تمهيد:

الإثبات الجنائي نشاط إجرائي موجه مباشرة للوصول إلى اليقين القضائي طبقًا لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي[١](*)، وبمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين[٢].

والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة ، فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات ، ووسيلة الإثبات هي كل ما يستخدم في إثبات الحقيقة – فهي نشاط يبذل في سبيل اكتشاف حالة أو مسألة أو شخص أو شيء ما أو ما يفيد في إظهار عناصر الإثبات المختلفة – أي الأدلة – ونقلها إلى المجال الواقعي الملموس[٣] ، وتثير مسألة الإثبات في نظم الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق ، وذلك لجملة أمور لا يسعنا ذكرها كلها[٤] ، لكن نذكر أمثلة منها:-كالتخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة ، ويشكل انعدام الدليل المرئي (المفهوم) عقبة كبيرة أمام كشف الجرائم ، وقد يشكل تشفير البيانات المخزنة إلكترونيًا أو المنقولة عبر شبكات الاتصال عن بُعد عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة ، كما أن سهولة محو الدليل في زمن قصير تُعد من أهم

١- د. آمال عبد الرحيم عثمان – الإثبات الجنائي ووسائل التحقيق العلمية – دار النهضة العربية – القاهرة – ١٩٧٥م ص ٤.

* **استخدم الباحث طريقة التوثيق(الحواشي السفلية)** (**Footnote References**) .

٢- د. محمود محمود مصطفى – شرح قانون الإجراءات الجنائية – ط١١- القاهرة – ١٩٧٦م .– ص ٤١٤

٣- د. آمال عبد الرحيم عثمان –مصدر سابق– ص ٢٤.

٤- للمزيد من المعلومات انظر: د.سعيد عبد اللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – ط١ – دار النهضة العربية – القاهرة – ١٩٩٩م، ص ٩٥ وما بعدها.

الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت ، ومن الأمثلة الواقعية على ما تقدم ما حصل في دولة الإمارات العربية المتحدة ، حيث قام مشغل حاسوب بتهديد المؤسسة التي يعمل لديها بتنفيذ مجموعة من مطالبه، وذلك بعد أن حذف كافة البيانات الموجودة على الجهاز الرئيسي للمؤسسة، وقد رفضت المؤسسة الاستجابة لمطالبه فأقدم على الانتحار ، ووجدت المؤسسة صعوبة في استرجاع البيانات التي كانت قد حذفت[٥] ، وتتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد ، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثًا عن الأدلة وتحقيقها ، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية ، حيث أن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة ، ولما كانت أدلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال[٦] ، فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي إلى ضياع الدليل بل تدميره أحيانًا[٧] ، ويضاف إلى ذلك أن كل المعطيات ليس لها تجسيد دائم على أية دعامة ، بمعنى أنها لا توجد مسجلة على أسطوانة صلبة أو مرنة ولا على أية دعامة مادية منقولة أيًا كانت فقد توجد هذه المعطيات في الذاكرة الحية للحاسوب ، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة ، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية إلا أنه

---

[5]- وغيرها من الأمثلة الواقعية انظر: د.هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – ص ٣٥ وما بعدها، وانظر: د.عبد الفتاح –دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م- ص ٤٦.

[6]- يتردد الضحايا في الجرائم المعلوماتية عن كشف المعلومات حول ما يقع عليهم أو مؤسساتهم خوفًا من فقدان الثقة بهم أو الإساءة لسمعة مؤسساتهم والتبعات الاقتصادية المترتبة على ذلك ، انظر: الرائد كمال الكركي – جرائم الحاسوب ودور مديرية الأمن في مكافحتها – ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى ص ١٠ وما بعدها.– المستقبل – المنعقدة في عمان بتاريخ ٥/٧/١٩٩٩م

[7]- انظر: أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة – جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط١ – دار وائل – عمان – ٢٠٠١م- ص ٢٨٩-٢٩٧.

قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية ، وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن الجرائم المعلوماتية إلى السلطات المختصة[٨] ، بالإضافة لما تقدم من صعوبات ومشكلات[٩]. ،

مشكلة البحث:

ومن أهمية مشروعية الدليل الالكتروني الصادر عن التفتيش الجنائي

لجأ الباحث لعمل دراسته في البحث الحالي ردا على التساؤل عما إذا كان الدليل المستمد من التفتيش يحتاج إلى شروط وللإجابة عن هذا التساؤل يقسم الباحث هذا المطلب إلى مبحثين : المبحث الأول :في شروط الدليل الإلكتروني المستمدة من التفتيش ، والمبحث الثاني : في حجية الدليل الإلكتروني الناشئ عن التفتيش.

مشكلة البحث:

مشروعية الدليل الالكتروني الصادر عن التفتيش الجنائي "دراسة مقارنة"

المبحث الأول

شروط الدليل الإلكتروني المستمد من التفتيش

إن الأدلة الإلكترونية ، إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات ، أو الراسم ، وإما أن تكون مخرجات غير ورقية أو أن تكون إلكترونية : كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية[١٠] ، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على

---

[8]- لقد كشفت إحصائيات شركات التأمين في فرنسا عن أن نسبة الإبلاغ عن جرائم الحاسوب والإنترنت تتراوح بين (٥-١٠%) من مجموع الجرائم التي ارتكبت في هذا المجال، انظر د.جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية) – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م- ص ١١٦.

[9]- تعتبر الجريمة المعلوماتية جريمة بيضاء تعتمد على ذكاء عالٍ في ارتكابها ، انظر: محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – ٢٠٠١م- ص ١٠٣.

[10]-Welch , Thomas – Op . Cit - P.56.

الشاشة الخاصة به ، أو الإنترنت بواسطة الشاشات أو وحدة العرض المرئي[١١] ، ويكون الدليل باطلاً إذا استحصل عليه عن طريق مخالفة القانون ، ولهذا الموضوع أهمية بالغة لما يترتب على بطلان الدليل من آثار، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم ، فإذ ما شاب التفتيش الواقع على نظم الحاسوب عيب فإنه يبطله ، والتفتيش الذي يقوم به المحقق بغير الشروط التي نص عليها القانون يعتبر باطلاً بطلانًا مطلقًا ولا يجوز التمسك بما ورد في محضر التفتيش كما لا يجوز للمحكمة أن تعتمد عليه في حكمها[١٢]. ويقع عبء إثبات الجرائم المعلوماتية على عاتق النيابة العامة ، كما أن المدعي بالحق الشخصي يشارك النيابة العامة هذا العبء ، وفي أحيان أخرى ينقل القانون عبء الإثبات من النيابة العامة إلى عاتق المشتكى عليه[١٣] ، وأعطى المشرع الأردني النيابة العامة سلطة التحري وجمع الأدلة من خلال قانون أصول المحاكمات الجزائية ، وقد نصت المادة (١٧) منه على أنه: (١-المدعي العام مكلف باستقصاء الجرائم وتعقب مرتكبيها. ٢-ويقوم بذلك على السواء المدَّعون العامّون المختصون وفقًا لأحكام المادة (٥) من هذا القانون) ، والدليل المتحصل من تفتيش نظم الحاسوب والإنترنت لا يكون مشروعًا ، ويعتبر باطلاً إذا تم الحصول عليه بغير الشروط التالية:-

-الشرط الأول:يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات[١٤] : إن أهم هدف للدستور هو صيانة كرامة الإنسان

11- انظر: د.هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م- ص ١٤-٢٢.

12- أ. عبد الأمير العكيلي - أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية –ج١ – ط١ ص ٣٤٨.– مطبعة المعارف – بغداد – ١٩٧٥م

13- انظر: د. نائل عبد الرحمن صالح – محاضرات في قانون أصول المحاكمات الجزائية – ط١ – دار الفكر العربي – عمان – ١٩٩٧م- ص ١٧ وما بعدها.

14-وفي مشروعية الدليل المستمد من التفتيش ، انظر: د. رمزي رياض عوض ص ٨٥ وما – ١٩٩٧م – القاهرة – دار النهضة العربية – دراسة تحليلية تأصيلية مقارنة –المحاكمة وما قبلها بعدها.وانظر: د. أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة – دار النهضة العربية – القاهرة – ١٩٩٤م – ص ١٦ وما بعدها.

وحماية حقوقه لذلك تتضمن الدساتير الحديثة نصوصًا تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها ، بحيث يتقيد المشرع بها عند وضع قانون أصول المحاكمات الجزائية ، فنص الدستور الأردني في المادة (١٠) منه على أن: (للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المُبيّنة في القانون ، وبالكيفية المنصوص عليها فيه) ، ونصت كذلك المادة (١٨) من الدستور الأردني أيضًا على أنه: (تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية فلا تخضع للمراقبة أو التوقيف إلا في الأحوال المعينة في القانون) ، فهذه النصوص الواردة في الدستور تفرض على المشرع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها ، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام ، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها ، ونرى ضرورة أن يقوم المشرع الأردني بتشريع نصوص إجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب والإنترنت ، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانوني ، حماية للحقوق والحريات الفردية التي كفلها الدستور الأردني ، بالإضافة إلى المواثيق الدولية.

أما جزاء مخالفة القانون في الحصول على الأدلة فيترتب عليه جزاءات جنائية أو إدارية فضلاً عن الحكم بالتعويض ، فالموظف الذي يعهد إليه القانون بعمل فيتصرف على وجه مخالف يعد مقصرًا في عمله ومخالفًا في واجباته فيستحق المؤاخذة[١٥] ، والمهم هنا هو الجزاء الإجرائي إذ لا شك إن الدليل المستخلص عن طريق ارتكاب جريمة يكون باطلاً بطلانًا متعلقًا بالنظام العام ، ومن أمثلة ذلك ما نصت عليه المادة

[15]- انظر: د. علي حسن الطوالبه،التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة،ط١،عالم الكتب الحديث،اربد،٢٠٠٤م،ص١٧٩.

(٣٤٧) من قانون العقوبات الأردني على أنه: (١-من دخل مسكن آخر أو ملحقات مسكنه خلافًا لإرادة ذلك الآخر ، وكذلك من مكث في الأماكن المذكورة خلافًا لإرادة من له الحق في إقصائه عنها عوقب بالحبس مدة لا تتجاوز الستة أشهر) ، وكذلك نص المادة (٣٥٥) من قانون العقوبات الأردني التي جاء فيها: (يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من :١-حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الإطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الإطلاع وفقًا للمصلحة العامة.٢-كان يقوم بوظيفة رسمية أو خدمةٍ حكومية واستبقى بحيازته وثائق سرية أو رسومًا أو مخططات أو نماذج أو نسخًا منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقتضي ذلك طبيعة وظيفته. ٣-كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع.) ، ولم يقتصر المشرع في حمايته لأسرار الأفراد على الاطلاع عليها بطرق عادية بل شمل حتى الأسرار داخل المراسلات والبرقيات ، فنصت المادة (٣٥٦) عقوبات أردني على أنه: (١-يعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يسيء استعمال وظيفته هذه بأن يطلع على رسالة مظروفة أو يتلف أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسل إليه.

٢-ويعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين دينار من كان ملحقًا بمصلحة الهاتف وأفشى مخابرة اطلع عليها بحكم وظيفته أو عمله) ، وفي جميع هذه الحالات يرتب العمل المخالف للقانون لمن وقع عليه الحق في التعويض فضلاً عن استحقاق القائم به للعقوبة الجنائية مع وجوب بطلان هذا العمل كونه وليد جريمة ، وبالتالي بطلان الدليل الذي استمد منه هذا العمل ، لأن ما يبنى على الباطل يكون باطلاً ، ويرى الباحث إمكانية انطباق القواعد التقليدية على هؤلاء المذكورين في النصوص السابقة ، في حالة اطلاعهم بحكم وظائفهم على أسرار المواطنين عبر أجهزة الحاسوب أو شبكاته من خلال أدائهم لوظائفهم ، لكن يبقى التساؤل على من

تم ذكرهم أعلاه كشهود على الجريمة المعلوماتية ، فهل هم ملزمون أن يقوموا بطبع ملفات البيانات المخزنة في ذاكرة الحاسوب مفشين للسر ، أو الإفصاح عن كلمات المرور السرية ، أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج؟

لقد اختلف الفقه المقارن في الإجابة عن هذا التساؤل بين مؤيد ومعارض ويمكن بلورة هذا الخلاف في اتجاهين رئيسين هما[١٦]:-

-الاتجاه الأول: يذهب أصحابه إلى أنه ليس من واجب الشاهد ، وفقًا للالتزامات التقليدية للشهادة -أن يقوم بما تم ذكره سابقًا - ففي لوكسبورغ ، الشاهد ليس مجبرًا على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة ، وبالتالي من الصعب إجباره على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه في ذاكرة الحاسوب ، وإن كان يستطيع الوصول إليها نظرًا لمعرفته بكلمات المرور السرية[١٧] ، أما إذا تعاون الشاهد على هذا النحو فإن دوره يكون أقرب إلى الخبرة منه إلى الشهادة ، وفي ألمانيا ، تذهب غالبية الفقه إلى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب ، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب ، وفي تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية ، أو كشف شفرات تشغيل البرامج المختلفة.

ففي فرنسا يرى جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفًا بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج[١٨] ، ما عدا حالات المحافظة على سر المهنة ، فإنه يكون في حل من الالتزام بأداء الشهادة ،

---

[16]- للمزيد من المعلومات انظر: د. هلالي عبدالاه أحمد دراسة – التزام الشاهد بالإعلام في الجرائم المعلوماتية – ص ٥٢-٥٦.– ٢٠٠٠م – القاهرة – النسر الذهبي –مقارنة

[17]- Concil of Europe activites relaled to Information Technology , Data Protection and computer crime , esonka , Peter-Information and Communiction Technology Law – Oat 19 96.Vol.5.Issue 3.P177.

[18]- د.هشام محمد فريد رستم – جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة – مجلة الدراسات القانونية – جامعة أسيوط – العدد ١٧- ١٩٩٥م- ص ١١٧.

وفي هولندا يتيح قانون الحاسوب لسلطات التحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله ، كالإفصاح عن كلمات المرور السرية ، والشفرات الخاصة بتشغيل البرامج المختلفة ، أو حل رموز البيانات المشفرة[١٩].

الاتجاه الثاني: ويرى أنصاره أن من الالتزامات التي يجب أن يقوم بها الشاهد ، هي طبع ملفات البيانات ، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ، وفي إطار مشروعية الأدلة الإلكترونية ، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة ، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية ، أم في مجال التنقيب في جرائم الحاسوب والإنترنت ، كأن يستخدم أعضاء الضابطة العدلية طرقًا معلوماتية في أعمال التنصت على المحادثات الهاتفية ، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ، ومن بينها الأدلة المتحصلة من الحاسوب والإنترنت ، بطريقة شرعية ونزيهة ، ونفس الشيء نجده في سويسرا وبلجيكا[٢٠]. وفي بريطانيا ، قامت الشرطة بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناءً على موافقتها ، وقد أجرت الشاكية عدة مكالمات هاتفية مع الشخص الذي كانت الشرطة تشك في ارتكابه الجريمة ، وقد تم تسجيل هذه المكالمات التي تضمنت موضوعات تدين المتهم ، لكن القاضي استبعد هذه التسجيلات على أساس أنها تمت من خلال شرك خداعي[٢١] ، أما في هولندا ، فإذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية ، فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات ، وعدم

[19]- Jeffrey , Sassinsky – Computer Forensices – Op-cit – P.9.

[20]- انظر: د. هلالي عبداله أحمد –مصدر سابق – حجية المخرجات الكمبيوترية – ص ١٢١-١٢٢.

[21]- د. هلالي عبداله أحمد – المصدر السابق – ص ١٣٢.

إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية[٢٢] ، أما في اليابان فقد أصدرت محكمة مقاطعة (KOFV) حكماً أقرت فيه مشروعية التنصت للبحث عن الدليل ، حيث ضرورة التحريات ، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار،لكن الفقه الياباني ، يرى أن الأدلة الجنائية التي يتم الحصول عليها بطرق مشروعة يجب أن تكون مستبعدة سواء كانت تقليدية أم أدلة حاسوب أم أدلة إنترنت[٢٣]. ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية ، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة ، أو التحريض على ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية ، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي ، والاستخدام غير المصرح به للحاسوب ، والتنصت ، والمراقبة الإلكترونية عن بُعد[٢٤].

وتُعد من الطرق غير المشروعة أيضًا استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية[٢٥] ، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في ١٩٨١/١/٢٨م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية ، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ، ومستمدة بطرق مشروعة ، ومدة حفظها محددة زمنيًا ، وعدم إفشائها أو استعمالها في

---

[22]- إن البيانات التي تجمعها الشرطة عن الأشخاص من أجل حماية الأمن العام يجب أن تبقى تحت سلطة هؤلاء الموظفين بسبب وظيفتهم في حماية الأمن العام ، وهي أساس عملهم بهذه البيانات ، ومن ثم يجب منع غيرهم من الوصول إليها ممن ليس لهم نفس الاختصاص في إطار الحفاظ على سرية هذه البيانات وحق الخصوصية ، انظر: د. – ط٢- دار النهضة العربية – دراسة مقارنة – الحماية الجنائية للحياة الخاصة وبنوك المعلومات –اسامة عبدالله قايد ص ٩٣-٩٤.– ١٩٨٩م –القاهرة

[23]- د. هلالي عبدالاه أحمد- حجية المخرجات ص ١٣٧.– مصدر سابق –

[24]- انظر: د. جميل عبد الباقي الصغير ص ١١١.–مصدر سابق – أدلة الإثبات الجنائي–

[25]- د. جميل عبد الباقي الصغير-أدلة الإثبات الجنائي ص ١١٢.–المصدر السابق –

غير الأغراض المخصصة لها ، وحق الشخص المعني في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[٢٦] ، ولقد تضمن قانون الشرطة والإثبات الجنائي الإنكليزي لعام ١٩٨٤م ، تحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تقبل أمام القضاء ، وتضمن كذلك توجيهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب ، فأوصت المادة (١١) منه[٢٧] ، بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسوب المقبولة في الإثبات طبقًا للمادة (٦٩) من القانون نفسه ، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات المتعلقة بأمر قد تم تزويد الحاسوب بها في وقت معاصر لهذا الأمر أم لا ، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيانات من الحاسوب لديه دافع لإخفاء الوقائع أو تشويهها ، وقد نصت المادة (٦٩) على ثلاثة شروط أساسية هي[٢٨]:-

١-يجب ألا يوجد أساس معقول للاعتقاد أن البيان الخاطئ أو غير دقيق ، بسبب الاستعمال الخاطئ (الاستعمال غير الملائم للظروف أو للغرض الذي يستخدم من أجله الحاسوب).

٢-يجب أن تكون جميع المكونات المادية للحاسوب كانت تعمل بدقة وعلى نحو متوافق كما ينبغي.

٣-إن أيًا من الشروط المحددة (التي تدخل في متطلبات القبول) المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة ، ولقد قضت محكمة الاستئناف الجنائي في إنكلترا بذلك ، حيث بينت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسوب ، ويتلخص الحكم بما يلي: (أنه يبدو لهذه المحكمة – أنه من الخاطئ رفض أو إنكار

---

[26]- محمد محمد شتا –مصدر سابق ص ١٠٤-١٠٥.

[27]-Police and Criminal Evidence Act 1984- Op – Cit-P.28.

[28]-Police and Criminal Evidence Act 1984- Op – Cit-P.25..

أية مزايا أو صلاحيات مقررة وفقًا لقانون الإثبات ، يمكن بمقتضاها التوصل عن طريق التقنيات الجديدة والوسائل الحديثة التأكد من صحة وصدق التسجيل ، حيث يمكن التثبت من ذلك ، وكذلك يمكن التعرف بوضوح على الأصوات المسجلة ، والمستخلص أيضًا هو أن الدليل وثيق الصلة بالموضوع ، من جهة أخرى ، يمكن قبوله ، ومن ثم تؤيد المحكمة قبول هذه الأشرطة ويجب أن ينظر دائمًا بعين الاعتبار إلى مثل هذا الدليل ، وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية)[٢٩].

–الشرط الثاني: يجب أن تكون الأدلة الإلكترونية غير قابلة للشك أي يقينية:يُشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة ، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين ، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية ، والمصغرات الفيلمية ، وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر ، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات ، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية ، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، ان يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.

ويشترط قانون البوليس والإثبات في بريطانيا لسنة ١٩٨٤م ، حتى تتحقق يقينية الأدلة الإلكترونية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة[٣٠] ، أما في كندا ، فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة ، لذا فإنها تحقق اليقين المنشود في الأحكام الجنائية.

---

[29]- انظر: د. سعيد عبد اللطيف حسن ص ١٩٩-٢٠٠.–مصدر سابق–

[30]- Naughan Bevan and Ken Lidstone – Aguide to the Police and Criminal Evidence Act 1984- Bulterworthe – London – 1985- P.497.

ونصت بعض قوانين الولايات في أمريكا ، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تُعد من أفضل الأدلة المتاحة لإثبات هذه البيانات ، وبالتالي يتحقق مبدأ اليقين لهذه الأدلة ، و تنص القواعد الفيدرالية على أن: (الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل ، كشرط مسبق لقبوله ، هو أن يفي بأمارة أو بينة كافية لأن تدعم اكتشاف (أو الوصول) إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعي بها)[٣١].

ويقرر الفقه الياباني قبول الأدلة المستخرجة من الحاسوب التي تم تحويلها إلى الصورة المرئية سواء كانت هي الأصل أم كانت نسخًا مستخرجة عن هذا الأصل ، وذلك استنادًا على الاستثناءات التشريعية المنصوص عليها في المادة (٣٢٣) من قانون الإجراءات الجنائية الياباني ، ففي هذه الحالة يتحقق اليقين الذي يبنى عليه الحكم الجنائي ، كما يمكن أن يتحقق اليقين لهذه المخرجات أيضًا من خلال التقارير التي يقدمها الخبراء ، وفي تشيلي ينص أحد القوانين الخاصة بالحاسوب على قبول السجلات الممغنطة للحاسوب وكذلك النسخ الناتجة عنها،ومعنى ذلك أن هذه السجلات وصورها تحقق اليقين المنشود لإصدار الأحكام الجنائية ، كما يتحقق هذا اليقين أيضًا عن طريق تقارير الخبراء الصادرة في عناصر معالجة البيانات (المادة ٢٢١ من قانون أصول المحاكمات الجزائية التشيلي)[٣٢].واعتبر المشرع الأردني نظام المعالجة الإلكتروني مؤهلاً لإثبات تحويل الحق مما يسهل على المحقق ضبط الدليل الإلكتروني وذلك من خلال نص المادة (٢١) من قانون المعاملات الإلكترونية رقم (٨٥) لسنة ٢٠٠١م ،والتي جاء فيها بأن : (أ- يعتبر نظام المعالجة الإلكتروني مؤهلاً لإثبات تحويل الحق في السند تطبيقاً لأحكام المادة (٢٠) من هذا القانون إذا

31- د. سعيد عبد اللطيف حسن –مصدر سابق– ص ١٥٩.

32- د. هلالي عبداله أحمد –حجية المخرجات الكمبيوترية– ص ٩٦.- مصدر سابق

كان ذلك النظام يسمح بإنشاء السند الإلكتروني وحفظه وتحويله وذلك بتوافر الشرطين التاليين مجتمعين:

١-إذا كانت النسخة المعتمدة من السند القابل للتحويل محددة بصورة غير قابلة للتغيير وذلك مع مراعاة أحكام الفقرة (ج) من هذه المادة.

٢-إذا كانت النسخة المعتمدة من السند تدل على اسم الشخص الذي تم سحب السند لمصلحته وأن السند قابل للتحويل وتضمنت اسم المستفيد.

ب-ترسل النسخة المعتمدة وتحفظ من قبل الشخص الذي يملك الحق فيها أو الشخص المودعة لديه لمصلحة صاحب الحق في السند.

ج-١-تعتمد النسخ المأخوذة عن النسخة المعتمدة التي حدث عليها تغيير أو إضافة بموافقة من الشخص الذي يملك حق التصرف في السند.

٢-يؤشر على كل نسخة مأخوذة من السند بأنها معتمدة أو غير معتمدة.

٣-تعرف كل نسخة مأخوذة من النسخة المعتمدة بأنها نسخة مطابقة للنسخة المعتمدة.). يتضح من هذا النص إمكانية إثبات الحق مما يُمكن المحقق من استخدام هذه الوسائل أيضًا بالإضافة للوسائل السابق الإشارة إليها في تفتيش نظم الحاسوب والإنترنت.

الشرط الثالث: إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسوب والإنترنت:ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[٣٣] ، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب ، أم كانت بيانات مدرجة في حاملات البيانات ، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية ، كل هذه ستكون محلاً للمناقشة عند

33- قرار محكمة النقض المصرية في ١٩٨٦/١١/٢٠م ص ٩٤٣.– المبادئ القانونية – رقم ١٧٩ –

الأخذ بها كأدلة إثبات أمام المحكمة ، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات ، يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي ، لكن بصفة مباشرة أمام القاضي ، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الحواسيب، وأيضًا بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي ، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة[٣٤] ، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم[٣٥] ، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم ، أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة وكشفًا للحق.

ومن القواعد العامة المستقرة في القانون الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية ، إلا في حالات استثنائية حصرها القانون بشروط مشددة[٣٦] ، ويُعزى عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع ، ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجنائية الإلكترونية ، على سبيل المثال ، لقد تضمنت القواعد الفيدرالية الأمريكية نصًا يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية استثناءً للبينة السماعية ، وبناءً على تلك القواعد تعد التقارير والمعلومات والبيانات المحفوظة في أي شكل ، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها

---

[34]- والشاهد المعلوماتي : هو الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسوب والذي تكون لديه معلومات جوهرية لازمة لولوج لنظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ، ص ٢٣ وما بعدها. – مصدر سابق – التزام الشاهد–انظر: د. هلالي عبدالاه أحمد

[35]- انظر: د. محمد فهمي طلبه وآخرون– دائرة المعارف الحاسب الإلكتروني – مجموعة كتب دلتا – ص ٣١ وما بعدها.– مطابع المكتب المصري الحديث – القاهرة – ١٩٩١م

[36]- وهناك استثناءات على هذه القاعدة نص عليها القانون انظر: المواد (١٥٦ ،١٥٧ ، ١٦٢) من قانون أصول المحاكمات الجزائية الأردني.

من الأدلة السماعية ، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آليًا بأسلوب علمي[٣٧].

وللإجابة عن التساؤل الذي طُرح في مقدمة هذا المطلب حول إمكانية ضبط الأدلة ومشروعيتها إذا كانت النهاية الطرفية للنظام المعلوماتي في منزل آخر غير منزل المتهم ، فقد أجاز قانون جريمة الحاسوب الهولندي في المادة (٢٥/أ) منه ، إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلي... موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول..في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها ، وبالتالي أجاز المشرع للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من المحقق المختص ، إلا أن هذه السلطة غير مطلقة بل هي مقيدة بقيود ثلاثة هي[٣٨]:

١-ألا تكون النهاية الطرفية المتصل بها الحاسوب موجودة ضمن إقليم دولة أخرى حتى لا يؤدي الاتصال بها إلى انتهاك لسيادة الدولة الإقليمية.

٢-أن تحتوي النهاية الطرفية المتصل بها الحاسوب على بيانات ضرورية بصورة كافية لظهور الحقيقة.

٣-أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.

---

[37]- انظر: د.محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها في الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧- - العدد ٣٣-السنة ١٧ – الرياض – أبريل ٢٠٠٢م- ص ١٢٨-١٢٩.

[38]- د.عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - – دراسة مقارنة – (د.ت)- ص ٣٤٧.

ويبقى السؤال ، ماذا لو كانت النهاية الطرفية في إقليم دولة أخرى ، فكيف يمكن ضبط الدليل الإلكتروني في هذه الحالة؟ يلاحظ إن المادة (٢٥/أ) من قانون الحاسوب الهولندي استثنت هذه الحالة ، فيمكن الحصول على الأدلة حتى لو كانت في إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمني والقضائي والخاصة بالتفتيش وضبط الأدلة، وأخيرًا فإن متحصلات الجريمة المعلوماتية[٣٩] ، التي يتم ضبطها يجب أن تعرض على القاضي المختص بكافة مفرداتها وعناصرها ، وذلك لأن حيادية القاضي توجب عليه أن لا يقيم قضاءه إلا على ما طرح أمامه وكان موضوع الفحص والتحقيق والمناقشة.ويترتب على مناقشة أدلة الحاسوب والإنترنت:

النتيجة الأولى : عدم جواز أن يقضي القاضي في الجرائم المعلوماتية بناءً على معلوماته الشخصية.

والنتيجة الثانية: ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والإنترنت بشكل يتماشى مع التقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسوب والإنترنت.

المبحث الثاني

حجية الدليل الإلكتروني الناشئ عن التفتيش

إنَّ حجية المخرجات المتحصلة من الحاسوب ، هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر، بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية، من قوة استدلالية في كشف الحقيقة[٤٠].

[39]- انظر: د.هلالي عبداللاه أحمد – تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م- ص ١٣٩ وما بعدها.

[40]- د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية- مصدر سابق- ص٢٢.

لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي القوانين ذات الصياغة اللاتينية، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني، فإن حجية الأدلة الإلكترونية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات جرائم الحاسوب والإنترنت ، ولا لمدى حرية القاضي الجنائي في تقدير هذه الأدلة

ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية، وفي فرنسا مشكلة حجية المخرجات المتحصلة من الحاسوب على مستوى القانون الجنائي ليست ملحة أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة[٤١]، ويدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل أجهزة التصوير وأشرطة التسجيل وأجهزة التنصت، وقد قضت محكمة النقض الفرنسية: (إن أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي)[٤٢]، وكذلك الحال بالنسبة لكل من ألمانيا وتركيا ولوكسمبورج واليونان والبرازيل[٤٣]، وكل هذه الدول تخضع الأدلة الإلكترونية لحرية القاضي في الاقتناع الذاتي، بحيث تكون بمقدوره أن يطرح مثل هذه الأدلة–رغم قطعيتها من الناحية العلمية– ذلك عندما يجد أن الدليل الإلكتروني لا يتسق منطقيًا مع ظروف الواقعة وملابساتها[٤٤].

أما في النظم الإنجلو سكسونية التي يحدد المشرع فيها أدلة الإثبات ويقدر قيمتها الإقناعية، في طليعة هذه الدول التي تتبنى هذا النظام، بريطانيا، التي أصدرت قانون إساءة استخدام الحاسوب في عام ١٩٩٠م، الذي لم يتناول الأدلة الناتجة عن الحاسوب، وربما كان السبب هو وجود قانون البوليس والإثبات الجنائي لسنة ١٩٨٤م

41- د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية-المصدر السابق- ص ٤٢-٤٣.

42- د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية -المصدر السابق- ص ٤٣.

43- للمزيد من المعلومات عن هذه الدول أنظر: د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية -المصدر السابق- ص٤٤-٤٦.

44- Welch, Thomas- Op- cit- p55.

الذي حوى تنظيمًا محددًا لمسألة قبول مخرجات الحاسوب والإنترنت، كأدلة إثبات في المواد الجنائية[٤٥]، وفي الولايات المتحدة الأمريكية تناولت بعض القوانين حجية الأدلة الإلكترونية، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسوب لسنة ١٩٨٤م، الصادر في ولاية (أيوا)، من أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة ٧١٦/أ/١٦)، كما يتضح من قانون الإثبات الصادر في عام ١٩٨٣م في ولاية كاليفورنيا، من أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات[٤٦]، وفي كندا، يمكن قبول السجلات الناجمة عن الحاسوب، إذا توافرت شروط معينة، وتنص المادة (٢٩) من قانون الإثبات الكندي على عدد من الشروط التي يجب توافرها قبل عمل صورة (Copy)، من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان (MC Mullen)، بإنه يشترط لكي تكون سجلات الحاسوب مقبولة بوصفها نسخًا حقيقية من السجلات الإلكترونية، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفًا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كافٍ[٤٧]. وتنص قواعد الإثبات الفيدرالية الأمريكية، على أن النسخة المطابقة للأصل لها ذات حجية الأصل، أيًا كانت الطريقة أو الوسيلة المستخدمة في النسخ، كالطباعة، والتصوير، والتسجيل الميكانيكي، والتسجيل الإلكتروني، بما يسمح بقبول

---

[45] -لقد صدر تشريع الإثبات بالحاسوب في إنكلترا عام ١٩٨٣م، وقد ركز بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه والتي تزود بشهادة شفوية تكون مقبولة والتي يتم تقديرها من قبل المحكمة المختصة- انظر د. سعيد عبد اللطيف حسن- مصدر سابق- ص ١٩٤.

[46]- Csonka, peter – OP. Cit- P176-177.

[47] - للمزيد من المعلومات انظر: د. هلالي عبد الاه احمد-حجية المخرجات الكمبيوترية - مصدر سابق- ص٥٥-٥٧.

مخرجات الحاسوب في الإثبات، والغالب الأعم في القضاء الأمريكي أنه يُعول على قبول دليل السجلات المحتفظ بها على الحاسوب[٤٨].

أما في القوانين ذات الاتجاه المختلط ، وهي التي تجمع ما بين النظامين اللاتيني والانجلوسكسوني، فيعتمد النظام المختلط على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطًا في بعض الأحوال، أو يعطي القاضي الحرية في تقدير الأدلة القانونية، مثل القانون الإجرائي الياباني، وقد حصر المشرع الياباني طرق الإثبات المقبولة بما يأتي: (أقوال المتهم، وأقوال الشهود، والقرائن، والخبرة)، أما بالنسبة لأدلة الحاسوب والإنترنت، فيقرر الفقه الياباني، أن السجلات الإلكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب والإنترنت، سواء كانت هي الأصل أم كانت نسخة من هذا الأصل[٤٩].

وتنص المادة (١١٣) من قانون الإجراءات الجنائية الشيلي، على إمكانية استخدام الأفلام السينمائية، والحاكي (الفونوغراف)، والنظم الأخرى الخاصة بإنتاج الصورة، والصوت، والاختزال، وبصفة عامة أية وسائل أخرى، قد تكون ملائمة، ووثيقة الصلة، وتفضي إلى استخلاص المصداقية، يمكن أن تكون مقبولة كدليل إثبات[٥٠]، ويرى الفقه الشيلي، أن الدليل الناتج عن الحاسوب والإنترنت، يمكن أن يكون مقبولاً في المحكمة، كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل

[48] - انظر: د. سعيد عبد اللطيف حسن- مصدر سابق- ص ١٦٥.

[49] - نقلاً عن د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية -مصدر سابق ص ٦٢.

[50] - انظر: د. هلالي عبد الاه أحمد- حجية المخرجات الكمبيوترية -المصدر السابق- ص ٦٤-٦٦.

المعلومات، وحجة الفقه الشيلي تستهدف توسيع مظلة الوسائل العلمية الحديثة في الإثبات، لتغطي العناصر الإثباتية الناتجة عن جرائم المعلوماتية[٥١].

تعد مراقبة المكالمات السلكية واللاسلكية – تحت رقابة القضاء– من الوسائل الملائمة لضبط ما يفيد في كشف الحقيقة أحيانًا، وقد أحاط المشرع إجراء المراقبة الهاتفية واللاسلكية بضمانات معينة فلا يجوز إجراؤها إلا بأمر مسبب من القضاء وبصورة مشروعة.

لكن ما القوة الإثباتية للتسجيلات الصوتية المُسجلة إلكترونيًا؟

إن الصوت عند تسجيله إلكترونيًا ، لا يحتمل الخطأ، ويصعب التلاعب به، ويمكن للخبراء أن يكتشفوا أي تلاعب أو خداع بوسائل تقنية عالية الكفاءة، ومن ثم يمكن القول بأن التسجيل الصوتي الممغنط يمكن أن تكون له حجة دامغة في الإثبات[٥٢].

ويمكن باستخدام تكنولوجيا للحواسيب الحديثة والإنترنت وطرق الاتصال المعلوماتي السريع، أن يستخدم تسجيل الفيديو لإثبات تُهم استعمال القسوة أو إساءة استعمال السلطة من قبلِ أعضاء الضابطة العدلية ضد المواطنين، كما يمكن استخدامها لتسجيل عمليات القبض والتفتيش وضبط الأدلة والآثار الأخرى الناجمة عن الجريمة تسجيلاً دقيقًا، كما يمكن استخدامها كتقنية عالية الكفاءة لعمل المعاينات اللازمة لمسرح الجريمة[٥٣]، ويشترط الفقه لمشروعية الدليل المستمد من المراقبة والتسجيل توافر الشروط التالية[٥٤]:–

---

51 -انظر: د. عفيفي كامل عفيفي- مصدر سابق- ص ٣٧٣-٣٧٤.

52 -د. سعيد عبد اللطيف حسن- مصدر سابق- ص ٢١١.

53 - بيل جيتس وآخرون – المعلوماتية بعد الإنترنت (طريق المستقبل) - ترجمة أ.عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م - ص ٤٢٥.

54 - للمزيد من المعلومات حول هذا الموضوع انظر: د.ممدوح خليل البحر – أصول المحاكمات الجزائية الأردني – ط١ – دار الثقافة – عمان – ١٩٩٨م - ص ٥٥٨-٧٥٠.

١-إذا لم يكن التسجيل منطويًا على اعتداء على حق يحميه القانون، فيكون الدليل في هذه الحالة مشروعًا، ويمكن للمحكمة أن تستند إليه في قضائها بالإدانة أو بالبراءة.

٢-تحديد دقيق لشخصية الشخص المراد تسجيل أحاديثه أو بريده الإلكتروني كل ما كان ذلك ممكنًا في حالة الإنابة للتفتيش.

٣-تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرح لها بذلك، والمدة الجائز خلالها التقاط الحديث خلالها.

ويمكن استخدام "حاسوب الجيب" على أنه " أداة تبرئة" إذ يمكن أن تكون التوقيعات المشفرة من خلاله دليل براءة غير قابل للدحض في مواجهة أية اتهامات باطلة، فلو أن شخصًا ما أتُهم بأمر معين أو جريمة معينة فبإمكانه أن يُدافع عن نفسه من خلال ما هو مُسجل من أقوال وأفعال في أي وقت[٥٥]. أما البريد الإلكتروني، فعند إرسال رسالة من خلاله فإنه يكون لدى الشخص المستقبل توقيعًا رقميًا (إلكترونيًا)، ويكون المستقبل وحده القادر على استعماله، وسيتم تشفير الرسالة، بحيث لن يتمكن من حل شفرتها إلا الشخص المقصود إرسالها إليه، ويمكن لهذه الرسالة أن تكون معلومات من أي نوع، مشتملة على الصوت والفيديو، أو تحويلات بنكية، وسيكون بإمكان متلقي الرسالة أن يتأكد من أن الرسالة مرسلة بالفعل من الشخص الذي أرسلها، وتحديد وقت إرسالها بالضبط، وأنها لم تتعرض لأي تلاعب، وأن الآخرين لا يستطيعون فك شفرتها، وبالتالي يمكن استخدام هذه المعلومات كحجة في الإثبات الجنائي[٥٦].

55 - وهو حاسوب بحجم صغير جدًا يمكن وضعه داخل الجيب، ويمكن ربطه بمونيوتر أكبر وبالشبكة العامة بمكتب العمل الخاص، ويمكن للمستخدم أن يحفظ فيه كل ما يريد من أرقام ومواعيد، بالإضافة لاستخدامه ككاميرا تصوير وخلوي- انظر: بيل جيتس- مصدر سابق- ص٤٢٣-٤٢٤.

56 - د. سعيد عبد اللطيف حسن- مصدر سابق- ص ٢٣٢-٢٣٣.

ويستخدم التوقيع الإلكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما، أن يلفق أو يزور المفترض كتابة أو إرسال الوثيقة فيه فسيكون هذا التلفيق أو التزوير قابلاً للكشف، وسوف يرد ذلك الاعتبار للقيمة الإثباتية للصور الفوتوغرافية والفيديوية، ولقد أضاف علم التصوير للإثبات الجنائي قيمة علمية بما له من أثر في نقل صورة صادقة للأماكن والأدلة إلى كل من يعنيه الأمر، اعتمادًا على آلة التصوير والأفلام التي لا تعرف الكذب، بيد أنه لا يمكن إنكار الآثار السلبية والخطيرة التي تنشأ عن استخدام هذه الوسائل، لما قد يحدثه في الحياة الخاصة إذا لم توضع له الضوابط الكافية[٥٧]، وتختلف حجية التوقيع الإلكتروني في الإثبات المدني عنه في الإثبات الجنائي، حيث يخضع في الإثبات المدني لقواعد شكلية، أما في الإثبات الجنائي فيخضع تقديره لمطلق سلطة قاضي الموضوع، واقتناعه بصحته وقوته الإثباتية[٥٨]، كما أن وجود نظام تسجيل الدخول في شبكة الإنترنت يسمح بتحديد الأشخاص الذين دخلوا أو حاولوا الدخول بعد ارتكاب الفعل الجرمي، وتعد حالات ضبط مرتكب الفعل متلبسًا نادرة أو أنها وليدة الصدفة، وحتى لو تم ضبطه متلبسًا، فقد يرجع ذلك إلى خطأ في نظام الحاسوب أو الشبكة أو الأجهزة الأخرى[٥٩]، أو عن طريق مراقبة الشرطة بعد ملاحظة وجود بعض الاعتداءات، والفقه الفرنسي يعتبر انتهاك نظام الأمن لبعض المواقع المحمية، دليل حتمي وقرينة قاطعة على وجود القصد الجرمي وسوء نية

---

57 - وللمزيد من المعلومات انظر: د. عبد الحافظ عبد الهادي عابد- الإثبات الجنائي بالقرائن دراسة مقارنة- دار النهضة العربية- القاهرة ١٩٩٨م- ص ٥٦٣ وما بعدها.

58 -لقد أصبح التوقيع الإلكتروني بديلاً عن التوقيع التقليدي ويؤدي ذات الوظيفة فيما يتعلق بالوثائق والرسائل الإلكترونية، وهو مهم من حيث أنه يحدد شخصية الموقع، ويعبر عن إرادته في التزامه بمضمون الوثيقة وإقراره لها، وهو دليل على حضور أطراف التصرف وقت التوقيع، أو حضور من يمثلهم قانونًا أو اتفاقًا- انظر: د. سعيد عبد اللطيف حسن- مصدر سابق- ص ٢٤٤ وما بعدها، وانظر: د. هدى حامد قشقوش- الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت- دار النهضة العربية- القاهرة- ٢٠٠٠م- ص٧١ وما بعدها.وانظر: د. محمد المرسي زهرة – حجية التوقيع الإلكتروني في الإثبات- الجوانب القانونية الناجمة عن استخدام الحاسب الآلي في المصارف – المصدر السابق – ص ١٤٥ وما بعدها.

59 - د. عبد الفتاح بيومي حجازي- مصدر سابق- ص ٤٦.

مرتكب الفعل[٦٠]، ويمكن للماسحات الضوئية، وطابعات الليزر أن تكون أداة ارتكاب الجريمة، ففي عام ١٩٩٤، قام أحد الأشخاص في مدينة دلاس الأمريكية بتزوير أجازات قيادة سيارات التاكسي باستخدام الماسحات الضوئية، وطابعات الليزر، كما جرت محاولات لإصدار بطاقات التأمين، وأوامر صرف مالية، وبعض أنواع الصكوك من خلال استخدام برمجيات الرسوم المتطورة، وأنظمة الطباعة المتخصصة[٦١].

ويخلص الباحث إلى تأييد الرأي الفقهي الذي يرى أن المحاكم الجنائية قد لا تواجه مشاكل في تعاملها مع الأدلة الجنائية الإلكترونية (الرقمية)، وذلك للأسباب التالية[٦٢]:

١-الثقة التي اكتسبها الحاسوب والإنترنت والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات[٦٣].

٢-ارتباط الأدلة الجنائية الإلكترونية وآثارها بالجريمة موضوع المحاكمة.

٣-وضوح الأدلة الإلكترونية، ودقتها في إثبات العلاقة بين الجاني والمجني عليه، أو بين الجاني والسلوك الإجرامي.

٤-إمكانية تعقب آثار الأدلة الإلكترونية والوصول إلى مصادرها بدقة.

٥-قيام الأدلة الإلكترونية على نظريات حسابية مؤكدة لا يتطرق إليها الشك مما يقوي من تقنية الأدلة الإلكترونية.

---

60 - انظر: د. أحمد حسام طه تمام- الجرائم الناشئة عن استخدام الحاسوب- (الحماية للحاسوب)- دراسة مقارنة- دار النهضة- القاهرة ٢٠٠٠م- ص ٢٧٤-٢٧٥.

61- Flusche, Karl J. – Computer Crime and analysis of Computer evidence – Itain't Just hackers and phreakers anynore- Information System Security – Spring 1998-Vol.7. Issue 1. P. 24.

62 - انظر: د. محمد الأمين البشري- مصدر سابق ص١٢٧-١٢٨.

63 - ويحقق الحاسوب قدرًا من التأمين، والسرعة في تبادل المعلومات بين أجهزة وأقسام الشرطة وصولاً إلى المجرم أو يمكن التدخل قبل وقوع الجريمة، ويمكن الاستفادة من الحاسوب في تحليل نتائج البحث الجنائي الفني والعلمي، ومضاهاة البصمة ونقلها لوحدات الشرطة، ويكفل الحاسوب سرية المعلومات الشخصية التي تصل إلى وحدات التسجيل الجنائي- انظر: اللواء د. محمد الأمين-العدالة الجنائية ومنع الجريمة – دراسة مقارنة – ط١- أكاديمية نايف العربية للعلوم الأمنية- الرياض- ١٩٩٧- ص ٣٠٣ وما بعدها.

٦-الأدلة الجنائية الإلكترونية يدعمها- عادة- رأي خبير- وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم وفق شروط وقواعد نظمها القانون وأقرها القضاء.

النتائج والتوصيات:

يُعد التفتيش من أشد إجراءات التحقيق أثرًا على الحرية الشخصية، وجب علينا أن نذكر ما نراه ضروريًا لتعديل النصوص التشريعية القائمة، لإيجاد أحكام جديدة تحقق الغرض منه، وتوفق بين صالح الجماعة في ضرورة حمايتها، ومصلحة الفرد في حماية حريته.

وتوصل الباحث إلى عدة نتائج وتوصيات أهمها حسب خطة البحث:

أولاً: يرى الباحث إمكانية تطبيق القواعد العامة في تفتيش نظم الحاسوب والإنترنت على المتهم بناءً على وجود قرائن قوية تنبئ بحيازته لأشياء أو أدلة تتعلق بجريمة، أو أنه يخفي بيانات أو برامج استخدمت في ارتكاب الجريمة.

ثانيًا: تثير مسألة الإثبات في نظم الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق ، كالتخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة ، ويشكل انعدام الدليل المرئي (المفهوم) عقبة كبيرة أمام كشف الجرائم ، وقد يشكل تشفير البيانات المخزنة إلكترونيًا أو المنقولة عبر شبكات الاتصال عن بُعد عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة ، كما أن سهولة محو الدليل في زمن قصير تُعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت.

ثالثًا: وفي سبيل تحقيق العدالة وضمان حق المشتكى عليه عند إجراء التفتيش على نظم الحاسوب والإنترنت، يرى الباحث ضرورة حضور المشتكى عليه عند تفتيش حاسوبه أو نظمه وكذلك في حالة تفتيش حاسوب أو نظم غيره إذا كان الأمر متعلقًا

بضبط الدليل ضده وذلك لإتاحة الفرصة أمام المشتكى عليه لمواجهته بالدليل المترتب عن التفتيش ، شريطة ألا يسبب حضوره إضرارًا بسير التحقيق.

رابعًا: يقع عبء إثبات الجرائم المعلوماتية على عاتق النيابة العامة ، كما أن المدعي بالحق الشخصي يشارك النيابة العامة هذا العبء ، وفي أحيان أخرى ينقل القانون عبء الإثبات من النيابة العامة إلى عاتق المشتكى عليه. إن الاختصاص في إجراء التفتيش على نظم الحاسوب والإنترنت في التشريعات المقارنة، هي كاختصاص أصيل للنيابة العامة وبصورة استثنائية لأعضاء الضابطة العدلية، مع ضرورة تعديل بعض النصوص الإجرائية للإشارة إلى الجانب المعلوماتي، وضرورة إعداد وتهيئة هذه السلطة بشكل متميز لمواجهة الجرائم المعلوماتية.

التوصيات:

أولاً: لكي يُعد الدليل المستخلص من تفتيش وضبط نظم الحاسوب والإنترنت مشروعًا يوصي الباحث بضرورة توافر ثلاثة شروط في الدليل الإلكتروني المستمد من التفتيش وهي:-

أ-يجب الحصول على الدليل المستمد من التفتيش بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات.

ب-يجب أن تكون الأدلة الإلكترونية غير قابلة للشك أي يقينية.

جـ-إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسوب والإنترنت.

ثانيًا: لقد أكدت التوصية التي أصدرها المجلس الأوروبي لعام ١٩٩٥م، والخاصة بمشاكل الإجراءات الجنائية الوطنية على ضرورة الأخذ بالتوصيات التالية لكي تلائم النصوص القانونية التطور الحاصل في هذا المجال، ويوصي الباحث المشرع الجزائي العربي أن يأخذ بها:-

١-أن توضح القوانين إجراءات تفتيش أجهزة الحاسوب وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.

٢-أن تسمح الإجراءات الجنائية للجهات القائمة على التفتيش بضبط برامج الحاسوب والمعلومات الموجودة بالأجهزة وفقًا لذات الشروط الخاصة بإجراءات التفتيش العادية.

ثالثًا: ومن أجل ضمان حفظ أسرار المشتكى عليه غير المتعلقة بالجريمة من الاطلاع عليها يوصي الباحث بإتباع القائم بالتفتيش التعليمات التالية:

١-على القائم بالتفتيش أن يلتزم واجب الحيطة والحذر أثناء التفتيش فلا يطلع إلا على الأشياء أو الأماكن التي يحتمل أن يجد فيها بيانات أو برامج أو أشياء أو أدلة أو براهين لها علاقة بالجريمة.

٢-على المحقق أن لا يسترسل في الاطلاع عما ظهر أمامه صدفة.

٣-أن يحاول المحقق -ما وسعه الجهد-عدم اطلاع غيره على محتويات الحاسوب محل التفتيش.

رابعًا: ضرورة إصدار دليل إرشادي تقني وقانوني حول صور جرائم الحاسوب والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية ومواصلة تحديث هذا الدليل بشكل دوري وكلما دعت الحاجة لذلك وتعميمه على العاملين في مجال التحقيق في الميدان وعلى أجهزة القضاء، والاستفادة من الدليل الصادر عن المنظمة العالمية للشرطة الجنائية الإنتربول.

المراجع:

١. د. آمال عبد الرحيم عثمان – الإثبات الجنائي ووسائل التحقيق العلمية – دار النهضة العربية – القاهرة – ١٩٧٥م.

٢. . محمود محمود مصطفى – شرح قانون الإجراءات الجنائية – ط١١– القاهرة – ١٩٧٦م.

٣. د.سعيد عبد اللطيف حسن – لإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – الجرائم الواقعة في مجال تكنولوجيا المعلومات – ط١ – دار النهضة العربية – القاهرة – ١٩٩٩م.

٤. د.هشام محمد فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – ١٩٩٤م.

٥. د.عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دراسة متعمقة في جرائم الحاسب الآلي والإنترنت – دار الكتب القانونية – القاهرة – ٢٠٠٢م.

٦. الرائد كمال الكركي – جرائم الحاسوب ودور مديرية الأمن في مكافحتها – ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف – نظرة إلى المستقبل – المنعقدة في عمان بتاريخ ١٩٩٩/٧/٥م.

٧. أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة – جرائم الحاسب الآلي والإنترنت – دراسة تحليلية مقارنة – ط١ – دار وائل – عمان – ٢٠٠١م.

٨. د.جميل عبد الباقي الصغير – أدلة الإثبات الجنائي والتكنولوجيا الحديثة – (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية) – دراسة مقارنة – دار النهضة العربية – القاهرة – ٢٠٠١م.

٩. محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة – الإسكندرية – ٢٠٠١م.

١٠. د.هلالي عبد اللاه أحمد – حجية المخرجات الكمبيوترية في الإثبات الجنائي – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م.
١١. أ.عبد الأمير العكيلي – أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية –ج١ – ط١ – مطبعة المعارف – بغداد – ١٩٧٥م.
١٢. د.نائل عبد الرحمن صالح – محاضرات في قانون أصول المحاكمات الجزائية – ط١ – دار الفكر العربي – عمان – ١٩٩٧م.
١٣. د. رمزي رياض عوض – مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها – دراسة تحليلية تأصيلية مقارنة – دار النهضة العربية – القاهرة – ١٩٩٧م.
١٤. د. أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة – دار النهضة العربية – القاهرة – ١٩٩٤م.
١٥. د. علي حسن الطوالبه،التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة،ط١،عالم الكتب الحديث،اربد،٢٠٠٤م.
١٦. د. هلالي عبدالاه أحمد – التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة – النسر الذهبي – القاهرة – ٢٠٠٠م.
١٧. د.هشام محمد فريد رستم – جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة – مجلة الدراسات القانونية – جامعة أسيوط – العدد ١٧– ١٩٩٥م.
١٨. د.محمد فهمي طلبة وآخرون – دائرة المعارف الحاسب الإلكتروني – مجموعة كتب دلتا – مطابع المكتب المصري الحديث – القاهرة – ١٩٩١م.
١٩. د.محمد الأمين البشري – الأدلة الجنائية الرقمية – مفهومها ودورها في الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد ١٧– – العدد ٣٣–السنة ١٧ – الرياض – أبريل ٢٠٠٢م.

٢٠. د.عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة – (د.ت).

٢١. د.هلالي عبداللاه أحمد – تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي – دراسة مقارنة – ط١ – دار النهضة العربية – القاهرة – ١٩٩٧م.

٢٢. بيل جيتس وآخرون – المعلوماتية بعد الإنترنت (طريق المستقبل) – ترجمة أ.عبد السلام رضوان – سلسلة عالم المعرفة – المجلس الوطني للثقافة والفنون الآداب – العدد ٢٣١ – الكويت – مارس ١٩٨٨م.

٢٣. د.ممدوح خليل البحر – أصول المحاكمات الجزائية الأردني – ط١ – دار الثقافة – عمان – ١٩٩٨م.

٢٤. د. عبد الحافظ عبد الهادي عابد– الإثبات الجنائي بالقرائن – دراسة مقارنة– دار النهضة العربية– القاهرة ١٩٩٨م.

٢٥. د. أحمد حسام طه تمام– الجرائم الناشئة عن استخدام الحاسوب– (الحماية للحاسوب)– دراسة مقارنة– دار النهضة– القاهرة ٢٠٠٠م.

٢٦. د. محمد الأمين–العدالة الجنائية ومنع الجريمة – دراسة مقارنة – ط١– أكاديمية نايف العربية للعلوم الأمنية– الرياض– ١٩٩٧.