إثبات جرائم الاعتداء على حق المؤلِّف عبر الإنترنت
في التشريع الجزائري (دراسة مقارنة)

أ/ نزيهة مكاري
معهد علوم التسيير والاقتصاد
المركز الجامعي برج بوعريريج

ملخص :
إذا كان هناك بعض الأدلة التقليدية التي قد تصلح لإثبات الجرائم التي تقع باستخدام الوسائل الإلكترونية، إلا أنها تكون في حاجة إلى تطوير مستمر لكي يمكنها أن تتناسب مع الطبيعة الخاصة بتلك الجرائم.

لذا نستعرض في هذه الورقة بعض أدلة الإثبات التقليدية ودورها في إثبات جريمة الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت ضمن العناصر التالية :

- المعاينة التقنية لمسرح جرائم الاعتداء الإلكتروني على حق المؤلف عبر الانترنت.
- تفتيش أنظمة الحاسب الآلي المستخدمة في جرائم الاعتداء الإلكتروني عبر الإنترنت .
- الشهادة الإلكترونية في مجال جرائم الاعتداء الإلكتروني على حق المؤلف عبر الانترنت .
- الخبرة التقنية في مجال الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت .

Résume :

Si il existe des preuves qui servent de mai traditionnelle la preuve des crimes qui se produisent par des moyens électroniques, mais ils sont dans le besoin de développement continu pour pouvoir être en rapport avec la nature de ces crimes. Ainsi, dans le présent document, nous passons en revue certains des éléments de preuve et le rôle traditionnel de prouver le crime d'agression mail à droit d'auteur à travers l'Internet dans les éléments suivants:

- Contrôle technique de la scène de l'attaque, électronique de droit d'auteur à travers l'Internet.

- Inspection des systèmes informatiques utilisés dans les crimes électronique à travers l'Internet.

- le témoignage électronique de crimes dans le domaine de l'électronique de l'attaque sur le droit d'auteur sur l'Internet.

- L'expertise technique dans le domaine de l'électronique de l'attaque sur le droit d'auteur sur l'Internet.

مقدمة

الإنترنت وما يرتبط به من مسائل قانونية أصبح يمثل فصلاً متميزاً من فصول القانون المعاصر. فتبدأ بعقود الاشتراك في الإنترنت وأنواعها وعقد إنشاء موقع وعقود التجارة الإلكترونية أي ما يمكن تسميته بالتنظيم القانوني للتعامل مع الإنترنت وعن طريق الإنترنت. أما الشق الثاني فهو حماية الحقوق في مواجهة الإنترنت، وفي مقدمة ذلك حماية حقوق المؤلف في مجال الإنترنت.

والواقع أن خطورة الإنترنت على حق المؤلف تتأتى عادة من أن إدخال المعلومة على الشبكة يكون عن طريق ترقيمها وتفاعلها. وهنا قد يحدث تحويراً أو تعديلاً في المصنف، فالتحول إلى شبكة المعلومات الرقمية لا يخلو في حد ذاته من مخاطر بالنسبة لحق المؤلف، وكيفية إثبات جرائم الاعتداء على حق المؤلف عبر الإنترنت. فالإثبات هو الهدف الجوهري

التي تسعى إلى تحقيقه إجراءات الخصومة الجنائية منذ نشأتها بتحريك الدعوى الجنائية وحتى انقضائها، بإصدار حكم نهائي في مواجهة شخص ما[1]، والحكم حتى يأتي مطابقا للحق يجب أن يبنى على أساس ثابت من الواقع والقانون، وذلك بأن تتجه إجراءات الخصومة الجنائية نحو إظهار كافة العناصر اللازمة للوصول إلى الحقيقة بشأن الإتهام الموجه إلى شخص معين بإعتباره فاعلاً أوشريكاً في جريمة هو ما يشكل موضوع الإثبات في الخصومة الجنائية بوجه عام[2] ووسائل الإثبات هي المعاينة، وندب الخبراء والتفتيش وضبط الأشياء وسماع الشهود والاستجواب[3].

وليس على المحقق التزام إتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساساً بمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتِّبها وفقا لما تقضي به هذه المصلحة وما تسمح به هذه الظروف. ومن هنا تظهر أهمية الموضوع والإشكالية الذي يحاول هذا المقال التطرق لها بالعرض والتحليل، وعليه يمكن طرح الإشكالية التالية : **هل وسائل الإثبات التقليدية قادرة علي إثبات هذا النوع من الجرائم الإلكترونية؟**

لذا سوف نقصر دراستنا على وسائل إثبات جرائم الإعتداء الإلكتروني على حق المؤلف مع الأخذ في الحسبان تطور مفاهيمها في الوسط الإلكتروني الجديد بطريقة تضمن أن تلك الوسائل التقليدية لا تزال فعالة في بيئة تكنولوجية تتميز بالتلاشي والتبخر[4]، وبما يساهم في توفير عقيدة صحيحة لدى القاضي[5].

وفي ضوء ذلك نرى تقسيم هذه الدارسة إلى أربعة مباحث

المبحث الأول
المعاينة التقنية لمسرح جرايم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت.

1- تعريف المعاينة التقنية لمسرح جرائم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت.

لم يحدد المشرع المقصود بالمعاينة الأمر الذي دعا الفقه لتصدي لتعريفها حيث عرفها البعض بأنها "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة"[6]. والمعاينة أيا كان التعريف الموضوع لها تتطلب أن تنتقل النيابة العامة أو قاضي التحقيق إلى مكان وقوع الجريمة لمباشرتها وذلك لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة في الجريمة أثناء الإجراء[7]، فطبقا لنص المادة 79 من قانون الإجراءات الجزائية الجزائري والتي تنص على أنه :

"ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها.

و يخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته. ويستعين قاضي التحقيق دائماً بكاتب التحقيق

و يحرر محضراً بما يقوم به من إجراءات". ويقابل هذا النص المادة 90 من قانون العقوبات المصري.

أما في فرنسا يمكن إجراء المعاينة عن طريق المحضر أو الخبير بناءاً على طلب الشخص المعني بعد موافقة القاضي المتخصص بناءاً على طلب على عريضة طبقا للمادة 145 من قانون المرافعات المدنية الفرنسي الجديد[8]. خاصة إذا كانت المعاينة تجري في مكان خاص، حتى ولو كان مفتوحا للجمهور مثل مقاهي الإنترنت.

ويجب على الطالب أن يقدم تبريرا لطلبه بإجراء المعاينة بأن يقدم ما يفيد أن هناك اعتداء على حقوقه. فإثبات الاعتداء أمر ضروري لإقامة الدليل على الدعوى التي سيقوم برفعها وذلك خشية زوال هذه المعلومات من على شبكة الإنترنت[9].

هذا وقد أجاز المشرع الأمريكي لعضو النيابة العامة أن يعجل بإجراء المعاينة خشية ضياع الأدلة وذلك بإرسال رسالة إلى مزود خدمة الإنترنت يلزمه فيها بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذ هذا الإجراء أو غيره[10].

وإذا كانت المعاينة تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة عامة إجرائية مقررة في هذا الشأن إلا أنه في إطار جرائم الإنترنت والخاصة بالاعتداء على حقوق المؤلف فإن الانتقال يعد من الموضوعات الجديدة، وذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي، وإنما يجب أن تكون بالضرورة عبر العالم الافتراضي فيستطيع عضو سلطة التحقيق أن يقوم بالمعاينة في مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به.

كما يمكن أن يلجأ إلى مقهى الإنترنت أو أن ينتقل إلى مقر مزود الخدمة الذي يعد أفضل مكان يمكن من خلاله إجراء المعاينة. ذلك أنه في كل الأحوال يلزم أن يقوم المحقق بالمعاينة من خلال حاسب أو حاسب خادم ومن ثم فإن مشكلة الانتقال المادي إلى محل ارتكاب الواقعة الإجرامية لا تشكل عائق أمام عضو النيابة وإنما المشكلة تكون من خلال الانتقال إلى العالم الافتراضي حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال أثر الجريمة[11] ولهذا يجب أن يعجل بإجراء المعاينة خشية ضياع الأدلة [12].

لا تتمتع المعاينة في مجال كشف غموض جرائم الإنترنت المعلوماتية والمتعلقة بالاعتداء على حقوق المؤلف من الأهمية التي تلعبها في مجال الجريمة التقليدية ومرد ذلك إلى الاعتبارات الآتية[13]:

أن جرائم الاعتداء على المصنفات الإلكترونية عن طريق شبكة الإنترنت قلما أن يترتب عليها آثار مادية. فجميع ما ينتج عن تلك الجرائم من أدلة ما هو إلا بيانات غير مرئية [14].

- أن عدداً كبيراً من الأشخاص قد يتردد على مكان مسرح الجريمة خلال الفترة الزمنية التي تتوسط ارتكابها واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها هو ما يثير الشك في الدليل المستمد من المعاينة. كما أن الجناة كثيرا ما يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة من خلال مقاهي الإنترنت [15].

- مشكلة تبخر الدليل الإلكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثواني.

ونظرا لأن الأمر يتعلق بعملية فنية تقنية فإنه يجوز أن يلتمس طالب المعاينة من القاضي أن يصرح له بتعيين خبير فني متخصص في الإنترنت ليكون بصحبة المحقق، وذلك حتى يمنع أي تشكيك في صحة الدليل المستمد منه.

2- كيفية إجراء المعاينة التقنية لمسرح جرائم الاعتداء على حق المؤلف عبر الإنترنت:

وحتى تصبح معاينة مسرح جرائم الاعتداء على حق المؤلف عبر الإنترنت لها فائدة في كشف الحقيقة عنها وعن مرتكبيها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[16].

-القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريقه الجرائم وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخلفية وملحقاته الأخرى على أن يراعي تسجيل زمان ومكان والتاريخ الذي التقط فيه كل صورة [17].

- ملاحظة طريقة إعداد نظام الحاسب بعناية بالغة.

- حفظ الموقع عن طريق :

- ✓ استخدام خاصية الحفظ Save as المتوافرة في نظام التشغيل ويترتب عليها بطبيعة الحال حفظ الموقع المخالف الذي ظهر على الشاشة.
- ✓ تحميل من المصنف المقلد Downloading أو طباعتها أو استخراجها في هيئة ورقية أو على أقراص صلبة أو مرنة.
- ✓ -التأكد من سلامة الحاسب الآلي أو الحاسب الخادم بحيث تكون سلطة التحقيق قد احتفظت بما يسمح بالتأكيد على دقة مصدر الدليل الإلكتروني[18].

- يجب أن يلاحظ وأن يتم إثبات الحالة التي تكون عليها توصيلات وكابلات الحاسب والتي تكون متصلة بمكونات النظام وذلك حتى يسهل القيام بعملية المقارنة وتحليل لها عند عرض الموضوع على المحكمة.

- عدم التسرع في نقل أي مادة معلوماتية (المصنفات المقلدة) من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزّنة.

- القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسب الورقية التي قد تكون ذات صلة بالجريمة وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.

- يجب أن تقتصر عملية المعاينة على مأموري الضبط سواء كانوا من الباحثين أو المحققين ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في المجال المعلوماتي ممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[19].

ففي الولايات المتحدة الأمريكية توجد نيابة متخصصة بأعمال التحقق في جرائم الحاسب والاتصالات وهي مشكلة من مجموعة من أعضاء النيابة العامة تلقوا تدريبات مكثفة على نظام المعالجة الآلية للبيانات وتم منحهم صلاحيات كبيرة في مجال الاستعانة بغيره من خبراء وزارة العدل لاسيما قسم جرائم الحاسب والعدوان على حقوق الملكية الفكرية، يفيد التخصص هنا أعضاء النيابة العامة في كيفية التعامل مع الدليل الرقمي وكيفية بناء عريضة الاتهام قبل تقديمها للمحاكمة لكي يتم توجيه الاتهام بشكل صحيح فلا ينجو المجرم بفعلته[20].

8- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات على بعد أو من جهاز آخر داخل المبنى[21].

المبحث الثاني
تفتيش أنظمة الحاسب الآلي المستخدمة في جرائم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت

رغم تعدد التعريفات التي أضفاها الفقه على فكرة التفتيش إلا أنها تُجمِع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة.
إلا أن الثورة التكنولوجية التي حدثت والتي أمكن بموجبها بث وتخزين المصنفات الإلكترونية بأشكالها المختلفة عبر شبكات الحاسب الآلي المستخدمة في ارتكاب تلك الجرائم ومدى خضوعها للتفتيش. وما هي الضوابط التي يجب إتباعها في تلك الحالة[22]؟ وهذا ما سوف نتناوله في هذه الدراسة على النحو التالي :

1- مدى قابلية مكونات وشبكات الحاسب المستخدمة في جرائم الاعتداء على حق المؤلف للتفتيش .

تتكون نظم الحاسب الآلي من مكونات مادية Hardware ومكونات منطقية Software كما أنه تربطه بغيره من الحاسبات شبكات اتصال بعدية[23]على المستوى المحلي أو الدولي لذا فقد ثار التساؤل الخاص
بمدى خضوع مكونات الحاسب المستخدمة في جرائم الاعتداء على حق المؤلف عبر الإنترنت للتفتيش ؟ وفى هذا الصدد يجب التفرقة بين حالتين :

الحالة الأولى : مدى خضوع مكونات الحاسب المادية المستخدمة في جرائم الاعتداء على حق المؤلف عبر الإنترنت للتفتيش. الواقع أن تفتيش المكونات المادية للحاسب بأوعيتها المختلفة بحثاً عن شيء يتصل بجريمة معلوماتية خاصة بالاعتداء على حقوق المؤلف وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة. بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، هل هو من الأماكن العامة أم من الأماكن الخاصة. إذ أن لصفة المكان أهمية خاصة في مجال التفتيش.إذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حُكمَه. فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونيا في التشريعات المختلفة[24].

وبالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكونات الحاسب سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد.

ومن التطبيقات التشريعية التي تجيز تفتيش مكونات الحاسب الآلي من خلال ما تخوله بعض التقنيات الإجرائية لسلطة التحقيق من اتخاذ أي إجراء أو أي شيء لازم لجمع الأدلة والحفاظ عليها طبقا للمادة 251 من قانون الإجراءات الجنائية اليوناني[25] والمادة 487 من القانون الجنائي الكندي. وفي لوكسمبورغ يمكن القول بصفة عامة أن

التفتيش يشمل كل الأشياء التي تكون مفيدة في إظهار الحقيقة[26] وهناك قلة من التشريعات تنص صراحة على تفتيش مكونات الحاسب الآلي[27] وكذلك المرشد الفيدرالي لتفتيش وضبط نظم الحاسب الآلي في الولايات المتحدة[28]. وكذلك هناك بعض القوانين التي تقدم قواعد تفصيلية للتفتيش تطبق على مكونات الحاسب وبياناته في حالات معينة. ومن ذلك قانون المنافسة في كندا فهو يزود الشخص الذي يحمل إذناً بالتفتيش إمكانية أن يستخدم أي نظام للحاسب الآلي والتفتيش على أي بيانات يحتويها أو تكون متاحة لهذا النظام كما يمكنه أن يسجل أو يعمل على تسجيل تلك البيانات في شكل مطبوعات أو مخرجات أخرى[29].

الحالة الثانية : مدى تفتيش المكونات المعنوية للحاسب الآلي المستخدم في جرائم الاعتداء على حق المؤلف عبر الإنترنت .

لقد ثار خلاف بشأن مدى جواز تفتيش المكونات المعنوية للحاسب الآلي تمهيدا لضبط الأدلة الإلكترونية الخاصة بجرائم الاعتداء على حق المؤلف عبر الإنترنت.

حيث ذهب الرأي الأول أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل الأدلة الإلكترونية بمختلف أشكالها. فالمادة 251 من قانون الإجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضرورياً لجمع وضبط الدليل، ولذلك فإن تفتيش وضبط المصنفات المقلدة المخزنة في الذاكرة الداخلية للحاسب لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمراً للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية وذلك وفقا لما يراه الفقه اليوناني.

وعلى النقيض من ذلك هناك رأي آخر يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على الأدلة الإلكترونية غير المادية. يقترح على هذا الرأي لمواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية لتفتيش عبارة الأدلة المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور الفني الحديث هي (البحث عن الأدلة المادية والإلكترونية)[30] وهذا الاقتراح أولى بالإتباع.

1.1- مدى خضوع شبكات الحاسب للتفتيش

يثار التساؤل حول أثر تفتيش الأنظمة المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة، هل يمتد تفتيش كمبيوتر معين إلى الأجهزة المرتبطة به داخل البلاد.وفي هذه الصورة يمكن التفرقة بين الفرضين التاليين:

الفرض الأول : اتصال حاسب المتهم بحاسب موجود في مكان آخر داخل الدولة .

أُثِيرَ تساؤل هام يتعلق بمدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب في منزل المتهم متصل بحاسب آخر مملوك لشخص آخر غير متهم؟

وجدت بعض التشريعات المقارنة حلا لهذه المشكلة كما في الولايات المتحدة عندما أجازت التوجيهات الداخلية الخاصة بإجراءات التفتيش الصادر لمقر شركة معينة إلى فروعها الكائنة في نفس العقار[31].

كما نصت المادة 17 فقرة (أ) من القانون الفرنسي رقم 239 لسنة2003 بشأن الأمن الداخلي الصادر في 18 مارس 2003 بـأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهم عملية البحث والتحري. فتنص المادة 17 منه على أنه : "يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم التفتيش على البيانات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر ما دامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتدءاً من النظام الرئيسي" [32]

وتسمح الاتفاقية الأوربية لجرائم الإنترنت لعام 2001 للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كمبيوتر معين إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش. فتنص المادة 19 من القسم الرابع على أنه :

"من حق السلطة القائمة بالتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الكمبيوتر الأصلي محل التفتيش".

وعلى العكس من ذلك فإن هناك من التشريعات المقارنة مثل سويسرا وبلجيكا ما يقصر أثر إذن التفتيش على الأجهزة الموجودة في مكان محدد دون امتدادها إلى الأجهزة المرتبطة[33].

الفرض الثاني : اتصال حاسب المتهم بحاسب في مكان آخر خارج الدولة :

يظهر أحيانا في أثناء التحقيقات أنه من الضروري تفتيش جهاز كمبيوتر متواجد في الخارج كما لو تعلق الأمر بشركة وفروعها في الخارج حيث ترتبط أجهزة الشركة بعضها ببعض وأحيانا ترتبط بعض الأجهزة بقاعدة بيانات متواجدة في الخارج.

هذا وتسمح التشريعات المقارنة بتفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة فتجيز المادة 17 فقرة 2 من قانون الأمن الداخلي الفرنسي لمأموري الضبط القضائي أن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت في خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية،

وفي نفس الاتجاه صدرت عن المجلس الأوربي توصيات تجيز أن يمتد تفتيش الكمبيوتر إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة. فتنص التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه : "لسلطة التحقيق عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها، ما دام أنه من الضرورة التدخل الفوري للقيام بذلك ".

كما نصت التوصية رقم17 على أنه : "يمكن أن يمتد نطاق تفتيش الكمبيوتر إلى النظام المتواجد في الخارج، إذا كان من الضروري اتخاذ إجراءات عاجلة في هذا الشأن. ويتعين أن يوجد أساس قانوني لامتداد مجال هذا النوع من التفتيش، حتى لا

يُشكّل ذلك الإجراء مخالفة لسيادة دولة أجنبية لذلك فإنه من الضروري الحصول على موافقة الدولة التي يمتد التفتيش إلى نظام يتواجد على إقليمها".

وجدير بالذكر أنه من المستقر عليه أن قواعد القانون الجنائي سواء الموضوعية أو الإجرائية تتعلق بسيادة الدولة. فتقضي القاعدة العامة بعدم جواز تطبيق قانون العقوبات الأجنبي على إقليم الدولة وكذلك عدم نفاذ إذن التفتيش أو القبض أو غير ذلك من الإجراءات القانونية الصادرة من السلطات الأجنبية على إقليم دولة أخرى.

ولذلك تنتهي اللجنة الأوربية للمشكلات الجنائية التابعة للمجلس الأوربي إلى القول بأن التفتيش والضبط والإجراءات القسرية الأخرى التي تقع على إقليم دولة أخرى تعتبر غير مشروعة إلا إذا كان القانون الدولي يجيزها[34].

3.1- مدى جواز تفتيش البريد الإلكتروني

يتمتع صاحب البريد الإلكتروني بالحق في حرمة الحياة الخاصة بالنسبة للمصنفات المتواجدة داخل البريد الإلكتروني لجهاز الكمبيوتر الخاص به. وتقيم أحكام القضاء التماثل بين مراسلات البريد الإلكتروني والمراسلات التي تتم عن طريق البريد العادي. وبناءً عليه لا يجوز التدخل للإطلاع على البريد الإلكتروني دون إذن صاحبه ما لم يصدر إذن قضائي بذلك.وتطبيقا لذلك قضي في كندا ببطلان الدليل المستمد من البريد الإلكتروني لأحد الأشخاص دون موافقة من هذا الأخير[35].

2- ضوابط تفتيش الحاسب الآلي المستخدم في ارتكاب جرائم الاعتداء على حقوق المؤلف عبر الإنترنت.

تضمنت معظم التشريعات الوطنية على ضوابط معينة يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات الماسة بالحرية كالتفتيش وتنقسم الضوابط العامة للتفتيش إلى نوعين من الضوابط ضوابط موضوعية وضوابط شكلية وذلك على النحو التالي :

أولاً- الضوابط الموضوعية لتفتيش نظام الحاسب الآلي المستخدم في جرائم الاعتداء على حق المؤلف عبر الإنترنت :

تنحصر الضوابط الموضوعية لتفتيش نظم الحاسب الآلي المستخدم في **(أ):** وقوع جريمة الاعتداء على حق المؤلف عبر الإنترنت **(ب):** لا بد من اتهام شخص معين بارتكاب هذه الجريمة **(ج):** لا بد من توافر أمارات قوية أو قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره وذلك على النحو التالي :

أ- وقوع جريمة الاعتداء على حق المؤلف عبر الإنترنت:

أدرج المشرع الجزائري مصنفات الحاسب الآلي ضمن برامج وقواعد بيانات وما يماثلها من مصنفات ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة 4 من الأمر رقم 03/05 المتعلق بحقوق المؤلف والحقوق المجاورة، وهذا ما ذهب إليه المشرع المصري في المادة 181 من القانون رقم 82 لسنة 2002 والخاص بحماية حقوق الملكية الفكرية[36].

وقد شدد المشرع الجزائري في عقوبة الاعتداء على حق المؤلف في المادة 394 مكرر2 من قانون العقوبات الجزائري المضافة بقانون رقم 04/15 بقوله "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 دج إلى 5000000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي :

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو اتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها فى هذا القسم .

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان، المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"، كما نصت المادة 394 مكرر3من قانون العقوبات الجزائري مضافة بالقانون رقم04/15 على أن تُضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام وفي جميع الأحوال تقضي المحكمة بمصادرة الأجهزة والبرامج محل الجريمة أو المتحصل منها و كذلك المعدات والأدوات المستخدمة في ارتكابها.

ويجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة أو المواقع التي استغلها المحكوم عليه في ارتكاب الجريمة مدة لا تزيد على ستة أشهر.

وتقضي المحكمة بنشر ملخص الحكم الصادر بالإدانة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب مسكن المحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها وعلى نفقة هذا الأخير[37].

ب- اتهام شخص أو أشخاص معينين في ارتكاب جرائم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت:

ينبغي أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب جريمة معلوماتية خاصة بحقوق المؤلف بوصفه فاعلاً لها، أو شريكاً فيها مما يستوجب اتهامه فيها. وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش التي تؤيد نسبة تلك الجريمة المعلوماتية إلى ذلك الشخص بوصفه فاعلاً أو شريكاً[38].

جـ- توافر قرائن قوية على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم:

من المستقر عليه في التشريعات المقارنة أن الإذن بالتفتيش يلزم أن يصدر بناءاً على تحريات جدية فلا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش بمجرد وقوع جنحة اعتداء على حق المؤلف واتهام شخص معين بارتكابها بل يجب أن تتوافر لدى المحقق أسباب كافية بأنه يوجد في مكان أو لدي الشخص المراد تفتيشه أدوات استخدمت في الجريمة المعلوماتية أو أشياء متحصل منها. أو أدلة الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره[39].

فيكفي إذن تفتيش الحاسب الإلكتروني أن يكون قد صدر استنادا إلى دلائل كافية عن جريمة ما وفي هذا ما يجعل اكتشاف الجريمة العرضية مبررا لاتخاذ الإجراءات الجنائية بصددها حتى ولو لم تكتشف الجريمة الأصلية التي من أجلها صدر إذن التفتيش(40).

وبالإضافة إلى الدلائل الكافية، فإنه يجب أن يحدد في إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء التي يجب ضبطها (الحاسبات الآلية المراد ضبطها) والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي(41)، وتقدير جدية التحريات وكفايتها لإصدار الإذن بالتفتيش هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق تحت إشراف محكمة الموضوع.

-محل التفتيش الخاص بنظم الحاسب الآلي:

هي كل مكونات الحاسب سواء كانت مكونات مادية أو معنوية أو شبكات اتصال خاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب محل التفتيش والمستخدم في ارتكاب جرائم الاعتداء على حق المؤلف عبر الإنترنت.

فالمكونات المادية للحاسب هي وحدة المدخلات أو وحدات الإدخال ووحدة الذاكرة الرئيسية ووحدة الحساب والمنطق ووحدة المخرجات ووحدات التخزين الثانوية وان كل وحدة من هذه الوحدات الست تشمل على مجموعة من المفردات المعلوماتية. كما تنقسم المكونات المنطقية للحساب إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز أو برامج التطبيقات طبقا لاحتياجات العميل. وأنه يمكن لأي شخص لديه جهاز حاسب ومودم وخط تلفون الدخول في شبكات اتصال الحاسب الآلي سواء كانت محلية أو عالمية(42).

كما يشمل مصطلح الحاسب الآلي الملحقات التي تدخل مباشرة في وحدة المعالجة المركزية CPU والذاكرة الرئيسية والتي تتصل مباشرة بوحدة المعالجة المركزية (43).

-السلطات المختصة بتفتيش نظم الحاسب الآلي المستخدمة في جرائم الاعتداء على حق المؤلف عبر الإنترنت :

الأصل أن تقوم سلطة التحقيق الأصلية بتفتيش النظم المعلوماتية المختلفة بنفسها بندب مأموري القضاء وفقا للقواعد الإجرائية المنصوص عليها في هذا الخصوص.

وفي هذه الحالة يجب أن يحدد في إذن الندب بالتفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (الحاسب الإلكتروني – المصنفات الإلكترونية المقلدة) والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي(44). بحيث لا يترك شيء للسلطة التقديرية لرجل الشرطة الذي سيقوم بتنفيذ الأمر.

فمن المبادئ المقررة أنه إذا قام مأمور الضبط القضائي بتفتيش أشياء لم يحددها الإذن الصادر بالتفتيش فإن ذلك يجعل التفتيش باطلا. وذلك استنادا إلى أن القائم بالتفتيش قد خالف الإذن بالتفتيش ويسمِي القانون الأمريكي تلك الحالة بالمخالفة الواضحة للإذن(45).

أوضحت أحكام القضاء الأمريكي على أنه إذا كان الإذن صادر لتفتيش جهاز الكمبيوتر في موضعه فإن هذا الإذن يسمح بتفتيش ملحقات الجهاز من أدوات مثل الطابعة والديسكات والأقراص الممغنطة.

ومما يؤيد أن الإذن بضبط وتفتيش ملفات معينة يشمل ضبط وتفتيش الجهاز بأكمله أو بعض الأجهزة محمية بكلمات مرور، الأمر الذي يقتضي ضبط الجهاز بأكمله للتغلب على هذه العقبة من الناحية الفنية. وقد اعترف القضاء الأمريكي بهذه الضرورة العملية في أحكامه[46].

ويرى جانب من الفقه ضرورة أن يتصف الإذن الصادر بالتفتيش من حيث إتاحة مساحة واسعة لمأموري الضبط في تنفيذ الإذن بالتفتيش ولكن بضوابط معينة بحيث لا يتجاوز ذلك الهدف المقصود من صدور الإذن عن طريق تحديد مجال التفتيش وما يستتبعه بالضرورة من تتبع من خلال شبكة المعلومات إذا كان ذلك ضرورة، ويخضع تقرير ذلك لسلطة القاضي التقديرية من حيث توافر حالة الضرورة أو عدم توافرها بحيث يكون إذن التفتيش متضمنا الآتي[47].

- البحث عن أدلة محصّلة من كيان الحساب المنطقي والتي يدخل فيها برامج التطبيق ونظام التشغيل.
- البيانات المستخدمة بواسطة برنامج الحساب أو كيانها المنطقي.
- السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

وينعقد الاختصاص بإصدار إذن التفتيش للجهة القضائية التي يتواجد فيها محل التفتيش، شيئاً كان أو شخصا وذلك وفقا للمادة رقم 41 من قانون الإجراءات الجنائية الأمريكي الفيدرالي.

ويلاحظ أن الاختصاص ينعقد للجهة التي أصدرت إذن التفتيش مادام محل التفتيش كان واقعاً في دائرة تلك الجهة حتى وإن تغيّر مكانها بعد ذلك قبل تنفيذ الإذن أو الإجراء وانتقل إلى دائرة أخرى[48].

2.2-الضوابط الشكلية لتفتيش نظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على حق المؤلف عبر الإنترنت:

بالإضافة إلى الضوابط الموضوعية لتفتيش نظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على حق المؤلف توجد ضوابط أخرى شكلية يجب مراعاتها عند ممارسة هذا الإجراء صوناً للحريات الفردية من التعسف والانحراف في استخدام السلطة وتتمثل هذه الضوابط في الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش وتحرير محضر التفتيش وأسلوب تنفيذه. وذلك على النحو التالي:

أ-الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الحاسب الآلي المرتكبة في بعض جرائم الاعتداء على حق المؤلف:

من أهم الضمانات الشكلية مما يتطلبه القانون في الجرائم من حضور شخص أو أشخاص أثناء التفتيش والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط ونجد أن معظم تشريعات قانون الإجراءات المختلفة لا تسوي بين تفتيش الشخص وتفتيش المنازل وما في حكمها فيما يتعلق باستلزام هذا الإجراء. ومن هذه التشريعات قانون الإجراءات الجنائي المصري والجزائري وإن كان الاثنين قد عنيا بمسألة حضور المتهم أو من يُنيبه أثناء تفتيش المنزل فإنه لم يشترط لصحة تفتيش الأشخاص حضور شهود[49] وبالنسبة لتفتيش المنزل وما في حكمه نجد أن المشرع قد

غير في الضمانات. وفقا للشخص القائم به حيث يشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة أحد مأموري الضبط القضائي، وعلى أن يكون هذان الشاهدان بقدر الإمكان من أقارب المتهم البالغين أو من القاطنين معه في المنزل.

أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة فيصبح اتخاذ الإجراء دون حاجة إلى استدعاء شهود (المادة 82 من قانون الإجراءات الجزائية الجزائري) وفي حالة قيام مأمور الضبط القضائي بمباشرة التفتيش بناء على ندبه لذلك من سلطة التحقيق فإن المسألة لا تتطلب حضور شاهدين في حالة عدم حضور المتهم أو من ينوبه.

وفي فرنسا استوجبت الفقرة الأولى من المادة 57 من قانون الإجراءات الجنائية[56] أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش. وأضافت الفقرة الثانية من نفس المادة أنه إذا استحال حضوره، وجب على مأمور الضبط القضائي أن يكلفه بتعيين من يمثله. فإذا استحال ذلك كان لمأمور الضبط القضائي أن يختار شخصين يشهدان الإجراء الذي يقوم به من غير الأشخاص الخاضعين لسلطته الإدارية[50].

أما في الولايات المتحدة الأمريكية فقد جرى العمل على إصدار أوامر تفتيش دون إخطار مسبق في الدعاوي الجنائية المتعلقة بالكمبيوتر وذلك على الرغم من المخاطر التي قد تترتب على استخدام مثل هذه الأوامر.

ب-محضر تفتيش نظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على حق المؤلف:

بما أن التفتيش عمل من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلاً خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوبا باللغة الرسمية وأن يحمل تاريخ تحديده وتوقيع محررُه وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.

وبالنسبة لمحضر تفتيش نظم الحاسب الآلي فإنه يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنية المعلومات ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسب يرافقه للاستعانة به في مجال الخبرة الفنية الضرورية[51] فلا شك أن وجود معالج بيانات سوف يساعد في صياغة مسودة المحضر بحيث تتم تغطية كل الجوانب الفنية في عملية التفتيش والضبط التي تتم بالإضافة إلى المحافظة على الأدلة المتحصل عليها من كل تلف[52].

جـ-أسلوب تفتيش نظم الحاسب الآلي المستخدمة في ارتكاب جرائم الاعتداء على حق المؤلف:

فلا بد أن يكون القائم بالتفتيش لنظم الحاسب الآلي مدربا تدريبا فنيا خاصا على كيفية التعامل مع تقنية المعلومات وأنظمة معالجة البيانات ومع الأدلة الناجمة عن الحاسب بشكل وافي ودقيق حتى لا تتلف أو تتلاشى من ذاكرة الحاسب الآلي ففي الولايات المتحدة تسببت الشرطة – نظراً لنقص خبرة رجالها – في إتلاف ما كان قد سلم إليها من الملفات والبرامج بوصفها أدلة عن وجود الجريمة المعلوماتية[53].

والواقع أنه من الضروري الارتفاع بمأمور الضبط القضائي إلى المستوى اللائق للتطور التقني في مجال تكنولوجيا المعلومات[54] وذلك بعد دورات تدريبية مكثفة لمأمورى الضبط القضائي على كافة مستوياتهم في تقنيات الحاسب الآلي.

3- ضبط الأدلة الرقمية الناشئة عن جرائم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت.

يقصد بالضبط في قانون الإجراءات الجنائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها[55] ويعد ضبط النتيجة النهائية التي تنتهي إليها إجراءات التفتيش في هذه الحالة يستلزم اتخاذ إجراءات تقنية محددة لكي يمكن القيام بضبط الأدلة المذكورة فلا تصلح الإجراءات المادية المعروفة للقيام بضبط الأدلة وكما هو الشأن في العالم المادي، باستثناء عملية الفصل الضرورية بين الحساب الآلي وبين كل شخص ليس له علاقة بالقائمين على الدعوى الجنائية[56]. وذلك خشية قيام المتهم أو من له علاقة أو مصلحة ما بتدمير الأدلة بإزالتها من الحاسب والمشرِّع المقارن يدرك مدى أهمية ضبط وتحريز الأدلة الرقمية. فقد قام المشرِّع الأمريكي في المرشد الفيدرالي بتحديد أساليب الضبط المختلفة وفقا لطبيعة كل مخالفة والقانون الصادر بشأنها فيجوز وفقاً للقانون الأمريكي مصادرة القطع الصلبة (في الحاسب الآلي ومكوناته المادية) حال وجود انتهاك لحقوق المؤلف أو العدوان عليه عبر الإنترنت، كما هو مقرر في قانون حقوق المؤلف[57].

وإذا كانت مصادرة أجهزة الحاسب الآلي أيا كانت طبيعة نشاطه والذي ارتكبت جرائم الاعتداء على حق المؤلف بمقتضاه أهم وسائل الضبط في جرائم الاعتداء على حق المؤلف بواسطة التقنيات الحديثة فإن مثل هذا الإجراء قد لا يكون هناك إمكانية دائمة في اتخاذه كما ولو كان الضبط يتم عن بعد في حالة اتخاذ إجراءات جنائية عن بعد. ولذلك اتجه المشرِّع المقارن إلى الاعتراف بوجود أساليب أخرى تصلح لكي يتم الضبط بمقتضاها مثل النسخ Copy في حالة عدم وجود إمكانية لضبط القطع الصلبة التي تخزن عليها المصنفات المقلدة فيتم مثلاً نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياته وهنا نجد أسلوب النسخ يصلح تماماً أن ينتج عنه دليل رقمي مقبول أمام القضاء . وإلى جوار النسخ يوجد أيضا أسلوب تجميد التعامل مع الحاسب الآلي أو أحد القطاعات المكوِّنة له والتي تم استخدامها في ارتكاب الجريمة، والتي تحتوي على ما يفيد في الأدلة على ارتكابها. ومثل هذا الإجراء، يصلح أن يتخذ في مواجهة الحاسبات الخادمة التي تحتوي على مواقع القرصنة وكذلك يصلح أسلوب التجميد هذا إذا كان القرص الصلب يحتوي على ملفات مشفرة، وتحتاج بالتالي إلى فك شفرتها لكي يمكن التعرف على محتوياتها الإجرامية أو يكون الدخول إلى الحاسب الآلي يحتاج إلى كلمة مرور Password فالتجميد هنا يساعد خبراء المعمل الجنائي على القيام بعملهم دون خوف من ضياع الدليل[58]. وفي كندا نجد المادة 487 من القانون الكندي تعطي سلطة إصدار إذن لضبط أي شيء طالما تتوافر أسس معقولة للاعتقاد أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلاً على وقوع الجريمة وحتى الآن فإن هذا النص يفسر بوضوح تام على أنه يسمح بضبط بيانات الحاسب غير المادية.

وفي لوكسمبورج فالضبط يشمل بصفة عامة "كل الأشياء التي تفيد في إظهار الحقيقة" وفي هذا الخصوص فإنه يكون من المقبول لدى الفقه هناك أن ضبط مكونات الحاسب وما يستند عليه من دعائم مادية يتضمن البيانات التي تفترض أنها بداخله وفي فرنسا ذهب جانب من الفقه إلى الاعتراف بأن للبرامج كياناً مادياً ملموساً يتمثل في نبضات إلكترونية أو إشارات إلكترونية مغناطيسية أو ممغنطة[59].

كما أكد المجلس الأوربي في التوصية رقم 13 (95) R على أنه يتعين مراجعة القوانين في مجال الإجراءات الجنائية للسماح باعتراض الرسائل الإلكترونية وتجميع للبيانات المتعلقة بتداول المعلومات في حالة التحقيقات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو سلامة الاتصالات أو أنظمة الكمبيوتر.

كما صرحت الاتفاقية الأوربية في شأن جرائم الإنترنت بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجنائية فتنص المادة (19 من القسم الرابع) على أن كل دولة طرف من حقها أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة أن تقوم بتفتيش أو الدخول إلى نظام الكمبيوتر أو جزء منه أو المعلومات المخزنة به.

المبحث الثالث
الشهادة الإلكترونية في مجال جرايم الاعتداء الإلكتروني على حق المؤلف عبر الإنترنت

1- تعريف الشهادة الإلكترونية في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت.

الشهادة الإلكترونية E- Testimpony فهي تطلق على نوعية من الشهادة لا يكون فيها الشاهد حاضراً جلسة التحقيق (الابتدائي أو النهائي) بذاته المادية، أي جسداً، وإنما تتم عبر وسائل إلكترونية أو رقمية[60].

1.1- المقصود بالشاهد في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت .

ويقصد بالشاهد في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت، الفني صاحب الخبرة والتخصص في تقنية الحاسب والذي تكون لديه معلومات عن شبكة الإنترنت وشبكات الاتصال والحاسبات الخادمة الخاصة إذا كانت مصلحة التحقيق تقتضي البحث عن أدلة الجريمة داخلها[61]وهي تشمل بهذا المفهوم عدة طوائف أهمها مستخدمي الحاسب الآلي، خبراء البرمجة، المحللون، مهندسو الصيانة الخبراء التقنيين، مقدمي الخدمات الوسيطة[62].

2.1- التزامات الشاهد في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت :

إذا كان يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة اللجوء إلى المواقع أو الحاسبات[63]التي تأوي مصنفات مقلدة

باحثا عن الأدلة الجرمية فإنه يبقى أن نتساءل هل يلتزم الشاهد أن يقوم بطبع المصنفات المقلدة المخزنة في ذاكرة الحاسوب أو الإفصاح عن كلمة المرور السرية اللازمة للولوج إلى المواقع التي تتيح تلك المصنفات أو الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج.وما يترتب على ذلك من أضرار رغم أن تعاون الشهود المشتبه فيهم والمجني عليهم له أهمية قصوى في كشف وإثبات تلك الجرائم(64).

اختلف الفقه في الإجابة على هذا التساؤل بين المؤيد والمعارض ويمكن بلورة هذا الاختلاف في اتجاهين رئيسيين هما :

الاتجاه الأول : يذهب القائلون بهذا الاتجاه أنه ليس من واجب الشاهد – وفقا للالتزامات التقليدية للشهادة – أن يقوم بالإفصاح عن كلمات المرور أو الشفرات المتاحة بالبرامج المختلفة.

ففي ألمانيا أن الغالبية العظمى من الفقهاء يرون عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب الآلي، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.

وكذلك في تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة(65).

أما بالنسبة لقانون الإجراءات الجنائية المصري رقم 150 لسنة 1950 فقد خول المشرع لمأمور الضبط القضائي سلطة سماع أقوال من تكون له معلومات عن الوقائع الجنائية ومرتكبيها (م 29 من ق أ ج) وأن يسمع في حالة التلبس بالجريمة أقوال الأشخاص الحاضرين في محل الواقعة ومن يمكن الحصول منه على إيضاحات في شأن الجريمة (م31 من ق أ ج) وأن يطلب من الحاضرين عدم مبارحة محل الواقعة أو الابتعاد عنها وأن يستحضر في الحال ما يمكن الحصول منه على إيضاحات في شأن الواقعة (م 32 ق أ ج) (66).

ويلتزم الشاهد بالحضور بنفسه في المكان والزمان المحددان للاستماع إلى شهادته ويؤدي الشهادة بعد حلف اليمين وأن يقول الحقيقة. ويرى جانب من الفقه أن الالتزامات التي فرضها قانون الإجراءات الجنائية المصري على الشاهد لا تضمن التزامه بالمعاونات الفعالية في التحقيق الجنائي الذي يجري بشأن الجريمة التي يدلي فيها بشهادته، ويؤدي ذلك لأنه لا يمكن بالتزام الشاهد بالإدلاء بما لديه من معلومات لازمة للولوج لنظام المعالجة الآلية للبيانات تنقيبا عن أدلة الجريمة داخله فالشاهد غير ملزم بالتعاون فيما يجاوز علمه أو الإدلاء بمثل هذه المعلومات(67).

الاتجاه الثاني : يرى أنصار هذا الاتجاه أن من الالتزامات التي يلتزم بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة. ففي فرنسا يرى بعض الفقهاء أنه طالما أن المشرع لم ينظم هذه المسألة فإن لا مناص من تطبيق القواعد العامة في الشهادة، وعلى ذلك فإن الشهود الذين يقع على عاتقهم الالتزام بأداء الشهادة يكونوا مكلفين بالكشف عن كلمات المرور السرية التي يعرفونها وشفرات تشغيل البرامج، ماعدا حالات المحافظة على سر المهنة فإنهم يكونون في حِلّ من هذا الالتزام(68).

وفي هولندا يتيح مشروع الحاسب الآلي لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة للولوج داخله للإفصاح عن كلمة المرور السرية والشفرات الخاصة بتشغيل النظام ويتم تكليف القائم على تشغيل النظام المعلوماتي بحل رموز هذه البيانات.

2- مدى قبول الشهادة الإلكترونية أمام سلطات التحقيق

تفترض هذه النوعية من الشهادات حصولها في التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضر جسدياً أو مادياً في الجلسة، إلا إذا توفرت الوسائل اللازمة التي يمكن من خلالها الحصول على أقواله بشكل سمعي ومرئي.

والقضاء الأمريكي حتى مرحلة ظهور فكرة الدوائر الاتصالية المتكاملة كان يرفض بقوة إمكانية إحداث اتصال صوتي بين الجلسة والشاهد، فالقضاء الأمريكي مثلاً يعتبر كل ما يمكن أن يصوره شخص من خارج الجلسة نظرا للدعوى من قبيل شهادة السماع التي لا تُقبل البتة أمامه لأجل ذلك تقررت مواد استدعاء الشاهد في قانون الإجراءات الجنائية التي تصل إلى حد إقامة الجزاء على مخالفته أمر الحضور للمحكمة.

أما بعد ظهور فكرة الدوائر الاتصالية المتكاملة من مغلقة ومفتوحة[69] فقد أثير مدى إمكانية قبول الشهادة الفورية عبرها وهو الأمر المقبول فقها، سيما وأن الشاهد في الغالب من الأحيان يبرز في هيئته الكاملة في هذا الإطار، فيبدو كما لو كان حاضراً أو يثور مظاهر مصداقية في رد فعله الطبيعي حين تعرضه لأسئلة الدفاع والاتهام أثناء سير جلسة التحقيق. ولقد كانت بداية الأخذ بنظام الشهادة الإلكترونية الفورية في القضاء الأمريكي عندما واجه القضاء مشكلة الإدلاء بالشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبول نظام الشهادة الإلكترونية الفورية طالما كانت هناك أسباب في القانون تدعو إليه، وفي قضية استلزمت إدلاء شخص محصن لسماع شهادات عبر دوائر تلفزيونية مغلقة شريطة أن يكون حضور الشاهد عبر الدوائر المذكورة كما لو كان حاضراً الجلسة بالفعل حيث يكون كل ما يدور في الجلسة مرئياً له بالمقابل لرؤية من هو في الجلسة له[70] وهذا ما تم توضيحه سابقاً.

3- موقف القانون الجزائري والمصري من قبول الشهادة الإلكترونية في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت

لم يتعرض قانون الإجراءات الجزائية الجزائري والمصري بالنص على قبول أو عدم قبول الشهادة التي يدلى بها الشاهد وهو غير حاضر جسدياً مادياً أمام سلطة التحقيق والمحكمة وذلك من خلال الوسائل الإلكترونية ويرجع السبب في ذلك في رأينا كون قانون الإجراءات الجزائية الجزائري والمصري قد أجازا للمحكمة إذا اعتذر الشاهد بأعذار مقبولة عن إمكان الحضور أن تنتقل إليه وأن تسمع شهادته، على أن يكون ذلك بعد إحضار النيابة العامة وباقي الخصوم الذين لهم أن يحضروا بأنفسهم أو بواسطة وكلائهم وأن يوجهوا للشاهد الأسئلة التي يرون لزوم توجيهها إليه ويجوز في هذه الحالة أن يكون انتقال المحكمة بكامل هيأتها أو تندب بذلك أحد أعضائها أو قاضيا آخر[71].

المبحث الرابع
الخبرة التقنية في مجال جرايم الاعتداء الالكتروني على حق المؤلف عبر الإنترنت

1- تعريف الخبرة التقنية وأهميتها:

1.1- تعريف الخبرة التقنية.

هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقيم الأدلة والوسائل القانونية التي يحتاج تقديرها إلى معرفة فنية ودراية علمية لا تتوفر لدى عضو السلطة القضائية المختصة بحكم عمله وثقافته والخبرة التقنية في مجال المساعدة القضائية تعد أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنولوجيا المعلومات والإنترنت، ذلك أنه تؤدي دوراً لا يستهان به إزاء نقص المعرفة القضائية الشخصية لظاهرة الإنترنت[72].

2.1- دور الخبرة التقنية في مجال جرائم الاعتداء على حق المؤلف عبر الإنترنت :

وللخبرة أهمية بالغة في مجال الجرائم المعلوماتية الخاصة بالاعتداء على حقوق المؤلف عبر الإنترنت وذلك نظراً لتشعب وتنوع أنواع الشبكات والحاسبات المرتبطة بها، كما أن التطورات الحادثة في هذا المجال سريعة

ومتلاحقة يصعب على المتخصص تتبعها واستيعابها لدرجة يمكن القول معها الآن أنه لا يوجد خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها وكذلك لا يوجد خبير قادر على التعامل مع كافة أنواع الجرائم التي ترتكب بواسطتها[73].

ومما يقوي ضرورة الاستعانة بخبير أن كثيراً ما تفشل جهات التحقيق في جمع الأدلة الالكترونية بل أن المحقق في كثير من الأحيان يدمر الدليل الفني كنتيجة خطا أو إهمال أو جهل في التعامل معه ُلذلك ترك المشرع للمحقق الحرية كاملة في هذا الشأن ليمكنه من كشف الحقيقة.

ومن أهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية الخاصة بالاعتداء على حقوق المؤلف عبر الإنترنت[74].

- وصف تركيب الحاسب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها بالإضافة إلى الأجهزة الملحقة به وكلمات المرور أو السر ونظام التشغيل.
-وصف طبيعة بيئة الحاسب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردد موجات البث وأمكنة اختزانها.
-وصف الوضع المحتمل لأدلة الإثبات والشكل والهيئة التي تكون عليها.
- بيان كيف عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.
- بيان كيف يمكن عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يلحقها تلف.
- بيان كيفية تجسيد الأدلة في صورة مادية ينقلها إذا أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[75].

2- أساليب عمل الخبير التقني

و للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها وهو في إطار القيام بعمله أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه.
و هناك أسلوبان لعمل الخبير التقني :
الأول : القيام بتجميع لمجموعة المواقع التي تشكل جريمة اعتداء على حقوق المؤلف في ذاتها، ثم القيام بعملية تحليل، فني لها بمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها
و كيف تم التواصل إلى معرفتها ومن ثم التوصل في النهاية إلى معرفة بروتوكول الإنترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذه المواقع.
الثاني: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكِّل موضوعها جريمة في ذاته وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على التعريف على كيفية التعامل مع القنابل الزمنية والمنطقية وتركيبها والقيام بفكها وحفظها.

3- سلطة المحكمة في تقدير رأي الخبير التقني عن جرائم الاعتداء على حق المؤلف عبر الإنترنت.

يعتبر رأي الخبير رأياً استشارياً لا يُلزم المحكمة فلها أن تأخذ به أو تطرحه ولها أن تأخذ برأي الخبير ولو لم يكن جازما في المسألة التي طلب الرأي منها، ولها أن تأخذ ببعض ما جاء في تقرير الخبير دون البعض الأخر
أو أن تأخذ بما جاء في تقرير الخبير الذي ندبته سلطة التحقيق الابتدائي وتطرح تقرير الخبير الذي هي ندبته أثناء المحاكمة.

يرى جانب من الفقه أن القاضي يظل الخبير الأعلى، حتى ولو كانت المسألة الفنية في مجال الإنترنت قد تعرض لها خبير الإنترنت وأخذ القاضي برأيه، بل أنه حتى في حالة رفض الأخذ برأي الخبير فإن القاضي ليس ملزماً بسلوك محدد كالاستعانة بخبير أخر يقدم تقريراً فنياً، فليس في القانون ما بعد الإلزام وإنما منطق الإلزام هنا هو السعي إلى إبراز الحقيقة ومثل هذا المنطق لا يجعل الخبير في مستوى عمل القاضي، بل يظل دور القاضي قائما في المفاضلة بين التقارير الفنية المقدمة إليه[76].

الخـــــاتمـة

بعد أن صار المجتمع المعلوماتي حقيقة لا تجريد، باتت حاجته واضحة لنصوص تشريعية في مختلف فروع القانون تلائم تمركز مقوماته وسائر أنشطته حول المعلومات وتقنياتها، وتكفل مواجهته للأشكال المستحدثة عن استخدام هذه التقنية خاصة في مجال إثبات الجريمة المعلوماتية بصفة عامة،وجرائم الاعتداء علي حق المؤلف عبر الإنترنت بصفة خاصة.
لذا نوصي بمقترحات قد تساعد في كيفية إثبات هذا النوع من الجرائم كما يلي :
أولاً: تحديد السلطات المختصة بإجراء التفتيش والضبط في بيئة البرمجيات (الأموال المعنوية) وتفتيش نظم الحاسبات المتصل بعضها بالآخر (شبكات الحاسب computer networks).

ثانياً : واجب المعاونة الفعالة من جانب المجني عليه والشهود وغيرهم من مستخدمي المعلومات والبرمجيات عدا المشتبه فيه، وبوجه خاص تقديم المعلومات المخزنة داخل النظام في شكل واضح للاستخدام للأغراض القضائية.

ثالثاً : إدخال تعديلات تشريعية لمواجهة المشاكل التي يمكن أن تتسبب فيها القواعد القائمة الخاصة بقبول الأدلة عند تطبيقها أثناء الإجراءات القضائية، على تسجيلات ومخرجات الحاسبات.

أما القواعد الجنائية الموضوعية فينبغي أن يُراعى عند تعديلها أو استخدامها، عدم تأسيس على حالة التطور التقني الراهنة فقط والتعبير عن المفاهيم الفنية والأجهزة من منظور الوظيفة والاستخدام أكثر من منظور التقنية، عدم الإفراط في التجريم أو الدخول في تفصيلات تعوق تطبيق النصوص في العمل، مع التزام الوضوح والدقة في تحديد السلوك المجرّم، وتجنب التعبيرات المطاطة والغامضة.

رابعاً : التصدي بحزم لظاهرة القرصنة وتقليد برامج الكمبيوتر والإنترنت وتشديد العقاب على مرتكبيها لأضرارها الواضحة بصناعة البرمجيات وتكنولوجيا المعلومات مما يؤثر بالسلب على اقتصاد الدولة فيجب التوسع في إسباغ الحماية الجنائية لبرامج الحاسب الآلي.

خامساً : عدم كفاية وملاءمة القواعد القانونية العقابية التقليدية في مكافحة جرائم الحاسب الآلي والإنترنت كالسرقة والنصب وخيانة الأمانة، وغيرها من مسميات كان محلها معلومات (برامج) لاختلاف الطبيعة القانونية للمعلومات، إذا ما قُورِنت بغيرها من المنقول ذلك أنها من طبيعة معنوية أو مال معنوي.

سادساً : إن المشرع الجزائري شأن المشرع العربي في كثير من البلاد العربية مدعو إلى التدخل لملاحقة السرعة المطَّرِدَة لظاهرة الإجرام المعلوماتي ومواجهتها. ومكافحتها بنصوص صريحة واضحة يُراعى في وضع هذه النصوص العقابية الجديدة سمات المجرم المعلوماتي، وطبيعة المصلحة المحمية والصعوبات القائمة في مجال إثبات تلك الجريمة، وسد الفراغ التشريعي في هذا الخصوص سواء من الناحية الموضوعية أو الإجرائية، وضرورة تشديد العقاب على جرائم المعلوماتية والدخول غير المشروع في نظام المعالجة الآلية للمعلومات والعقاب على الاعتداءات التي تقع على الكيانات المنطقية (البرامج).

عقد مؤتمرات، وندوات، ودورات تدريبية لرجال الضبطية القضائية ورجال النيابة العامة والقضاء وتأهيل كل من يعمل بالحقل البوليسي أو القضائي للتعرف على كيفية ارتكاب جرائم الحاسب الآلي والإنترنت وكيفية ضبطها، مع التوازن بين حق الأفراد في الحصول على المعلومات وأسرارهم وحريتهم الشخصية، ومبدأ الشرعية وحق الدولة في حماية أمنها المعلوماتي والنظام العام والآداب العامة داخلها، وقد أوضحت توصيات المؤتمر الدولي الثاني للتحقيق الجنائي المنعقد في أمستردام في الفترة من 5-15 ديسمبر 1999م والذي شارك فيه 170 من العلماء والخبراء ورجال القانون لتؤكد القناعة بضرورة تدريب رجال الشرطة والنيابة والقضاء، لذا كانت دعوة المؤتمر هي مزيد من التعليم والتدريب لكل تلك الفئات. وفي مواجهة المجرم المعلوماتي لا بد من تأهيل سبل مقاومته ورجال هذه المقاومة، فلابد من وجود رجال الشرطة أو الضبطية القضائية المعلوماتية. دون المساس بحماية حق الأفراد وحياتهم الخاصة، ويجب العمل على تطوير وسائل المراقبة والتحري والاستدلال كالمراقبة الإلكترونية والمراقبة عن بعد والاستفادة من تجارب الدول المتقدمة في هذا المجال.

الهوامش

(1) أنظر : د. ياسر أنور علي ، د. أمال عثمان : شرح قانون الإجراءات الجنائية دار الثقافة الجامعية 1997 ، ص 399 .

(2) أنظر : د. السيد العتيق : النظرية العامة للدليل العلمي في الإثبات الجنائي – رسالة دكتوراه – كلية الحقوق جامعة عين شمس 1993 ، ص20

(3) أنظر : د. أحمد فتحي سرور : الوسيط في قانون الإجراءات الجنائية – دار النهضة العربية 1985 ، ص 287 .

(4)Convention sur la cyber criminalite STE ^{2} , No 185 , Rapport explicatif , adopté le 8 Novembre 2001 . p. 37 , REVUE PENTENTIAIRE , Droit pénal N°1 Avril 2002 , P . 178 .

(5) أنظر : د. أولريش شيبة : جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات – المؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة 1993 – ص 57 .

(6) أنظر : د. محمود نجيب حسني : شرح قانون الإجراءات الجنائية – دار النهضة العربية 1982 – ص 655 .

(7) أنظر : د. محمد عنب : معاينة مسرح الجريمة – رسالة دكتوراه – أكاديمية الشرطة – كلية الدراسات العليا – القاهرة 1988 – ص 13 و ما بعدها .

(8) BENSOUSSAN (Alain) :
Utilisation de l'outil informatique a usage professionnel , 17 Novembre 2000, sur le site :
http://www.alainbensoussan.com/base_de_données/internet/support/support_01.html

(9) أنظر : د . جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – دار النهضة العربية 2001 ، ص 28

(10) Dariel Morris – Tracking a computer Haker US Attorneys bulletin 2/2001 p, 3 available at www. U.S.A . gov/ criminal / cybercrime USA may 2001 htm .

(11) أنظر :د. أبو بكر يونس :الجرائم الناشئة عبر الإنترنت – رسالة دكتوراه كلية الحقوق- جامعة عين شمس 2004 – ص 895.

(12) Dariel Morris – Tracking a computer Haker US Attorneys bulletin 2/2001 p, 3 available at www. U.S.A . gov/ criminal / cybercrime USA may 2001 htm .

(13) SEDALLAIN (V) Droit de Internet Réglementation , responsabilités , contrats , collection AUI . Paris 1996 . p . 136 .

(14) أنظر : د. سعيد عبد اللطيف : إثبات جرائم الكمبيوتر المرتكبة عبر الإنترنت – دار النهضة العربية 1999 – ص 110 .

(15) ALTRY – BONNART (Catherine) L'arsenal penale juridique sur INTERNAT , G,P . 22 .. llet 1997 , p. 26 .

(16)أنظر :د.هشام فريد رستم ،الجوانب الإجرائية للجرائم المعلوماتية – مكتبة الآلات الحديثة – أسيوط 1994 – ص 59 وما بعدها.

(17) Robert w .Taylor , Computer Crime In criminal investingation ,Hill , INC fifth Edition , 1992.p540.

(18) Prof sousan Brenner – Model code of cybercrime investigation procedure p .24 uni dayton school of law avaible online at http :// cybercrimes . Net .Mccip/Mccip . htm.

(19) أنظر : د . أيمن عبد الحفيظ : حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية – مجلة مركز بحوث الشرطة – العدد 25جانفي 2004 – ص367 .

(20) Daniel A.Morris – Traking computer hacker U.S.Attorney bulletien 2/2001 p.3 avilable at www.U.S.A gov/criminal/cybercrime U.S.A May 2001 htm.

(21) أنظر : د. محمد الأيمن البشري : التحقيق في جرائم الحاسب الآلي – بحث مقدم إلى مؤتمر القانون والإنترنت – ماي 2000 – جامعة الإمارات – ص30.

(22) أيمن عبد الحفيظ : حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية – مجلة مركز بحوث الشرطة – العدد 25 يناير 2004 – ص380.

(23) محمد فهمي طلبة : الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني – القاهرة 1991 – مطابع الكتاب المصري الحديث 1992- ص10 وكذلك :

د/ علاء الدين مصطفى : الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني – موسوعة دلتا كمبيوتر – مطابع الكتاب المصري – ص32.

(24) أنظر : د. هلالي عبد اللاه : تفتيش نظم الحاسب الآلي – دار النهضة العربية 1997- ص74.

(25) VASSILAK,(irini) computer crimes and other crimes against information technology in greece R.I.D.P.1993.P.371.

(26) JAEGER (Marc) les crimes informatique et d'autre crimes dans le domaine de la technologie informatique au luexenbourg R.I.D.P.1993 P.467.

(27) FREBRACHE (David) technology of computer viruses " SPRINGER – VERLQY london.ltd 1992.p.233.

(28) Yair eail – new fedral guidine for searching & seizing computer the internet la journal 2001.www.tili.com/content/litigation headline/02050/02/htm.

(29) Dorham cole the emerging structures of criminal information law : tracing the comun of a New Poradigm "R.I.D.P.1993.P.119.

(30) Gessin(R) Le droit penal et l'infprmatique 1982.p.38.

(31) VERBIEST (THIBAULT) : La protection juridiques du cyber consommateur , Litec, Paris , 2002.p.122.

(32) Loi 18 mars 2003 pour la securite interieure article 17/2 .www.legifrance.Gouv.fr/w. Aspad/Un Texte Degorf ? Numjo – 21/06/2003.

(33) **VERBIEST (THIBAULT)** : La protection juridiques du cyber consommateur , Litec, Paris , 2002.p.127.

(34) Conseil de L'EUROPE , la criminalite informatique recommandation No R(89) g sur la criminalite en relation avec ordinateur et rapport final du comite européén pour les problem crimnels, strsbourg, conseil du Europe.

(35) David.G.Masse www.mase.org/preuve courrie/.thm.p.II.

(36) راجع المادة 181 من قانون حماية حقوق الملكية الفكرية رقم 82 لسنة 2002 – منشورة بالجريد الرسمية بالعدد22 مكرر 2 جويلية 2002 ود. محمود عبد الرحيم الديب –حماية حقوق الملكية الفكرية في مجال الإنترنت – دار الجامعة الجديدة للنشر 2005- ص 66 .

(37) أنظر : د/ علي عبد القادر القهوجي: الحماية الجنائية لبرامج الحاسب الآلي – دار الجامعة الجديدة للنشر 1998 ص5.

د/ عبد الرشيد مأمون، د/ محمد السامي الصادق: حقوق المؤلف في ضوء القانون رقم 82 لسنة 2002 دار النهضة العربية 2004 – ص532 وكذلك:

د/ عبد الحفيظ بالقاضي: حق المؤلف وحدود حمايته جنائيا – رسالة دكتوراه كلية الحقوق جامعة الرباط 1995 ص300.

د/ أسامة عبد الله قايد: الحماية الجنائية لحق المؤلف – دار النهضة العربية 1991 – ص56 .

(38) أنظر : د. هلالي عبد اللاه – تفتيش نظم لحاسب الآلي وضمانات المتهم المعلوماتي – دار النهضة العربية 1997 ، ص 115 .

(39) أنظر : د . عبد الله حسين محمود: سرقة المعلومات المخزنة في الحاسب – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس 2001 – ص 308 .

USA V.RYMOND WONG, App 9 th Cir, No. 02.10070 Cr- 00-40069 – CW, jeune (40) 26, 2003.
(41) Kenethe.fink v. state of delaware, supp, cr delaware, no .244,2002(inoo – 05-1272 thru 1274, inoo-05. 1260 thru. Inoo – 05-1272 thru 1285, and inoo-05-1752 thru february 21.2003.
(42) د/محمد فهمي طلبة : الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني – موسوعة دلتا كمبيوتر– مطابع الكتاب المصري الحديث 1991- ص 107.
(43) د/ محمد السيد خشبة : مقدمة في الحسابات الإلكترونية – القاهرة 1974 – ص 21.
(44) KANEYH(E) V. State of delaware, supp, Cr Dalaware, No 344, 2022(IN00-05-1272-Thru 1274) Febreary 21, 2003.
(45) United States v. hargus 128 f.3d 1358 , 1363(10 th cir 1997)
www.cybercrime.gov/smanual 2002.htm, p.50.
(46) United states v. Gawrisiak, 972 F. Supp 853 (D.N.J 1997) www.cybercrime.gov/smanual 2002.htm.
(47) أيمن عبد الحفيظ: حدود شرعية أجهزة الشرطة في مواجهة الجرائم المعلوماتية – مجلة مركز بحوث الشرطة – العدد 25 يناير 2004 – ص 280 .
(48) شيماء عبد الغني: الحماية الجنائية للتعاملات الإلكترونية – رسالة – كلية الحقوق جامعة المنصورة 2005 – ص244 ،240.
(49) د/ ياسر أنور علي، د/ أمال عثمان: شرح قانون الإجراءات الجنائية – دار الثقافة الجامعية 1997 – ص419.
(50) د/ هلالي عبد الله : تفتيش نظم الحاسب الآلي – دار النهضة العربية 1997- ص165.
(51)Code de procedure prnale, Dalioz 1995-1996.
(52) ERMAN (sahir) les crimes informatique et d'autres crimes dans le domaine de la techonologie informatique en Turquie R.I.D.P. 1993.P.623.
(53) Dorham cole the emerging structures of criminal information law : tracing the contours of a New Poradigm General raport for the A.I.D.P COLLOCIUM "R.I.D.P.1993.P.110.
(54) راجع قرصنة الكمبيوتر المصرفي وهم أم حقيقة – بيروت – مجلة المصارف العربية – العدد 84 جانفي 1987 – ص 52.
(55)YANN PADOVA un apercu de la lutte contre la cyber criminalite en France, Revue de science criminelle et de droit pénal coparé Fevrier 2003 , p.770.
(56) د/ مأمون سلامة: شرح قانون الإجراءات الجنائية – دار الفكر العربي – ص358.
(57)James Garity and Eoghan Casey – INTERNET Misuse in the workplace A lawyer's primer p.13.
(58) أنظر : د .عمر محمد بن يونس: الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي (المرشد الفدرالي الأمريكي لتفتيش وضبط نظام الحاسب الآلي وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية)، دار الفكر العربية 2005 – ص219.
(59) أنظر : د.أبو بكر يونس : الجرائم الناشئة عن الأنترنت – رسالة دكتوراه كلية الحقوق – عين الشمس 2004 – ص 871.
(60) PIRAEOF (Donald) Computer crimes against information technology in Canada(R.I.D.P) 1993 p.241.
(61) SAGROS (pierre) et MASSE 5 Michel) « le droit penal et informatique » études du 15 Nov 1990 publication d'institut de science criminelle de faculté droit de poitiers éd. Cujas Tom IV, p.25.
(62) أنظر :د . عمر محمود أبو بكر : الجرائم الناشئة عن استخدام الأنترنت الأحكام والموضوعية والإجرائية – رسالة دكتوراه كلية الحقوق – جامعة عين شمس 2004 – ص 945.
(63) أنظر : د . هلالي عبد اللاه : التزام الشاهد بالإعلام في الجرائم المعلوماتية – دار النهضة العربية 1997 ص 23 وما بعدها.

(64) Nicolas IDE Les responsabilités des INTERMIDIERES sur les INTERNET. R.I.D.A.186.Octobre 2000.P.1.

(65) أنظر : د. هلالي عبد اللاه : التزام الشاهد بالإعلام في الجرائم المعلوماتية – دار النهضة العربية 1997 ص 23 وما بعدها

وكذلك د/ عبد الله حسين محمود – سرقة المعلومات المخزنة في الحاسب الآلي – رسالة دكتوراه – كلية الحقوق جامعة عين الشمس 2000 – ص 389.

(66) أنظر : د. محمد أبو العلا عقيدة : مواجهة الجرائم الناشئة عن استخدام الحاسب الآلي – بحث مقدم لمؤتمر حول الكمبيوتر والقانون – الفيون 1994 – ص 121 .

(67) ERMAN (sahir) les crimes informatique et d'autres crimes dans le domaine de la 4techonologie informatique en Turquie R.I.D.P. 1993.P.62.

(68) أنظر : د. هشام فريد رستم : الجوانب الإجرائية للجرائم المعلوماتية – دار الآلات الحديثة – أسيوط 1994 – ص 91.

(69) Carlos Kunsenuller, computer crimes and other crignes against information technology R.I.D.P.1993.P.259.

(70) FRANCILLON (jaques) Les crimes informatique et d'autre crimes dans le domaine de la technologie informatique en France. R.I.D.P.1993, p.309.

(71) الدوائر المغلقة تعني انغلاق الدوائر الاتصالية بين جهتين فأكثر يتم تحديدها مسبقا وبحيث لا يستطيع الغير الدخول على هذه الدائرة .

(72) Pater r schiam & harvey m.stone – taking testimony through closed circuit television avaialble at http//www.jextra.com/ egi-bin/fcat prod / ljextra / data /texts / 091297 3 html.

(73) أنظر : د. مأمون محمد سلامه : قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام القضاء بدون ناشر 2005 ص902.

(74) د/عمر بن يونس : الجرائم الناشئة عن استخدام الإنترنت_ رسالة كلية الحقوق جامعة عين شمس 2004- ص1031

(75) Philipe Stanly, Computer Crime Investigation and Investigators Computers Security North Holland 1998,P.310-311

(76) بحث مقدم من مركز البحوث والدراسات بشرطة دبي – الإمارات العربية المتحدة بعنوان جرائم الكمبيوتر.