السابقة على علم بحقيقتها بالعقوبات المنصوص عليها في المادة المذكورة، وبغرامة مالية من ألف إلى عشرة آلاف ريال» (المادة ٦ من نظام مكافحة التزوير السعودي الصادر بالمرسوم الملكي رقم (١١٤) وتاريخ ٢٦/ ١١/ ١٣٨٠هـ) ، ونصت المادة العاشرة على ما يلي : «من قلد أو زور توقيعاً أو خاتماً لشخص آخر أو حرف، بطريق الحك أو الشطب أو التغيير، سنداً أو أي وثيقة خاصة عوقب بالسجن من سنة إلا ثلاث سنوات»(المادة (١٠) من نظام مكافحة التزوير السعودي الصادر بالمرسوم الملكي رقم (١١٤) وتاريخ ٢٦/ ١١/ ١٣٨٠هـ)، ونصت الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير الصادر بناء على تعميم وزير العدل رقم ١٣/ ت/ ٢٧٠٥ في ٢٤/ ٧/ ١٤٢٦هـ والمرسوم الملكي رقم م/ ١٦ في ٨/ ٧/ ١٤٢٦هـ وقرار مجلس الوزراء رقم ١٦٧ في ٣/ ٧/ ١٤٢٦هـ المتضمن إضافة مادتين إلى نظام مكافحة التزوير الصادر

بالمرسوم الملكي رقم (١١٤) في ٢٦/ ١١/ ١٣٨٠هـ على ما يلي : «كل من زور الصور الضوئية أو المستندات المعالجة آلياً أو البيانات المخزنة في ذاكرة الحاسب الآلي أو على شريط أو أسطوانة ممغنطة أو غيرها من وسائط، أو استعملها وهو عالم بتزويرها يعاقب بالعقوبات الواردة في هذا النظام».

القضية الأولى: تزوير في محررات رسمية بسجلات مستشفى للولادة واستعمالها في استخراج شهادات ميلاد وإضافة الأبناء إلى دفتر العائلة

أولاً : نوع القضية

أ ـ تزوير في محررات رسمية وسجلات الحاسب الآلي

ب ـ رقم القضية : ٥١٧/ ٥/ ق لعام ١٤٢٦هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (ع، ش) بالاتفاق مع موظفي أحد المستشفيات الخاصة بالولادة والأطفال بمكة المكرمة بإدخال زوجته (خ، أ) موريتانية الجنسية للولادة بالمستشفى، وتدوينها بمساعدة العاملين في المستشفى على أنها زوجته السعودية الجنسية (م، ب)، وإثبات ذلك في سجلات المستشفى، وفي بلاغي الولادة لوليديه (م، ع)، و(ع، ع)،ومن ثم استعمال المستندات المزورة في التقدم للأحوال المدنية واستخراج شهادتي ميلاد للوليدين على أن والدتهما هي (م، ب) السعودية الجنسية،وإضافتهما إلى دفتر العائلة.

وبعدما علمت زوجته الموريتانية بفعلته أبلغت السلطات المختصة (مكافحة التزوير) التي قامت بالقبض على المتهم، وبعد ضبط الإفادات

وجمع الاستدلالات، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، وقام بالاعتراف بتفاصيل ارتكابه للتزوير، وتم ضبط المحررات المزورة. وطالبت هيئة الرقابة والتحقيق بمعاقبته وفقاً لأحكام المادتين ٥، ٦ من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم لمحاكمته تقدم المتهم (ع، ش) بتقريرين طبيين له ولولده يفيد بإصابتهما بمرض السكر، ومعاناته هو من ارتفاع ضغط الدم، مع اعترافه بما نسب إليه من أفعال.

وقد قررت الدائرة الجزائية توقيع عقوبة السجن لمدة سنة على المذكور وتغريمه مبلغ (١٠٠٠) ريال، مع وقف تنفيذ العقوبة.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام الجاني باستعمال الأوراق المزورة وهو يعلم بتزويرها واستفاد منها في إضافة الأبناء إلى دفتر العائلة، فالتزوير يجب أن يكون بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

٢ ـ أكـد تقريـر الأدلة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشف في السجلات والدفاتر التي تم تدوين الوليديـن عـلى أنهـما أبنـاء الزوجـة السـعودية، وذلك مـن خلال مضاهـاة الخطـوط والتوقيعـات باسـتخدام المجاهـر الإلكترونية لتأكيـد اعترافـات المتهم، مما يثبـت فاعلية الأسـاليب التقليدية في إثبـات جريمـة التزويـر الإلكـتروني (انظـر الدراسـة النظرية ص ص٥٨ـ٥٩، ولمزيـد مـن المعلومات انظـر : إدارة الأدلـة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأسـاليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طـوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وترتيب استجواب المتهمين والشـهود وذلك لحين الحكم في القضية، وهو مـا يعـرف بالتوقيـف الاحـتياطـي، مما يثبـت فاعلية الأسـاليب الإجرائيـة في إثبـات جريمـة التزويـر الإلكتروني (انظر الدراسـة النظريـة ص ص٦٥ـ٦٨، ولمزيـد من المعلومات انظـر : العريان، ٢٠٠٤م، مرجع سابق، ص١٣؛ البشرى، ٢٠٠٠م، مرجع سابق، ص ص٣٦٦ـ٣٦٧).

القضية الثانية: تزوير في سـجلات الحاسب الآلي لمدرسة لاستخراج شهادة دراسية مزورة

أولاً : نوع القضية

أ ـ تزوير شهادة مدرسية

ب ـ رقم القضية : ٥٩٣/ ٥/ ق لعام ١٤٢٦هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (ب، ص) سعودي الجنسية ويعمل بمكتب الإشراف التربوي بمحافظة خيبر، ومدير ثانوية أوس بن حبيب الأنصاري سابقاً بإدخال معلومات تخالف الواقع في سجلات الحاسب الآلي بإدخال اسم الطالب (ي، ح) ضمن طلبة المدرسة، وإدخال درجات وهمية للطالب في الاختبارات النصفية للصف الدراسي الثاني ١٤٢٥/ ١٤٢٦هـ في حين أن الطالب لم يكن قد التحق بالمدرسة، ولم يؤد الاختبارات بها، كما قام بالتزوير في محرر رسمي هو ورقة إجابة لطالب آخر وذلك بتعديل الدرجة التي حصل عليها الطالب بعد التحاقه بالمدرسة في مادة الكيمياء من صفر إلى ٢٤ بعد تدوين درجات وهمية على فقرات الأسئلة، ومن ثمَّ قيامه أيضاً بإدخال الدرجة المعدلة في سجلات الحاسب الآلي، وإقصاء المحضر المعد من مدرسي المادة وموظفي الكنترول، وبذلك تمت جريمة التزوير، حيث استخدم المتهم المحررات المزورة سواء يدوياً أو إلكترونياً بإدخال معلومات غير صحيحة في سجلات الحاسب الآلي، وقدمها إلى مرجعه على أنها صحيحة.

واستندت هيئة الرقابة والتحقيق في توجيه الاتهام على الآتي :

١ ـ إفادة المتهم بأنه هو من قام بقبول الطالب بالمدرسة.

٢ ـ أقوال وكيلي المدرسة التي أدانت المدير.

٣ ـ أقوال معلمي المدرسة التي أدانت المدير.

٤ ـ ثبوت عدم وجود اسم الطالب خلال فترة الامتحانات النصفية في سجل قيد الطلاب بالمدرسة.

٥ ـ ثبوت وجود علاقة بين الطالب والمتهم؛ لأن والد الطالب زميل في العمل لأشقاء المتهم.

٦ ـ كون المتهم مدير المدرسة والمسؤول عن سجلاتها في الحاسب والكنترول وهي السجلات المعتمدة.

٧ ـ علم المتهم بكيفية إدخال البيانات بالحاسب الآلي.

٨ ـ ثبوت المخالفة الإدارية بقبول الطالب دون التقيد بالأنظمة والتعليمات المنظمة لذلك.

وبعد ضبط الإفادات وجمع الاستدلالات، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، وقد أنكر المتهم جميع ما نسب إليه باستثناء قبول الطالب بالمدرسة، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المادتين الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم لمحاكمته ذكر المتهم أن والد الطالب حضر إليه خلال الاختبارات النصفية للفصل الدراسي الثاني، وأبدى له ظروفه الأسرية، وطلب منه قبول ابنه كطالب منتظم، وبعد التحقق من أوراقه، أحاله المدير إلى الوكيل لإكمال إجراءات التسجيل بالحاسب الآلي وانتهى دوره عند هذا الحد. وأنكر إدخال درجات وهمية بالحاسب الآلي، كما أنكر تعديل درجات الطالب الآخر في مادة الكيمياء من صفر إلى (٢٤)، كما أنكر إقصاء المحضر المعد من مدرسي المادة وموظفي الكنترول.

وقد قضت الدائرة الجزائية ببراءة المتهم (ب، ص) مما نسب إليه من تزوير إلكتروني وتزوير بيانات محرر.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسمية هي الإجابات المعدلة وتغيير الدرجة من صفر إلى (٢٤) في مادة الكيمياء، بجانب التزوير الإلكتروني بإدخال بيانات غير صحيحة في سجلات الحاسب الآلي واستعمالها لدى المرجع الإداري في إصدار شهادة تخرج حاسوبية.

أ ـ وقع التزوير في المحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، بعدما قام المتهم باستعماله بتقديم الدرجة المزورة وهو يعلم بتزويرها واستفاد منها في إدخال الدرجة إلى الحاسب الآلي باعتبارها الدرجة الحقيقية الحاصل عليها الطالب في المادة، مع تعمد إخفاء محضر غش الطالب في الاختبار، فالتزوير يجب أن يكون بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال درجات تفيد بنجاح الطالب واجتيازه الاختبارات النصفية بنجاح، واستعمالها في ذلك لدى المرجع الإداري بالرغم من أن الطالب لم يكن قد التحق بالمدرسة، فضلاً عن إدخال درجات مادة الكيمياء التي حصل فيها الطالب الآخر على (صفر) نتيجة

ضبطه وتسجيل محضر غش له، على أنه نجح بها وحصل على (٢٤) درجة. وقد أشارت إلى ذلك الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف في السجلات والدفاتر التي أكدت عدم تدوين اسم الطالب أثناء فترة الاختبارات التي وجد في سجل الحاسب الآلي أنه قد اجتازها بنجاح، وكذلك أكدت عدم وجود محضر يفيد قيام الطالب بالغش أو تدوين المحضر في سجلات الكنترول بالمدرسة، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وترتيب استجواب المتهمين والشهود وذلك لحين الحكم في القضية، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، مرجع سابق، ص١٣؛ البشرى، ٢٠٠٠م، مرجع سابق، ص ص٣٦٦ـ٣٦٧).

٤ ـ لم تتمكن جهات التحقيق من استخدام الأساليب المادية التي تثبت شخصية من قام بالدخول على النظام وتغيير نتائج الطالب في

سـجلات الحاسـب الآلي لأن هناك عدة أفراد مصرح لهم بالدخول ولا يوجـد كـود مخصـص لكل فـرد منهـم لكـي يمكن اسـتخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخـدم مـن مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظـام، وما قام به من إجراء بسـبب تعدد المسـتخدمين من وكلاء المدرسـة والمدير وغيرهم (انظر الدراسـة النظرية ص ص٦٠ـ٦٤، ولمزيـد مـن المعلومات انظر حجازي، ٢٠٠٥م، مرجع سـابق، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، مرجع سابق، ص٢١٩؛ Ara-biat, 2002؛ العنزي، ٢٠٠٣م، مرجع سابق، ص١٠٢).

القضيـة الثالثـة: تزوير في سـجلات الحاسـب الآلي لإدارة الأحوال لاستخراج بطاقة أحوال مزورة

أولاً : نوع القضية

أ ـ استخراج بطاقة أحوال مزورة

ب ـ رقم القضية : ٤٥/ ٢٢/ ٥/ ق لعام ١٤٢٥هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (خ، ح) أردني الجنسية والمدعو (ح، ر) سعودي الجنسـية في المساهمة من موظفين حسني النية في استخراج بطاقة أحوال باسم (ف، ر) سعودي الجنسية وشقيق (ح، ر)، حيث ادعى (ح، ر) أن (خ، ح) شقيقه وأنه فقد بطاقة الأحوال الخاصة به ويريد استخراج بطاقة أخـرى بدل فاقد. وتطلب ذلك ارتكاب التزوير في محررات رسـمية وعرفية

هـي الأوراق والنماذج التي تم تعبئتها للحصول على البطاقة، والتوقيع عليها من قبل المتهمين ومن قبل الموظفين، وكذلك إدخال هذه البيانات بالحاسب الآلي للحصـول على البطاقة المزورة، وتم اسـتخراج البطاقـة المزورة والموقع على أوراقها تزويراً المتهم الأول (خ، ح) ومن ثم انتحل شخصية شقيق المتهم الثاني (ح، ر) الذي ساعده في ارتكاب التزوير بالاتفاق والمساعدة.

وبعد ضبط الإفادات وجمع الاسـتدلالات، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب التقليدية والإجرائية والمادية، أصر (خ، ح) الأردني الجنسـية على أنه (ف، ر) سـعودي الجنسية، وبعد إعادة التحقيق معه في مكافحة التزوير بتاريخ ٢٨/ ١١/ ١٤٢٤هـ اعترف بالجريمة، وأن المتهـم الثـاني (ح، ر) ذهب معه إلى الأحوال المدنيـة بالمدينة المنورة وذكر للموظفين أنه شـقيقه وأنه فقد بطاقة الأحوال ويرغب في الحصول على بطاقة أخـرى، وقـام (خ، ح) بتعبئـة الاسـتمارات والتعهدات والإقـرارات، ووقع عليها على أنه (ف، ر)، وتم استكمال الإجراءات ثم تصوير (خ، ح) وإدخال البيانات والصورة بالحاسـب الآلي وسـجلاته وإصدار البطاقة باسم (ف، ر) ولكنها تحمل صورته، واستعماله البطاقة في العمل لدى شركة «كاستيال» بعد أن وقع على إجراءات تعيينه منتحلاَ شخصية (ف، ر) وهو على علم بذلك.

تـم إرسـاله إلى هيئة الرقابـة والتحقيق لإقامة الدعـوى تجاهه، واعترف بجميـع مـا أدلى بـه في محضر مكافحـة التزوير، وأن هدفه مـن ذلك هو طلب العيش وأن المتهم الثاني (ح، ر) هو من ساعده على ذلك.

وبالتحقيق مع المتهم الثاني (ح، ر) أنكر ما نسـب إليه من مسـاعدة (خ، ح) في استخراج بطاقة الأحوال، وأنه لم يراجع الأحوال المدنية ولا يعلم شيئاً عن الموضوع. إلا أن (ع، ح) الذي يعمل بالأحوال المدنية بالمدينة المنورة أكد كلام المتهم الأول (خ، ح).

ولذلك طالب ممثل الادعاء بالهيئة بمعاقبة المتهمين وفقاً لأحكام المواد الخامسة والسادسة والعاشرة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم اعترف المتهم الأول بجميع ما نسب إليه، بينما أصر المتهم الثاني على الإنكار.

وقد قضت الدائرة الجزائية بإدانة المتهم الأول (خ، ح) أردني الجنسية بارتكاب جريمة تزوير واستعمال وسجنه سنة واحدة تحتسب من تاريخ توقيفه على ذمة هذه القضية مع تغريمه ألف ريال، وإدانة المتهم الثاني (ح، ر) سعودي الجنسية بما نسب إليه من تزوير وسجنه سنة واحدة مع تغريمه مبلغ ألف ريال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير في محررات رسمية هي الاستمارات والنماذج التي تم تعبئتها ببيانات غير صحيحة واستعمالها في التعيين لدى شركة «كاستيال»، بجانب التزوير الإلكتروني بإدخال بيانات مزورة (الصورة) بالحاسب الآلي واستخراجها بمعلومات وبيانات لا تخص صاحب الصورة.

أ ـ التزوير في المحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة العاشرة من نظام مكافحة التزوير التي سبق ذكرها، وقد وقع التزوير بعدما قام المتهم بتعبئة النماذج والاستمارات والتوقيع عليها منتحلاً اسم (ف، ر)، فالتزوير

يقـع بتغيير الحقيقة في محرر مكتـوب وموجود في الأصل (انظر الدراسـة النظرية ص ص٥١ـ٥٢؛ ولمزيد مـن المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزويـر الإلكـتروني وقع نتيجـة إدخال بيانـات غير صحيحة في ذاكـرة الحاسـب الآلي، وذلـك مـن خـلال إدخـال البيانات الخاصة بالمتهم (ف،ر) واستخراجها من الحاسب الآلي بصورة المتهم (خ، ح) أردني الجنسـية، ومن ثم استعمال البطاقة المزورة في التعيـين لدى شركـة «كاسـتيال» منتحلاً شـخصية (ف، ر) باسـتعمال البطاقة المزورة حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكـد تقريـر الأدلـة الجنائيـة المثبـت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشـف عن توقيع (خ، ح) على أوراق ونماذج استخراج بدل فاقد للبطاقة مع توقيعه على استلام بطاقة الأحوال في السجل الخاص بالأحوال المدنية، وذلك من خلال مضاهاة الخطوط والتوقيعات باستخدام المجاهر الإلكترونية لتأكيد اعترافات المتهم، ممـا يثبـت فاعليـة الأسـاليب التقليديـة في إثبـات جريمـة التزويـر الإلكـتروني (انظـر الدراســة النظريـة ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أمـا الأسـاليب الإجرائية فتمثلت في التحقيق مـع المتهم، واحتجازه طـوال فترة التحقيق لمنعه من محاولة طمـس معالم جريمته، وترتيب استجواب المتهمين والشهود وذلك لحين الحكم في القضية، وهو ما يعـرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأسـاليب الإجرائية

في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، مرجع سابق، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات غير صحيحة بسجلات الحاسب لإصدار بطاقة أحوال مزورة، وتم التعرف على الموظف الذي أجرى التغيير (لم يتم عقابه لأنه أجرى التغيير بحسن نية)من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، مرجع سابق، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الرابعة: تزوير في سجلات الحاسب الآلي بالجوازات واستعمال جواز سفر مزور

أولاً : نوع القضية

أ ـ استعمال جواز سفر مزور

ب ـ رقم القضية : ٥٤٩/ ٢٢/ ٥/ ق لعام ١٤٢٤هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (ب، ح) باكستاني الجنسية بشراء جواز سفر من (ب، خ) الذي غادر المملكة بتأشيرة خروج وعودة ولم يعد، ووضع صورته محل صورة (ب، خ)، ومن ثم دخوله المملكة منتحلاً شخصية (ب، خ). وبذلك يكون قد ساهم في ارتكاب تزوير في سجلات الحاسب الآلي بمساعدة موظفين حسني النية، وباستعمال الجواز المزور في دخول المملكة تقع جريمة التزوير التقليدي والإلكتروني. وبعد دخول المملكة قام (ب، ح) بشراء إقامة من شخص مجهول في ينبع ووضع صورته عليها، وزور الاسم أيضاً إلى (ب، خ) واستخدمها في توقيع محررات وعقود تنفيذ مقاولات مع شركات مرافق الكهرباء والمياه بالجبيل وينبع منتحلاً اسم (ب، خ)، وبذلك يكون قد ارتكب جريمة التزوير في محررات ووضع توقيع مزور.

وأهم أدلة الاتهام التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف (ب، ح) بما ارتكبه من تزوير.

٢ ـ أقوال مكفول (ب، خ) الذي أفاد أن مكفوله ذهب إلى باكستان بتأشيرة خروج وعودة ولكن لم يعد.

وبعد ضبط الإفادات وجمع الاستدلالات، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، واعترف المتهم بما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة والعاشرة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم لمحاكمته كرر المتهم اعترافه

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهم لمدة سنة واحدة من تاريخ توقيفه وتغريمه مبلغ ألف ريال عن جريمة التزوير والاستعمال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسمية هي تغيير الصورة في جواز السفر، وتغيير الاسم والصورة في الإقامة، واستعمالهما في تزوير محررات رسمية وتعاقدات مع جهات حكومية بانتحال شخصية آخر، بجانب التزوير الإلكتروني بإدخال بيانات غير صحيحة لدى الجوازات من خلال استعمال الجواز المزور في الدخول إلى المملكة.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة العاشرة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام المتهم بتعبئة النماذج والاستمارات والتوقيع عليها منتحلاً اسم (ف، ر)، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة

بجواز سفر (ب، خ) والتي تحمل صورة (ب، ح) في الحاسب الآلي بجوازات مطار الملك عبد العزيز الدولي والسماح له بدخول المملكة، أي وقع التزوير باستعمال الجواز في الدخول إلى المملكة، وأيضاً الاستفادة من الجواز المزور في التعاقد مع شركات حكومية لإنجاز مقاولات بانتحال شخصية (ب، خ)، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن الصورة الشمسية التي وضعها (خ، ح) في جواز السفر مكان صورة (ب، خ) الذي غادر المملكة ولم يعد، بجانب الكشف عن توقيع (خ، ح) على العقود والمستندات واستلام المبالغ والدفعات، وذلك من خلال مضاهاة الخطوط والتوقيعات باستخدام المجاهر الإلكترونية لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وترتيب استجواب المتهمين والشهود وذلك لحين الحكم في القضية، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات غير صحيحة بسجلات الحاسب بمساعدة الموظفين حسني النية، وتم اكتشاف الموظف الذي أجرى تسجيل بيانات الدخول بحاسب الجوازات (لم يتم عقابه لحسن نيته) من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الخامسة: تزوير في سجلات الحاسب الآلي بالجوازات واستعمال جواز سفر مزور

أولاً : نوع القضية

أ ـ استعمال جواز سفر مزور

ب ـ رقم القضية : ٣٥/ ٤/ ق لعام ١٤١٩هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (غ، ش) باكستاني الجنسية باستعمال جواز سفر مزور خاص بأخيه (م، ش) باكستاني الجنسية، الذي مرض في باكستان ولم يستطع الحضور، فاستغل (غ، ش) الشبه بينهما، و دخل

المملكة منتحلاً شخصية (م، ش). وبذلك يكون قد ساهم في ارتكاب تزوير في سجلات الحاسب الآلي بمساعدة موظفين حسني النية، وباستعمال الجواز المزور في دخول المملكة تقع جريمة التزوير التقليدي والإلكتروني. وبعد دخول المملكة قام (غ، ش) بالتزوير محررات عرفية هي سجلات وبيانات النقل الجماعي في الحصول على تذكرة سفر من جدة إلى جيزان، بالجواز المزور منتحلاً شخصية (م، ش) وبذلك تقع جريمة التزوير التقليدية.

وأهم أدلة الاتهام التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف (غ، ش) بما ارتكبه من تزوير.

٢ ـ ضبط بطاقة النقل الجماعي المزورة بحوزته أثناء القبض عليه.

٣ ـ إبلاغ كفيل صاحب الجواز الأصلي عن المتهم المذكور وأنه لا يعمل لديه، وأنه منتحل شخصية مكفوله السابق (م، ش).

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية ، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، واعترف المتهم بما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة والعاشرة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم لمحاكمته كرر المتهم اعترافه.

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهم لمدة سنة واحدة من تاريخ توقيفه وتغريمه مبلغ ألف ريال عن جريمة التزوير والاستعمال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسمية هي استعمال جواز سفر لشخص آخر، واستعماله في التزوير في محررات رسمية هي أوراق شركة النقل الجماعي والحصول على تذكرة سفر باستعمال الجواز الخاص بالغير والانتقال به من جدة إلى جيزان، بجانب التزوير الإلكتروني بإدخال بيانات غير صحيحة لدى الجوازات من خلال استعمال الجواز المزور في الدخول إلى المملكة.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة العاشرة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام المتهم بتعبئة النماذج والاستمارات والتوقيع عليها منتحلاً اسم (ف، ر)، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في قاعدة البيانات في الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بجواز سفر (م، ش) في الحاسب الآلي بجوازات مطار الملك عبد العزيز الدولي والسماح بدخول (غ، ش) المملكة، أي وقع التزوير باستعمال الجواز في الدخول إلى المملكة، وأيضاً الاستفادة من الجواز المزور في الحصول

عـلى تذكرة بشركـة النقل الجماعي للانتقال مـن مكة إلى جيزان بانتحال شخصية (م، ش)، وذلك حسب ما نصت عليه الفقرة (ب) مـن المادة الرابعة عشرة من نظام مكافحة التزوير السـابق ذكرها.

٢ ـ أكـد تقريـر الأدلـة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشـف عن صورة (غ،ش) باستخدام المجاهر الإلكترونية للتأكد من أنها لا تخصه وتخص أخاه الذي يشـبهه كثيراً (م، ش) لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٥٨ـ٥٩، ولمزيـد مـن المعلومـات انظـر : إدارة الأدلـة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأسـاليب الإجرائية فتمثلـت في التحقيق مع المتهم، واحتجازه طـوال فترة التحقيـق لمنعه من محاولة طمس معـالم جريمته، وهو ما يعرف بالتوقيف الاحـتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكـد تقريـر الأدلـة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب المادية بالدخول على النظام وتسـجيل بيانات دخـول غير صحيحة بسجلات الحاسب بالجوازات، وتم التعرف على الموظف الذي قام بإدخـال البيانـات غير الصحيحة (لم يعاقب لحسـن نيته) من خلال الكود المخصص له باستخدام تقنيات التتبع واسـترجاع المعلومات والحصول على اسم المسـتخدم من مركز المعلومات الوطني User)

(name وهـذا الإجـراء يتبـع في الجهـات الحكوميـة للتعـرف على اسـم المسـتخدم ووقت اسـتخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأسـاليب المادية في إثبات جرائـم التزوير الإلكتروني (انظـر الدراسـة النظريـة ص ص٦٠ـ٦٤، ولمزيـد مـن المعلومات انظـر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م،ص١٠٢).

القضية السادسـة: تعديل وضع مـن قـادم للعمرة إلـى قـادم للعمل في سجلات الحاسب الآلي بالجوازات

أولاً: نوع القضية

أ ـ تزوير الغرض من القدوم

ب ـ رقم القضية: ٧١٢/ ٥/ ق لعام ١٤٢٦هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (و، هـ) سعودي الجنسية بتقاضي مبلغ من المال على سـبيل الرشـوة لتعديل وضع المتهم (إ، ر) مصري الجنسية مـن قـادم للعمرة إلى قادم للعمـل، وقام المتهم (و، هـ) بتعديل وضع المتهم (إ، ر) والغرض من قدومه بتغيير ذلك في بيانات في سجلات الحاسب الآلي بجوازات المدينة المنورة، فتمت جريمة التزوير.

كما استغل المتهم الثاني (إ، ر) البرنت المزور وقدمه لقنصلية بلاده مدعياً فقدان جواز السفر، واستخرج جواز سفر جديد، ومن ثم قدمه للمسؤولين في جـوازات مطار الأمير محمد بن عبد العزيز في المدينة المنورة للحصول على إقامة نظامية رغم علمه بحقيقة وضعه والهدف من قدومه.

وأهـم أدلة الاتهام التي اسـتندت عليها هيئة الرقابـة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف (إ، ر) بما ارتكبه من تزوير.

٢ ـ مـا جاء في النسـخة المروقية المسـتخرجة من جـوازات مطار الأمير محمد بن عبد العزيز بأن (و، هـ) هو الذي قام بالتعديل في المحررات وتغيـير وضع المتهم وبرقمه الشـخصي للدخول عـلى النظام وتغيير الهـدف مـن القدوم وأثناء فـترة مناوبته وهو عـلى رأس العمل (من قادم للعمرة إلى قادم للعمل).

٣ ـ ثبات استعمال المتهم الثاني (إ، ر) للمحرر المزور.

وبعـد ضبـط الإفادات وجمع الاسـتدلالات من قبل مكافحـة التزوير، والحصـول على تقرير الأدلـة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب التقليديـة والإجرائيـة والمادية، تم إرسـاله إلى هيئة الرقابـة والتحقيق لإقامة الدعـوى تجاهه، واعترف المتهم بما نسـب إليه، ولذلك طالـب ممثل الادعاء بالهيئـة معاقبته وفقاً لأحكام المادتين الخامسـة والسادسـة مـن نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعـد إحالتـه إلى الدائـرة الجزائيـة بديوان المظـالم لمحاكمته كـرر المتهم اعترافه. ولم تستطع الدائرة الجزائية سماع أقوال المتهم الأول (و، هـ) لإصابته بجلطة دماغية أسـفرت عن إصابته بشـلل نصفي وعـدم القدرة على الكلام أو التركيز، مما لا يسـمح باسـتجوابه أو سـماع أقواله، ومن ثم قررت الدائرة الجزائية وقف سير الدعوى ضده لحين تحسن أحواله الصحية.

وقد قضـت الدائرة الجزائيـة بتوقيع عقوبة حبس المتهـم (إ، ر) مصري الجنسـية لمدة سـنة واحـدة من تاريـخ توقيفه وتغريمـه مبلغ ألـف ريال عن جريمة التزوير والاستعمال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير إلكتروني بإدخال بيانات غير صحيحة لدى الجوازات من خلال تغيير الغرض من القدوم من قدوم للعمرة إلى قدوم للعمل، بجانب تزوير تقليدي في المحررات نتيجة استعمال المحرر الإلكتروني المزور (البرنت) من قبل المتهم الثاني (إ، ر).

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير التي سبق ذكرها، وقد وقع التزوير بعدما قام المتهم باستعمال البرنت الصادر من الجوازات لإصدار جواز سفر من قنصلية بلاده، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال تغيير البيانات الخاصة بالمتهم (إ، ر) من قادم للعمرة إلى قادم للعمل، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ تتمثل الأساليب الإجرائية في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف

بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ ٦٨، ولمزيد من المعلومات انظر: العريان، ٢٠٠٤م، مرجع سابق، ص١٣؛ البشرى، ٢٠٠٠م، مرجع سابق، ص ص٣٦٦ـ٣٦٧).

٣ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات قدوم غير صحيحة بسجلات الحاسب بالجوازات، وذلك لتغيير الهدف من القدوم من قادم للعمرة إلى قادم للعمل، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، مص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية السابعة: تزوير في سجلات الحاسب الآلي بالجوازات واستعمال جواز سفر مزور

أولاً: نوع القضية

أ ـ استعمال جواز سفر مزور

ب ـ رقم القضية: ٧٤/ ٥/ ق لعام ١٤٢٧هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (أ، م) تشادي الجنسية باستعمال جواز سفر مزور صادر من بلاده باسم (إ، ن)، وقد سبق أن أبعد من المملكة بعد ارتكاب جريمة سرقة، ووضع على القائمة السوداء بالمنع من دخول المملكة مرة أخرى. ولذلك فقد قام باستخراج جواز مزور باسم آخر والدخول به إلى المملكة ومن ثم ساهم مع موظفي الجوازات حسني النية في ارتكاب جريمة التزوير في سجلات الحاسب الآلي بالدخول بمعلومات تخالف الواقع، وإثبات وقائع كاذبة في صورة وقائع صحيحة ،وكذلك قام بالتوقيع على محاضر التحقيقات بالاسم المزور، وبذلك يكون قد استعمل الجواز المزور في الدخول إلى المملكة، وكذلك قام بالتوقيع على الأوراق الرسمية بالاسم المزور رغم علمه بحقيقة اسمه.

وأهم أدلة الاتهام التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ـ صحيفة سوابق المتهم المرفقة بملف القضية التي تثبت ارتكابه جريمة سرقة سابقة وسجنه وإبعاده من المملكة.

٢ ـ إصرار المتهم على الاسم المنتحل خلال جميع مراحل التحقيق.

٣ ـ خطاب مدير إدارة مكافحة التزوير الذي أفاد أن اسمه الحقيقي هو (أ، م).

٤ ـ ثبوت قيامه باستعمال المحرر المزور (جوار السفر) الذي قدم بموجبه للمملكة منتحلاً اسماً مغايراً لاسمه الحقيقي تزويراً.

وبعـد ضبـط الإفادات وجمع الاسـتدلالات من قبل مكافحـة التزوير، والحصـول على تقرير الأدلـة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب التقليديـة والإجرائيـة والماديـة تم إرسـاله إلى هيئة الرقابـة والتحقيق لإقامة الدعـوى تجاهه، وأصر المتهم على إنكاره، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسـة والسادسـة والتاسـعة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعـد إحالته إلى الدائرة الجزائية بديوان المظالم لمحاكمته أصر المتهم على إنكاره.

وقد قضت الدائرة الجزائية بديوان المظالم بتوقيع عقوبة حبس المتهم لمدة سـنة واحدة من تاريخ توقيفـه وتغريمه مبلغ ألف ريال عـن جريمة التزوير والاستعمال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسـمية هي اسـتعمال جـواز سـفر مـزور، واسـتعماله في التزويـر في محررات رسـمية هي المحـاضر التي قام بالتوقيع عليها بالاسـم المنتحل في الجواز المزور، بجانـب التزويـر الإلكـتروني بإدخـال بيانـات غـير صحيحة لدى الجـوازات من خلال اسـتعمال بيانات الجواز المـزور في الدخول إلى المملكة.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليـه المادة الخامسـة والمادة السادسـة والمادة التاسـعة من نظام مكافحـة التزوير السـابق ذكرهـا، وقد وقع التزويـر بعدما قام

المتهم بالدخول باستعمال جواز السفر المزور، وكذلك بالتوقيع على المحاضر بالاسم المزور الذي انتحله، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بجواز السفر المزور الذي يحتوي على اسم منتحل لكي يتمكن من الدخول لأن الجواز الأصلي السابق سبق أن تم إبعاده به من المملكة، أي وقع التزوير باستعمال الجواز في الدخول إلى المملكة، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن توقيعات (أ، م) بالاسم المنتحل (إ، ن)، وكذلك الكشف عن الاسم الحقيقي المسجل بالجوازات على الجواز الذي يحمل نفس الصورة ولكن بالاسم المنتحل (إ، ن) باستخدام المجاهر الإلكترونية للتأكد من انتحال الاسم الجديد، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما

يعرف بالتوقيف الاحـتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكـد تقريـر الأدلـة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب الماديـة بالدخول على النظام وتسـجيل بيانات دخول غير صحيحة لأنها لجواز سفر مزور بسجلات الحاسب بالجوازات، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة (لم يتم عقابه لحسـن نيته) من خلال الكود المخصص له باستخدام تقنيات التتبع واسـترجاع المعلومـات والحصـول على اسـم المسـتخدم مـن مركز المعلومـات الوطنـي (User name) وهذا الإجـراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قـام به مـن إجراء مما يثبت فاعلية الأسـاليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسـة النظرية ص ص٦٠ـ٦٤، ولمزيد مـن المعلومـات انظـر حجـازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبـد المطلـب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الثامنة: تزوير مستندات رسمية وإدخالها في سجل الحاسب الآلي

أولاً : نوع القضية

أ ـ تزوير مستندات رسمية في سجلات الحاسب الآلي.

ب ـ رقم القضية : ٨١/ ٤/ ق لعام ١٤١٩هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (م، ش) بالتسلل إلى المملكة وأسرته والإقامة في محافظة صبياء والإقامة بها لمدة سنتين، ومن ثمَّ تعرف بمواطن سعودي (ع، هـ) واتفق معه على استعمال بطاقة أحواله مقابل مبالغ مالية، وقام باستخراج بطاقة أحوال تحمل بيانات (ع، هـ) ولكن بالصورة الشخصية للمتهم (م، ش)وبذلك يكون قد ارتكب تزويراً إلكترونياً في سجلات الحاسب الآلي بالتعاون مع موظفين حسني النية بإدارة الأحوال المدنية، كما استعمل البطاقة في استخراج رخصة قيادة خصوصي من مرور جدة، وجواز سفر من جوازات جدة، وسجل تجاري من فرع وزارة التجارة بجدة، وجميع هذه الأعمال استعمل فيها البطاقة المزورة، بما يعني وقوع جريمة التزوير التقليدية في المحررات، فضلاً عن وقوع جريمة التزوير الإلكتروني بإدخال بيانات مغلوطة إلى سجلات الحاسب الآلي الخاصة بتلك الجهات، بجانب استعمال تلك المستندات المزورة مع علمه بتزويرها.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهم بما نسب إليه في جميع مراحل التحقيق.

٢ ـ ضبط المحررات والوثائق المزورة بحوزته.

٣ ـ المتهم من أرباب السوابق.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، واعترف المتهم بجميع ما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم كرر المتهم اعترافه.

وقد قضت الدائرة الجزائية بديوان المظالم بتوقيع عقوبة حبس المتهم لمدة سنة ونصف من تاريخ توقيفه وتغريمه مبلغ ألف ريال عن جريمة التزوير والاستعمال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات ووثائق إلكترونية رسمية هي استخراج بطاقة أحوال مزورة، واستعمالها في استخراج محررات رسمية مزورة هي رخصة قيادة وجواز سفر وسجل تجاري التي قام بالتوقيع على نماذج استخراجها بالاسم المنتحل في الجواز المزور، بجانب التزوير الإلكتروني بإدخال بيانات غير صحيحة لدى الأحوال المدنية والجوازات ومصلحة السجل التجاري من خلال استعمال بيانات بطاقة الأحوال المزورة.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما

نصت عليه المادة الخامسة والمادة السادسة السابق ذكرها، وقد وقع التزوير بعدما قام المتهم باستخراج البطاقة المزورة، واستعمالها في استخراج رخصة قيادة، وجواز سفر، وسجل تجاري، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة ببطاقة الأحوال من خلال استخراج بطاقة أحوال ببيانات (ع، هـ) سعودي الجنسية، ولكن تحمل صورة (م، ش) يماني الجنسية، فضلاً عن إدخال البيانات المزورة في سجلات الحاسب الآلي الخاص بإدارة المرور لاستخراج رخصة قيادة، وفي سجلات الحاسب الآلي الخاص بالجوازات لاستخراج جواز سفر، وفي سجلات الحاسب الآلي بالسجل التجاري لاستخراج سجل تجاري، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن صورة (م، ش) المثبتة على البطاقة التي تخص (ع، هـ) وكذلك التوقيع باسم (ع، هـ) على نماذج استخراج رخصة قيادة خصوصي، وجواز سفر، وسجل تجاري باستخدام المجاهر الإلكترونية للتأكد من أنها مزورة لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩،

ولمزيد من المعلومات انظر: إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمتـــه، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م،ص ص٣٦٦ـ٣٦٧).

٤ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام بالأحوال المدنية والجوازات وإدارة المرور والسجل التجاري وتسجيل بيانات غير صحيحة بسجلات الحاسب الخاص بهذه الجهات، وتم التعرف على الموظفين الذين قاموا بإدخال البيانات غير الصحيحة (لم يتم عقابهم لحسن نيتهم) من خلال الكود المخصص لكل منهم باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضيـة التاسـعة: رفع مخالفـات بغرض نقل ملكية سـيارة وإعادتها بعد تمام النقل بطريقة غير نظامية

أولاً : نوع القضية

أ ـ تزوير في سجلات الحاسب الآلي بالمرور

ب ـ رقم القضية : ٤١٣/ ٥/ ق لعام ١٤٢٨هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (ر، ج) عريف بشـعبة مرور ينبع، والمدعو (م، ج) عريف بشـعبة مرور ينبع بارتكاب عملية تزوير في سجلات الحاسـب الآلي بشـعبة مـرور محافظة ينبع، حيـث قـام الأول (ر، ج) بعملية تعديـل غير نظامية على ملكية سـيارة مؤقتـاً إلى الثـاني (م، ج) بناء على طلبه لرفـع المخالفـات المرورية عن صاحب السـيارة ثم التجديـد والعودة بها إلى المالـك الأسـاسي، وبذلك تمت الجريمـة. كما قام (أ، ع) وكيل رقيب بشـعبة مرور محافظة ينبع بارتكاب تزوير في سـجلات الحاسـب الآلي بشـعبة مرور محافظة العلا بإجراء عملية تعديل غير نظامية على ملكية عدة سـيارات مؤقتاً من مالكيها الأساسـيين إلى مالكين جدد، ثم أعيدت إلى مالكيها الأساسـيين في نفـس اليوم والسـاعة لكـي يتم رفـع المخالفات عن أصحاب السـيارات الأساسيين، ثم العودة بها إلى ملكيتهم بعد التجديد.

وبعـد ضبـط الإفادات وجمع الاسـتدلالات من قبل مكافحـة التزوير، والحصـول على تقرير الأدلـة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب التقليديـة والإجرائيـة والمادية، تم إرسـاله إلى هيئة الرقابـة والتحقيق لإقامة الدعـوى تجاههـم، واعـترف المتهـمان (ر، ج) و(م، ج) بما نسـب إليهما، بينما

تقدم المتهم الثالث (أ، ع) بمبررات، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم كرر المتهمان (ر، ج) و(م، ج) اعترافهما وأبديا رغبتهما على عدم العودة إلى ما أقدما عليه أبداً.

أما المتهم الثالث (أ، ع) فقد ذكر أن توجيهه يتم من الإدارة، وأن مدير وحدة مرور العلا وجهه بتسجيل معاملات المراجعين لإنهاء إجراءاتهم وعدم تعطيلهم، فضلاً عن حداثة استعمال الحاسب الآلي وقلة الخبرة به، كما أن الاستمارات جددت ولم تثبت في الحاسب الآلي، لأن السيارات التي عليها مخالفات لا يمكن تثبيتها في الحاسب الآلي إلا بعد نقل ملكيتها، وأنه لا مصلحة له إلا تسهيل معاملات المراجعين.

وقد قضت الدائرة الجزائية بديوان المظالم بتوقيع عقوبة الحبس لمدة سنة مع إيقاف التنفيذ ضد كل من المتهم الأول (ر، ج) والمتهم الثاني (م، ج)، بينما قضت ببراءة المتهم الثالث (أ، ع).

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بإدخال بيانات غير صحيحة في سجلات الحاسب الآلي بالمرور بنقل ملكية سيارات مؤقتاً لرفع المخالفات المرورية، ومن ثم إعادة ملكيتها بعد التجديد للمالكين الأصليين.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت

عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام المتهمون بتجديد الاستمارات دون دفع المخالفات المرورية المقررة، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بنقل ملكية السيارات مؤقتاً، لتلافي دفع المخالفات المرورية، ومن ثم إعادتها بعد النقل والتجديد لمالكيها الأصليين أيضاً في سجلات الحاسب الآلي، أي أن الغرض هو التحايل ورفع المخالفات المرورية، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ تمثلت الأساليب الإجرائية في التحقيق مع المتهمين، واحتجازهم طوال فترة التحقيق لمنعهم من محاولة طمس معالم جريمتهم، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٣ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات دخول غير صحيحة بسجلات الحاسب بالمرور من خلال نقل ملكية مؤقت

لرفع المخالفات عن السيارة، ومن ثم إعادة الملكية إلى مالكيها الأصليين بعد التجديد واستخراج الاستمارات، وتم التعرف على الموظفين الذين قاموا بإدخال البيانات غير الصحيحة من خلال الكود المخصص لكل منهم باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م،ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية العاشرة: تغيير مهنة تزويراً في سجلات الحاسب الآلي

أولاً: نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي

ب ـ رقم القضية: ٤٤٦/ ٢٢/ ٥/ ق لعام ١٤٢٤هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (ع، ب) سعودي الجنسية ويعمل برتبة رئيس رقباء صحي في مستشفى الملك عبد العزيز العسكري بتبوك بدفع رشوة مبلغ مالي مقداره (١٥٠٠) ريال للمدعو (ف، ع) لتقديمها إلى موظف الأحوال المدنية بتبوك لتعديل مهنة (ع، ب) من عسكري إلى متسبب في سجلات الحاسب الآلي لكي يتمكن من السفر إلى الخارج، حيث يمنعه

عمله العسكري من ذلك. وفعلاً قام (ف، ع) بدفع المبلغ لموظف الأحوال المدنية، وتم تعديل مهنة المذكور إلى متسبب بدلاً من عسكري في سجلات الحاسب الآلي مع إصدار بطاقة أحوال تثبت ذلك، كما استخدم (ع، ب) الجواز الذي تم تعديل المهنة به بناء على بطاقة الأحوال في السفر خارج المملكة عدة مرات، وهو يعلم بتزوير المهنة، وبذلك وقعت عمليه التزوير الإلكتروني والتقليدي.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهم المصدق شرعاً.

٢ ـ خطاب مدير إدارة شؤون الأفراد بالخدمات الطبية بالقوات المسلحة المذيل بخطاب مدير الأحوال المدنية بأنه قد تم تعديل مهنة المذكور إلى عسكري في حفيظة نفوسه لالتحاقه بالخدمة العسكرية.

٣ ـ ما تضمنته شريحة الحاسب الآلي من أن مهنة المذكور متسبب على الرغم من كونه لا يزال عسكرياً برتبة رئيس رقباء.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، واعترف المتهم بجميع ما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم كرر المتهم اعترافه، وتقدم بتقارير طبية وإجازات مرضية تثبت تعرضه لحادث مروري أسفر عن

إصابات بالعمود الفقري، وأنه بصدد طلب تقرير طبي لإحالته على التقاعد.

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهم لمدة سنة من تاريخ توقيفه وتغريمه مبلغ ثلاثة آلاف ريال مع إيقاف تنفيذ عقوبة السجن نظراً لظروفه الصحية.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي للأحوال المدنية بطريقة غير نظامية، وكذلك تزوير في محررات رسمية هي استخراج بطاقة أحوال مزورة لأنها تحمل مهنة غير المهنة الحقيقية وبدون مسوغ نظامي، واستعمالها في تغيير المهنة بجواز السفر، واستعمال جواز السفر في السفر للخارج بما يخالف اللوائح والأنظمة العسكرية.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام المتهم بتعديل المهنة في البطاقة المزورة، واستعمالها في استخراج بطاقة أحوال بالمهنة الجديدة، وجواز سفر بالمهنة الجديدة، مما يعني وقوع التزوير التقليدي في ضوء التوقيع على النماذج اللازمة لاستخراج هذه المستندات، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بتعديل المهنة من عسكري إلى متسبب، ووقع التزوير التقليدي باستخراج البطاقة التي تحمل مهنة مزورة، واستعمالها في تعديل المهنة بجواز السفر والتوقيع على النماذج بالمهنة الجديدة المزورة، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن المهنة المزورة في بطاقة الأحوال وجواز السفر، وكذلك التوقيع على نماذج واستمارات استخراج بطاقة الأحوال وجواز السفر بالمهنة الجديدة المزورة لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتغيير المهنة تزويراً بسجلات الحاسب

بالأحـوال المدنيـة، وكذلـك في سـجلات الحاسـب بالجـوازات لاسـتخراج جواز بالمهنة المزورة بمعنى إدخال بيانات غير صحيحة بسجلات الحاسـب بالأحوال المدنية والجوازات، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة من خلال الكـود المخصـص له باسـتخدام تقنيات التتبع واسـترجاع المعلومات والحصول على اسـم المسـتخدم من مركز المعلومات الوطني (User name) وهـذا الإجراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأسـاليب المادية في إثبات جرائـم التزوير الإلكتروني (انظر الدراسـة النظـريـة ص ص٦٠ـ٦٤، ولمزيـد مـن المعلومـات انظـر حجـازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبـد المطلـب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضيـة الحاديـة عشرة: إصـدار وكالـة شرعية مزورة في سـجلات الحاسب الآلي بكتابة العدل

أولاً: نوع القضية

أ ـ إصدار وكالة شرعية مزورة

ب ـ رقم القضية: ١٤٠/ ٢٢/ ٥/ ق لعام ١٤٢٤هـ

ثانياً: الوقائع

تتلخـص وقائـع القضيـة في قيـام كل مـن (ت، م) و(ع، ب) و(ع، ن) والمـرأة (ن، هـ) سـعوديي الجنسـية، بتقديم (ن، هـ) لعمـل وكالة شرعية بانتحـال شـخصية (ف، ح) سـعودية الجنسـية لصرف مسـتحقات الضمان

الاجتماعي الخاصة بها؛ وذلك لكونها مريضة ومقعدة ولا تستطيع الحركة.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهمين في جميع مراحل التحقيق بما أقدموا عليه.

٢ ـ ما جاء في خطاب كاتب العدل.

٣ ـ ضبط المحرر المزور.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههم، واعترف المتهمون بجميع ما نسب إليهم، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالتهم إلى الدائرة الجزائية بديوان المظالم كرر المتهمون اعترافاتهم، وأفادوا أنهم فعلوا ذلك بحسن نية وبتفويض شفهي من (ف، ح) المقعدة والتي لا تستطيع الحركة، وأن الوكالة لازمة لصرف مستحقاتها من الضمان الاجتماعي، وتوجه قسم مكافحة التزوير لسؤال (ف، ح) فأفادت بصحة ذلك.

وقد قضت الدائرة الجزائية بديوان المظالم بتوقيع عقوبة حبس المتهمين لمدة سنة من تاريخ توقيفهم ودفع غرامة مالية مقدارها ألف ريال لكل منهم مع إيقاف تنفيذ عقوبة السجن نظراً لحسن نيتهم، وتعذر حضور صاحبة الشأن لكبر سنها وعجزها عن الحركة.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير في محررات رسمية إلكترونية هي استخراج وكالة شرعية في غير حضور الموكلة، بنية استعمالها في صرف مستحقات الموكلة التي لم تحضر إلى الضمان الاجتماعي نظراً لكبر سنها وعجزها عن الحركة، مما تطلب انتحال شخصيتها والتوقيع بدلاً منها (تقليد توقيعها)، بجانب التزوير الإلكتروني في سجلات الحاسب الآلي في كتابة العدل الثانية.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بمجرد انتحال الشخصية والتوقيع بدلاً من (ف، ح) على الأوراق الخاصة بطلب استخراج صك وكالة شرعية، وتوقيع الشهود على ذلك، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات التي تحتوي التوقيع المزور بسجلات الحاسب الآلي، واستعمالها في استخراج صك الوكالة الشرعية، ووقع التزوير التقليدي بالتوقيع على طلب الوكالة الشرعية سواء من منتحلة الشخصية، أومن الشهود، وذلك حسب ما نصت عليه الفقرة

(ب) مـن المادة الرابعة عشرة من نظام مكافحة التزوير السـابق ذكرها.

٢ـ أكـد تقريـر الأدلـة الجنائيـة المثبـت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشـف عـن توقيع (ن، هـ)، وكذلك صورتها والتأكـد أنها ليسـت (ف، ح) لتأكيـد اعترافات المتهمـين، مما يثبت فاعليـة الأسـاليب التقليديـة في إثبـات جريمة التزويـر الإلكتروني (انظـر الدراسـة النظريـة ص ص٥٨ـ٥٩، ولمزيد مـن المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهم طوال فترة التحقيق لمنعهم من محاولة طمس معالم جريمتهم، وهو ما يعرف بالتوقيف الاحـتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكـد تقريـر الأدلـة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب المادية بالدخول على النظام وتسـجيل بيانات غير صحيحة بسـجل الحاسـب الآلي في كتابة العدل، وتـم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة (لم يتم عقابه لحسن نيته) من خلال الكود المخصص له باستخدام تقنيات التتبع واسـترجاع المعلومات والحصول على اسـم المسـتخدم من مركز المعلومات الوطني (User name) وهـذا الإجراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظام، وما قام به من إجراء مما يثبت

فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الثانية عشرة: تزوير محررات مصرفية وكشوفات حسابات بنكية ومعالجة بيانات بالحاسب الآلي

أولاً: نوع القضية

أ ـ تزوير محررات مصرفية.

ب ـ رقم القضية: ٧٣/ ٤/ ق لعام ١٤١٩هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام (ع، غ) سعودي الجنسية ويعمل مديراً لمؤسسة الراجحي للصيرفة بارتكاب تزوير في محررات مصرفية عرفية صادرة عن مؤسسة الراجحي التجارية للصيرفة وهي:

١ـ أوامر الصرف وطلبات السحب لعدد من المودعين والمتعاملين مع المؤسسة، فكان يطلب منهم التوقيع على أوامر الصرف وطلبات السحب وهي خالية، ومن ثم يدون مبالغ مالية غير التي طلبها أصحابها ويستولي على الفارق.

٢ ـ تعديل اسم المودع في أمر إيداع بمبلغ أربعين ألف ريال من (ع، ع) إلى (ع، ج) لسابق أخذه هذا المبلغ من حسابه.

٣ ـ جعل أمر إيداع واقعة كاذبة في صورة واقعة صحيحة، حيث أثبت في

نسخة الإيداع للعميل (ر، ش) المبلغ الحقيقي (٣٠٠٠٠٠) ريال، وفي النسخ لدى المؤسسة (١٠٠٠٠٠) ريال واستولى على الفارق.

٤ـ السحب من كشوفات الحسابات المعالجة آلياً بالحاسب والخاصة ببعض العملاء، ووضع عليها الأرصدة قبل السحب موهماً إياهم صحتها.

٥ ـ إصدار كشف حساب مزور ونسبه صدوره للمؤسسة لأحد العملاء الذي اكتشف وجود نقص في حسابه.

٦ ـ استعمال المحررات سالفة الذكر مع علمه بتزويرها عندما احتج بها أمام مؤسسة الراجحي التجارية للصيرفة مع علمه بتزويرها.

وقد بلغ مجموع المبالغ التي استولى عليها تزويراً في المحررات المصرفية أربعة ملايين ومائتين واثنين وتسعين ألف ريال.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهم بما نسب إليه ومصادقته عليه شرعاً أمام الهيئة.

٢ ـ ضبط بعض المحررات محل التزوير.

٣ ـ أقوال بعض المودعين من تدوينه مبالغ غير التي طلبوها عند طلباتهم السحب وأخذ الفارق.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، تم إرساله إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاهه، واعترف المتهم بجميع ما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم كرر المتهم اعترافاته.

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهم لمدة ثلاث سنوات من تاريخ توقيفه عن جريمة تزوير واستعمال في أوراق مصرفية مع تغريمه مبلغ ثلاثة آلاف ريال، وإلزامه بإعادة مبلغ قدره أربعة ملايين ومائتان واثنان وتسعون ألف ريال لمؤسسة الراجحي التجارية للصيرفة.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير في محررات عرفية عبارة عن أوراق مصرفية، وكشوفات حساب عملائها معالجة آلياً بنية استعمالها في صرف مبالغ إضافية والاستيلاء عليها، وكذلك سحب من حسابات بعض المودعين، وإيهامهم بكشوفات حساب مزورة أنهم هم الذين سحبوا الأموال. والتزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بمجرد تغيير قيمة المبالغ المسحوبة والمودعة، وتغيير كشوفات الحسابات، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

٢ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن توقيعات (ع، غ) بأسماء العملاء لسحب وإيداع الأموال وتحويلها لحسابات بعضهم البعض أو لحسابه الخاص باستخدام المجاهر الإلكترونية لتأكيد اعترافات

المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على سجلات الحاسب بالبنك والقيام بعمليات إيداع وسحب وهمية وإخفاء السجلات الحقيقية لإدارة المراجعة والحسابات، وتم ذلك باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم، مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضيـة الثالثـة عـشرة: تغيـير في سـجلات الحاسـب الآلي الخاصـة بالحضور والانصراف

أولاً : نوع القضية

أ ـ تغيير في سجلات الحضور والانصراف

ب ـ رقم القضية : ٥٤٨/ ٥/ ق لعام ١٤٢٦هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (أ، ح) سـعودي الجنسـية مراقب إنشـاءات بالمسـاهمة مع مجهول في التزوير في محررات رسـمية هي سـجلات الحاسب الآلي بأمانة المدينة المنورة الخاصة بحضور وانصراف منسوبي الأمانة وبلدياتهـا الفرعيـة بإثبـات وقائـع كاذبة في صـورة وقائع صحيحـة بإثبات حضـوره للعمل وهو متغيب عنـه، أي يقوم أحد العاملـين بإثبات حضوره وهو أصلاً متغيب عن العمل.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ـ أقـوال المسـؤولين في بلديـة البيـداء وزمـلاء المتهـم في العمـل بعدم حضوره لمقر العمل.

٢ ـ تراجع الشـاهد (م، س) عن شـهادته لدى الهيئة بحضور المتهم لمقر عمله.

٣ ـ عدم تقديم المتهم دليلاً كافياً على حضوره للعمل يمكن الركون إليه سوى أقوال مرسلة.

٤ ـ ما جاء في خطاب مرجعه ببلدية البيداء.

وبعد ضبط الإفـادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصـول على تقرير الأدلـة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب الإجرائيـة والماديـة، تـم إرسـاله إلى هيئة الرقابـة والتحقيق لإقامـة الدعوى تجاهـه، وأنكـر المتهم جميع ما نسـب إليه، ولذلك طالب ممثـل الادعاء بالهيئة معاقبتـه وفقـاً لأحكام المواد الخامسـة والسادسـة من نظام مكافحـة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائـرة الجزائية بديوان المظالم كرر المتهم إنكاره، وذكر أنـه كان يعمـل خلال الأيـام التي اتهم بالغيـاب فيها في بداية الـدوام ويقوم بجـولات ميدانية حسـب طبيعة عمله، ويعود في نهايـة الدوام لتمرير كارت الدوام حضوراً وانصرافاً في الحاسب الآلي، وقدم المتهم ثلاثة مشاهد تثبت أنه كان يقوم بجولات ميدانية على المسـجد بحي العزيزية بالمدينة المنورة، وأكد المشهد الثاني أن المتهم كان يشرف على التعديلات بالدور الثاني والملحق بناء على طلب مقدم إلى البلدية، والمشـهد الثالث يفيـد أنه كان يقوم بزيارة عمارة والده أثناء جولاته الميدانية.

وقد قضت الدائرة الجزائية بديوان المظالم ببراءة المتهم مما نسب إليه.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضيـة المطروحـة عبـارة عـن تزويـر إلكـتروني باسـتعمال كارت الحضـور والانصراف لتسـجيل حضـور موظف وانصرافـه تزويراً بغـير حضوره الفعلي، واسـتغلال ذلك في قضـاء المصالح الخاصة، وعدم الالتزام بالدوام أو زيارة الأهل والأقارب.

٢ ـ وقع التزوير الإلكتروني نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وهي إثبات أن الموظف متواجد وقت الدوام، وكذلك إثبات وقت انصرافه، أي أنه حضر في الوقت المحدد وانصرف في الوقت المحدد، بالرغم من شهادة رؤسائه وزملائه بعدم تواجده سواء وقت الحضور أو الانصراف، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ تمثلت الأساليب الإجرائية في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، مرجع سابق، ص١٣؛ البشرى، ٢٠٠٠م، مرجع سابق، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات حضور وانصراف (أ، ح) في الموعد المحدد، ولم يتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة، لتعدد المستخدمين ولعدم تخصيص كود لكل فرد مصرح له باستخدام جهاز الحضور والانصراف، مما يحول دون التعرف على اسم المستخدم باستخدام تقنيات التتبع واسترجاع المعلومات من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على

اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الرابعة عشرة: تغيير مهنة تزويراً في سجلات الحاسب الآلي

أولاً: نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي

ب ـ رقم القضية: ٦٢١/ ٢٢/ ٥/ ق لعام ١٤٢٥هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام كل من المدعو (ع، ب) سعودي الجنسية ويعمل برتبة وكيل رقيب في مدرسة المظلات، والمدعو (خ، ب) ويعمل برتبة عريف في الكتيبة الثامنة مشاة بمساعدة (ج، ج) الذي توفي، بالتزوير في سجلات الحاسب الآلي عن طريق تغيير البيانات الرسمية المثبتة في الحاسب الآلي ببيانات مخالفة للواقع بتعديل مهنتهما من عسكري إلى طالب، واستخرجا بطاقة أحوال بالمهنة المعدلة، واستخرجا بناء عليها جواز سفر بنفس المهنة المعدلة وتمكنا من السفر به إلى الخارج عدة مرات دون علم مرجعهما، وهما يعلمان بتزوير المهنة، وبذلك وقعت عمليه التزوير الإلكتروني والتقليدي.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام:

١ ـ اعتراف المتهمين المصدق شرعاً.

٢ ـ وجود الشريحة التي تفيد أن مهنة كل منهما طالب.

٣ ـ ما تضمنته شريحة الحاسب الآلي من أن مهنة المذكورين متسبب على الرغم من كونهما لا يزالان على رأس العمل بمهنة عسكري.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهما إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههما، حيث اعترف المتهمان بجميع ما نسب إليهما، وذكرا أنهما يزوران والديهما المريضين والمقيمين بالأردن، كما ذكر المتهم الأول (ع، ب) أنه متزوج ولديه طفلة، وذكر المتهم الثاني (خ، ب) أن عقد نكاحه قبل سنة وأنهما اللذان يعولان والديهما وطلبا مراعاة ظروفهما، ولذلك طالب ممثل الادعاء العام بالهيئة معاقبتهما وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد تحويلهما إلى الدائرة الجزائية بديوان المظالم كرر المتهمان اعترافاتهما، ونفس المبررات التي تقدما بها في هيئة الرقابة والتحقيق وطالبا بمراعاة ظروفهما، وقد تأكدت الدائرة الجزائية من خلو صحائف سوابقهما من السوابق الجنائية.

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهمين لمدة سنة لكل منهما وتغريمهما مبلغ ألف ريال لكل منهما مع إيقاف تنفيذ عقوبة السجن نظراً لظروف والديهما الصحية، ونظراً لاعترافهما في جميع مراحل التحقيق وتيقن الدائرة الجزائية من تحقق عنصر الردع والزجر لديهما.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي للأحوال المدنية بطريقة غير نظامية، وكذلك تزوير في محررات رسمية هي استخراج بطاقة أحوال مزورة لأنها تحمل مهنة غير المهنة الحقيقية وبدون مسوغ نظامي، واستعمالها في تغيير المهنة بجواز السفر، واستعمال جواز السفر في السفر للخارج بما يخالف اللوائح والأنظمة العسكرية.

٢ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما قام المتهمان بتعديل المهنة في البطاقتين المزورتين من عسكري إلى طالب ، واستعمالها في استخراج بطاقة أحوال بالمهنة الجديدة، وجواز سفر بالمهنة الجديدة، مما يعني وقوع التزوير التقليدي في ضوء التوقيع على النماذج اللازمة لاستخراج هذه المستندات، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

٣ ـ توافرت في الجريمة جميع عناصر الركن المعنوي، حيث اتجهت الإرادة إلى تعديل المهنة في بطاقة الأحوال تزويراً ، واستعمالها في استخراج بطاقة أحوال بمهنة جديدة، واستعمالها في تعديل المهنة بجواز السفر، وترتب عليه إدخال بيانات غير صحيحة في سجلات

الحاسب بالأحوال المدنية والجوازات، وكذلك اتجهت الإرادة إلى التوقيع على النماذج والاستمارات الخاصة بتعديل المهنة، وهنا تتوافر أيضاً أركان التزوير المعنوي بجعل واقعة مزورة في صورة واقعة صحيحة، أو جعل واقعة غير معترف بها في صورة واقعة معترف بها (انظر الدراسة النظرية ص٧٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص١٤٢).

٤ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن البطاقة الصادرة بالمهنة المزورة، وكذلك التوقيعات على الاستمارات والنماذج التي تشتمل المهنة المزورة لاستخراج جواز سفر واستخدامه في السفر للخارج، باستخدام المجاهر الإلكترونية للتأكد من مطابقتها وتأكيد اعترافات المتهمين، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٥ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهما طوال فترة التحقيق لمنعهما من محاولة طمس معالم جريمتها، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٦ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية

بالدخـول عـلى النظـام وتغيير مهنة دون مسـوغ نظامي بسـجلات الأحوال المدنية ـ وكذلك بسجلات الحاسب بالجوازات لاستخراج جـواز بالمهنة الجديدة، وتم التعرف عـلى الموظف الذي قام بإدخال البيانـات غـير الصحيحة من خلال الكود المخصص له باسـتخدام تقنيات التتبع واسـترجاع المعلومات والحصول على اسم المستخدم مـن مركز المعلومات الوطنـي (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظـام، ومـا قـام به مـن إجراء ممـا يثبت فاعليـة الأسـاليب المادية في إثبـات جرائـم التزويـر الإلكـتروني (انظر الدراسـة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومـات انظر حجـازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبـد المطلـب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية الخامسة عشرة: تغيير مهنة تزويراً في سجلات الحاسب الآلي لتيسير إجراءات الاستقدام

أولاً: نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي.

ب ـ رقم القضية: ٤٨٢/ ٥/ ق لعام ١٤٢٧هـ.

ثانياً: الوقائع

تتلخـص وقائع القضية في قيام المدعو (م، ذ) سـعودي الجنسـية ويعمل برتبة رئيس رقباء بجوازات ينبع، باستقبال طلبات من كل من (ف، ع) و(ط، ن) ويحمل كل منهما الجنسية السعودية، لتعديل مهنة الأجانب لتيسير استقدام

أسرهم، وبلغ عدد الذين تم تعديل مهنهم بطريقة غير نظامية وبدون مسوغ نظامي (١٣٦) عملية، وقد تقدم كل من المتهمين (ج، س)، و(ع، ج)، و(م، ف)، و(أ، غ)، و(م، ع) من الجنسية الباكستانية بطلبات لتغيير مهنهم بطريقة غير نظامية وبدون إرفاق مستندات رسمية لتغيير المهنة، وفعلاً قام (م، ذ) بتغيير مهنهم بعد الحصول على مبالغ مالية، وقد استعمل (ج، س)، و(ع، ج)، و(م، ف)، و(أ، غ)، و(م، ع) الإقامات المعدلة المهنة وهم يعلمون أنها تم تغييرها بطريقة غير نظامية، كما استفاد كل من (أ، غ) و(م، ع) من هذا التغيير في استقدام أسرتيهما من الباكستان، أي أنهما استعملا المحررات المزورة.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ خطاب مدير عام مركز المعلومات الوطني الذي يؤكد قيام (م، ذ) بتعديل مهن (١٣٦) أجنبياً باستعمال الرقم السري الخاص به للدخول على النظام بالحاسب الآلي بالجوازات.

٢ ـ خطاب مدير جوازات منطقة الرياض بأن الختم الخاص بتعديل المهن على أساس الإقامات العائدة للعمال الذين تم تعديل مسميات مهنهم غير مطابق للنموذج الأصلي.

٣ ـ إفادة المتهمين الثاني والثالث باستقبال طلبات تعديل مسميات مهن العمال الأجانب في مكتبهما.

٤ـ أقوال المتهمين (ج، س)، و(ع، ج)، و(م، ف)، و(أ، غ)، و(م، ع) من أنهم تقدموا لمكاتب خدمات مختلفة لتعديل مهنهم الحقيقية دون الرجوع للجوازات لتقديم طلبات تعديل المهنة مما يدل على أن التغيير تم بطريقة غير نظامية.

٥ ـ خطاب جوازات ينبع المتضمن أن جميع عمليات تعديل المهن للعمال المذكورين ليس لها أي مستند نظامي.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههم، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة والتاسعة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالتهم إلى الدائرة الجزائية بديوان المظالم أنكر المتهم الأول (م، ذ) جميع ما نسب إليه، وبرر تعديل المهن باستعمال رقمه السري للدخول على النظام بأنه يترك أحياناً جهاز الحاسب الآلي الذي يعمل عليه مفتوحاً أثناء قضاء بعض المهام، وربما أن أحداً قد دخل على النظام وعدل المهن، وذكر المتهمان (أ، غ)، و(م، ع) أنهما راجعا مكتب خدمات لتعديل المهنة بحيث تسمح باستقدام عوائلهما من الباكستان، وتقاضى المكتب من كل منهما (١٥٠٠) ريال نظير تغيير المهنة، فضلاً عن تسلم إقامتيهما وجوازي سفريهما، وبعد عدة أيام سلمهما المكتب الإقامة وجوازي السفر وبهما تعديل المهنة إلى فني كهربائي، وبناء عليه قاما باستقدام عائلتيهما، وأنكر المتهمان الثاني والثالث (ط، ن) أي علاقة لهما بالموضوع.

وقد قضت الدائرة الجزائية بديوان المظالم بحبس المتهم الأول (م، ذ) سنة واحدة عن جريمة تزوير في سجلات الحاسب الآلي بتعديل مهنة دون مسوغ نظامي، وحبس المتهمين (ج، س)، و(أ، غ)، و(م، ع) سنة واحدة عن جريمة التزوير والاستعمال مع تغريم كل منهم ألف ريال، والحكم غيابياً

بإدانة المتهمين (ع، ج) و(م، ف) عن جريمة التزوير والاستعمال وحبسهما سنة واحدة مع تغريم كل منهما ألف ريال، وبراءة المتهمين (ف، ع)، و(ط، ن) من التهمة المنسوبة إليهما.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي بالجوازات بطريقة غير نظامية من خلال تعديل المهنة دون أية مستندات نظامية، وكذلك تزوير في محررات رسمية هي تعديل المهنة في الإقامة وفي جواز السفر دون مسوغ نظامي، واستعمالها في استقدام الأسرة، أي الاستعمال بعد التزوير.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة التاسعة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما تم الدخول على سجلات الحاسب الآلي من قبل (م، ذ) وتغيير المهنة دون مسوغ قانوني، ومن ثم تعديل المهنة في الإقامة وجواز السفر، وكذلك تقديم طلبات تغيير المهنة، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بتعديل المهنة للمقيمين للتمكن من استقدام الأسرة دون

مسـوغات نظامية، وكذلك بإدخال بيانات بحاسب الجوازات لاسـتخراج جواز سـفر بمهنة مزورة، ووقع التزوير التقليدي باستخراج الإقامة والجواز اللذين يحملان مهنة مزورة ، وذلك حسـب ما نصت عليه الفقرة (ب) من المـادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ ـ أكـد تقريـر الأدلـة الجنائيـة المثبت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشف عن تغيير المهنة في الإقامات والجوازات دون مسـوغ نظامي، ممـا يثبت فاعلية الأسـاليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيـد من المعلومـات انظـر : إدارة الأدلة الجنائيـة، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهم طوال فترة التحقيق لمنعهم من محاولة طمس معالم جريمتهم، وهو ما يعرف بالتوقيف الاحـتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتغيير المهنة في سجلات الجوازات دون مسوغ نظامـي، وتم التعرف عـلى الموظف الذي قام بإدخـال البيانات غير الصحيحة من خلال الكود المخصـص له باسـتخدام تقنيات التتبع واسـترجاع المعلـومـات والحصول على اسـم المسـتخدم من مركز

المعلومـات الوطنـي (User name) وهذا الإجـراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظام، ومـا قـام به مـن إجراء مما يثبـت فاعلية الأسـاليب الماديـة في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيـد من المعلومـات انظـر ازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلـب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنـزي، ٢٠٠٣م، ص١٠٢).

القضية السادسة عشرة: تغيير مهنة تزويراً في سجلات الحاسب الآلي بالجوازات

أولاً : نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي

ب ـ رقم القضية : ٣٨/ ٤/ ق لعام ١٤٢٠هـ.

ثانياً: الوقائع

تتلخـص وقائع القضيـة في قيام المدعو (ع، م) يماني الجنسـية و(س، غ) سعودي الجنسـية بدفع مبلغ (٥٠٠) ريال على سبيل الرشوة إلى الجندي (م، ح) بـإدارة جوازات منطقة جيزان لتعديل مهنـة (ع، م) في الإقامة من عامل تربية مواشي إلى عامل، بينما قام (أ، ش) بالتوسط بين (ع، م) و(س، غ) لدفع الرشـوة للجندي (م، ح) الذي قام فعلاً بتعديل المهنة في الحاسـب الآلي دون مسـوغ نظامي، وبهـذا تقع الجريمة بمسـاهمة كل مـن (ع،م) و(س،غ) و(أ، ش) في دفع الرشوة وقيام (م، ح) بتغيير المهنة دون مسوغ نظامي.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعترافات المتهم الأول (ع، م) والثاني (أ، ش) بتحقيقات مكافحة التزوير بالجوازات المصدق عليها شرعاً.

٢ ـ ما ثبت من مطالعة رخصة الإقامة محل التحقيق من وجود تغيير المهنة بالصفحة.

٣ ـ محضر إثبات الواقعة من قبل أفراد مكافحة التزوير بالجوازات، حيث تعرف المتهم الرابع (م، ح) لدى عرضه عليه ضمن مجموعة من أفراد الجوازات وأصر على أنه من قام بتعديل المهنة في رخصة الإقامة.

٤ ـ ما تضمنه الإقرار الخطي للمتهم (ع، م) أمام مكافحة التزوير بالجوازات المرفق بالأوراق من اعتراف أنه تقدم للشرطة والجوازات مدعياً فقدان رخصة إقامته حتى لا ينكشف ما تم من تعديل في رخصة إقامته.

٥ ـ أقوال المتهم الثالث أنه كان يرغب في تعديل مهنة مكفوله، ولم يتمكن بالطرق النظامية.

٦ ـ مصلحة المتهم الثالث في التزوير لعمله مع كفيله بغير المهنة القادم من أجلها.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههم، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة والتاسعة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالتهم إلى الدائرة الجزائية بديوان المظالم ذكر المتهم الأول (ع، م) أنه دفع المبلغ كرسوم للتغيير بطريقة نظامية، ولم يعلم بالتغيير غير النظامي إلا بعد القبض عليه وأنه تسلم المبلغ من الكفيل (س، غ) وسلمه للجندي (م، ح).

وقد قضت الدائرة الجزائية بالديوان بحبس المتهم الأول (ع، م) يماني الجنسية والمتهم الثاني (أ، ش) يماني الجنسية سنة واحدة عن جريمة التزوير مع تغريم كل منهما ألف ريال، وعدم إدانة المتهم (س، غ) سعودي الجنسية، وعدم إدانة المتهم (م، ح) سعودي الجنسية.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي بالجوازات بطريقة غير نظامية من خلال تعديل المهنة دون أية مستندات نظامية، وكذلك تزوير في محررات رسمية هي تعديل المهنة في الإقامة.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة التاسعة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعدما تم الدخول على سجلات الحاسب الآلي من قبل (م، ح) وتغيير المهنة دون مسوغ قانوني، ومن ثم تعديل المهنة في الإقامة وجواز السفر، وكذلك تقديم طلبات تغيير المهنة، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر

الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بتعديل المهنة دون مسوغات نظامية، وكذلك بإدخال بيانات بحاسب الجوازات لاستخراج برنت بالمهنة المزورة، ووقع التزوير التقليدي باستخراج الإقامة التي تحمل المهنة المزورة، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن إقرار خطي للمتهم (ع، م) يدعي فيه فقدان إقامته ورغبته في استخراج إقامة جديدة لكي لا ينكشف التزوير في الإقامة القديمة، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتغيير المهنة للمتهم (ع، م) بسجلات الحاسب بالجوازات، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية السابعة عشرة: تغيير مهنة تزويراً في سجلات الحاسب الآلي

أولاً : نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي مقترناً بالرشوة

ب ـ رقم القضية : ٢٢/ ٥/ ق لعام ١٤٢٤هـ

ثانياً: الوقائع

تتلخص وقائع القضية في قيام المدعو (م، ع) سعودي الجنسية ويعمل بإدارة الأحوال المدنية بتبوك بأخذ ثلاثة آلاف ريال من (ف، م) سعودي الجنسية، ومبلغ خمسة عشر ألف ريال من (إ، ع) لتعديل مهن أشخاص في الحاسب الآلي من عسكريين إلى متسببين. وقد قام (م، ع) بارتكاب تزوير

في محررات رسمية وسجلات الحاسب الآلي بتعديل مهن بعض الأشخاص بطريقة غير مشروعة ودون مسوغ نظامي واستعمال البعض لهذه التعديلات في السفر إلى خارج المملكة، وبذلك تقع جريمة التزوير والاستعمال.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف (م، ع) المصدق شرعاً بأنه قام بتعديل مهنة (ف، م) من عسكري إلى متسبب بناء على توسط (إ، ع) وتقاضي مبلغ ثلاثة آلاف ريال، وأنه قام بتعديل مهن بعض الأشخاص الذين توسط لهم المتهم الثالث (إ، ع).

٢ ـ اعتراف المتهم الثالث (إ، ع) بأنه اتفق مع (م، ع) على إحضار عدة أشخاص ليغير مهنهم من عسكريين إلى متسببين مقابل مبالغ مالية.

٣ ـ ما تضمنته شريحة الحاسب الآلي من تعديل مهنة المتهم الثاني (ف، م) من عسكري إلى متسبب، وسافر عدة مرات بموجب هذا التعديل.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههم، واعترف المتهم بجميع ما نسب إليه، ولذلك طالب ممثل الادعاء بالهيئة معاقبته وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالته إلى الدائرة الجزائية بديوان المظالم كرر المتهمون اعترافاتهم.

وقد قضت الدائرة الجزائية بتوقيع عقوبة حبس المتهمين الثلاثة لمدة سنة من تاريخ توقيفهم وتغريم كل منهم مبلغ ألف ريال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي للأحوال المدنية بطريقة غير نظامية، وكذلك تزوير في محررات رسمية هي استخراج بطاقة أحوال مزورة لأنها تحمل مهنة غير المهنة الحقيقية وبدون مسوغ نظامي، واستعمالها في تغيير المهنة بجواز السفر، واستعمال جواز السفر في السفر للخارج بما يخالف اللوائح والأنظمة العسكرية.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها ، وقد وقع التزوير بعدما قام المتهم بتعديل المهن في البطاقات المزورة، واستعمالها في استخراج بطاقات أحوال بالمهنة الجديدة، وجواز سفر بالمهنة الجديدة، مما يعني وقوع التزوير التقليدي في ضوء التوقيع على النماذج اللازمة لاستخراج هذه المستندات، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بتعديل المهنة من عسكري إلى متسبب، ووقع التزوير التقليدي باستخراج البطاقة التي تحمل مهنة مزورة، واستعمالها في تعديل

المهنة بجواز السفر والتوقيع على النماذج بالمهنة الجديدة المزورة السابق ذكرها.

٢ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن بطاقات الأحوال بالمهن المعدلة دون مسوغ نظامي من عسكريين إلى متسببين، وكذلك فحص التوقيعات على نماذج واستمارات استخراج جواز سفر بالمهنة الجديدة باستخدام المجاهر الإلكترونية لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر: إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهم، واحتجازه طوال فترة التحقيق لمنعه من محاولة طمس معالم جريمته، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتعديل مهنة دون مسوغ نظامي من عسكري إلى متسبب، فضلاً عن التزوير في سجلات الحاسب الآلي باستخدام جوازات سفر بالمهنة المعدلة تزويراً، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على

اسـم المسـتخدم من مركز المعلومات الوطنـي (User name) وهذا الإجـراء يتبـع في الجهـات الحكوميـة للتعرف على اسـم المسـتخدم ووقـت اسـتخدامه للنظام، ومـا قام به مـن إجراء مما يثبـت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظريـة ص ص٦٠ـ٦٤، ولمزيـد مـن المعلومات انظـر حجـازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Ara-biat, 2002؛ العنزي، ٢٠٠٣م،، ص١٠٢).

القضية الثامنة عشـرة: إضافـة زوجـة إلى إقامـة زوجـها تزويـراً فـي سجلات الحاسب الآلي

أولاً : نوع القضية

أ ـ إضافة زوجة إلى إقامة زوجها تزويراً

ب ـ رقم القضية : ٩٩٠/ ٥/ ق لعام ١٤٢٨هـ

ثانياً: الوقائع

تتلخـص وقائـع القضية في توسـط (ع، ح) سـوداني الجنسـية و(ع، م) سوداني الجنسية لدى (د، ج) سعودي الجنسية ويعمل جندي أول بجوازات الرياض بغرض تعديل الهدف من قدوم زوجة (ذ، ب) باكستاني الجنسية من قـدوم للعمـرة إلى قدوم لمرافقة الزوج، وإضافتها عـلى إقامته، مما ترتب عليه تزوير في محررات رسـمية هي سـجلات الحاسـب الآلي، بجانب اسـتخراج رخصة إقامة مزورة.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ـ اعتراف المتهمين (ذ، ب) و(ع، ح) و(ع، م) في جميع مراحل التحقيق.

٢ ـ وجود رقم الكود الخاص بالمتهم الرابع (د، ج) على التعديل في رقم الدخول والمدون على جواز سفر زوجة المتهم الثاني.

٣ ـ وجود قضية أخرى للمتهم الرابع مازالت في هيئة الرقابة والتحقيق عـن المتهـم الرابع (د، ج) بإضافة زوجـة إلى إقامة زوجها وتعديل الغرض من قدومها من عمرة إلى إضافة مع زوجها.

وبعـد ضبـط الإفادات وجمع الاسـتدلالات من قبل مكافحـة التزوير، والحصـول على تقرير الأدلـة الجنائية المثبت لواقعة التزوير باتباع الأسـاليب التقليدية والإجرائية والمادية، تم إرسـالهم إلى هيئـة الرقابة والتحقيق لإقامة الدعـوى تجاههم، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسـة والسادسـة والتاسـعة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعـد إحالتهم إلى الدائـرة الجزائية بديوان المظالم أفـاد المتهم الأول (ذ، ب) أن (ع، م) طلب منه أن يسـاعده في اسـتخراج إقامة لزوجة المتهم الأول (ع، ح) التـي دخلـت المملكة بتأشـيرة عمـرة، فاتصل عـلى (خ، ش) الذي طلب ثمانية آلاف وخمسـمائة ريال، وأخذ جواز السفر والإقامة والنقود، وتم اسـتلامه بعد شـهرين بعد إضافة الزوجة على جواز السـفر والإقامة، ولكن (ع، م) أبلـغ (ذ، ب) أن الإقامـة مـزورة وطالبه برد النقـود، وطلب منه (ذ، ب) أن يرد النقود بالتقسـيط على شـهور، واتصل على (خ، ش) لكنه لم يرد، وأنـه كان مجرد وسـيط. وذكر المتهم الثـاني (ع، ح) أنه ذهب لمكتب خدمات وقابل (ع، م) الذي أفاده بإمكانية تحويل الغرض من القدوم وإضافة الزوجة من قادمة للعمرة إلى إقامة نظامية من خلال المكتب في الرياض، واتفقوا على

قيمة الأتعاب (٨٥٠٠) ريال واستلم جواز السفر والإقامة، وبعد شهرين أحضرهما، ولكنه فوجىء بأنها مزوران بعد مراجعته لمكتب خدمات لتجديد الإقامة، فقام بإبلاغ جوازات المدينة، ولم يعلم مطلقاً بالتزوير وبمجرد علمه سارع بالإبلاغ، وأنه عندما قدم أوراقه للمكتب كان يقصد تصحيح الوضع وليس ارتكاب التزوير. ولم يحضر المتهم الثالث (ع، م)، أما المتهم الرابع (د، ج) فأنكر قيامه بتزوير بيانات بالحاسب الآلي بالجوازات ولا في جواز سفر وإقامة المتهم الثاني (ع، ح)، وأفاد بصدور حكم بعدم إدانته في قضية مماثلة.

وقد قضت الدائرة الجزائية بإدانة المتهم (ذ، ب) باكستاني الجنسية بالتزوير وعقابه بالحبس لمدة سنة واحدة وتغريمه مبلغ ألف ريال مع إيقاف عقوبة السجن وعدم إدانته بجريمة الاستعمال. وبراءة المتهمين (ع، ح) و(د، ج). وإدانة المتهم (ع، م) بسجنه سنة واحدة مع تغريمه بمبلغ ألف ريال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير في سجلات الحاسب الآلي للجوازات بطريقة غير نظامية وذلك بتغيير غرض القدوم للزوجة من قادمة للعمرة إلى إقامة بإضافتها لإقامة زوجها، وكذلك تزوير في محررات رسمية هي استخراج تأشيرة إقامة مزورة وبدون مسوغ نظامي.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة والمادة التاسعة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بوضع تأشيرة مزورة على الإقامة والجواز بإضافة الزوجة، فالتزوير

يقـع بتغيير الحقيقة في محرر مكتـوب وموجود في الأصل (انظر الدراسـة النظرية ص ص٥١ـ٥٢؛ ولمزيد مـن المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزويـر الإلكـتروني وقع نتيجـة إدخال بيانـات غير صحيحة في ذاكـرة الحاسـب الآلي، وذلـك مـن خـلال إدخـال البيانات الخاصـة بتغيـير الغرض من القدوم مـن أداء العمرة إلى الإقامة مع زوجها، ووقع التزوير التقليدي باسـتخراج التأشـيرة التي تتضمن الإقامة مع الزوج سـواء في الإقامة أو في جواز السـفر، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكـد تقريـر الأدلـة الجنائيـة المثبـت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشـف عن صـورة زوجة (ذ، ب) المضافة إلى إقامته وكذلك الأختام المستخدمة التي اتضح أنها مزورة باستخدام المجاهـر الإلكترونيـة لتأكيـد اعترافـات المتهـم، ممـا يثبـت فاعليـة الأسـاليب التقليديـة في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر: إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهم طـوال فترة التحقيق لمنعهم مـن محاولة طمس معالم جريمتهم، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام من قبل (د، ج) وتغيير الهدف من القدوم من أداء العمرة إلى الإقامة مع الزوج بسجلات الحاسب بالجوازات، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية التاسعة عشرة: تزوير صكوك حصر إرث في سجلات كتابة العدل وإثبات نسب في سجلات الحاسب بالأحوال تزويراً

أولاً : نوع القضية

أ ـ تزوير صكوك حصر إرث وسجلات الحاسب بالأحوال.

ب ـ رقم القضية : ١٦٤/ ٤/ ق لعام ١٤١٩هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في (ع، هـ) سعودي الجنسية، و(ع، ن) يماني

الجنسية، و(ج، ح) يماني الجنسية، و(ح، ح) يماني الجنسية ساهموا مع موظفين حسني النية في محكمة محافظة الحرث بمنطقة جازان في تزوير محررين رسميين بإثبات وقائع وأقوال كاذبة في صورة واقعة صحيحة من خلال ادعاء وفاة شخص يدعى (ع، هـ) وأن ورثته (ف، هـ) وأولاده (م، ع، ح، ع، أ، س) لتمكين أصحاب الأسماء الوهمية من الحصول على الجنسية السعودية استناداً إلى صكي حصر الإرث.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهمين بما نسب إليهم في التحقيقات المصدقة شرعاً.

٢ ـ ضبط المحررات المزورة بحوزة المتهمين.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة الدعوى تجاههم، ولذلك طالب ممثل الادعاء العام بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعد إحالتهم إلى الدائرة الجزائية بديوان المظالم كرر المتهمون اعترافاتهم.

وقد قضت الدائرة الجزائية بإدانتهم عن جريمة التزوير بحبس كل منهم سنة واحدة مع دفع غرامة مالية مقدارها ألف ريال.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير في سجلات

الحاسب الآلي بكتابة العدل، وكذلك تزوير في محررات رسمية هي استخراج صك شرعي مزور، واستعمالها في استخراج بطاقات أحوال للمنسوبين تزويراً بأنهم ورثة سعوديون.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسة والمادة السادسة من نظام مكافحة التزوير السابق ذكرها، وقد وقع التزوير بعد الإدلاء بأقوال كاذبة وتسجيلها لدى كاتب العدل، وإدخالها على سجلات الحاسب الآلي لاستخراج الصك الشرعي الوهمي، بغرض استعماله في استخراج هويات سعودية عبارة عن بطاقات أحوال، فالتزوير يقع بتغيير الحقيقة في محرر مكتوب وموجود في الأصل (انظر الدراسة النظرية ص ص٥١ـ٥٢؛ ولمزيد من المعلومات انظر العريان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وكذلك من خلال إدخال البيانات الخاصة باستخراج صك حصر إرث وهمي، واستعماله في استخراج بطاقات الأحوال وإثبات أنهم سعوديون في سجلات الأحوال. ووقع التزوير التقليدي باستخراج الصكوك الوهمية، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب التقليدية من خلال الكشف عن توقيعات المتهمين على أوراق استخراج صك حصر الإرث، فضلاً عن إدلائهم بأقوال كاذبة للقاضي في كتابة العدل، بجانب التوقيع على الأوراق والمستندات

والنماذج الخاصة باستخراج بطاقات الأحوال باستغلال صك حصر الإرث، وذلك باستخدام المجاهر الإلكترونية للتأكد من التوقيعات، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٥٨ـ٥٩، ولمزيد من المعلومات انظر : إدارة الأدلة الجنائية، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهم طوال فترة التحقيق لمنعهم من محاولة طمس معالم جريمتهم، وهو ما يعرف بالتوقيف الاحتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبات جريمة التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٥ـ٦٨، ولمزيد من المعلومات انظر : العريان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات غير صحيحة بسجلات الحاسب بكتابة العدل، وتم التعرف على الموظف الذي قام بإدخال البيانات غير الصحيحة (لم يتم عقابه لحسن نيته) من خلال الكود المخصص له باستخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسم المستخدم من مركز المعلومات الوطني (User name) وهذا الإجراء يتبع في الجهات الحكومية للتعرف على اسم المستخدم ووقت استخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأساليب المادية في إثبات جرائم التزوير الإلكتروني (انظر الدراسة النظرية ص ص٦٠ـ٦٤، ولمزيد من المعلومات انظر حجازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبد المطلب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

القضية العشرون: تغيير مهنة تزويراً في سجلات الحاسب الآلي

أولاً : نوع القضية

أ ـ تغيير مهنة تزويراً في سجلات الحاسب الآلي.

ب ـ رقم القضية : ٦٠/ ٢٢/ ٥/ ق لعام ١٤٢٣هـ.

ثانياً: الوقائع

تتلخص وقائع القضية في قيام كل من (ي، خ) سعودي الجنسية ويعمل بالأحوال المدنية بمحافظة تيماء، و(ط، م) سعودي الجنسية ويعمل بالأحوال المدنية بمحافظة خيبر، بتقاضي رشوة مقابل تغيير مهن العسكريين إلى متسببين لتمكينهم من السفر إلى الخارج، حيث ارتكاب تزوير في سجلات الحاسب الآلي بالأحوال المدنية بتعديل مهن المتهمين من الثالث حتى الثاني عشر بطريقة غير مشروعة دون اتباع الإجراءات النظامية من عسكريين إلى متسببين، وزودا المذكورين بشرائح من الحاسب الآلي بعد تعديل مهنهم، مما مكنهم من استخراج جوازات سفر والسفر بها خارج البلاد مخالفين التعليمات العسكرية.

وأهم الأدلة التي استندت عليها هيئة الرقابة والتحقيق لتوجيه الاتهام :

١ ـ اعتراف المتهمين المصدق شرعاً.

٢ ـ ثبوت استعمال بعضهم للمحررات المزورة والاحتجاج والسفر بها.

وبعد ضبط الإفادات وجمع الاستدلالات من قبل مكافحة التزوير، والحصول على تقرير الأدلة الجنائية المثبت لواقعة التزوير باتباع الأساليب التقليدية والإجرائية والمادية، تم إرسالهم إلى هيئة الرقابة والتحقيق لإقامة

الدعـوى تجاههـم، واعترف المتهمون بجميع ما نسـب إليـه، ولذلك طالب ممثل الادعاء بالهيئة معاقبتهم وفقاً لأحكام المواد الخامسة والسادسة من نظام مكافحة التزوير وقرار مجلس الوزراء رقم ٢٢٣ لسنة ١٣٩٩هـ.

وبعـد إحالتهـم إلى الدائـرة الجـزائيـة بديـوان المظـالم كـرر المتهمـون اعترافاتهم.

وقـد قضت الدائـرة الجزائية بتوقيع عقـــوبات تتراوح ما بين السـجن والغرامة.

ثالثا : تحليل مضمون القضية

بدراسة القضية اتضح ما يلي :

١ـ القضية المطروحة عبارة عن تزوير إلكتروني بتغيير بيانات في سجلات الحاسب الآلي للأحوال المدنية بطريقة غير نظامية، وكذلك تزوير في محررات رسمية هي استخراج بطاقة أحوال مزورة لأنها تحمل مهنة غير المهنة الحقيقية وبدون مسـوغ نظامي، واسـتعمالها في تغيير المهنة بجواز السـفر، واستعمال جواز السفر في السـفر للخارج بما يخالف اللوائح والأنظمة العسكرية.

أ ـ التزوير في الوثائق الرسمية والمحررات الرسمية حسب ما نصت عليه المادة الخامسـة والمادة السادسـة من نظام مكافحة التزوير السـابق ذكرهـا ، وقـد وقـع التزوير بعدما قـام المتهـم بتعديل المهـن في البطاقـات المزورة، واسـتعمالها في اسـتخراج بطاقات أحـوال بالمهنة الجديدة، وجواز سـفر بالمهنة الجديـدة، مما يعني وقـوع التزوير التقليـدي في ضوء التوقيع على النـماذج اللازمة لاسـتخراج هـذه المسـتندات، فالتزويـر يقع بتغيـير الحقيقة في

محـرر مكتوب وموجود في الأصل (انظر الدراسـة النظرية ص ص٥١ـ٥٢؛ ولمزيـد مـن المعلومات انظر العريـان، محمد علي، مرجع سابق، ص ص١٣٨ـ١٤٠).

ب ـ التزوير الإلكتروني وقع نتيجة إدخال بيانات غير صحيحة في ذاكرة الحاسب الآلي، وذلك من خلال إدخال البيانات الخاصة بتعديل المهنة من عسكري إلى متسبب، ووقع التزوير التقليدي باستخراج البطاقة التي تحمل مهنة مزورة، واستعمالها في تعديل المهنة بجواز السفر والتوقيع على النماذج بالمهنة الجديدة المزورة، وذلك حسب ما نصت عليه الفقرة (ب) من المادة الرابعة عشرة من نظام مكافحة التزوير السابق ذكرها.

٢ـ أكـد تقريـر الأدلـة الجنائيـة المثبـت لواقعـة التزوير اتباع الأسـاليب التقليدية من خلال الكشـف عن بطاقات الأحـوال التي تم تعديل المهنة بها تزويراً دون مسـوغ نظام، وإفادات الجهات العسـكرية بأن المذكورين عسـكريون وعلى رأس العمل برتب عسـكرية، وكذلك مضاهـاة التوقيعات عـلى النماذج والاسـتمارات لاسـتخراج جواز سـفر بالمهنة المعدلة تزويراً ودون مسـوغ نظامي يسـتوجب تعديلها لتأكيد اعترافات المتهم، مما يثبت فاعلية الأساليب التقليدية في إثبات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظريـة ص٥٨ـ٥٩، ولمزيـد من المعلومـات انظـر : إدارة الأدلة الجنائيـة، ٢٠٠٩م، ص ص١ـ٢).

٣ـ أما الأساليب الإجرائية فتمثلت في التحقيق مع المتهمين، واحتجازهم طوال فترة التحقيق لمنعهم من محاولة طمس معالم جريمتهم، وهو ما

يعرف بالتوقيف الاحـتياطي، مما يثبت فاعلية الأساليب الإجرائية في إثبـات جريمـة التزوير الإلكـتروني (انظر الدراسـة النظرية ص ص٦٥ـ٦٨، ولمزيـد مـن المعلومـات انظـر : العريـان، ٢٠٠٤م، ص١٣؛ البشرى، ٢٠٠٠م، ص ص٣٦٦ـ٣٦٧).

٤ ـ أكد تقرير الأدلة الجنائية المثبت لواقعة التزوير اتباع الأساليب المادية بالدخول على النظام وتسجيل بيانات دخول غير صحيحة بسجلات الحاسـب بالأحوال وكذلـك بالجوازات من خـلال تغيير المهنة من عسـكريين إلى متسـببين، واسـتخدام البطاقـة المزورة في اسـتخراج جواز سـفر بالمهنة المعدلة ـ أي التزوير في سـجلات الحاسـب الآلي بالجـوازات، وتم التعـرف على الموظف الذي قـام بإدخال البيانات غـير الصحيحـة سـواء في الأحـوال أو في الجـوازات مـن خـلال الكود المخصص له باسـتخدام تقنيات التتبع واسترجاع المعلومات والحصول على اسـم المسـتخدم من مركز المعلومات الوطني (User name) وهـذا الإجراء يتبع في الجهات الحكومية للتعرف على اسـم المسـتخدم ووقت اسـتخدامه للنظام، وما قام به من إجراء مما يثبت فاعلية الأسـاليب المادية في إثبات جرائـم التزوير الإلكتروني (انظر الدراسـة النظريـة ص ص٦٠ـ٦٤، ولمزيـد مـن المعلومـات انظـر حجـازي، ٢٠٠٥م، ص ص٣٦ـ٦٥؛ عبـد المطلـب، ٢٠٠١م، ص٢١٩؛ Arabiat, 2002؛ العنزي، ٢٠٠٣م، ص١٠٢).

يتضح مما سبق أن الأساليب التقليدية والأساليب الإجرائية والأساليب المادية لمكافحة التزوير الإلكتروني ذات فاعلية كبيرة في إثبات جريمة التزوير الإلكتروني، ولكن هناك ثغرة، فعدم اقتناع الجهات القضائية بوسائل الإثبات

الإلكترونية كالتعرف على مرتكب جريمة التزوير الإلكتروني من خلال اسم المستخدم الذي يتم معرفته من خلال مركز المعلومات الوطني باستخدام تقنيات التتبع واسترجاع المعلومات التي أثبتت فاعلية في معرفة اسم المستخدم الذي قام بإجراء التزوير أو التعديل بحسن نية في ضوء معرفة رقم المستخدم المصرح له بالدخول على النظام، حيث يمكن تحديد وقت إجراء التغيير ورقم المستخدم بدقة، وتبقى إدعاءات بعض الأفراد بنسيان الجهاز يعمل أثناء قضاء بعض المهام من المبررات التي مازالت الجهات القضائية تأخذ بها لعدم قناعتها بالأدلة الإلكترونية، ولذلك جاءت معظم الأحكام بوقف تنفيذ العقوبات على من يثبت ارتكابهم جريمة التزوير والتغيير الإلكتروني من المصرح لهم بالدخول على النظام، بالرغم من الآثار السلبية المترتبة على ذلك، فارتكاب التزوير الإلكتروني يترتب عليه سلبيات عديدة، وأخطار جمة نتيجة زيادة الإقبال على التعاملات الإلكترونية، مما يجعلها سوقاً رائجاً للتزوير الإلكتروني وضمان الموظف الذي ارتكب التزوير التذرع بترك الجهاز كوسيلة للهروب من العقاب، فالأولى تغليظ العقوبة، لأن حتى ترك الجهاز يعمل إهمال جسيم يترتب عليه أخطار شديدة تستوجب توقيع عقوبة الحبس والغرامة، ومن ثم فصل الموظف من عمله لأن إيقاف تنفيذ العقوبة معناه إعادته إلى عمله ومكافأته على تكبيد الدولة خسائر باهظة وحرمانها من تحصيل رسوم مخالفات مرورية، وقد لا يقتصر الأمر على ذلك، بل يمتد ليؤثر على الأمن الداخلي في حالة السماح بسفر العسكريين بعد تغيير مهنهم تزويراً، مما قد يترتب عليه تسريب أسرار عسكرية من قبل البعض قد تمس أمن الدولة الوطني، ولذلك يرى الباحث ضرورة تغليط العقوبة وتوجيه القضاء باعتماد الدليل الإلكتروني كدليل إثبات يقيني.

الفصل الخامس

ملخص الدراسة ونتائجها وتوصياتها

٥ .ملخص الدراسة ونتائجها وتوصياتها

يتناول هذا الفصل ثلاثة عناصر رئيسة هي : ملخص الدراسة، وعرض لأهم نتائج الدراسة، وطرح لتوصياتها.

٥ .١ ملخص الدراسة

اشتملت الدراسة على خمسة فصول بالإضافة إلى المراجع والملاحق، وقد انطلقت فكرة هذه الدراسة من سعيها لإثبات فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني في ضوء انتشار التعاملات الإلكترونية التي تكتنفها خطورة لجوء بعض الملمين باستخدام التقنية في القيام بعمليات تزوير إلكترونية من شأنها أن تقلل من مصداقية التعاملات الإلكترونية في ضوء انخفاض قدرة الأساليب التقليدية على مواجهة هذه الجرائم، وعدم قناعة الجهات القضائية بالأدلة الرقمية والإلكترونية كوسائل إثبات يقينية وتذرعها بإمكانية تزوير الأدلة الإلكترونية، وعدم قناعتها التامة بيقينية هذه الأدلة في ضوء تذرع بعض المخول لهم باستخدام النظام ممن يرتكبون جرائم التزوير باستخدام آخرين للجهاز نتيجة تركه يعمل أثناء قضاء بعض مهام العمل الأخرى.

وقد تحددت إشكالية الدراسة في التعرف على مدى فاعلية الأساليب التقليدية والإجرائية والمادية في إثبات جريمة التزوير الإلكتروني، في ضوء ما تتيحه هذه الوسائل من قدرات وإمكانات تتضافر مع بعضها لتكوين الرؤية المستقبلية اللازمة لقبول الأدلة الإلكترونية والرقمية كوسيلة إثبات جازمة لا تقبل الشك في إثبات جريمة التزوير الإلكتروني بما يساعد على زيادة الثقة

بالتعاملات الإلكترونية، واستغلالها في تطوير أداء المنظمات الأمنية لمواجهة عمليات التزوير واكتشافها بمجرد وقوعها.

٥ . ٢ أهم نتائج الدراسة

بعد أن تم تفسير وتحليل البيانات المستقاة من أجوبة المبحوثين خلصت الدراسة إلى نتائج سوف يتم عرضها حسب أهمية العبارات.

٥ . ٢ . ١ النتائج الخاصة بخصائص جريمة التزوير الإلكتروني

١ ـ تتسم جريمة التزوير الإلكتروني بخصائص مهمة جداً.

٢ ـ إن الخصائص المهمة جداً التي تتسم بها جريمة التزوير الإلكتروني هي :

أ ـ يتوافر فيها القصد الجنائي الخاص (التزوير).

ب ـ تشكل اعتداء على النظام المعلوماتي.

جـ ـ تعتبر من الجرائم العابرة للحدود الجغرافية.

د ـ لا تحتاج لعنف جسدي أو مقاومة كالجرائم التقليدية.

هـ ـ تتطلب حرفية وإتقاناً في التنفيذ.

و ـ تهدف في الغالب إلى تحقيق أرباح مالية.

ز ـ يتوافر فيها القصد الجنائي العام.

ح ـ تحتاج لخبرة وتخطيط علمي مدروس لارتكابها.

ط ـ تؤدي إلى فقد الثقة في التعاملات المالية الإلكترونية.

ي ـ إمكانية ارتكابها بطرق التزوير المعنوي (جعل واقعة مزورة في صورة واقعة صحيحة).

ك ـ قد يرتكبها في الغالب خبراء على درجة عالية من الكفاءة في استخدام الحاسب الآلي.

٣ ـ إن الخصائص المهمة التي تتسم بها جريمة التزوير الإلكتروني هي :

أ ـ تتطلب استخدام تقنيات الاختراق والتعدي.

ب ـ سهولة إتلاف الأدلة الإلكترونية التي تشير لمرتكبها.

جـ ـ لا يوجد لها أثر مادي ظاهر.

د ـ يصعب تتبع مرتكبيها والقبض عليهم.

٥ . ٢ . ٢ النتائج الخاصة بالوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني

١ ـ توجد وسائل مهمة لارتكاب جريمة التزوير الإلكتروني.

٢ ـ إن الوسائل المهمة جداً لارتكاب جريمة التزوير الإلكتروني هي :

أ ـ تتم من خلال أدوات كسر كلمات السر Password Crackers.

ب ـ تتم عن طريق إفشاء الرقم السري من قبل الموظفين لزملاء العمل بحسن نية.

٣ ـ إن الوسائل المهمة لارتكاب جريمة التزوير الإلكتروني هي :

أ ـ تتم باستخدام برامج فك التشفير.

ب ـ تتم عن طريق المحاولة المتكررة من خلال استخدام لوحة المفاتيح.

جـ ـ تتم عن طريق مولدات أرقام البطاقة الائتمانية C.CNumbers Generators.

د ـ تتم عن طريق الأجهزة ومحركات الأقراص المرنة والليزر.

هـ ـ تتم عن طريق أدوات التجسس على رزم البيانات Packet Sniffers.

و ـ تتم عن طريق الثقوب التي تتخلل بعض البرامج Programs Holes.

ز ـ تتم عن طريق الشبكة الواسعة WAN والبرامج المرتبطة بها.

ح ـ تتم عن طريق الشبكة المحلية LAN وبرامج التشارك في الموارد.

ط ـ تتم عن طريق التخفي الشبكي Anonymity.

ي ـ تتم عن طريق تمويه العنوان الشبكي IP Spoofing.

ك ـ تتم عن طريق لواقط ضربات لوحة المفاتيح Key Loggers.

ل ـ تتم عن طريق شبكة VPN والبرامج التي تعمل عليها.

م ـ تتم عن طريق التقاط الأشعة المنبعثة من الحاسب الآلي.

٥ . ٢ . ٣ النتائج الخاصة بصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية

١ - توجد صور مهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية.

٢ ـ إن الصور المهمة جداً للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية هي :

أ ـ قيام صاحب الصلاحية بتغيير بيانات أجنبي من قادم للعمرة إلى قادم للعمل.

ب ـ تغيير مهنة مقيم إلكترونياً تزويراً لتيسير إجراءات استقدام أسرته.

جـ ـ دخول صاحب صلاحية بطريقة عير مشروعة على النظام لرفع المخالفات المرورية عن سيارة لحين نقل ملكيتها إلكترونياً.

د ـ استخراج تأشيرات إلكترونية مزورة للحج والعمرة.

هـ ـ استخراج تأشيرات إلكترونية مزورة لاستقدام العمالة.

و ـ استخراج بطاقات الائتمان البنكية (فيزا – ماستركارد) مزورة.

ز ـ استخراج رخص قيادة إلكترونية عامة وخاصة مزورة.

ح ـ استخراج رخص سير إلكترونية مزورة للمركبات.

٣ ـ إن الصور المهمة للتزوير الإلكتروني في الدوائر الحكومية الإلكترونية هي :

أ ـ استخراج جواز سفر إلكتروني مزور.

ب ـ استخراج رخص بناء إلكترونية مزورة.

جـ ـ استخراج ضمانات بنكية إلكترونية مزورة.

د ـ استخراج شهادة إلكترونية مزورة للزكاة والدخل.

هـ ـ تزوير محررات استخراج السجل المدني إلكترونياً.

و ـ استخراج بطاقات أحوال إلكترونية مزورة.

ز ـ استخراج وكالات شرعية إلكترونية مزورة.

٥ . ٢ . ٤ النتائج الخاصة بسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني

١ ـ توجد سمات مهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني.

٢ ـ إن السمات المهمة جداً للمجرم الإلكتروني في جرائم التزوير الإلكتروني هي :

أ ـ يتمتع بالمهارة في استخدام الحاسب الآلي.

ب ـ يهدف في الغالب من ارتكاب جريمة التزوير المعلوماتي إلى الحصول على منفعة.

جـ ـ يتمتع بالاحترافية بذكاء.

د ـ يرتكب جريمة التزوير لمصلحته الخاصة.

هـ ـ يتمتع بالقدرة على اختراق نظم المعلومات وتحييد جدران الحماية وبرامج مكافحة الفيروسات.

و ـ يثابر في محاولات متكررة لاختراق المواقع.

٣ ـ إن السمات المهمة للمجرم الإلكتروني في جرائم التزوير الإلكتروني هي :

أ ـ يستخدم أساليب متطورة لسرقة منظومة التوقيع الإلكتروني.

ب ـ يبتكر أساليب جديدة لتزوير المحررات الإلكترونية.

جـ ـ لديه قدرة فائقة على المعالجة الإلكترونية للنصوص والكلمات.

د ـ يسرع في تدمير الأدلة الرقمية التي استخدمها في ارتكاب جريمة التزوير المعلوماتي.

هـ ـ يرتكب جريمة التزوير لمصلحة الآخرين.

و ـ يعمل غالبيتهم في المنظمات التي يقع عليها التزوير في مجال نظم المعلومات.

ز ـ يمتلك علاقات إنسانية جيدة مع الآخرين.

ح ـ يرتكب التزوير لإثبات قدراته على الاختراق والتعدي.

ط ـ يرتكب جريمة التزوير رداً على الاستغناء عن خدماته.

٥ . ٢ . ٥ النتائج الخاصة بسمات المجني عليه في جرائم التزوير الإلكتروني

١ ـ توجد سمات مهمة للمجني عليه في جرائم التزوير الإلكتروني.

٢ ـ إن السمات المهمة جداً للمجني عليه في جرائم التزوير الإلكتروني هي :

أ ـ تخفي الجهات (البنوك والمؤسسات المالية) خبر تعرضها للتزوير خوفاً من فقدان ثقة العملاء بها.

ب ـ المعاناة من ضعف نظم الحماية الخاصة بالحاسب الآلي.

جـ ـ قلة الخبرة اللازمة لاكتشاف الفيروسات المستخدمة في ارتكاب التزوير.

٣ ـ إن السمات المهمة للمجني عليه في جرائم التزوير الإلكتروني هي :

أ ـ الانخداع بالعروض التجارية الوهمية.

ب ـ الخسارة المالية نتيجة عدم الاحتراز في الإدلاء ببيانات البطاقات الائتمانية.

جـ ـ مساهمة قلة الخبرة في استخدام الشبكة في سهولة الاستيلاء على البيانات المهمة.

د ـ المنظمات المالية أكثر تعرضاً للاختراق والتعدي والتزوير من المنظمات الأخرى.

هـ ـ المعاناة من العشوائية في استقبال البريد الإلكتروني.

و ـ الانخداع بإغراءات التخفيضات الوهمية من قبل الجناة.

ز ـ تتعرض المنظمات للاختراق والتعدي لارتكاب التزوير أكثر من الأفراد.

ح ـ التنقل بين صفحات الإنترنت دون هدف واضح.

ط ـ التعرض للابتزاز من قبل المواقع المشبوهة.

ي ـ التعرض للحرج عند استخدام المسمى في المواقع المشبوهة.

ك ـ تقوم المؤسسات المالية المجني عليها في الغالب بتعويض عملائها المتضررين من جرائم التزوير الإلكتروني.

ل ـ تستجيب بعض الجهات المجني عليها لطلبات المبتزين.

٥ . ٢ . ٦ النتائج الخاصة بفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني

١ ـ يتبع المحقق الجنائي أساليب فعالة جداً في إثبات جرائم التزوير الإلكتروني.

٢ ـ إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني هي:

أ ـ الاستعانة بخبراء الحاسب الآلي في فهم المصطلحات.

ب ـ الاستفادة من علم الحاسب الجنائي في إثبات جريمة التزوير الإلكتروني.

جـ ـ الإسراع في إجراء المعاينة للأجهزة المشتبه في ارتكابها جرائم التعدي والاختراق.

د ـ الإسراع في إجراء المعاينة للأجهزة المتعرضة للاختراق والتعدي.

هـ ـ تحديد دور كل فرد أثناء مداهمة المكان المشتبه بوجود الأجهزة به.

و ـ إجراء التحريات اللازمة عن موقع الأجهزة المشتبه بها.

ز ـ التحفظ على تقنيات الاتصال المرتبطة بالحاسب الآلي.

ح ـ تسجيل طبيعة عمل كل فرد متواجد في مكان ارتكاب الجريمة.

ط ـ التحفظ على الأجهزة المشتبه بها وملحقاتها.

ي ـ أخذ إفادات المتواجدين في المكان.

ك ـ تمكين خبراء الحاسب الآلي من توجيه الأسئلة الفرعية اللازمة لإثبات التهمة.

ل ـ إعداد الأسئلة بالاتفاق مع خبراء الحاسب الآلي الجنائي قبل توجيهها للمتهمين.

م ـ طلب خبراء الحاسب الآلي حضور التحقيق إذا تطلب ذلك.

ن ـ وقف خدمة الاتصال بالحاسب من خلال خادمات الملفات حتى لا تسبب الاتصالات بإتلاف الأدلة.

س ـ ترتيب استجواب المتهمين حسب توجيهات خبراء الحاسب الآلي.

٥ . ٢ . ٧ النتائج الخاصة بفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني

١ ـ يتبع المحقق الفني أساليب فعالة جداً في إثبات جرائم التزوير الإلكتروني.

٢ ـ إن الأساليب الفعالة جداً في إثبات جرائم التزوير الإلكتروني هي :

أ ـ الاستعانة بمركز المعلومات لمعرفة المستخدم الذي قام بعملية التزوير من الموظفين في الإدارات الإلكترونية التابعة لها.

ب ـ عمل نسخة كاملة من البيانات الموجودة على الحاسب الآلي الذي تعرض للاختراق والتعدي.

جـ ـ توثيق البيانات التي استخدمت في جرائم تزوير المحررات الإلكترونية.

د ـ استخدام تقنيات التتبع للعثور على البريد الإلكتروني للمخترق.

هـ ـ استخدام تقنيات استرجاع المعلومات لاسترجاع الملفات والبيانات المحذوفة التي استخدمت في الاختراق والتعدي.

و ـ استخدام برامج إزالة الإخفاء لتحديد عناصر الدليل الرقمي المخبأة.

ز ـ استخدام برامج فك التشفير لاكتشاف الأدلة المشفرة.

ح ـ الاستعانة بتقنيات تتبع الذبذبات لتحديد موقع الجهاز الذي استخدام في الاختراق والتعدي.

ط ـ استخدام برامج البحث عن المفردات النصية للعثور على المحرر المعلوماتي المزور.

ي ـ نسخ الدليل الرقمي.

ك ـ تحليل الدليل الرقمي.

ل ـ عرض الدليل الرقمي.

م ـ استخدام أقراص فك كلمة المرور للدخول على المواقع المحجوبة.

٣ـ إن الأسلوب الفعال في إثبات جرائم التزوير الإلكتروني هو : استخدام برامج الاستنساخ الجنائي للأقراص الضوئية.

٥ . ٢ .٨ النتائج الخاصة بالمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني

١ـ توجد معوقات مهمة جداً تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية جداً.

٢ ـ إن المعوقات المهمة جداً التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية جداً هي :

أ ـ ندرة البرامج التدريبية اللازمة لتأهيل المحققين لإثبات جرائم التزوير الإلكتروني.

ب ـ قلة إلمام بعض المحققين بالبرامج الخاصة بالتعدي والاختراق والتزوير.

جـ ـ قلة إلمام المحققين بمجال الحاسب الجنائي في إثبات الجريمة.

د ـ قلة الإمكانات الفنية اللازمة لإثبات جرائم التزوير المعلوماتي.

هـ ـ قلة خبرات السلطات المسؤولة عن ضبط وإثبات جرائم التزوير الإلكتروني والتحقيق فيها.

و ـ قصور التعاون الدولي في مجال مكافحة جرائم التزوير المعلوماتي.

ز ـ ثقة الجهات القضائية في الدليل الإلكتروني قاصرة نظراً لإمكانية تزويره.

ح ـ تكتم الجهات المجني عليها عن البلاغ خوفاً من فقدان الثقة بتعاملاتها (المنظمات المالية).

ط ـ محاكاة المحرر الإلكتروني المزور للأصل تماماً، فلا يوجد به شطب أو كشط يدل على تزويره ترتكب بسببه جرائم أخرى.

ي ـ إمكانية ارتكابها من مسافات بعيدة تتعدى إقليم الدولة (غير قارية).

ك ـ إمكانية التخلص من الأجهزة المستخدمة في التزوير الإلكتروني بحرقها أو تدميرها.

ل ـ عدم كفاية الأدلة للإدانة في جرائم التزوير المعلوماتي.

م ـ إمكانية التخلص من الأجهزة المستخدمة في التزوير الإلكتروني بحرقها أو تدميرها.

ن ـ عدم تخلف الآثار المادية الملموسة كما في حالة الجرائم التقليدية.

٣ ـ إن المعوق المهم الذي يؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني بدرجة قوية هو : سهولة التخلص من الأدلة الإلكترونية بمحوها.

٥ . ٢ . ٩ النتائج الخاصة باختلاف رؤية المبحوثين نحو فاعلية الأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني باختلاف متغيراتهم الشخصية والوظيفية

١ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، وفاعلية كل أسلوب من الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت طبيعة أعمالهم.

٢ ـ توجد فروق ذات دلالة إحصائية بين رؤية مفردات الدراسة لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية تعزى

إلى متغير طبيعة العمل، وكانت الفروق الدالة إحصائياً لصالح المحققين الجنائيين، أي أن المحققين الجنائيين أكثر إدراكاً لصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، نظراً لأن المحققين الجنائيين يهتمون بصور وأشكال جريمة التزوير سواء كانت تغيير بيانات في سجلات الحاسب الآلي، أو سرقة منظومة التوقيع الإلكتروني، أو تغيير مهنة واستخدامها إصدار وثائق ثبوتية مزورة، فهم أكثر إلماماً بتصنيفات جرائم التزوير الإلكتروني وتكييفها القانوني، بخلاف المحققين الفنيين الذين يركزون على الجوانب الفنية لارتكاب ووقوع جريمة التزوير الإلكترونية، وكيفية التقاط الأدلة الإلكترونية اللازمة لإثباتها بالطرق والتقنيات الفنية.

٣ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة التزوير الإلكتروني، وصور جريمة التزوير الإلكتروني في الدوائر الحكومية الإلكترونية، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت أعمارهم.

٤ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكتروني، والوسائل المستخدمة في ارتكاب جريمة

التزويـر الإلكتروني، وصور جريمة التزويـر الإلكتروني في الدوائر الحكومية الإلكترونية، وسمات المجرم الإلكتروني في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائـم التزوير الإلكتروني، وفاعلية الأسـاليب التي يتبعها المحقق الفنـي في إثبات جرائم التزوير الإلكـتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأسـاليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت مؤهلاتهم التعليمية.

٥ ـ لـدى مفـردات الدراسـة رؤيـة متشـابهة نحـو خصائـص جريمـة التزويـر الإلكـتروني، والوسـائل المسـتخدمة في ارتـكاب جريمـة التزويـر الإلكتروني، وسـمات المجرم الإلكـتروني في جرائم التزوير الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني مهما اختلفـت جهات أعمالهـم، وفاعلية الأسـاليب التـي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفنـي في إثبات جرائـم التزوير الإلكتروني مهـما اختلفت جهات أعمالهم.

٦ ـ لدى مفردات الدراسة رؤية متشابهة نحو خصائص جريمة التزوير الإلكـتروني، وسـمات المجني عليـه في جرائم التزويـر الإلكتروني، وفاعليـة الأسـاليب التـي يتبعهـا المحقـق الجنائي في إثبـات جرائم التزوير الإلكتروني، وفاعلية الأسـاليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني مهما اختلفت المنطقة التي يعملون بها.

٧ ـ لـدى مفـردات الدراسـة رؤيـة متشـابهة نحـو خصائـص جريمـة التزويـر الإلكـتروني، والوسـائل المسـتخدمة في ارتـكاب جريمـة التزويـر الإلكتروني، وصور جريمة التزويـر الإلكتروني في الدوائر الحكومية الإلكترونية، وسمات المجرم الإلكتروني في جرائم التزوير الإلكـتروني، وسـمات المجني عليـه في جرائم التزويـر الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكـتروني، والمعوقـات التـي تـؤدي إلى عـدم فاعليـة الأسـاليب المسـتخدمة مـن المحقـق الجنائـي والفني في إثبـات جرائـم التزوير الإلكتروني مهما اختلفت رتبهم العسكرية.

٨ ـ لـدى مفـردات الدراسـة رؤيـة متشـابهة نحـو خصائـص جريمـة التزويـر الإلكـتروني، والوسـائل المسـتخدمة في ارتـكاب جريمـة التزويـر الإلكتروني، وصور جريمة التزويـر الإلكتروني في الدوائر الحكومية الإلكترونية، وسمات المجرم الإلكتروني في جرائم التزوير الإلكـتروني، وسـمات المجني عليـه في جرائم التزويـر الإلكتروني، وفاعليـة الأسـاليب التـي يتبعهـا المحقـق الجنائي في إثبـات جرائم التزوير الإلكتروني، وفاعلية الأسـاليب التي يتبعها المحقق الفني في إثبـات جرائم التزويـر الإلكتروني، والمعوقات التـي تؤدي إلى عدم فاعلية الأسـاليب المسـتخدمة من المحقق الجنائـي والفني في إثبات جرائـم التزويـر الإلكـتروني مهـما اختلف عـدد سـنوات خبراتهم العملية في مجال العمل.

٩ ـ لـدى مفـردات الدراسـة رؤيـة متشـابهة نحـو خصائـص جريمـة التزويـر الإلكـتروني، والوسـائل المسـتخدمة في ارتـكاب جريمـة التزويـر الإلكتروني، وسـمات المجرم الإلكـتروني في جرائم التزوير

الإلكتروني، وسمات المجني عليه في جرائم التزوير الإلكتروني، وفاعلية الأساليب التي يتبعها المحقق الفني في إثبات جرائم التزوير الإلكتروني، والمعوقات التي تؤدي إلى عدم فاعلية الأساليب المستخدمة من المحقق الجنائي والفني في إثبات جرائم التزوير الإلكتروني مهما اختلف عدد الدورات التدريبية التي حصلوا عليها في مجال جرائم التزوير الإلكترونية.

٥ .٣ توصيات الدراسة

في ضوء الإطار النظري للدراسة ، والنتائج التي أسفرت عنها ، يتقدم الباحث بالتوصيات التالية :

١ ـ حث المحاكم والجهات القضائية على الأخذ بالدليل الرقمي والدليل الإلكتروني كدليل إثبات في جرائم التزوير الإلكتروني.

٢ ـ إلحاق العاملين في التحقيق الجنائي والفني بدورات تدريبية متقدمة في مجال الحاسب الجنائي لتزويدهم بالمهارات اللازمة للتحقيق في جرائم التزوير الإلكتروني.

٣ ـ تزويد الجهات المختصة بالتحقيق في جرائم التزوير الإلكتروني بالإمكانات المالية والفنية والكوادر البشرية المؤهلة لاكتشاف الأدلة الإلكترونية الدامغة، وتقديمها كأدلة إثبات يقينية.

٤ ـ تشجيع الجهات المجني عليها في عمليات الاختراق والتعدي والتزوير بالإبلاغ عما تعرضت له من أعمال، مع مراعاة جهات التحقيق السرية لضمان تحديد المواقع المشبوهة، والقبض على مرتكبي جرائم التزوير الإلكتروني.

٥ ـ نشر الثقافة الإلكترونية بين أفراد المجتمع من خلال تثقيفهم بخطورة

الإدلاء ببياناتهم عبر الإنترنت، وخطورة التصفح العشوائي للإنترنت، والانبهار بالعروض الوهمية.

٦ ـ إعداد استراتيجية متكاملة لحماية نظم المعلومات بالأجهزة الأمنية، مع تأمينها بنظم حماية فعالة تقي من الاختراق والتعدي والتزوير.

٧ ـ حث الشركات العاملة في مجال نظم المعلومات على إنتاج برمجيات حديثة للتتبع واسترجاع المعلومات لسهولة كشف حالات الاختراق والتعدي والتزوير.

٨ ـ استقطاب خبراء نظم المعلومات لرفع قدرة العاملين في مكافحة التزوير على اكتشاف حالات التزوير الإلكتروني بمجرد وقوعها.

٩ ـ مضاعفة العقوبات على المصرح لهم بالدخول على النظام في حالة اكتشاف قيامهم بإساءة استغلال الثقة في ارتكاب عمليات تزوير إلكتروني، لتلافي الأخطار الأمنية الناتجة عن التهاون في العقوبات المفروضة عليهم.

١٠ ـ تجنب استخدام برامج منسوخة، أو منقولة من الإنترنت والحرص على استخدام النسخ الأصلية من البرمجيات.

١١ ـ وضع دليل إجرائي مكتوب يحدد خطوات استخدام نظم المعلومات في الأجهزة الأمنية، والعقوبات المترتبة على إساءة استخدامه من قبل العاملين

١٢ ـ التنسيق والتعاون بين المركز الوطني للمعلومات والأجهزة الأمنية، للتأكد من وجود وثائق رسمية ومسوغات نظامية لأي حالة تغيير للبيانات والمعلومات في سجلات الحاسب الآلي بالأجهزة الأمنية.

١٣ ـ إنشاء إدارة تختص بالتعاون الدولي في مجال مكافحة جرائم المعلوماتية بصفة عامة، وجرائم التزوير الإلكتروني بصفة خاصة.

دراسات مستقبلية

١ ـ إجراء دراسة عن دور ما يستجد من تقنيات التتبع الحديثة والتقنيات الحديثة في كشف جرائم التزوير الإلكتروني.

٢ ـ إجراء دراسة عن مشروعية الدليل الرقمي في الإثبات الجنائي.

المراجـــــع

أولاً : المراجع العربية

إبراهيم، حسنين محمود (١٩٨١م). الرسائل العلمية الحديثة في الإثبات الجنائي. مصر، دار النهضة العربية.

إبراهيم، حسين محمود (١٤٠٧هـ). الأساليب العلمية الحديثة في مجال مكافحة الجريمة. الرياض، جامعة نايف العربية للعلوم الأمنية.

إبراهيم، محمد سعد (٢٠٠٨م). «التجربة الماليزية والتحقيق في الجرائم الإلكترونية». ورقة مقدمة ضمن الحلقة العلمية الدليل الرقمي والتحقيق في الجرائم الإلكترونية المنعقدة في الفترة من ٢٢-٢٤/ ١٢/ ١٤٢٩هـ. الرياض، جامعة نايف العربية للعلوم الأمنية.

الأبرش، محمد رياض ومرزوق، نبيل (١٩٩٩م). الخصخصة آفاقها وأبعادها. بيروت، دار الفكر المعاصر.

أبو بكر، محمد عبد الله (٢٠٠٧م). موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت. الإسكندرية، المكتب العربي الحديث.

أبو شامة، عباس (١٩٩٢م). المعايير النموذجية المطلوبة لرجل الأمن. الرياض، جامعة نايف العربية للعلوم الأمنية.

أبو العينين، عبد الفتاح محمد (١٩٩٢م). القضاء والإثبات في الفقه الإسلامي مع المقارنة بقانون الإثبات اليمني. القاهرة، جامعة الأزهر.

أبو القاسم، أحمد أحمد (١٤١٤هـ). الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص. الرياض، جامعة نايف العربية للعلوم الأمنية.

أبو النـور، عوض منصور (١٩٩٦م). مقدمة في علم الحاسـب الإلكتروني، وبرمجة بيسك. (ط٥)، إربد – الأردن، دار الأمل.

أحمـد، هلالي عبـد الله (١٩٨٧م). النظرية العامة للإثبـات في المواد الجنائية. القاهرة، دار النهضة العربية.

ـــــــــــــــ (٢٠٠٣م). الجوانـب الموضوعيـة والإجرائيـة لجرائـم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١م. القاهرة، دار النهضة العربية.

إدارة الأدلـة الجنائيـة (٢٠٠٩م). الأجهـزة المسـاعدة في فحص المسـتندات والوثائق. الرياض، الأمن العام.

آرلفـين، جوني وآخرون (١٩٩٧م). الإنترنـت للمبتدئين (ترجمة فوزي عبد المنعم). الرياض، مكتبة جرير.

آل بـن علي، عبـد الله محمـد (٢٠٠٧م). «تقنية المعلومـات والاتصالات في خدمـة القطاعـات الأمنيـة، نظـرة عامـة». مؤتمـر تقنيـة المعلومـات والأمـن الوطني المنعقد في الرياض في الفترة من ٢١-٢٤ ذي القعدة ١٤٢٨هـ الموافـق ١-٤ ديسـمبر ٢٠٠٧م. المجلـد (٣)، الريـاض، رئاسة الاستخبارات العامة.

الأمـن العـام (٢٠٠٩م). بيان بأعـداد المحققين الجنائيـين والفنيين العاملين في مكافحـة التزوير وأبحاث التزوير بالأمن العام. شـؤون الضباط، الرياض، مطابع الأمن العام.

بحر، عبد الرحمن (١٩٩٩م). معوقات التحقيق في جرائم الإنترنت. رسـالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.

برينتون، كريس وهنت، كاميرون (٢٠٠٣م). نظم تأمين الشبكات، مرجع شامل لنظم تأمين الشبكات (ترجمة خالد العامري). القاهرة، دار الفاروق للنشر والتوزيع.

البشرى، محمد الأمين (٢٠٠٤م). التحقيق في الجرائم المستحدثة. الرياض، جامعة نايف العربية للعلوم الأمنية.

بوادي، حسنين المحمدي (٢٠٠٥م). الوسائل العلمية الحديثة في الإثبات الجنائي. الإسكندرية، منشأة المعارف بالإسكندرية.

بوساق، محمد بن المدني (٢٠٠٢م). اتجاهات السياسة الجنائية المعاصرة والشريعة الإسلامية. الرياض، جامعة نايف العربية للعلوم الأمنية.

تاج الدين، مدني عبد الرحمن (٢٠٠٤م). أصول التحقيق الجنائي وتطبيقاتها في المملكة العربية السعودية. الرياض، معهد الإدارة العامة.

ثروت، جلال (٢٠٠٠م). نظم القسم الخاص في قانون العقوبات. الإسكندرية، منشأة المعارف.

الجندي، إبراهيم صادق والحصيني، حسين حسن (٢٠٠٢م). تطبيقات تقنية البصمة الوراثية D.N.A في التحقيق والطب الشرعي. الرياض، جامعة نايف العربية للعلوم الأمنية.

الجنبيهي، منير محمد والجنبيهي، ممدوح محمد (٢٠٠٥م). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها. الإسكندرية، دار الفكر الجامعي.

الحبشي، فادي (١٩٩٠م). المعاينة الفنية لمسرح الجريمة والتفتيش. الرياض، جامعة نايف العربية للعلوم الأمنية.

حجـازي، عبد الفتاح بيومـي (٢٠٠٢م). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت. القاهرة، دار الكتب القانونية.

ـــــــــــــ (٢٠٠٥م). الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنـت، دراسـة متعمقـة في جرائـم الحاسـب الآلي والإنترنت. المحلة الكبرى، دار الكتب القانونية.

ـــــــــــــ (٢٠٠٧م). التجـارة الإلكترونيـة في القانـون العـربي النموذجي لمكافحة جرائـم الكمبيوتر والإنـــترنت. المحلة الكبرى، دار الكتب القانونية.

الحجيـلان، صلاح إبراهيـم (٢٠٠٦م). الملامـح العامة لنظـام الإجراءات الجزائيـة السـعودي ودوره في حمايـة حقـوق الإنسـان. بـيروت، منشورات الحلبي الحقوقية.

حسـن، سـعيد عبد اللطيـف (١٩٩٩م). إثبات جرائـم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات. القاهرة، دار النهضة العربية.

حسـن، علي عوض (١٩٩٦م). جريمـة البلاغ الكاذب. الإسـكندرية، دار المطبوعات الجامعية.

حسـني، محمود نجيب (١٩٨٢م). شرح قانون العقوبات، القسـم الخاص. القاهرة، دار النهضة العربية.

ـــــــــــــ (١٩٨٣م). شرح قانون العقوبات، القسم العام. (ط٥)، القاهرة، دار النهضة العربية.

ـــــــــــــ (١٩٨٨م). شرح قانـون الإجـراءات الجنائيـة. (ط٢)، القاهرة، دار النهضة العربية.

حسين، خليفة كلندر عبد الله (٢٠٠٢م). ضمانات المتهم في مرحلة التحقيق الابتدائي في قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية.

الحمدان، عبد الرحمن بن عبد العزيز والقاسم، محمد بن عبد الله (٢٠٠٤م). أساسيات أمن المعلومات. الرياض، مطابع الحميضي.

حمدي، محمد (١٩٩٦م). الإعلام والمعلومات، دراسة في التوثيق الإعلامي. الرياض، جهاز تلفزيون الخليج العربي.

الحميد، محمد دباس ونينو، ماركو إبراهيم (٢٠٠٧م). حماية أنظمة المعلومات. عمّان، دار الحامد للنشر والتوزيع.

الخشروم، محمد مصطفى وموسى، نبيل محمد (١٩٩٩م).إدارة الأعمال، المبادئ والمهارات والوظائف. (ط٢)، الرياض، مكتبة الشقري.

خضر، عبد الفتاح (١٩٨٨م). جرائم التزوير والرشوة في المملكة العربية السعودية. القاهرة، مكتب صلاح الحجيلان للمحاماة والاستشارات القانونية.

الخليفة، هند بنت سليمان (٢٠٠٧م). «الحاسب الجنائي في الدول الغربية، دراسة استطلاعية». مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من ٢١-٢٤ من ذي القعدة ١٤٢٨هـ الموافق ١-٤ ديسمبر ٢٠٠٧م. المجلد (٢)، الرياض، رئاسة الاستخبارات العامة.

خليل، عدلي (١٩٩٣م). البلاغ الكاذب والتعويض عنه. القاهرة، دار النهضة العربية.

الدغيدي، مصطفى محمد (٢٠٠٤م). التحريات والإثبات الجنائي. القاهرة، شركة ناس للطباعة.

راتشمان، دافيد وآخرون (٢٠٠١م). الإدارة المعاصرة (ترجمة رفاعي محمد رفاعي ومحمد سيد أحمد). الرياض، دار المريخ.

الردادي، أحمد بن دخيل الله (٢٠٠٠م). معاينة مسرح الجريمة بين النظرية والتطبيق. جدة، الدار السعودية للأبحاث والنشر.

رستم، هشام محمد فريد (١٩٩٣م). الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة. أسيوط، مكتبة الآلات الحديثة.

السبهان، فهد إبراهيم (١٩٩٥م). استجواب المتهم بمعرفة سلطة التحقيق. الإمارات العربية المتحدة، مطبعة بن دسمال ومكتبتها.

سرور، أحمد فتحي (١٩٨٥م). الوسيط في قانون الإجراءات الجنائية. القاهرة، دار النهضة العربية.

سلامة، مأمون محمد (١٩٩١م). الإجراءات الجنائية في التشريع المصري. القاهرة، دار الفكر العربي.

السماك، علي (١٩٩٠م). الموسوعة الجنائية في القضاء الجنائي العراقي. ج١، بغداد، مطبعة الجاحظ.

السنهوري، عبد الرازق (١٩٥٦م). الوسيط في شرح القانون. ج٢، القاهرة.

الشاذلي، فتوح عبد الله (١٩٩٨م). قانون العقوبات، القسم العام. الإسكندرية، دار المطبوعات الجامعية.

الشاذلي، فتوح وعفيفي، عفيفي كامل (٢٠٠٣م). جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. بيروت، منشورات الحلبي الحقوقية.

الشاعر، عبد الرحمن بن إبراهيم (٢٠٠٤م) تقنية المعلومات والاتصال. الرياض، دار ثقيف للنشر والتأليف.

شاهين، بهاء (١٩٩٦م). شبكة إنترنت. (ط٢)، القاهرة، العربية لعلوم الحاسب.

شاهين، بهاء (٢٠٠٠م). العولمة والتجارة الإلكترونية، رؤية إسلامية. (ط٢)، القاهرة، الفاروق الحديثة.

شتا، محمد محمد (٢٠٠٠م). فكرة الحماية الجنائية لبرامج الحاسب الآلي. القاهرة، دار الجامعة الجديدة للنشر.

الشدي، طارق عبد الله (٢٠٠٠م). آلية البناء الأمني لنظم المعلومات. الرياض، دار الوطن للطباعة والنشر والإعلام.

شلباية، مراد وفاروق، علي (٢٠٠١م). مقدمة إلى الإنترنت. عمان، دار المسيرة للنشر والتوزيع.

الشمري، توفيق (١٩٩١م). أمن المعلومات. الرياض، المديرية العامة لكلية الملك فهد الأمنية والمعاهد.

الشنواني، صلاح (١٩٩٩م). إدارة الأفراد والعلاقات الإنسانية مدخل الأهداف. الإسكندرية، مؤسسة شباب الجامعة.

الشهري، حسن بن أحمد والعطوي، صالح بن محمد (٢٠٠٧م). «دراسة الوضع الحالي لتدريس وتطبيق أنظمة وتشريعات الجريمة الإلكترونية في المملكة». ورقة مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، الجرائم الإلكترونية الملامح والأبعاد المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من ٥-٧ ربيع الثاني ١٤٢٨هـ الموافق ٢٢-٢٤ أبريل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

الشوا، محمد سامي (١٩٩٣م). «الغش المعلوماتي كظاهرة إجرامية مستحدثة». بحث مقدم ضمن فعاليات المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات» في الفترة من ٢٥-٢٨ أكتوبر. القاهرة، الجمعية المصرية للقانون الجنائي.

ـــــــــــــــ (٢٠٠٠م). ثورة المعلومات وانعكاساتها على قانون العقوبات. القاهرة، دار النهضة العربية.

الشوابكة، محمد أمين (٢٠٠٦م). جرائم الحاسوب والإنترنت، الجريمة المعلوماتية. عمّان، دار الثقافة للنشر والتوزيع.

الصغير، جميل عبد الباقي (١٩٩٩م). الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري. القاهرة، دار النهضة العربية.

الصغير، جميل عبد الباقي (٢٠٠١م). الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت. القاهرة، دار النهضة العربية.

الصيفي، عبد الفتاح مصطفى (٢٠٠٢م). تأصيل الإجراءات الجنائية. الإسكندرية، دار المعرفة الجامعية.

طنطاوي، إبراهيم حامد مرسي (١٩٩٧م). سلطات مأمور الضبط الجنائي. (ط٢)، القاهرة، دار النهضة العربية.

عالم، محمد أسعد، وشاهين، محمد عبد السميع (٢٠٠٥م). ثورة الاتصالات والمعلومات وأثرها على الحياة المعاصرة. الرياض، مطبعة النرجس التجارية.

عبد الرحيم، محمد لطفي (٢٠٠٧م). «الجرائم المعلوماتية، التحديات

والحلـول». ورقـة مقدمـة ضمن فعاليـات ندوة المجتمـع والأمن في دورتها الخامسـة، الجرائم الإلكترونية الملامح والأبعاد المنعقدة بكلية الملـك فهد الأمنية بالريـاض في الفترة من ٥-٧ ربيع الثاني ١٤٢٨هـ الموافق ٢٢-٢٤ أبريل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

عبـد السـتار، فوزيـة (١٩٨٨م). شرح قانـون العقوبـات، القسـم الخاص. القاهرة، دار النهضة العربية.

عبد المطلب، ممدوح عبد الحميد (٢٠٠١م). جرائم اسـتخدام الحاسب الآلي وشـبكة المعلومـات العالمية، الجريمة عبر الإنترنت. الشـارقة، مكتبة دار الحقوق.

ـــــــــــــــ (٢٠٠٧م). «أدلـة الصور الرقميـة». ورقة مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، الجرائم الإلكترونية الملامح والأبعاد المنعقـدة بكلية الملك فهد الأمنية بالرياض في الفترة مـن ٥-٧ ربيـع الثـاني ١٤٢٨هـ الموافـق ٢٢-٢٤ أبريـل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

العبـود، فهـد بـن نـاصر (٢٠٠٥م). الحكومـة الإلكترونيـة بـين التخطيط والتنفيذ. السلسلة الثانية (٤١)، الرياض، مكتبة الملك فهد الوطنية.

عـدس، عماد عـوض عـوض (٢٠٠٤م). التحريات كإجراء مـن إجراءات البحث عن الحقيقة. رسـالة دكتوراه غير منشورة، القاهرة، أكاديمية مبارك للأمن.

عـرب، يونـس (٢٠٠٦م). جرائم الكمبيوتـر والإنترنت، إيجـاز في المفهوم والنطـاق والخصائـص والصـور والقواعـد الإجرائيـة للملاحقـة والإثبات. القاهرة، دار النهضة العربية.

العريان، محمد علي (٢٠٠٤م). الجرائم المعلوماتية. الإسكندرية، دار الجامعة الجديدة للنشر.
العساف، صالح بن حمد (٢٠٠٠م). المدخل إلى البحث في العلوم السلوكية. (ط٢)، الرياض، مكتبة العبيكان.
عليان، ربحي مصطفى وغنيم، عثمان محمد (٢٠٠٠م). مناهج وأساليب البحث العلمي. عمّان، دار صفاء للنشر والتوزيع.
عمر، محمد عبد الحليم (٢٠٠٠م). «التجارة الالكترونية من منظور إسلامي». ورقة عمل مقدمة إلى الحلقة النقاشية الخامسة عشرة بمركز صالح كامل للاقتصاد الإسلامي في ٢٦/ ٢/ ٢٠٠٠م.
العكيلي، عبد الأمير وحربة، سليم إبراهيم (١٩٨١م). أصول المحاكمات الجزائية. ج١، الموصل، دار الكتب للطباعة والنشر.
العميري، محمد بن عبد الله (٢٠٠٤م). موقف الإسلام من الإرهاب. الرياض، جامعة نايف العربية للعلوم الأمنية.
العنزي، سلمان (٢٠٠٢م). وسائل التحقيق في جرائم نظم المعلومات. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.
عوض، محمد محيي الدين (١٩٦٣م). القانون الجنائي، مبادئه الأساسية ونظرياته العامة في التشريعين المصري والسوداني. القاهرة، المطبعة العالمية.
ـــــــــــــ (١٩٨١م). القانون الجنائي بمبادئه الأساسية ونظرياته العامة. القاهرة، مطبعة جامعة القاهرة.
ـــــــــــــ (١٩٨١م). القانون الجنائي مبادئه الأساسية ونظرياته العامة. القاهرة، مطبعة جامعة القاهرة.

عيد، محمد فتحي (٢٠٠٣م). الإنترنت ودوره في انتشار المخدرات. الرياض، جامعة نايف العربية للعلوم الأمنية.

فريد، هشام محمد (١٩٩٤م). الجوانب الإجرائية للجرائم المعلوماتية. أسيوط ـ جمهورية مصر العربية، مكتبة الآلات الحديثة.

الفنتوخ، عبد القادر (٢٠٠١م). الإنترنت للمستخدم العربي. (ط٢)، الرياض، مكتبة العبيكان.

القائفي، خالد بن عبد الله (٢٠٠٧م). «أمن وتشفير المعلومات وحماية الشبكة». مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من ٢١ـ٢٤ ذو القعدة ١٤٢٨هـ الموافق ١-٤ ديسمبر ٢٠٠٧م. المجلد (٣)، الرياض، رئاسة الاستخبارات العامة.

القاسم، محمد بن عبد الله (٢٠٠٥م). «سياسات أمن المعلومات». سلسلة إصدارات مركز البحوث والدراسات، الرياض، كلية الملك فهد الأمنية.

القحطاني، سالم بن سعيد وآخرون (٢٠٠٠م). منهج البحث في العلوم السلوكية. الرياض، المطابع الوطنية الحديثة.

قشقوش، هدى حامد (١٩٩٨م). «الصور الإجرامية لحالات السحب الإلكتروني من الرصيد». ورقة عمل مقدمة إلى ندوة الصور المستحدثة لجرائم بطاقات الدفع الإلكتروني المنعقدة في القاهرة في ١٤/ ١٢/ ١٩٩٨م. القاهرة، مركز بحوث الشرطة.

قشقوش، هدى حامد (٢٠٠٠م). «الإتلاف العمدي لبرامج وبيانات الحاسب الآلي». بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت

المنعقـد في الفترة مـن ١ ـ ٣ مايو ٢٠٠٠م. الإمارات العربية المتحدة، كلية الشريعة والقانون

قصيبـاتي، ياسر (٢٠٠٨م). «الهاتف الخلوي والدليل الرقمي». ورقة مقدمة ضمن الحلقة العلمية الدليل الرقمي والتحقيق في الجـرائم الإلكترونية المنعقـدة في الفترة مـن ٢٢-٢٤/ ١٢/ ١٤٢٩هـ. الريـاض، جامعة نايف العربية للعلوم الأمنية.

القهوجـي، علي عبد القـادر (١٩٩٢م). «الحماية الجنائية لبرامج الحاسـب». بحـث منشـور بمجلـة الحقـوق للبحـوث القانونيـة والاقتصاديـة التـي تصدرهـا كليـة الحقـوق، الإسـكندرية، كلية الحقـوق بجامعة الإسكندرية.

القهوجي، علي والشـاذلي، فتوح (١٩٩٩م). شرح قانون العقوبات، القسم الخاص. الإسكندرية، دار المطبوعات الجامعية.

قورة، نائلة عادل محمد (٢٠٠٥م). جرائم الحاسب الآلي الاقتصادية، دراسة نظرية. بيروت، منشورات الحلبي الحقوقية.

كامل، محمد فاروق عبد الحميد (١٩٩٩م). القواعد الفنية الشرطية للتحقيق والبحث الجنائي. الرياض، جامعة نايف العربية للعلوم الأمنية.

الكركـي، كـمال أحمـد (١٩٩٨م). «النواحـي الفنيـة لإسـاءة اسـتخدام الكمبيوتـر». بحث مقدم إلى ندوة الجرائـم الناجمة عن التطور التقني المنعقدة بعمان في الفترة من (٢٨ ـ ٢٩) أكتوبر ١٩٩٨م.

الكركـي، كـمال (٢٠٠٣م). «التحقيـق في جرائـم الحاسـوب». بحـوث المؤتمـر العلمـي الأول حول الجوانـب القانونية والأمنيـة للعمليات الإلكترونية. دبي، أكاديمية شرطة دبي.

مؤنس محب الدين، محمد (٢٠٠٦م). تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها. الرياض، جامعة نايف العربية للعلوم الأمنية.

ماهر، أحمد (٢٠٠٠م). السلوك التنظيمي، مدخل بناء المهارات. (ط٧)، الإسكندرية، الدار الجامعية.

محمد، عاصم يس (٢٠٠٧م). «أثر التقانة على المنظور والعمل الأمني». مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من ٢١-٢٤ من ذي القعدة ١٤٢٨هـ الموافق ١-٤ ديسمبر ٢٠٠٧م. المجلد (٣)، الرياض، رئاسة الاستخبارات العامة.

محمود، نيفين أمين (٢٠٠٧م). «تسرب المعلومات عن طريق الانبعاث الكهرومغناطيسي وطرق التأمين المقترحة». مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من ٢١-٢٤ من ذي القعدة ١٤٢٨هـ الموافق ١-٤ ديسمبر ٢٠٠٧م. المجلد (٣)، الرياض، رئاسة الاستخبارات العامة.

مدني، سالم بن حمزة (٢٠٠٧م). «مدة إمكانية تطبيق الحدود على الجرائم الإلكترونية». ورقة مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، الجرائم الإلكترونية الملامح والأبعاد المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من ٥-٧ ربيع الثاني ١٤٢٨هـ الموافق ٢٢-٢٤ أبريل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

المديرية العامة للجوازات (٢٠٠٩م). بيان بأعداد المحققين الجنائيين والفنيين العاملين في مكافحة التزوير وأبحاث التزوير بالجوازات. شؤون الضباط، الرياض، المديرية العامة للجوازات.

مرسي، إبراهيم حامد (د•ت). سلطـــات مأمورية الضبط القضائي. القاهرة، دار النهضة العربية.

مرسي، عبد الواحد إمام (١٩٩٦م). الموسوعة الذهبية في التحريات. القاهرة، دار المعارف.

المركـز الوطنـي للتصديق الرقمي (٢٠٠٨م). مهام المركـز الوطني للتصديق الرقمي. الرياض، وزارة الاتصالات وتقنية المعلومات.

المزيد، عبد العزيز والشـهري، عبد الله (٢٠٠٧م). «تشـفير البريد الإلكتروني لاتصـالات أكثر أماناً». مؤتمر تقنية المعلومات والأمن الوطني المنعقد في الرياض في الفترة من ٢١ـ٢٤ من ذي القعدة ١٤٢٨هـ الموافق ١ـ٤ ديسمبر ٢٠٠٧م. المجلد(٣)، الرياض، رئاسة الاستخبارات العامة.

المسـعودي، ريم بنت أحمد والحلبي، وديع بن صالح الطيار (٢٠٠٧م). «آلية استخدام التوقيع الإلكتروني في الوكالات بالمحاكم الشرعية بالمملكة العربية السعودية». ورقة مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، الجرائم الإلكترونية الملامح والأبعاد المنعقدة بكلية الملـك فهد الأمنية بالريـاض في الفترة من ٥ـ٧ ربيـع الثاني ١٤٢٨هـ الموافق ٢٢ـ٢٤ أبريل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

مصطفـى، محمـود محمـود (١٩٧٧م). الإثبـات في المواد الجنائيـة في القانون المقارن. القاهرة، مطبعة جامعة القاهرة.

ابن مفلح، برهان الدين بن إبراهيم بن محمد بن عبد الله (١٩٨٨م). الفروع. بيروت، دار الكتب العلمية.

الملـط، أحمـد خليفـة (٢٠٠٥م). الجرائـم المعلوماتيـة. القاهـرة، دار الفكـر الجامعي.

الموجان، إبراهيم بن حسين (٢٠٠٣م). إيضاحات على نظام الإجراءات الجزائية. الرياض، مكتبة الملك فهد الوطنية.

موسى، مصطفى محمد (٢٠٠٣م). أساليب إجرامية للتقنية الرقمية، ماهيتها، مكافحتها. القاهرة، در النهضة العربية.

النجيمي، محمد بن يحيى بن حسن (٢٠٠٧م). «الجرائم الإلكترونية من وجهة النظر الإسلامية والقانونية». ورقة مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، الجرائم الإلكترونية الملامح والأبعاد المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من ٥-٧ ربيع الثاني ١٤٢٨هـ الموافق ٢٢-٢٤ أبريل ٢٠٠٧م. الرياض، كلية الملك فهد الأمنية.

النمر، أبو العلا (١٩٩١م). الأدلة الجنائية في ضوء الفقه وأحكام النقض الجنائي، دراسة تحليلية للدليل الجنائي فقهاً وعملاً. القاهرة، دار الصداقة.

النمر، سعود بن محمد وآخرون (٢٠٠٦م). الإدارة العامة، الأسس والوظائف. (ط٦)، الرياض، مطابع الفرزدق التجارية.

الهيتي، محمد حماد مرهج (٢٠٠٥م). جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها. عمّان، دار المناهج للنشر والتوزيع.

وقيع الله، محمد أحمد (٢٠٠٣م). أساليب التزوير وطرق كشفها. الرياض، جامعة نايف العربية للعلوم الأمنية.

اليوسف، عبد الله بن عبد العزيز (١٩٩٩م). الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض، جامعة نايف العربية للعلوم الأمنية.

اليوسف، عبد الله بن محمد (٢٠٠٧م). أنظمة تحقيق الشخصية، نشأة وتطور. الرياض، جامعة نايف العربية للعلوم الأمنية.
يونس، عمر محمد أبو بكر (٢٠٠٦م). «مذكرات في الإثبات الجنائي عبر الإنترنت». ورقة عمل مقدمة ضمن ندوة الدليل الرقمي المنعقدة في القاهرة بتاريخ ٥/ ٨/ ٢٠٠٦م.

ثانياً: البحوث والدراسات

أبو مغايض، يحيى محمد علي (٢٠٠٤م). الحكومة الإلكترونية في المؤسسات العامة بالمملكة العربية السعودية. رسالة ماجستير غير منشورة، الرياض، جامعة الملك سعود.
الردادي، أحمد بن دخيل الله (١٩٨٩م). معاينة مسرح الجريمة بين النظرية والتطبيق. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.
الرشودي، أحمد بن عبد الله (٢٠٠٨م). حجية الوسائل الإلكترونية في الإثبات الجنائي، دراسة تأصيلية مقارنة تطبيقية. رسالة دكتوراه غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.
الشهري، عبد الله محمد (٢٠٠٢م). المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي، دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض. رسالة ماجستير غير منشورة، الرياض، جامعة الملك سعود.
العنزي، إبراهيم بن سطم (٢٠٠٤م). البصمة الوراثية ودورها في الإثبات الجنائي بين الشريعة الإسلامية والقانون الوضعي. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.

الملا، صالح أحمد عبد الله (١٩٩٤م). التنسيق النموذجي بين المحقق والخبراء في مسرح الجريمة. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.

المنشاوي، محمد بن عبد الله بن علي (٢٠٠٣م). جرائم الإنترنت في المجتمع السعودي. رسالة ماجستير غير منشورة، الرياض، جامعة نايف العربية للعلوم الأمنية.

ثالثاً: معاجم المصطلحات

إبراهيم، مصطفى وآخرون (١٣٩٢هـ). المعجم الوسيط. استانبول، المكتبة الإسلامية.

جميل، صليبا (١٩٧١م). المعجم الفسلفي. بيروت، دار الكتب اللبناني.

رابعاً، المجلات والدوريات

باتوباره، نواف عبد الله أحمد (١٩٩٨م). «منافع والتزامات ومخاطر بطاقة الائتمان». المجلة العربية للدراسات الأمنية والتدريب، السنة (١٣)، م (١٣)، ع(٢٥)، الرياض، جامعة نايف العربية للعلوم الأمنية.

البشرى، محمد الأمين (٢٠٠٠م). «التحقيق في جرائم الحاسب الآلي والإنترنت». المجلة العربية للدراسات الأمنية والتدريب، م(١٥)، ع(٣٠)، الرياض، جامعة نايف العربية للعلوم الأمنية.

ـــــــــــــ (١٤٢٣هـ). «الأدلة الرقمية ودورها في الإثبات». المجلة العربية للدراسات الأمنية والتدريب، م(١٧)، ع(٣٣)، الرياض، نايف العربية للعلوم الأمنية.

عبد المطلب، صلاح الدين عبد الحميد (٢٠٠٨م). «كيفية الاستفادة من المحاكاة الحاسوبية في أعمال البحث والتحقيق الجنائي». مجلة البحوث

الأمنيـة، م(١٦)، ع(٣٨). الريـاض، مركـز البحـوث والدراسـات بكلية الملك فهد الأمنية.

المسـند، صالـح والمهيني، عبد الرحمـن (٢٠٠١م). «جرائم الحاسـب الآلي، الخطـر الحقيقـي في عـصر المعلومـات». المجلـة العربية للدراسـات الأمنية والتدريب، السـنة (١٥)، م(١٥)، ع(٢٩)، الرياض، جامعة نايف العربية للعلوم الأمنية.

خامساً : المراجع الأجنبية

Arabiat (2002). [Online]. Available: http://www.aims.cjb.net[17.10.2002].

Ashbourn, Julian (2000). Biometrics: Advanced Identity Verification. London: Springer-Verlag Limited.

Casey, E, (2000) Digital Evidence Computer Crime, San Diego, CA: ACADMIC press.

Cert. C. (2002). CERT Advisories and Other Security Information. Pittsburgh, PA. (Online). Available: http://www.cert.org/. [25. 9. 2002].

Douglass, John and Burger, W. (1992). Crime Classification Manual- An Standard for Investigation. Toronto: Macmillan.

Erdonmez, E. (2002). Investigation of Computer Crime. Unpublished M.A., University of North Texas, Denton. Texas.

Etter, Barbara (2001) Computer Crime. Paper Presented to the 4th National Outlook Symposium on Crime in Australia, New Crimes or New Response. (online). Available. at: http://www.aic.gov.an/conferences/outlook4/Etter.pdf(19 -04-2003)

Fernandez, J., et. al. (2005). «Computer Forensics: a Critical need in Computer Science Programs. Journal of Computing Sciences in Colleges. pp. 315-322.

G. L. Peterson, et. al. (2007). «Graduate Digital Forensics Education at the Air Force Institute of Technology». In HICSS `07: Proceedings of the 40th Annual Hawii International Conference on System Sciences. IEEE Computer Society.

Goodman, Mark (1997). «Why The Police Don't Care About Computer Crimes». Harvard Journal of Law & Technology, Vol. 10, No. (3), 465-494.

Groover, Richard (1996). Overcoming Obstacles: Preparing for Computer-related Crime. New York: McGrowhell.

Hollis, s. David,s. B., David, J.I., Richard B. Wayne, c. & wayne, p.w. (2001) Electronic Crime Needs Assessment for State & local law Enforcement. (online). Available:

http://www.ncjrs.org/pdffi:les/nij/186276.pdf(19-10-2003)

Kelly, Harris (1995). Computer Crime: An Overview?

Marr, Kenneth (2003). Digital evidence subcommittee and discussion. Journal of forensic Identification. Vol. 53. No.6.

Nanavati, Thieme Nanavati (2002). Biometrics: Identity Verification in an Network World. New York: John Wiley & Sons Inc.

Rapalus, P. (2002). CSI/FBI Computer Crime and Security

Survey. Computer Security Institute with the Participation of the Federal Bureau of Investigation (FBI).

Smith, B. & komar B. (2003) Microsoft Windows Security. Washington: Microsoft Press.

Stephenson, Peter (1999). Investigating Computer Related Crimes. London: CRC.

Swanson, Charles, et. Al. (1981). Criminal Investigation. New Y ork: Random house.

Tillers, Peter (1999). Introduction to Program on Artificial Intelligence. New York: Yeshvia University Press.

Tim, W. (1998). Profits Embolden Hackers. Internet Week (march: 23).

Thompson, David (1991). Investigative Skills for the 1990s and Beyond. Paper Presented at the Conference: Asia Pacific Police Technology, Organized by the Australian Institute of Criminology, Canberra, 12-14 November 1991.

United Nations (1999). United Nations Manual on the Prevention and Control of Computer Related Crimes. Vienna.

Wahlert, Glenn (1998). Computer Crime in Australian Financial Sector. Paper Presented at the Conference: Crime Against Business. Organized by the Australian Institute of Criminology, Melbourne, 18-19 June 1998.

(www:http://online.securityfocus.com/infocus/124).