جامعة عبد الرحمن ميرة- بجاية-

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

الإثبات الجنائي في الجرائم المعلوماتية

مذكرة تخرج لنيل شهادة الماستر في الحقوق

قسم: القانون الخاص

تخصص: القانون الخاص والعلوم الجنائية

من إعداد الطالبتان

معمش زهية

غانم نسيمة

تحت إشراف الأستاذ

بن فردية محمد

أعضاء لجنة المناقشة:

* بن شعلال الحميد	رئيسا.
* بن فردية محمد	مشرفا.
* لعوارم وهيبة	ممتحنا.

السنة الجامعية: 2012-2013

بسم الله الرحمان الرحيم

«....وما توفيقي إلاّ بالله عليه توكلت
وإليه أنيب »

(سورة هود الآية .88.)

شكر و تقدير

الحمد لله الذي أنار لنا درب العلم والمعرفة،
وأعاننا على أداء هذا الواجب ووفقنا إلى انجاز هذا العمل
نتوجه بجزيل الشكر والامتنان إلى كل من ساعدنا من قريب أو من بعيد على انجاز هذا العمل، وفي تذليل ما واجهناه من صعوبات.
ونخص بالذكر الأستاذ المشرف بن فردية محمد الذي لم يبخل علينا بتوجيهاته ونصائحه القيمة التي كانت عونا لنا في إتمام هذا البحث.
لابد لنا ونحن نخطو خطواتنا الأخيرة في الحياة الجامعية من وقفة نعود إلى أعوام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل الغد لتبعث الأمة من جديد.
وقبل أن نمضي نقدم أسمى آيات الشكر والامتنان والتقدير والمحبة إلى الذين حملوا أقدس رسالة في الحياة.
إلى
الذين مهدوا لنا طريق العلم والمعرفة .
إلى
جميع أساتذتنا الأفاضل .

"كن عالما ... فإن لم تستطع فكن متعلما، فإن لم تستطع فأحب العلماء، فإن لم تستطع فلا تبغضهم"

-قائمة المختصرات-

باللغة العربية:

ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري

ق.ع.ج: قانون العقوبات الجزائري

ج.ر.ج.ج: جريدة رسمية جمهورية جزائرية

د.ط: دون طبعة

د.د.ن: دون دار النشر

د.ب.ن: دون بلد النشر

د.س.ن: دون سنة النشر

ع: عدد

ص: صفحة

الخ: إلى آخره

باللغة الفرنسية:

Op.cit : Opère- citato

P : Page

إهـــــــــداء

إلى التي لا يمكن للكلمات أن توفي حقها، وإلى التي لا يمكن للأرقام أن تحصي فضائلها .....

الأم التي ربتني وأنارت دربي وأعانتني بالصلوات والدعوات

وإلى أبي العزيز الذي عمل بكد في سبيلي وعلمني الكفاح وأوصلني إلى ما أنا عليه، إلى أغلى شخصان في هذا الوجود

" أمي وأبي" الحبيبين

إلى منبع المحبة والحنان وسندي في الدنيا

" إخواني وأخواتي"

إلى من لا تكفيني كل معاني الحب أهديه له

" الزوج العزيز"

إلى الأحبة ونبر السعادة "المشاغبين والمشاكسين"

"أبناء الأخوات"

إلى كل العائلة والأحباء والأصدقاء رفقاء الدرب في هذه الحياة

- نسيمة و زهية-

مقـــــــدمة

لقد مهدت الثورة الصناعية الطريق لظهور ثورة جديدة منذ أواخر القرن العشرين ألا وهي الثورة المعلوماتية، والتي غيرت حياة الأفراد بشكل كبير في مجالات عدة، نظرا لما تتميز به من سرعة ودقة في تجميع المعلومات وتخزينها ومعالجتها وكذا تبادلها بين الأفراد والشركات والمؤسسات المختلفة سواء كانت داخل الدولة أو بين عدة دول، كما تعتبر أيضا مستودعا للأسرار الخاصة والعملية للأشخاص خاصة بعدما حدث اندماج بين المعلوماتية والاتصال عن بعد، حيث أصبح الإنسان يعيش في البيئة العالمية للتقنية العالية للمعلومات، أين يعتبر الحاسب الآلي والانترنت محورا أساسيا لها.

وبقدر ما حققت تكنولوجيا المعلومات أثارا إيجابية من إنجازات وتطورات في المجال الرقمي من خلال الاعتماد عليها في الكثير من قطاعات الحياة، فإنها في الوقت نفسه مهدت إلى ظهور أنواع جديدة من الجرائم بالغة الخطورة، شكلت اعتداءات على الحياة الخاصة للأفراد وسببت في خسائر كبيرة لاقتصاد الدولة ألا وهي الجرائم المعلوماتية بشتى أنواعها، ذلك أن المجرم اليوم وجد تقنية عالية وأساليب حديثة تساعده في ارتكاب الجرائم دون أن يترك أثر للكشف عنها ومعرفة مصدرها، وكما يستطيع أيضا أن يقترف جريمته ضد مجموعة من المجني عليهم في أيّ مكان يرغب فيه وفي نفس الوقت بعد أن تم الربط بين الحاسب الآلي والشبكة العالمية للانترنت[1].

ومن بين أنواع الجرائم المعلوماتية التي نشهدها اليوم، جرائم اختراق شبكات المعلومات والبيانات، تزييف النقود بالوسائل الإلكترونية، تزوير المستندات الإلكترونية، إتلاف البرمجيات وتدميرها، ناهيك عن استخدام الحاسب الآلي كأداة في ارتكاب جرائم تقليدية مثل سرقة الأموال والنصب بواسطة الحاسب الآلي، إلى جانب المواقع الإباحية ودعارة الأطفال عبر الانترنت وغيرها من المواقع المخالفة للأخلاق والآداب العامة.

لذلك أدى الاستخدام غير المشروع للتقنية المعلوماتية إلى ظهور علم جديد في البحث الجنائي وهو علم البحث الجنائي الرقمي الذي يهتم بالدليل الرقمي بالنظر للآثار التي يتركها المتهم المعلوماتي

---

[1] سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية،–دراسة تحليلية تطبيقية–، رسالة ماجستير في العلوم الشرطية تخصص التحقيق و البحث الجنائي، كلية الدراسات العليا ،جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص.15.

أثناء ارتكابه لجريمة معلوماتية، فقد انعكس التطور الحاصل للوسائل الإلكترونية على قانون العقوبات والذي بدوره انعكس على قانون الإجراءات الجزائية، حيث أن هذا الأخير لا يمكن تطبيقه في ظل عدم إدراج هذه الجرائم المستحدثة في قانون العقوبات، كذلك فإن الإثبات الجنائي الذي يعد أهم موضوعات قانون الإجراءات الجزائية تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ووسائل ارتكاب الجريمة، فالإثبات عموما يهدف إلى بيان التطابق بين الشكل القانوني والواقعة المعروضة، وفي سبيل الإثبات يتم استخدام وسائل معينة وهي ما يسمى وسائل الإثبات التي تعتبر نشاط يبذل في سبيل اكتشاف حالة أو مسألة أو شيء ما يفيد في إظهار عناصر الإثبات أي الأدلة.

وتثير مسألة الإثبات في نظم الحاسوب والانترنت مشكلات في جمع الأدلة الجنائية، ذلك باعتبار أن الجرائم المعلوماتية غير مرئية حيث يمثل انعدام الدليل المرئي عقبة كبيرة أمام كشف الجرائم وقد يشكل تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر الانترنت صعوبة أمام إثباتها، كما أن سهولة محو الدليل تعد من أهم الصعوبات التي تعترض طرق الوصول إلى أدلة الإثبات الجنائي في مجال الجرائم المعلوماتية، ولا شك أن الطبيعة العالمية التي تتميز بها هذه الجرائم قد تثير مشكلات عدة تتعلق بتحديد الاختصاص المكاني وقواعد سريان القانون الوطني من حيث المكان، مما يزيد عقبة في الإثبات الجنائي لهذه الجرائم خاصة في حالات ارتكابها خارج النطاق المكاني للإقليم، لذلك فإن التنقيب في هذا النوع من الجرائم يحتاج إلى طرق إلكترونية فنية وتقنية تتناسب مع طبيعتها بشكل يمكنها من فك كلمات المرور السرية وترجمة النبضات الإلكترونية إلى بيانات مقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ونسبتها إلى فاعليها، وتدعى هذه الوسيلة بالدليل الرقمي، وكذلك تثير مسألة ضمان مصداقية هذا الدليل الرقمي للتعبير عن الحقيقة التي تهدف إليها الدعوى الجنائية في الجرائم المعلوماتية.

أهمية الموضوع

ولقد قمنا باختيار هذا الموضوع وجعلناه موضوع دراستنا في هذه المذكرة نظرا للأهمية البالغة لموضوع الإثبات الجنائي في الجرائم المعلوماتية، وتظهر هذه الأهمية من خلال اعتبار أن موضوع الجرائم المعلوماتية حديث وكثير الانتشار حاليا، كما أنه من الموضوعات التي تثير جدلا فقهيا لدى فقهاء القانون الجنائي، إضافة إلى تعلق هذا الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أمام القائمين على البحث وإثبات الجرائم المعلوماتية، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين

التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلائم مع طبيعتها الفنية.

وتكمن أيضا أهمية البحث في أن العلم قد أحدث الكثير من وسائل الإثبات من بينها الدليل الرقمي، والذي يطرح مسألة تقديره أمام القاضي الجنائي وتأثيره في إثبات الجرائم المعلوماتية خصوصا مع تضاؤل دور القاضي الجنائي أمام طبيعة هذه الجرائم لكونها تحتاج دائما إلى خبير معلوماتي باعتبارها مسائل فنية بحتة.

أهداف البحث

إن الغاية المرجوة من هذه الدراسة تتمثل أساسا في تحديد طرق وكيفية الوصول واستخـــلاص أدلة الإثبات الجنائية في الجرائم المعلوماتية، كما تهدف هذه الدراسة إلى تقديم رؤية خاصة بشأن التحقيق الجنائي في هذه الجرائم، كون أن مسرح الجريمة الرقمي هو مسرح افتراضي غير مرئي وكما تناولت الدراسة الصعوبات التي تواجه التحقيق الجنائي، ولفت الانتباه من خلال هذه الدراسة إلى أن الدليل الرقمي وتحديد ماهيته يعتبر من أهم أدلة الإثبات في الجرائم المعلوماتية، وقـــد تعرضت الدراسة أيضا إلى المشكلات التي تعيق تحديد الاختصاص المكاني في هذا النوع من الجرائم العابرة للحدود ومدى سلطة القاضي الجنائي في قبول الدليل الرقمي أمام المحاكم كدليل إثبات جنائي في الجرائم المعلوماتية.

إشكالية البحث

أما عن إشكالية هذا الموضوع، فباعتبار أن صعوبة كشف وضبط الدليل الرقمي المستخلص من الجرائم المعلوماتية وما يصاحب الحصول عليه من خطوات معقدة، واتساع مسرح هذه الجريمة الذي يتخطى غالبا حدود الدولة الواحدة، وعدم ملائمة القوانين والأنظمة أحيانا لبعض القضايا المطروحة في هذا المجال، ونظرا لما قد يثيره قبول الدليل الرقمي من مشكلات في الإثبات كدليل جنائي، ذلك أن مستودع هذه الأدلة هو الوسائل الإلكترونية التي يمكن التلاعب فيها وتغييرها عن الحقيقة التي يجب أن تعبرعنها. وعليه من خلال هذه الدراسة نسعى للإجابة عن التساؤل الرئيسي التالي: ما مدى حجّية الدليل الرقمي في مجال الإثبات الجنائي الإلكتروني؟

وتتفرع عن هذه الإشكالية عدة تساؤلات تتمثل فيما يلي:

1ــ كيف يمكن استخراج الدليل الرقمي بوصفه دليل إثبات أمام القضاء؟

2ــ هل تكفي القواعد الإجرائية المقررة لإثبات الجرائم التقليدية لكي تسري على الجرائم المعلوماتية؟

3ــ ما الدليل الرقمي ومراحله في الإثبات الجنائي؟

4ــ ما هي المشكلات التي تعيق سريان قواعد القانون الجنائي من حيث المكان في الجرائم المعلوماتية، وما هي شروط وأساس قبول الدليل الرقمي كدليل إثبات جنائي؟

الصعوبات التي يطرحها موضوع البحث

لا يفوتنا القول أنه تلقينا صعوبات جمة في اختيار موضوع البحث في حد ذاته، كون أن هذا الموضوع –الإثبات الجنائي في الجرائم المعلوماتية– حديث لم يسبق بحثه بوضوح وتعمق ولو أن هناك مراجع ومقالات تناولت هذا الموضوع، إلا أنها لم تعالجه من كل جوانبه أو أدرجته بشكل سطحي، إضافة إلى أن الجرائم محل الدراسة ترتبط بالحاسب الآلي مما يتطلب الإلمام بمكوناته وبنظام المعالجة الآلية للمعلومات والشبكات الإلكترونية، وكما يحتاج الأمر إلى دراية باللغة والمصطلحات التقنية والفنية، وهذا ما يتطلب جهد كبير ناهيك عن الجهد القانوني.

منهج البحث

سيتم إتباع في منهجية الدراسة الأسلوب العلمي المنهجي القائم على المنهج الوصفي التحليلي، الذي يقوم على وصف هذه الظاهرة وتحليل المواد التي تناولتها، ذلك لأن الدراسة تهتم بسبل كشف وضبط أدلة الإثبات الجنائية في الجرائم المعلوماتية من الناحية الفنية والقانونية، وعلى وجه التحديد بالدليل الرقمي من خلال تعريفه وتبيان تقسيماته وخصائصه وأنواعه وأمثلة عنه، مع توضيح محل الدليل الرقمي وتعداد مراحله ومدى قبوله أمام القضاء الجزائي.

خطة البحث

حتى نتمكن من معالجة الإشكالية المطروحة ارتأينا إلى تقسيم الخطة إلى فصلين، معتمدين في ذلك على التقسيم الثنائي للخطة. ففي الفصل الأول سنتناول فيه طرق الحصول على أدلة الإثبات الجنائي في الجرائم المعلوماتية والذي أدرجناه في مبحثين، وسندرس في المبحث الأول المعاينة والتفتيش في الجرائم المعلوماتية، وسنناقش في المبحث الثاني الضبط والخبرة القضائية في الجرائم المعلوماتية، أما الفصل الثاني قمنا بتوزيعه أيضا على مبحثين، ففي المبحث الأول تطرقنا إلى ماهية الدليل الرقمي كدليل إثبات في المواد الجنائية، وأما المبحث الثاني فقد تناولنا فيه مدى قبول الدليل الرقمي أمام القضاء الجزائي.

الفصـــــــل الأول

طرق الحصول على أدلة الإثبات الجنائي في الجرائم المعلوماتية

تعد الجريمة المعلوماتية كغيرها من الجرائم لها أركانها وعناصرها، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى في الجرائم التقليدية[1].

وتهدف إجراءات التحقيق في هذه الجرائم إلى جمع وفحص الأدلة الإلكترونية القائمة على وقوع الجريمة ونسبتها إلى فاعلها، ومن أهم هذه الإجراءات كما بينها القانون هي المعاينة، التفتيش، الخبرة القضائية، الضبط، سماع الشهود، مراقبة المحادثات وتسجيلها، الاستجواب، المواجهة والاعتراف، إلاَ أن بعض هذه الإجراءات لها دور ضئيل في بيئة تكنولوجيا المعلومات، فالشهادة مثلا تقريبا لا يمكن تصور ورودها على السلوك المكون للجريمة المعلوماتية، كون هذه الأخيرة تقتضي التلاعب في البيانات والبرامج فهي غير قابلة من حيث المبدأ لأن تشاهد من جانب الغير حتى يمكن أن يشهد به أمام القضاء شهادة مباشرة، وكما أن الاعتراف الذي يتم عن طريق الاستجواب أو السؤال أو طواعية لا يعد قضائيا كافيا ما لم يدعم بأدلة أخرى غيرها، وبالتالي سوف نقتصر الذكر على ما يصلح منها كأدلة إثبات في الجرائم المعلوماتية .

وهذا ما سوف نتناوله من خلال مبحثين على النحو التالي: المعاينة والتفتيش في الجرائم المعلوماتية(المبحث الأول)، الضبط والخبرة القضائية في الجرائم المعلوماتية(المبحث الثاني).

---

[1] تختلف الجريمة المعلوماتية عن التقليدية في أمور عدة، منها حداثتها وظهورها بظهور التكنولوجيا الرقمية واعتمادها على كيانات معنوية –موجات كهرومغناطيسية– في اقترافها، كما يتميز المجرم المعلوماتي عن التقليدي في كونه يتمتع بالذكاء واعتماده على الجانب الفكري في اقتراف الجريمة، خلافا للمجرم التقليدي الذي يعتمد في ارتكاب أغلب جرائمه على القوة العضلية، إضافة إلى الإلمام بالجوانب التقنية والفنية، وأكثر من ذلك التخصص في بعض الجرائم الهامة التي لا يقترفها إلا فنيون ومتخصصون في مجال علوم الحاسوب والشبكات والبرامج، لذلك نجد لدى المجرم المعلوماتي قدرة على إخفاء جريمته والتلاعب بالأدلة، لذا يجب على السلطات القضائية أن تتعامل مع هذه الجرائم بما يتناسب معها من أدلة إلكترونية، راجع فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جـــامعة الجزائـــر (1)، 2010– 2011 ، ص. 373.

المبحـــــث الأول

المعاينة والتفتيش في الجرائم المعلوماتية

إن التعامل في الجريمة المعلوماتية تتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والتفتيش من بين الإجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، عن طريق التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وكل هذا سواء تعلق بالمجرم المعلوماتي أو التقليدي (العادي) ما دام أن إجراءات الحصول على الدليل نفسها, وسوف نتعرض في هذا المبحث للمعاينة في الجرائم المعلوماتية في المطلب الأول وكذا التفتيش في الجرائم المعلوماتية في المطلب الثاني.

المطلب الأول

المعاينة في الجرائم المعلوماتية

تعتبر المعاينة من أهم إجراءات التحقيق والتي يمكن من خلالها الحصول على الدليل الجنائي بحيث يجوز للنيابة العامة أن تقوم به في غيبة المتهم إذا لم يتيسر له حضوره، وباعتبار أن المعاينة لها أهمية قصوى فسوف نتناولها من عدة جوانب كالتالي: الإطار القانوني للمعاينة في الجرائم المعلوماتية(الفرع الأول)، معاينة مسرح الجرائم المعلوماتية(الفرع الثاني).

الفرع الأول

الإطار القانوني للمعاينة في الجرائم المعلوماتية

ينبغي عند التطرق للإطار القانوني للمعاينة الوقوف عند التعريف بها، وتبيان أهميتها وطبيعتها، والسلطة المختصة بإجرائها وكيفية الانتقال، وشروط معاينة مسرح الجرائم المعلوماتية والذي سنورده كالتالي:

أولا – تعريف المعاينة وطبيعتها وأهميتها في مجال الجرائم المعلوماتية:

1– تعريف المعاينة:

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيه الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة وعن مرتكبها، وبالتالي يجب على السلطات المختصة

بإجراء المعاينة الانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة كل أو بعض الآثار المادية للجريمة التي تساعد في التنقيب عن الحقيقة، وحتى لا يقع الشك في الدليل المستنبط منه وهذا ما تضمنته نص المادة**(42)** من قانون الإجراءات الجزائية الجزائري[1].

2- طبيعة المعاينة وأهميتها في الجرائم المعلوماتية:

قد تكون المعاينة إجراء تحقيق أو استدلال، يستهدف إلى إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة، بحيث لا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأشخاص، فإذا تم إجراء المعاينة في مكان عام كانت إجراء استدلال، أما إذا اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق[2].

وتظهر أهمية المعاينة في كونها تقوم بإحاطة صورة شاملة لموقع الجريمة لجهة التحقيق والمحاكمة، وبكل ما يحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به، وهذا حتى يتسنى لضباط الشرطة القضائية والقضاة وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها[3].

وباعتبار المعاينة من أهم إجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من الناحية القانونية أو العملية، فمن الناحية القانونية تبدو أهميتها من عدَة اتجاهات منها تأكيد وقوع الجريمة أو

---

(1) عمرو حسين عباس، "بحث في أدلة الإثبات الجنائي والجرائم الإلكترونية" (المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من 26 – 27/ 04 /2008، مقر جامعة الدول العربية، ص. 16، أنظر الموقع الإلكتروني:

www.arabip.center.com/public/events/papers/paper 2-4. pdf.

وأنظر المادة 42 من قانون رقم 66-155، المتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06-22، المؤرخ في20/ 12/ 2006، ج.ر.ع.84 مؤرخة في 24/ 12/2006.

(2) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط. 1 ، دار الفكر الجامعي الإسكندرية، 2009، ص. 150.

(3) عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، د.ط. ، دار الكتب القانونية، مصر، 2007، ص. 180.

نفيها، صدق أقوال الواقعة، ركن الخطأ أو العمد فيها، تحديد الوصف القانوني لها، كما تساعد القاضي في تكوين قناعته؛ أماَ من الناحية العملية فهي تساعد المحقق على تحديد وقت ارتكاب الواقعة الإجرامية، ومعرفة علاقة الجاني بالمجني عليه، وتحديد الأسلوب الإجرامي الذي استعان به الجاني.

والمعاينة في مجال كشف غموض الجريمة المعلوماتية لا تتمتع بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية[1]، ومرد ذلك أن هناك تقريبا مسرحا للجريمة التقليدية، والتي يتمكن من خلالها الباحث والمحقق الجنائي التنقيب عن الواقعة عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة والتحفظ عن الأشياء التي لها علاقة بالواقعة الإجرامية، بينما لا توجد عادة مسرح للجريمة المعلوماتية باعتبار مكان الإغارة هو العالم الافتراضي أو عالم الفضاء الإلكتروني Cyber Space ، والذي يكون عادة الموقع أو المكتب الذي توجد فيه مكونات الحاسب الآلي المادية والمعنوية، والتي تكون محلا للجريمة أو أدلتها وهي تتمثل في الأجهزة والأنظمة والبرامج[2]، إذا فالانتقال للمعاينة في الجريمة المعلوماتية لا يكون إلى العالم المادي بل إلى العالم الافتراضي[3].

وتقل فرص الإفصاح والكشف عن الحقيقة المراد التوصل إليها من وراء معاينة الجريمة المعلوماتية لأسباب عدة منها:

– إن الجرائم التي تقع على نظم المعلوماتية والشبكات أو بواسطتها قلَما ينجم عن ارتكابها آثار مادية.

– إن عدد كبير من الأفراد يكونوا قد ترددوا على مسرح الجريمة خلال الفترة التي تتوسط عادة بين ارتكاب الجريمة واكتشافها، وهذا ما يفتح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو محو بعضها وهو ما يثير الشك على الدليل المستنبط من المعاينة[4].

– استطاعة الجاني من التلاعب في البيانات عن بعد أو محوها عن طريق قيام الجاني بالتدخل من خلال وحدة طرفية.

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 153.

[2] نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، د.ط.، دار الفكر الجامعي، الإسكندرية، 2007، ص. 217.

[3] جاسم خريبط خلف، "الضبط القضائي في جرائم الانترنت"، مجلة جامعة ذي قار، مجلة 4، ع.4، البصرة، 2009، ص.75.

[4] عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط. 2، دار النهضة العربية، القاهرة، 2001، ص. 365، 366.

[5] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 154.

3- السلطة المختصة بإجراء المعاينة لمسرح الجرائم المعلوماتية:

الأصل أن انتقال المحقق الجنائي لإجراء المعاينة أو لمباشرة أيَ إجراء آخر من إجراءات التحقيق أمر متروك للسلطة التقديرية له، فلا يقوم به إلاَ إذا كانت مصلحة من ورائه، لذلك جرى أن المعاينة هي من إجراءات التحقيق التي يترك أمر تقدير لزوم القيام بها إلى السلطة التي تباشر التحقيق[1]، وهذا ما قضت به نص المواد **(42،80،79)** من قانون الإجراءات الجزائية الجزائري على أن المعاينة تجرى إما من طرف قاضي التحقيق، وذلك بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته، وكما يمكن تمديد اختصاص قاضي التحقيق إذا استدعت ضرورة الحالة إلى دوائر اختصاص محاكم مجاورة، كما يتم أيضا إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر وقوع الجريمة إلى علمهم وانتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية .

ثانيا- كيفية الانتقال إلى العالم الافتراضي لمعاينة الجرائم المعلوماتية:

يتم إجراء معاينة الجريمة المعلوماتية المرتكبة عبر الانترنت كأيّ جريمة أخرى، عن طريق الانتقال إلى مكان الجريمة، غير أن الانتقال لا يكون إلى العالم المادي وإنما إلى الفضاء الإلكتروني، بالتالي يتم الانتقال إلى العالم الافتراضي لمعاينة الجريمة إمّا من قبل قاضي التحقيق أو ضابط الشرطة القضائية كالتالي:

- من مكتبه بالمحكمة من خلال جهاز الحاسوب الخاص به.
- اللجوء إلى مقهى الإنترنيت. Internet Café
- اللجوء إلى مكان عمل مزود خدمة الانترنيت[2].Internet Server provider

- كما يجوز له الانتقال من خلال مقر مكتب الخبير التقني المختص إذا سمح له القانون بذلك، وهذا ما نجده في مصر من خلال إدارة مكافحة جرائم المعلوماتية التابعة لوزارة الداخلية.

ومن هنا يستوجب على سلطة التحقيق الانتقال إلى العالم الافتراضي بالسرعة الكافية من أجل منع زوال ومحو آثار الجريمة[3].

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص .102.

[2] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس، 2004 ص. 895.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 156-157.

ثالثا: شروط صحة معاينة مسرح الجرائم المعلوماتية.

حتى تحقق المعاينة الغرض المرجو منها في كشف غموض الحادث ومعرفة الفاعل يجب التقييد بعدة شروط كالتالي:

1- سرعة الانتقال إلى مكان وقوع الجريمة المعلوماتية، على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها إلى مكان الواقعة[1].

2-السيطرة والتحكم على مكان وقوع الجريمة المعلوماتية، عند وصول سلطة التحقيق لمكان الحادث لمعاينته وجب أن تقوم بالسيطرة عليه وذلك:

- بمنع أي شخص من مبارحة مكان الواقعة ريثما تنتهي الضبطية القضائية من تحرياتها[2].
- منع تواجد أي شخص بداخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة سواء بقصد أو بخطأ.
- حماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص.
- قيام الخبراء كل حسب اختصاصه برفع الآثار بمسرح الجريمة.

3-الترتيب في المعاينة، ولضمان إجراء معاينة بصورة مرتبة ومتسلسلة ينبغي على السلطة المختصة الالتزام بالطرق التالية:

- تحديد نقاط البدء في المعاينة.
- عدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تماما[3].

4-الدقة والعناية الفائقة في معاينة مسرح الجرائم المعلوماتية، وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات فيما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح الضوئي (السكانير) والطابعة والأسطوانات المدمجة، وغير ذلك من الوسائل المستخدمة في اقتراف الجريمة المعلوماتية.

5-التحفظ على مسرح الجرائم المعلوماتية بعد المعاينة، لأن الهدف من الحفاظ على آثار الجريمة بعد انتهاء من المعاينة هو من أجل إمكانية العودة إليه كلّما أراد المحقق أو القاضي كشف غموض أو

---

[1] راجع المادة 42 من ق.إ.ج.ج.

[2] المادة 50 من ق.إ.ج.ج.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.158-160.

التأكد من آثار معينة.

6- تدوين المعاينة، ويكون ذلك كتابيا ورسميا وتصويريا.

الفرع الثاني

معاينة مسرح الجرائم المعلوماتية

يتولى قاضي التحقيق معاينة الآثار التي خلفها مستخدم شبكة الانترنت والتي تتمثل في الرسائل المرسلة منه أو التي يستقبلها وكل الاتصالات التي قام بها من خلال الكمبيوتر والشبكة العالمية، وكما أن الآثار الرقمية المستمدة من أجهزة الكمبيوتر قد تكون ثرية فيما تحتويه من معلومات مثل صفحات المواقع المختلفة Web pages، والبريد الإلكترونيE mail،الملفات المخزنة في الكمبيوتر الشخصي files stared...الخ.

إن معظم التشريعات الجنائية الحديثة لم تهتم بتعريف مسرح الجريمة ولم تقم بتحديد النطاق المكاني له كما هو الحال بالنسبة للتفتيش، وبالتالي فإن معظم التشريعات تعبر عنه بمحل الواقعة[1].

ولا توجد صعوبة مادية لتقرير صلاحية مسرح الجريمة المعلوماتية الذي يضم المكونات المادية، كأشرطة الحاسب، مفاتيح التشغيل، والأقراص وغيرها لمعاينتها من طرف ضابط الشرطة القضائية، وكذا وضع الأختام في الأماكن التي تمت معاينتها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها مع إخطار وكيل الجمهورية بذلك[2]، وقد رأى البعض بأنه لا يوجد مـــانع من وضع نص يمكن من خلاله السماح لضابط الشرطة القضائية بالانتقال عبر العالم الافتراضي خارج نطاق اختصاصه المكاني[3]، وهذا ما أخذ به المشرع الجزائري من خلال نص المادة **(05)** من القانون رقم **(09-04)** لسنة **2009** المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تضمنت تخويل السلطات لضباط الشرطة القضائية الحق بالتفتيش في النظم المعلوماتية ولو عن بعد وفقا لشروط المحددة في قانون الإجراءات الجزائية، وبالتالي فالتفتيش عن بعد لا يمكن أن يطرأ دون الانتقال إلى العالم الافتراضي[4].

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.161ـــ165.

[2] عبد الفتاح بيومي حجازي ، مرجع سابق، ص. 182.

[3] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 832.

[4] راجع المادة 05 من قانون رقم(09ـــ04) المؤرخ في 5/ 8/ 2009، يتضمن قانون الوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها،ج.ر.، الصادرة في 16/ 08/ 2009، ع. 47.

أولا- الخطوات الواجب مراعاتها قبل الانتقال إلى مسرح الجرائم المعلوماتية:

يجب على المحقق الجنائي أو ضابط الشرطة القضائية قبل الانتقال لإجراء المعاينة الالتزام بالخطوات التالية:

1-الحصول على معلومات مسبقة عن مسرح الجريمة من مالك المكان، ونوع وعدد أجهزة الكمبيوتر المتوقع مداهمتها وشبكاتها.

2-توفير الوسائل الضرورية للاستعانة بها في الفحص والتشغيل كالأجهزة والبرامج.

3-قطع التيار الكهربائي في المكان الذي تجرى فيه المعاينة لمنع الجاني من القيام بأي فعل يؤدي إلى تغيير أو محو آثار الجريمة.

4- إعداد فريق التفتيش من مختصين وفنيين[1].

ثانيا- قواعد معاينة مسرح الجريمة المعلوماتية:

1-القواعد الفنية لمعاينة مسرح الجريمة المعلوماتية:

باعتبار أن لمعاينة مسرح الجريمة المعلوماتية فائدة في كشف الحقيقة عنها وعن مرتكبها، فإن عند مباشرتها لابد من مراعاة قواعد وإرشادات فنية أهمها ما يلي:

- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسب وملحقاته، مع مراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة[2].

- عدم نقل أيّة مادة معلوماتية من محل الجريمة قبل إجراء الاختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أيّة مجالات لقوى مغناطيسية (ممرات مغناطيسية) يمكن أن تتسبب في محو البيانات المسجلة.

- القيام بحفظ المستندات الخاصة بالإدخال والمخرجات الورقية للحاسب التي لها صلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

- المحافظة على محتويات سلة المهملات وعدم تضييعها، مثل أوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة...الخ، وفحصها ورفع البصمات التي قد تكون على الأجزاء التي لها

---

[1] نبيلة هبه هروال، مرجع سابق،ص. 219.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكتروني، مرجع سابق، ص. 172

صلة بالجريمة المرتكبة[1].

-وضع مخطط تفصيلي للمنشأ الذي وقعت به الجريمة، مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم[2].

2- الإجراءات الأمنية الواجب مراعاتها في مسرح الجرائم المعلوماتية:

عند وصول الفريق إلى مسرح الجريمة يقوم بالتأمين والسيطرة على المكان والبدأ بالتفتيش على النحو التالي:

- السيطرة على أماكن المحيطة بمسرح الجريمة عن طريق إغلاق الطرق والمداخل، وكذا رصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال، والتحفظ على جميع الأشخاص الموجودين فيها.

-وضع حراس على كل جهاز حتى لا يتمكن أحد المتهمين من تغيير أو إتلاف المعلومات.

-تحديد أجهزة الحاسب الآلي الموجودة في مسرح الجريمة و تحديد مواقعها[3].

3- القواعد التحريزية الواجب إتخاذها من مسرح الجرائم:

وتتمثل هذه القواعد فيما يلي:

- ضبط وتحريز الدعائم الأصلية للمعطيات التي لها دلالة عند عرضها للمحكمة وعدم الاكتفاء بضبط النسخ، وكذا عدم الضغط على القرص بوضع أشياء ثقيلة عليه .

-توفير الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية وعدم وضعها في أماكن متربة أو مغبرة، لأن ذلك يؤثر على السطح المغناطيسي مما يجعله غير قابل للقراءة أو الكتابة.

-حماية وتأمين البرامج المضبوطة قبل تشغيلها فنيا.

-وضع علامات مادية خاصة تميز كل دليل إلكتروني عن غيره[4].

---

[1] أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة، 2007،ص. 246، 247.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 173.

[3] عبد الله حسين على محمود ، مرجع سابق، ص.367،368.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 177.

المطلب الثاني

التفتيش في الجرائم المعلوماتية

باعتبار أن التفتيش من أخطر الحقوق التي منحت للمحقق لكونه يمس بالحريات التي تكفلها وتصونها الدساتير عادة[1]، فإن التشريعات من بينها التشريع الجزائري قد وضع له عدة ضوابط سواء فيما يتعلق بالسلطة المختصة بمباشرته، أو التي تأذن بإجرائه، أو الأحوال التي تجوز فيها مباشرته وشروط اتخاذه، وكل هذا يمثل ضمانات الحرية الفردية أو حرمة المسكن. وهذا ما سوف نتطرق إليه من خلال فرعين: الإطار العام للتفتيش في الجرئم المعلوماتية (الفرع الأول) ، ضوابط تفتيش الجرئم المعلوماتية(الفرع الثاني).

الفرع الأول

الإطار العام للتفتيش في الجرائم المعلوماتية

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السّر، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن[2]، ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيدا لإظهار الحقيقة[3]، وسوف نتعرض في هذا المجال إلى التعريف بالتفتيش، خصائصه، ومدى قابلية جرائم الحاسوب والشبكات الإلكترونية للتفتيش عن أدلة الجريمة.

أولا- تعريف التفتيش:

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية، وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد إظهار الحقيقة وإسنادها إلى المتهم المنسوب إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويـــه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة

---

[1] من بين هذه الدساتير الدستور الجزائري، من خلال نص المادة 40 من قانون رقم(08-19)، المؤرخ في 15-11-2008، ج.ر.ع. 63، المؤرخة في 16-11-2008، والمتضمن الدستور الجزائري المعدل والمتمم، والتي تنص على ما يلي: "تضمن الدولة عدم انتهاك حرمة المسكن، فلا تفتيش إلا بمقتضى قانون..."

[2] خالد ممدوح إبراهيم، فن تحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص.180.

[3] المادة 81 من ق.إ.ج.ج.

والتي تشكل جناية أو جنحة [1] .

ثانيا- خصائص التفتيش:

يتميز التفتيش بناءا على التعريف السالف الذكر بعدة خصائص هي كالتالي:

1-أنه إجراء من إجراءات التحقيق:

يعتبر التفتيش من أوامر التحقيق الابتدائي والذي يدخل ضمن الاختصاصات العادية لقاضي التحقيق، وهذا ما قضت به نص المادة **(68-1)**، واستثناءا يجوز لضباط الشرطة القضائية القيام بهذا الإجراء بناءا على شروط وهذا ما بينته نص المادة **(17-1)**من خلال ما يلي: "يباشر ضباط الشرطة القضائية...، وإجراء التحقيقات الابتدائية"[2].

2- أنه يهدف إلى البحث عن أدلة مادية:

إن الهدف من التفتيش هو الوصول إلى الأدلة المادية للجريمة والتي تؤثر في اقتناع القاضي لأنه في الغالب ما يترك الجاني في مسرح الجريمة بعض الوسائل والأدوات التي يكون قد استخدمها في ارتكاب الجريمة، أو بصمات الأصبع إلى غير ذلك من الأدلة التي يستعين القاضي بها في الإثبات.

3- أن تكون الأدلة ناشئة عن جناية أو جنحة تحقق وقوعها:

باعتبار التفتيش عمل من أعمال التحقيق فلا يجوز إجراءه إلا إذا وقعت الجريمة بالفعل، وكانت مما يصفها القانون بجناية أو جنحة، بالتالي لا يجوز التفتيش في المخالفات نظرا لضآلتها، ولعدم خطورتها[3].

4- أن يقع التفتيش على محل يتمتع بحرمة المسكن أو الشخص:

يقع التفتيش على حرمة المسكن أو الشخص، ذلك أن قيام ضابط الشرطة القضائية بالبحث والتحري في الطرق العامة أو في الغابات...الخ، لا يعد تفتيشا لانتفاء حرمة المكان، وعليه فهو إجراء من إجراءات الاستدلال والذي يدخل في اختصاصاتهم العادية.

---

[1] علي محمود علي حموده، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، المؤتمر العالمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع1، دبي- الإمارات العربية المتحدة-26-28 نيسان 2003، ص. 24.

[2] راجع المادة 68-1، المادة 17-1 من ق.إ.ج.ج.

[3] هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، ط.1، دار النهضة العربية، القاهرة، 1997، ص.48،49.

5-أن يتم التفتيش وفقا للإجراءات القانونية المقررة:

يتم القيام بإجراء التفتيش وفقا للشروط القانونية، بحيث يجب مباشرته طبقا لإجراءات صحيحة فإذا شاب التفتيش الواقع على نظم الحاسوب عيب فإنه باطل[1]، لأن التفتيش الذي يقوم به المحقق بغير الشروط المنصوص عليها في القانون يعتبر باطل بطلان مطلق، وبالتالي لا يجوز التمسك بما ورد في محضر التفتيش وكما لا يجوز للمحكمة الاعتماد عليه في إصدار حكمها[2].

ثالثا- مدى قابلية جرائم الحاسوب والشبكات الإلكترونية لتفتيش عن أدلتها:

قد يرد محل التفتيش في البيئة المعلوماتية على المكونات المادية أو المعنوية للحاسب الآلي والتي نتعرض إليها فيما يلي:

1-مدى خضوع مكونات الحاسوب المادية والمعنوية للتفتيش عن أدلة الجريمة:

تشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته[3]، والتي تتمثل في شكل وحدات كوحدة الذاكرة، لوحة المفاتيح والشاشة ووحدة التحكم، وكل واحدة لها مهمة محددة، فهي لا تواجه صعوبات تعيق إجراءات التفتيش باعتبارها من المكونات المادية[4]، والتي يمكن إيجادها في مسكن المتهم أو مسكن غير المتهم[5]، والتي قد تتواجد أيضا في مكان عام، فهي بذلك تخضع للقواعد التي تحكم ذلك المكان، كما قد تتواجد هذه المكونات في حيازة شخص خارج مسكنه، فهي بذلك تخضع لقواعد تفتيش الأشخاص بوصف المكونات المادية للحاسوب أحد ملحقاته، وسواء كان الشخص الحائز المالك أو الغير، أما بالنسبة لمكونات الحاسوب المعنوية والمتمثلة في المعلومات والبيانات المعالجة آليا، فهي محل خلاف باعتبارها غير مادية[6].

---

[1] طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، د.ط. ، دار الجامعة الجديدة، الإسكندرية، د.س.ن.، ص. 371.

[2] علي حسن الطوالبه، "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة بحث منشور على شبكة الانترنت على موقع التالي:
www.policeme.gouv bh/reports/2011/April/13-14-2011/634383168746341670.pdf.

[3] موسى مسعود ارحومة، "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية"، المؤتمر المغاربي الأولى حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28،29- 09-2009، ص.7.

[4] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط. 1، دار الثقافة للنشر والتوزيع، 2011، ص. 158.

[5] راجع المادة 82 و83 من ق.إ.ج.ج.

[6] موسى مسعود ارحومة، مرجع سابق، ص. 7.

وقد نص المشرع الجزائري في المادة(**81**) من قانون الإجراءات الجزائية على عبارة – أشياء– فهذه العبارة يدخل في مضمونها الأشياء المادية والمعنوية[1] وهذا ما أدى ببعض الفقهاء الفرنسيين بالتفسير إلى أن برامج الحاسب الآلي ذات كيان مادي يشمل على نبضات وذبذبات إلكترونية ممغنطة قابلة للتخزين داخل الجهاز أو على الأقراص الصلبة، كما يجب الأخذ بعين الاعتبار القيـــمة التي يتمتع بها شيء محل الحماية الجنائية والتي قد تكون غالبا مصلحة اقتصادية يصل إليها صاحبها لذلك فالأشياء المعنوية مثلها مثل الأشياء المادية[2]،إلا أنَ العائق يكمن في صعوبة إجراء التفتـــيش والتحري عن الأدلة الإلكترونية وذلك راجع إلى:

–نقص المعرفة والدراية في فن التعامل مع البرامج والبيانات المخزنة ألياً من قبل السلطات المختصة بالتفتيش .

–صعوبة تحديد أو تخصيص محل التفتيش والأشياء التي يهدف إلى ضبطها، نظرا لارتباطها بالجوانب التقنية والفنية التي تتطلب من المختصين بالتفتيش على العلم بكيفية التعامل مع الأرقام السرية والبرامج والسجلات المخزنة في الحاسب الآلي.

–وجود صعوبة في التحكم بالأجهزة التي يستهدف تفتيش النظام المعلوماتي فيها خاصة عند وجود جهازين في مكانين مختلفين.

ويمكن الحد من هذه العوائق من خلال تدريب وتعليم جهات الشرطة والتحقيق في جرائم المعلوماتية مع مواكبة كل مستجدات التطور الرقمي في مجال التفتيش، وذلك لن يتأتى إلا بوجود نصوص قانونية تنص على تفتيش المكونات المعنوية للحاسب الآلي[3] .

أما بالنسبة للمشرع الجزائري، فقد تناول قواعد تفتيش نظم المعلوماتية من خلال إجازته لسلطة التحقيق القيام بإجراءات التفتيش في منظومة معلوماتية[4].

2– مدى خضوع شبكات الحاسب الآلي للتفتيش:

قد يكون حاسب المتهم متصل بغيره من الحواسيب عبر الشبكة الإلكترونية، وهنـــا يجب التمييز بين ما إذا كان حاسوب المتهم متصلا بآخر داخل إقليم الدولة، أو كان متصلا بحاسوب يقع في نطاق

---

[1] نصت المادة 81 من ق.إ.ج.ج.على أنه "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء..."

[2] علي محمود علي حموده، مرجع سابق، ص. 25.

[3] فايز محمد راجح غلاب، مرجع سابق، ص .311.

[4] راجع المادة 03 من قانون رقم (09–04) المؤرخ في 05–08–2009.

إقليم دولة أخرى.

أ- حالة وجود جهاز متصل بجهاز المتهم داخل الدولة:

تكمن المسألة في هذه الحالة في تجاوز الاختصاص المكاني للسلطة المختصة بالتفتيش، كما أنه يعتبر بمثابة العدوان على حقوق الأفراد وحرياتهم، ذلك عند قيام سلطة التحقيق بتفتيش جهاز له علاقة بجهاز المتهم داخل الدولة.

وقد أجازت بعض التشريعات للأشخاص القائمين على التفتيش امتداد هذا الأخير على سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان أخر، حيث أنه يمكن امتداد الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع أخر حينما يهدف ذلك إلى إظهار الحقيقة دون وجوب صدور إذن مسبق من قاضي التحقيق وذلك بشرطين هما:

- أن تكون النهاية الطرفية المتصلة بالحاسب الآلي موجودة داخل الدولة المعنية.

-أن تتضمن النهاية الطرفية المتصلة بالحاسب الآلي بيانات مخزنة تستهدف إظهار الحقيقة[1].

وبخصوص القانون الجزائري فقد تضمن في التعديل الجديد لقانون الإجراءات الجزائية نصوص قانونية إجرائية فيما يخص بتوسيع بعض الصلاحيات في مجال التفتيش، ذلك في بعض أنواع من الجرائم من بينها الجريمة المعلوماتية، حيث يجوز لقاضي التحقيق أن يأمر ضابط الشرطة القضائية للقيام بالتفتيش أو حجز ليلا أو نهارا في أي مكان على امتداد التراب الوطني [2].

ب-حالة وجود جهاز متصل بجهاز المتهم خارج الدولة:

تعد هذه المسألة من المشكلات التي تواجه إجراء التحقيق وبالخصوص مسألة التفتيش، ذلك لما توصلت إليه الدول من خلال برمجيات يمكنها القيام بإجراء التفتيش والذي لا يستند إلى مبرر قانوني من جهة، وباعتباره اعتداء على خصوصيات الأفراد وأجهزة حواسبهم من جهة أخرى[3].

غير أن مشكلة تفتيش مكونات الحاسب الآلي خارج الإقليم الوطني الجزائري قد حلَت، وذلك بموجب القانون رقم(**09-04**) لسنة2009 من خلال تعاون السلطات الأجنبية وفقا لمبدأ المعاملة بالمثل

---

(1) فايز محمد راجع غلاب، مرجع سابق، ص. 312، 313.

(2) راجع المادة 47 من ق.إ.ج.ج.

(3) عمر محمد أبو بكر بن يونس، مرجع سابق، ص.315،316.

في إطار اتفاقيات دولية في هذا الصدد[1] .

وتتصل هذه المسألة مباشرة بالبعد الدولي فلا يمكن الحديث عن القضاء عليها إلاَ في ظل تعزيز وتبادل التعاون الدولي في إطار اتفاقيات دولية أو إقليمية أو ثنائية[2] مع تفعيل آليات المساعدة الدولية في مجال القضائي وتسليم المجرمين، وذلك باحترام مبدأ المساواة بما يفضي أنه لا مجال للدول المتقدمة في مجال المعلوماتية الرقمية أن تتحكم في أنظمة الغير والتجسس عليها بحجة ما يقتضيه إجراء التحقيق من تمديد التفتيش عن بعد بين الدول[3].

الفرع الثاني

شروط تفتيش الجرائم المعلوماتية

يعتبر التفتيش انتهاك على الحق في الخصوصية الفردية، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية، لذا عمدت الدول على إحاطته بالضمانات القانونية حتى لا يتم إساءة استخدامه وسوف نتناول في هذا الإطار ما يلي:

أولا- الشروط الموضوعية لتفتيش الجرائم المعلوماتية:

يشترط أن يتوافر في التفتيش سببا له، وأن يكون محله الحاسوب بكل مكوناته المادية والمنطقية والشبكة الإلكترونية، بالإضافة إلى وجود سلطة مختصة للقيام به، وعلى ضوء ما سبق فإن القواعد الموضوعية لتفتيش نظم المعلوماتية تتمثل فيما يلي:

1- أسباب تفتيش النظم المعلوماتية:

ترتب على إجراء التفتيش خلاف فقهي حول مدى مشروعية التفتيش في الجرائم المعلوماتية بين الذين يرون قابلية النصوص التقليدية لتطبيق هذا الإجراء في الجرائم المعلوماتية، مع الذين يتجهون إلى وجوب استحداث نصوص تشريعية جديدة تجرّم الأفعال، وأثناء غياب تشريعات جديدة فلا مجال للحديث عن سبب تفتيش الحاسب الآلي، غير أن هذه المشكلة لا يمكن أن تثير سبب التفتيش في الجرائم المعلوماتية في الدَول التي تضمنت نصوص قانونية للتجريم والعقاب على مثل هــذه الجرائــم

---

[1] راجع الفقرة 3 من المادة 5 القانون رقم (09-04) المؤرخ في 05-08-2009.

[2] لقد حدث في ألمانيا جريمة غش بيانات الحاسب الآلي، أين اتضح عند جمع إجراءات التحقيق وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا مع شبكة اتصالات في سويسرا التي تم تخزين المشروعات فيها، وقد تمكنت سلطات التحقيق الألمانية من ضبط ملفات البيانات عن طريق التماس المساعدة المتبادلة بين الدولتين، راجع علي محمود علي حموده، مرجع سابق، ص. 26.

[3] فايز محمد راجح غلاب، مرجع سابق، ص. 315، 316.

إلاَ أن المشكلة تكمن في الدَول التي لم تجرم الأفعال غير المشروعة الناشئة عن أنظمة الحاسب الآلي أين قد يكون التفتيش فيها باطلا[1].

وبالتالي فقد تناول المشرع الجزائري سبب التفتيش في أكثر من نص منها المادة **(44)** من قانون الإجراءات الجزائية والتي نصت على ما يلي : "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلاَ بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش" [2].

وعليه لكي يعتبر التفتيش في مجال الجريمة المعلوماتية مشروعا، لابد من توافر شروط والتي نوردها فيما يلي:

– وجوب وقوع جريمة معلوماتية سواء كانت جناية أو جنحة، وبالتالي تستبعد المخالفات نظرا لقلة أهميتها باعتبارها لا تصل إلى درجة المساس بحريات الأشخاص أو انتهاك لحرمات منازلهم[3] .

–اتهام شخص أو أشخاص معينين بارتكاب الجريمة أو المشاركة فيها.

–توافر أمارات قوية أو قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره[4].

ولذلك فلا يجرى التفتيش إلاَ إذا توافرت لدى قاضي التحقيق أسباب كافية مقنعة، أي تواجد أدوات أو أشياء استعملت في ارتكاب الجريمة أو متحصلة منها، أو مستندات إلكترونية يحتمل أن يكون لها فائدة في التفتيش عن الحقيقة سواء لدى المتهم المعلوماتي أو غيره والتي تتواجد في المكان أو عند الشخص المراد تفتيشه[5] .

2– محل تفتيش النظم المعلوماتية:

لكي يكون التفتيش صحيحا يجب أن يرد على المحل الذي قد يكون الشخص أو المكان، وهذا

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص. 317– 319.

[2] المادة 44–1 من ق.إ.ج.ج.

[3] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص. 210، 211.

[4] هلالي عبد اللاه أحمد، مرجع سابق، ص. 115.

[5] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتي، د. ط.، دار الجـــامعة الجديدة، الإسكندرية، د.س.ن.،ص.405.

المحل يجب أن يكون محددا أو قابل لتحديد وجائزا قانونا [1]، وبالتالي فالشخص الذي يقوم بتفتيش نظم المعلوماتية، قد يكون من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، أو من مشغلي، أو مستخدمي الحاسب، أو مقدمي الخدمة، أو من مهندسي الصيانة والاتصالات، أو من مديري نظم المعلوماتية، أما الأشخاص الذين يقوم عليهم التفتيش هم أيّ أشخاص آخرين يكون بحوزتهم معدات أو أجهزة معلوماتية أو أجهزة حاسب آلي محمول أو تلفونات متصلة بجهاز المودم أو مستندات، وفي كل الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به [2] .

وبخصوص القانون الجزائري فهو لم يتضمن تفتيش الأشخاص كإجراء التحقيق باستثناء في بعض إجراءات التحقيق الجمركي، أين يمكن لأعوان الجمارك القيام بتفتيش الأشخاص في حالة إخفاء بضاعة مغشوشة وفقا لما نصت عليه المادة **(42)** من قانون الجمارك، وكذا نص المادة **(61)** من قانون الإجراءات الجزائية التي نصت بطريقة غير مباشرة على تفتيش الأشخاص في حالة التلبس بناء على القبض[3].

وبالنسبة لتفتيش المنازل وما في حكمها كمحل لتفتيش نظم المعلوماتية، فيقصد به محل الإقامة أو المأوى والملحقات المخصصة لمنافعها والتي يستخدمها الشخص سواء بصفة دائمة أو مؤقتة متى وجدت فيه مكونات الكمبيوتر المادية أو المعنوية أو شبكات اتصال خاصة[4] .

فقد تطرق المشرع الجزائري لتفتيش المنازل في نص المادتين**(82،83)** من قانون الإجراءات الجزائية، والتي تتضمن تفتيش منزل المتهم أو غير المتهم، فعلى قاضي التحقيق عند مباشرة التفتيش في هذه الحالة أن يلتزم بالشروط الواردة في المادتين **(45،47)** من نفس القانون واللتان تناولتا أحكما في مجال التفتيش، حيث يوجب على ضابط الشرطة القضائية أو قاضي التحقيق مراعات قواعد معينة وكما شملت المادتين على قواعد خاصة بكيفية التعامل مع الأوراق أو المستندات[5].

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العرابية للعلوم الأمنية، الرياض، 2007، ص. 19.

[2] هلالي عبد اللاه أحمد، مرجع سابق، ص. 126.

[3]. راجع المادة 42 من قانون رقم (98–10) المؤرخ في 22 غشت 1998، المتضمن قانون الجمارك المعـدل والمتمم، والمادة 61 من ق.إ.ج.ج.

[4] هلالي عبد اللاه أحمد، مرجع سابق، ص. 132.

[5] أنظر المادة 45، 47 من ق.إ.ج.ج.

3-السلطة المختصة بتفتيش النظم المعلوماتية:

الأصل أن تقوم بإجراء تفتيش نظم الحاسب الآلي سلطة التحقيق الأصلية المتمثلة في قاضي التحقيق والنيابة العامة، إلاَ أنه يجوز لضباط الشرطة القضائية أن يقوموا بهذا الإجراء بناء على تفويض صادر من السلطة المختصة، وهذا ما سنبينه تباعا.

أ-إجراء تفتيش النظم المعلوماتية بمعرفة سلطة التحقيق الأصلية:

إن المشرع الإجرائي المصري أناط الاختصاص بالتفتيش كإجراء تحقيق للنيابة العامة كسلطة أصلية ولقاضي التحقيق في حالات خاصة[1]، وهذا عكس ما قضى به المشرع الجزائري حيث جعل سلطة تحقيق الأصلية من اختصاص قاضي التحقيق[2] باعتباره مختص بإجراء كل التحقيقات بما فيها التفتيش، لكن في كل الحالات التي يقوم فيها بهذا الإجراء لابد من إخطار وكيل الجمهورية الذي له الحق في مرافقته[3]، واستثناءا يجوز لوكيل الجمهورية أن يقوم ببعض إجراءات التحقيق، لأن الاختصاص الأصيل بمباشرته يعود لقاضي التحقيق وحده دون سواه[4].

ولا يكفي توافر صفة قاضي التحقيق لكي يقوم بإجراء التفتيش، بل لابد أن يكون مختصا سواء من ناحية الاختصاص المكاني أو النوعي، فيتحدد اختصاص قاضي التحقيق محليا إماَ بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في ارتكابهم الجريمة أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان القبض قد حصل لسبب آخر.

كما يجوز تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في جرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية وغيرها.

بالإضافة إلى الاختصاص المكاني يجب أن يتوافر الاختصاص النوعي المتمثل في نوع الجريمة التي يختص بها المحقق بالتفتيش، وبالنسبة للقانون الجزائري نجد أن قاضي التحقيق يختص بإجـــراء

---

[1] هلالي عبد اللاه أحمد، مرجع سابق، ص. 133.

[2] يجب الإشارة إلى أن قاضي التحقيق لا يختص بالقضية إلاَ بناء على طلب من وكيل الجمهورية أو شكوى مصحوبة بإدعاء مدني، وذلك بعد أخذ بعين الاعتبار نص المواد 67 و73، وبعد دخول القضية في حوزته يكون مختصا وله أن يقوم بكل الإجراءات راجع نص المادة38-1 من ق.إ.ج.ج.

[3] راجع المواد 79، 82 من ق.إ.ج.ج.

[4] راجع المواد 56-1، 59-1، 117-1 من ق.إ.ج.ج.

التحقيقات بما فيها التفتيش في الجنايات والجنح المتلبس بها[1].

ويبدو أنه لمّا كانت سلطة التحقيق الأصلية غير مطالبة بالقيام بالتفتيش بنفسها في كل الحالات إذ قد لا يكون لها وقتا كافيا، خاصة إذا تعددت الأمكنة التي يتم تفتيشها أو الأشخاص المراد تفتيشهم، ففي هذه الحالة يجوز لقاضي التحقيق أن يندب أحد قضاة التحقيق أو أحد ضباط الشرطة القضائية[2]، وهذا ما سوف نراه .

ب- إجراء تفتيش النظم المعلوماتية بمعرفة ضباط الشرطة القضائية:

يتمتع قاضي التحقيق وحده بالاختصاص الأصيل لإجراء التحقيق، ونظرا لكثرة هذه الإجراءات وتنوعها أجاز له القانون أن يندب غيره- ضباط الشرطة القضائية- للقيام ببعضها وفقا لشروط يجب توافرها وتطبيقها بحذافيرها[3].

وبالتالي فإن ضابط الشرطة القضائية المنتدب الذي يختص في الجريمة التقليدية هو نفسه الذي يختص في الجريمة المعلوماتية، ويتحقق إجراء التفتيش نظم المعلوماتية بمعرفة ضابط الشرطة القضائية، في الحالات التالية[4] هي:

-التفتيش بناء على إذن قضائي بإجرائه:

باعتبار أن قاضي التحقيق غير ملزم في كل الحالات بمباشرة التفتيش، فإنه يجوز له أن يندب أحد ضباط الشرطة القضائية للقيام بهذا الإجراء و هذا ما يسمى بالإنابة القضائية، لذلك فلا يجوز لضباط الشرطة القضائية القيام بإجراء التفتيش إلا بعد حصوله على إذن من السلطة المختصة[5].

وقد حدد المشرع الجزائري الاختصاص المكاني لضباط الشرطة القضائية ويكون ذلك إما بمكان وقوع الجريمة، أو بمكان إقامة المتهم، أو بمكان القبض عليه، وكـما مدد اختصاصـهم في حـالة

---

(1) راجع المادة 40 من ق.إ.ج.ج.

(2) هلالي عبد اللاه أحمد، مرجع سابق، ص. 138.

(3) ومن شروط الواجب توافرها للقيام بالإنابة القضائية ما نصت عليه المواد 138، 139، 142، من ق،إ.ج.ج. التي تتضمن ما يلي:أن تصدر الإنابة من قاضي التحقيق المختص إقليميا، وأن تصدر إلى قاضي، أو ضابط الشرطة القضائية، وأن تنصب الإنابة على إجراء أو بعض إجراءات التحقيق الابتدائي، وعليه إذا كان التفويض عاما، كانت الإنابة باطلة، ويجب أن تكون الإنابة صريحة ومكتوبة، وغيرها من شروط التي يجب مراعاتها.

(4) طارق إبراهيم الدسوقي عطية، مرجع سابق، ص. 428.

(5) راجع المادة 44 من ق.إ.ج.ج. المادة 40 من الدستور الجزائري.

الاستعجال إلى كافة دائرة الاختصاص المجلس القضائي الملحقين به، ومدد أيضا بالنسبة لبعض الجرائم الخطيرة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني[1] .

-التفتيش بناء على حالة التلبس بالجريمة:

لا يختلف التفتيش في حالة التلبس في نظم الحاسب الآلي عن الجريمة التقليدية، لذلك يجوز لضابط الشرطة القضائية المنتدب في أحوال التلبس بالجنايات والجنح المعلوماتية تفتيش نظم الحاسب الآلي[2]، هذا ما تضمنته نص المادة **(44)** من قانون الإجراءات الجزائية الجزائري.

-التفتيش بناء على موافقة المتهم:

يجب أن تكون الموافقة من طرف صاحب الشأن بالتفتيش صريحة ومكتوبة بخط يده، فإذا كان لا يعرف الكتابة يذكر ذلك في المحضر ويذكر فيه هذه الموافقة؛ أمّا بخصوص جرائم الحاسب الآلي فإنه لا توجد نصوص قانونية مشابهة تخص تفتيش نظم المعلوماتية بناء على موافقة المتهم سواء في مصر أو في القانون المقارن، لذلك فإن هذا الفراغ يمكن تغطيته بالقواعد التقليدية[3].

ثانيا- الشروط الشكلية لتفتيش الجرائم المعلوماتية:

إلى جانب الضوابط الموضوعية لتفتيش نظم الحاسب الآلي، هناك ضوابط أخرى ذو طابع شكلي يجب مراعاتها والأخذ بها أثناء القيام بالتفتيش، والتي تتمثل فيما يلي:

1-الأشخاص المطلوب حضورهم أثناء التفتيش:

يشترط لقيام التفتيش كضمانة حضور صاحب المكان المراد تفتيشه، حيث اعتبر غالبية الفقه أن حضور المتهم للتفتيش من الأحكام الأساسية التي يجب الالتزام بها ويترتب على مخالفتها بطلان إجراء التفتيش[4].

2-أسلوب تنفيذ التفتيش:

قام القانون الأمريكي بتنظيم أسلوب تنفيذ التفتيش في نظم الحاسب الآلي، حيث يبدأ رجال الشرطة بالهجوم في الوقت نفسه وبشكل سريع على جميع منافذ المكان، باعتبار أن هذه الخطة تقلل من وقوع إصابات بين فرق رجال الشرطة، وبعد ذلك يقومون بسرعة فائقة باستبعاد الأشخاص

---

[1] راجع المادة 16 من ق.إ.ج.ج.

[2] طارق إبراهيم الدسوقي عطية، مرجع سابق، ص. 437.

[3] هلالي عبد اللاه أحمد، مرجع سابق، ص.162.

[4] فايز محمد راجح غلاب، مرجع سابق، ص. 334.

المشتبهين فيهم على الحواسب الموجودة في المكان حتى لا يتم تغيير أو حذف أو تدمير الأدلة التي تثبت إدانتهم، حيث يوضع المتشبه فيهم في غرفة مع حراسة أمنية، وتفتيشهم في نفس الوقت مع إعلامهم أن كل أقوالهم ستأخذ بعين الاعتبار ويمكن أن يكون دليل إدانتهم، حيث يوجد مكان في المنزل يعتبر النقطة الساخنة والتي يكون فيها جهاز حاسب آلي متصل بخط هاتفي أو أكثر من ذلك.

وفي هذه الحالة يتم وضع النقطة الساخنة في فريق يتكون من خبيران فنيان أجاز لهم القاضي بالتفتيش، فالأول يسمى بالمكتشف مهمته نزع مقبس الكهرباء الخاص بسائر الأجهزة، ويقوم بالبحث عن الأقراص والمستندات وغير ذلك، والثاني يسمى بالمسجل مهمته تصوير كامل الأجهزة والأدوات المتصلة بها على الحالة التي تم ضبطها، كما يقوم أيضا بتصوير جميع الغرف الأخرى المتواجدة في المكان كضمانة لعدم إدعاء أحد المشتبه فيهم بسرقة منزله وقت التفتيش، بالإضافة إلى أجهزة الفيديو والتسجيل الصوتي التي يتم من خلالها ترقيم الأشياء المضبوطة[1].

3-تحديد ميعاد التفتيش:

يعتبر ميعاد التفتيش أحد أهم الضمانات الشكلية، بحيث لا يجوز إجراؤه خارج الأوقات المحددة قانونا ما عدا في الأحوال الاستثنائية المقررة قانونا[2].

فلا يجوز البدء في التفتيش قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، إلا إذا طلب صاحب المنزل ذلك، أو وجهت نداءات من الداخل، أو في الحالات الاستثنائية التي أقرّها القانون[3]، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي يجوز إجراء التفتيش فيها في كل ساعة من ساعات الليل والنهار بناء على إذن مسبق من وكيل الجمهورية المختص، ذلك لأن المكونات المعنوية للحاسب الآلي وشبكة الاتصال قد تكون عرضة لإخفاء أو تغيير أو تدمير أو تلاعب بالبيانات المخزنة والتي تعتبر أدلة إلكترونية لإظهار الحقيقة، مما قد يؤدي بالجاني في ظرف ثواني إلى إفساد هذه الأدلة وعرقلة عمل التحقيق، لذلك استوجب هذا الأمر على التشريعات الحديثة إضـــافة الجريمة المعلوماتية كإستثناء عن أوقات التفتيش نظرا لطبيعة أدلتها الخاصة[4].

---

[1] عبد الله حسين على محمود، مرجع سابق، ص. 382.

[2] فايز محمد راجح غلاب، مرجع سابق، ص.328.

[3] راجع المادة 47 من ق.إ.ج.ج.

[4] فايز محمد راجح غلاب، مرجع سابق، ص. 329، 330.

المبحث الثاني

الضبط والخبرة القضائية في الجرائم المعلوماتية.

تلعب الضبط والخبرة دورا هاما في مجال الإثبات الجنائي للأدلة المعلوماتية خاصة في ظل تزايد تطور التكنولوجيا الرقمي، فبعد انتهاء المحقق الجنائي من إجراء التفتيش يقوم بضبط الأشياء التي يراها ضرورية، ومن ثم يأتي دور الخبير الذي يقوم بالتنقيب عن الحقيقة بناء على الأشياء المضبوطة، ثم يقدم الدليل المستنبط للقاضي الذي يمكن أن يبني حكمه بناء عليه، وهذا ما سوف نعالجه من خلال مطلبين، في المطلب الأول الضبط في الجرائم المعلوماتية، أما في المطلب الثاني الخبرة القضائية في الجرائم المعلوماتية .

المطلب الأول

الضبط في الجرائم المعلوماتية

باعتبار أن النتيجة المترتبة عن إجراء التفتيش هو الضبط ، ففي هذه الحالة يجب إتباع إجراءات ضبط الأشياء والأدلة الرقمية، وهذا ما سيتم توضيحه بتعريف الضبط وطبيعته ومحله في الفرع الأول، ومدى صلاحية ضبط الأدلة في جرائم المعلوماتية في الفرع الثاني.

الفرع الأول

تعريف الضبط وطبيعته ومحله

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريده من حيازته وقت ضبطه كان الضبط بمثابة إجراء تحقيق، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة، فيكون الضبط بمثابة إجراء استدلال[1] .

ومن حيث محل الضبط فإنه لا يرد إلاَ على الأشياء المادية، لأن الأشياء المعنوية لا تصلح لأن تكون محلا لوضع اليد عليها [2]، والشرط اللازم لصحة الضبط أن يكون الشـــيء مفيـــد في كشـــف

---

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، ط.1، دار الثقافة للنشـــر والـــتوزيع، عمان، الأردن، 2011،ص. 168.

[2] أحمد بلال، مرجع سابق، ص.264.

الحقيقة فكل ما يحقق هذا الهدف يصح ضبطه كما أن الضبط لا يرد إلاَ على الأشياء، أما الأشخاص فلا يصلحوا محلا للضبط، وإنما المصطلح الأصح هو القبض والقبض يختلف تماما عن ضبط الأشياء[1] .

الفرع الثاني

مدى صلاحية ضبط الأدلة في الجرائم المعلوماتية

ثمة صعوبة إلى اعتبار مكونات الحاسب الآلي من الأشياء التي يمكن ضبطها وبالخصوص ضبط الشبكة الإلكترونية والمكونات المعنوية للحاسب الآلي التي تشمل محتوى أنظمة المعالجة الآلية للمعطيات، وفيما يلي نلقي الضوء على مدى قابلية كل من المكونات المادية والمعنوية والرسائل ومراقبة الاتصالات الإلكترونية لأن تكون محلا للضبط .

أولا- ضبط المكونات المادية للحاسب الآلي:

إن ضبط المكونات المادية للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته الأساسية والثانوية لا تثير أيّة صعوبة، لأن الضبط يرد على أشياء مادية كالدعامة المادية للبرامج والأسطوانات والأشرطة[2]. ومن المكونات المادية التي تكون محلا للضبط ما يلي:

وحدة المعالجة المركزية، لوحة المفاتيح والشاشة والفأرة، والأقراص والأشرطة المغناطيسية التي يقوم البعض بتخزينها في البنوك أوفي مراكز التوثيق الحكومية الأمنية، ولوحة الدوائر الإلكترونية، وأجهزة الاتصال عبر شبكة الانترنت كأجهزة المودم[3].

حيث أنه تخضع للضبط وحدة الذاكرة الرئيسية سواء كانت لقراءة البيانات، أم كانت معدة للقراءة والكتابة معا، وضبط وحدة التحكم ووحدة المخرجات وما تشمله من وسائل، كالشاشة والطابعة، وضبط وحدات التخزين الفرعية التي تشمل على أقراص ممغنطة بنوعيها المرن FLoppy disk، والصلب Hard disk، والأشرطة المغناطيسية Magnetic tape وضبط وحدة المدخلات input unit بما تشمله من مفردات كلوحة المفاتيح Key board، ونظم الإدخال المرئي Machine vision system نظام القراءة الضوئي، نظام الفأرة Mouse system ونظام القراءة الضوئية للحروف

---

[1] عبد الله حسين على محمود، مرجع سابق، ص. 397.

[2] عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ط. 2، منشورات الحلبي الحقوقية، بيروت- لبنان، 2007، ص. 373.

[3] عبد الله حسين على محمود، مرجع سابق، ص. 398-399.

Optical character Reader system [1].

وفيما يتعلق بضبط مكونات الحاسوب المادية في القانون الجزائري فإنه لا يوجد أي مانع من تطبيقها، مثلها مثل غيرها من الماديات التي تفي النصوص التقليدية بمواجهتها موضوعيا وإجرائيا، ومن القواعد التي تتعلق بإجراء الضبط وتطبق على المكونات المادية للحاسوب هو أن الضبط يعتبر إجراء من إجراءات التحقيق، لذا فلا يجوز ضبط الأشياء إلاَ وفقا للقانون، وذلك بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة[2]، فيتوجب عند إحصاء الأشياء المضبوطة التي تفيد في كشف الحقيقة وضعها في أحراز مختومة، ولا يجوز فتحها إلاَ بحضور المتهم مصحوبا بدفاعه[3]، كما يتوجب كذلك عدم ضبط الأوراق والمستندات التي يسلمها المتهم لمحاميه أو للخبير الاستشاري لأداء مهامه.

وباعتبار أنه لا خلاف حول ضبط مكونات الحاسب الآلي المادية ومواجهتها إجرائيا بالنصوص التقليدية، فإنه توجد بعض التشريعات تضمنت صراحة النص على تفتيش المكونات المادية[4]، ومن هذه التشريعات قانون المنافسة الكندي والقانون الإنجليزي الصادر في عام 1990 والذي يطلق عليه قانون إساءة استخدام الحاسب[5] .

ثانيا–ضبط المكونات المعنوية للحاسب الآلي:

تكمن المشكلة في الأشياء المعنوية للحاسب الآلي التي تتضمن البرامج والبيانات، ويثور التساؤل إلى مدى صلاحيتها كمحل للضبط، حيث أن البعض من الفقهاء يتجه إلى اعتبارها لا تصلح كمحل للضبط، وهذا ما ذهب إليه الفقه الألماني واللوكسمبرجي، أما البعض الآخر من الفقهاء يرون إمكانية تطوير النصوص التقليدية للضبط على البرامج والبيانات المخزنة، لكون الغاية من التفتيش تتحقق بضبط الأدلة المادية التي تفيد في كشف الحقيقة، ومن هذا الاتجاه الفقه الكندي الذي يرى أن غرض الضبط لم يقتصر بضبط الأشياء المادية المحسوسة، بل تطور إلى أغراض أخرى منها

---

[1] هلالي عبد اللاه أحمد، مرجع سابق، ص.198،199.

[2] فايز محمد راجح غلاب، مرجع سابق، ص.342،343.

[3] راجع المادة 84 من ق.إ.ج.ج.

[4] فايز محمد راجح غلاب ، مرجع سابق، ص. 248.

[5] هلالي عبد اللاه أحمد، مرجع سابق، ص.199.

الحصول على المعلومات والبيانات وضبطها للوصول إلى الأدلة [1]، غير أن المسألة الصعبة تكمن في الخلاف حول مدى خضوع المكونات غير المادية للحاسوب للضبط وفقا للنصوص التقليدية وكذا في إجراءات ضبطها سواء تعلق الأمر ببرامج الحاسوب أو بياناته[2] .

1-برامج الحاسب الآلي:

إن الأمر يتعلق بكيفية ضبط الأدلة في حالة استخدام الوسائل الفنية في نسخ أو إتلاف البرنامج كالفيروسات مثل حصان طروادة، مع قلة خبرة وتدريب الضبطية القضائية وسلطة التحقيق في جمع الأدلة في مجال الفني والتقني وهذا من الناحية الأولى، ومن الناحية الثانية تتمثل في قيام عملية ضبط الوسائل التقنية بواسطة الأنظمة والشبكات المعلوماتية الكبيرة، حيث يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لفترة زمنية يمكن أن تطول أو تقصر والذي يسبب خسائر وأضرار بالجهة مستخدمة النظام، وكذلك ينتج عن ذلك عدم مبادرة مستخدمي النظام المعلوماتي استعدادهم للتعاون ومساعدة سلطة التحقيق لما يمثله الضبط لهم من الاعتداء على حقوق الآخرين[3].

2- بيانات الحاسب الآلي:

بالنسبة لضبط البيانات (Data) التي تعد دليلا على ارتكاب الجريمة، هناك صعوبات كثيرة منها عدم وجود دليل مرئي يمكن للضبطية القضائية فهمه عن طريق القراءة، كما تتميز الجرائم التي يكون محلها بيانات الحاسب بعدم وجود أثار مادية يمكن من خلالها الاستدلال على أدلة في ارتكاب الجريمة ويظهر ذلك بشكل واضح في جرائم الاختلاس والتزوير باستخدام الحاسب الآلي، كذلك فالبيانات التي يمكن التوصل إليها يستطيع الجاني تدميرها أو محوها في مدة قصيرة، وهو ما يلزم للمحقق من فصح البيانات مع ضخامتها، ناهيك عن نقص الخبرة الفنية لعملية الفحص وما تتطلبه من تحديد البيانات التي تصلح كأدلة إدانة من عدمه، والأمر يزداد تعقيدا في حالة الأنظمة المعلوماتية المتصلة بنهاية طرفية أخرى تتعدى حدود الدولة إلى إقليم دولة أخرى[4] .

وقد نظم المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون رقم(**09-04**) تحت تسمية "حجز المعطيات المعلوماتية"، حيث قضت المادة (**06**) من نفس القانون على نسخ

---

[1] عفيفي كامل عفيفي، مرجع سابق، ص. 378.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 344.

[3] عفيفي كامل عفيفي، مرجع سابق، ص.374.

[4] مرجع نفسه، ص. 375.

المعطيات محل البحث، وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية التي تكتشفها السلطات المختصة عند القيام بالتفتيش في المنظومة المعلوماتية، وتكون هذه المعطيات تفيد إظهار الحقيقة وقابلة للحجز، وتوضع في الأحراز مع وجوب قيام السلطة المختصة بحماية سلامة المعطيات المخزنة في المنظومة المعلوماتية، كما يجوز استخدام الوسائل التقنية وفقا لما يستهدفه التحقيق لتشكيل أو إعادة تشكيل هذه المعطيات بشرط عدم المساس بمحتوى المعطيات.

أما المادة(**07**) من نفس القانون نصت على أنه في حالة استحالة إجراء الحجز وفقا لما نصت عليه المادة (**06**) وذلك لأسباب فنية، فعلى السلطة المختصة بالتفتيش القيام بالتقنيات الواجبة للمنع من الوصول إلى محتوى المعطيات أو نسخها مع الاحتفاظ بها من طرف الأشخاص المصرح لهم بذلك كذلك نص المادة(**08**) تعلقت بالمعطيات التي يشكل محتواها جريمة، فعلى السلطة المباشرة بالتفتيش أن تصدر أمر بتكليف أي شخص مؤهل فنيا وتقنيا لاستخدام الوسائل التقنية المناسبة من أجل منع الإطلاع على محتوى هذه المعطيات؛ أمَا المادة(**09**) من نفس القانون، فيتضح من خلالها أن المعلومات المتحصل عليها عن طريق المراقبة وفقا لهذا القانون، لا يجوز استخدامها إلاَ في الحدود الضرورية التي يقتضيها التحري أو التحقيق القضائي، وذلك تحت طائلة العقوبات التي نص عليها التشريع المعمول به[1].

ومن خلال مضمون هذه النصوص، نجد أن المشرع الجزائري تنبه للقصور الموجود في مصطلح ضبط الكيانات المنطقية للحاسوب، حيث استخدم مصطلح حجز وليس ضبط باعتبار أن مصطلح حجز يتلاءم مع الأشياء غير المادية[2].

ثالثا–ضبط الرسائل ومراقبة الاتصالات الإلكترونية:

سهلت ثورة المعلومات الاتصال بين الأفراد التي انعكس أثرها على مختلف ميادين الحياة، ومن ناحية أخرى فقد سببت الكثير من أضرار شخصية عن طريق جرائم عدَة مستحدثة خصوصا انتهـــاك أسرار الأشخاص بواسطة الوسائل الإلكترونية، ونظرا لصلة المراسلات بالحياة الخاصة للأفـــراد[3]

---

[1] راجع المواد من 6– 9 من قانون (09–04) المؤرخ في 05–08–2009 يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] فايز محمد راجع غلاب، مرجع سابق، ص.350.

[3] علي محمود علي حموده، مرجع سابق، ص.32.

عمدت الدول على حماية هذه الأسرار الشخصية عن طريق إرساء نصوص دستورية تضمن عدم الاعتداء على خصوصية المراسلات[1]، ومن بينها الدستور الجزائري الذي تضمن منع الإطلاع على المراسلات سواء كانت بريدية أو برقية أو هاتفية وذلك في نص المادة **(39)** من الدستور الجزائري التي تنص على أنه:" سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"[2].

غير أن القوانين الإجرائية تجيز ضبط الرسائل ومراقبة المحادثات الهاتفية وفقا لقواعد وشروط معينة، من أجل المحافظة على حقوق المجتمع ونظام الأمن والآداب العامة، وبناء على ذلك فهل تمتد المراسلات العادية إلى سائر المراسلات الإلكترونية المستخدمة؟[3] وهذا ما سنبينه من خلال ضبط المراسلات الإلكترونية بالنسبة للبريد الإلكتروني، والتنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي فيما يلي:

1- البريد الإلكتروني:

يقصد بالبريد الإلكتروني استخدام شبكات الانترنت من أجل نقل الرسائل بدلا من الطرق التقليدية، وباعتبار أن استعماله سهل أضحى من أكثر وسائل الانترنت استعمالا في الوقت الحالي.

وأهم مسائل تتعلق بالبريد الإلكتروني هو وجوب المحافظة على سريته، وهو ما أدى إلى إصطناع برامج تشفير خاصة به، حيث لا يمكن الإطلاع على رسائل الأشخاص إلاَ لمن يعرف الشيفرة. ولقد ساعد ذلك على ظهور التوقيع الإلكتروني في تيسير عملية التراسل عبر البريد الإلكتروني[4] ، فالتوقيع الإلكتروني يقوم بعملية محددة ويمنح مصداقية للوثيقة أو المحرر الإلكتروني بحيث يمكن من خلال هذا إكساب الوثيقة مصداقية لدى الغير أو الطرف الآخر مستقبل هذا المحرر أو الوثيقة[5].

وبهذا الخصوص ثار خلاف حول طبيعة الرسائل الإلكترونية واختلافها على الرسائل الورقية حيث يعتبرها البعض عبارة عن موجات كهرومغناطيسية وذبذبات إلكترونية تختلف تماما على المستندات المادية الورقية، والبعض الآخر يعتبرها مستند تقليدي، فالمستند أصبح مفهومه الذي يتفق

---

[1] علي محمود علي حموده، مرجع سابق، ص.32.

[2] المادة 39 من قانون رقم 08-19 المؤرخ في 15 نوفمبر 2008، المتضمن الدستور الجزائري المعدل والمتمم.

[3] فايز محمد راجح غلاب، مرجع سابق، ص. 351.

[4] علي محمود علي حموده، مرجع سابق، ص. 33.

[5] مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الانترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الحاج لخضر، باتنة، 2011، ص.196.

مع ثورة الاتصالات عن بعد بأنه كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية أو كتابة إلكترونية.

وقد أسفر الخلاف الحاصل حول طبيعة الرسائل الإلكترونية ومفهوم المستند، إلى تضارب بعض الأحكام التي تجرّم فعل الإطلاع عليها من طرف الغير من عدمه وفقا لما تضمنته النصوص التقليدية[1] .

وبالرجوع إلى النصوص القانونية يلاحظ بأن القانون الجزائري استحدث مصطلحات تقنية جديدة في نصوص قانونية جديدة تتلاءم مع ضبط الرسائل الإلكترونية في العديد من الجرائم في حالة التلبس أو التحقيق الابتدائي، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذه النصوص خصت عن النصوص التقليدية بجوانب تقنية تجيز بمقتضاها لقاضي التحقيق أو ضابط الشرطة القضائية المناب له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور[2].

وهذا ما يتضح من خلال نص المادة(**65 مكرر$_5$**) من قانون الإجراءات الجزائية ، حيث قضت هذه المادة على أنه في حالة الضرورة لإجراء أساليب تحريات خاصة في بعض من الجرائم منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية، أو وضع ترتيبات تقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام من طرف شخص أو عدة أشخاص في أماكن خاصة أو عامة أو التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص، وتتم هذه العمليات المأذون بها تحت المراقبة المباشرة لوكيل الجمهورية المختص، أما في حالة فتح تحقيق قضائي تتم العمليات بناء على إذن من قاضي التحقيق وتحت رقابته المباشرة[3].

وكما نصت المادة (**03**) من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على ما يلي: "مع مراعاة القوانين التي تراعي سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص.352.

[2] المواد من 65 مكرر$_5$–65 مكرر 10 من الباب الثاني من الكتاب الأول في الفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" من القانون رقم (06–22) المؤرخ في 20 ديسمبر 2006، يتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[3] المادة 65 مكرر$_5$ من ق.إ.ج.ج.

المنصوص عليها في الإجراءات الجزائية في هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية "[1].

2- التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:

يقصد بمراقبة المحادثات الهاتفية وتسجيلها بأنها إجراء من إجراءات التحقيق، تباشرها السلطة المختصة للبحث عن أدلة إثبات الجريمة ضد شخص نسبت إليه ارتكابها أو لديه أدلة تتعلق بها، وكانت هذه الجريمة على درجة من الخطورة لاتخاذ مثل هذا الإجراء الاستثنائي[2].

فقد أجازت بعض التشريعات التنصت والمراقبة الإلكترونية، منها التشريع الفرنسي والذي أجاز على اعتراض الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات، وكما أجاز التشريع الهولندي لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسب الآلي إذا كان الهدف منها ضبط الجرائم الخطيرة، وكذا إمكانية مراقبة التلكس والفكس ونقل البيانات[3].

أما بالنسبة للقانون الجزائري فقد استحدث في **ديسمبر** سنة **2006** نصوص قانونية تتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتي تضمنت عدة أحكام منصوص عليها من المواد (**65 مكرر$_5$** إلى **65 مكرر $_{10}$**) والتي نذكرها كالتالي:

-قيام العمليات المذكورة في نص المادة (**65 مكرر$_5$**) بشرط عدم المساس بالسر المهني بالنسبة لأماكن التي يشغلها أشخاص ملزمون بالمحافظة على أسرار الآخرين.

-وفي حالة اكتشاف جرائم أخرى بصورة عارضة، فلا يكون هذا سببا في بطلان الإجراءات.

-يجب أن يتعلق الإذن بجميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

-يجب أن يكون الإذن مكتوبا وسليم لمدة أقصاها (04) أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري والتحقيق.

-يجوز لوكيل الجمهورية أو لقاضي التحقيق أو لضابط الشرطة القضائية المأذون له، تسخير كل عون

---

[1] المادة 03 من قانون رقم (09-04) لسنة 2009.

[2] علي محمود علي حموده، مرجع سابق، ص.34.

[3] مرجع نفسه ، ص. 34،35.

مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للقيام بالجوانب التقنية للعمليات المشار إليها في المادة **(65 مكرر5)**.

-تحرير محضر من طرف السلطات المختصة بالبحث والتحري عن كل عملية اعتراض أو تسجيل للمراسلات، وكذلك عمليات وضع الترتيبات التقنية وعملية التقاط والتثبيت والتسجيل الصوتي والسمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية ونهاية العمليات.

-يوصف أو ينسخ ويودع المراسلات أو الصور أو المحادثات المسجلة في إظهار الحقيقة من طرف ضباط الشرطة القضائية المناب له ذلك، وكذلك نسخ وترجمة المكالمات الأجنبية بمساعدة مترجم يسخر لهذا الغرض[1].

غير أن هذه الأحكام لم تتضمن صراحة الرقابة على الاتصالات الإلكترونية، ومن أجل ذلك فقد شمل المشرع الجزائري فصل ثاني خاص بمراقبة الاتصالات الإلكترونية في القانون رقم **(09-04)** لسنة **2009** المتعلق بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وقد تعلقت بنوعين من الرقابة، رقابة وقائية هدفها الوقاية من الجرائم الخطيرة المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ أما الثانية فهي رقابة ضبطية قضائية تتضمن حالتين:

-الحالة الأولى، عندما يقتضي الأمر التحري والتحقيق في ذلك لاستصعاب القيام بذلك بالطرق العادية دون اللجوء إلى المراقبة.

-الحالة الثانية، وذلك في ظل متطلبات التبادل والمساعدة القضائية بين الدول[2].

المطلب الثاني

الخبرة القضائية في الجرائم المعلوماتية

تقدم الخبرة عونا كبيرا للقضاء ولجميع جهات المختصة بالدعوى الجنائية من خلال أداء مهمتها التي بدونها يستحيل الوصول إلى رأي بشأن المسائل الفنية، والتي من خلالها يمكن التوصل إلى ظهور الحقيقة المبنية على حقائق علمية فنية والذي يعتبر العنصر المميز لها عن غيرها من إجراءات

---

[1] المواد من 65 مكرر5- 65 مكرر10 من ق.إ.ج.ج.

[2] المادة 04 من القانون رقم(09-04) المؤرخ في 05-08-2009.

الإثبات[1]. وفي هذا المجال نتطرق إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية في الجريمة المعلوماتية كفرع أول و القواعد الفنية التي تحكمها كفرع ثاني، وكذا مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة كفرع ثالث.

الفرع الأول

القواعد القانونية التي تحكم الخبرة القضائية في الجرائم المعلوماتية

تظهر أهمية الخبرة في مجال الجريمة المعلوماتية لتعلقها الوثيق بالحاسبات وشبكات الاتصال المرتبطة بالتخصصات العلمية والفنية الدقيقة، ومع التطور السريع لها يصعب على المختصين مواكبتها واستيعابها، بالإضافة إلى أنه لا يوجد خبير يستطيع التعامل مع جميع الجرائم المعلوماتية نظرا لتعدد أنماط هذا النوع من الجرائم[2]، وسوف نتعرض في هذا الفرع إلى التعريف بالخبير والخبرة، وأنواعها، ومجالاتها في الجرائم المعلوماتية.

أولا-تعريف الخبرة والخبير:

تعد الخبرة إجراء من إجراءات جمع الأدلة بعد إحاطة الموضوع بمعلومات فنية تسمح باستنتاج والوصول إلى الدليل، فالخبرة تعتبر وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الأدلة أو تحديد مدلولها من خلال الاستعانة بالمعلومات العلمية، حيث يستند القاضي إلى الخبرة لاتخاذ القرار المناسب.

أما الخبير فهو كل شخص تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة[3].

ثانيا-تعيين الخبير المعلوماتي:

إن أهم صعوبة تواجه الخبرة هي تكوين الخبير المناسب للاستعانة به، باعتبار أن الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصة بتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصة في المسائل الفنية والعلمية[4]، فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال الجريمة المعلوماتية بشكل خاص

---

[1] أحمد بلال، مرجع سابق، ص.256.

[2] عبد الله حسين على محمود، مرجع سابق، ص.392.

[3] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص .24.

[4] عمر محمد أبو بكر بن يونس، مرجع سابق، ص.1034.

أن يتمتع بشروط خاصة، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادة ودراسات عليا في فرع التخصص، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفة من أجل مواكبة كل جديد يطرأ على تخصصه لأداء مهمته[1]، فيتطلب من الخبير أن يكون ملما بالجوانب الفنية والتقنية، ومنها ما يلي:

-المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور وأكواد التشفير...الخ.

- طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة لذلك.

-المواضيع الرقمية المحتمل تواجد فيها أدلة الإثبات والصور أو الأشكال التي تتخذها.

-الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة.

-الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب على ذلك إتلافها.

-التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها[2] .

وعليه فإن اختيار الخبير في مجال الجريمة المعلوماتية يتحدد بنوعية الجريمة المرتكبة، نظرا لأن الحاسبات وشبكة الاتصال ذات نماذج متعددة، وبالتالي لا يوجد خبير لديه معرفة متعمقة مع كافة أنواع الحاسبات وبرمجياتها وشبكاتها، كما أنه ليس هناك خبير قادر على التعامل مع أنواع الجرائم التي تكون هذه الوسائل الإلكترونية محلا لارتكابها أو أداة لها[3] .

فقد يكون الخبير سببا لفقدان الأدلة لعدم التخصص الدقيق في المسألة التي تطلب ضرورة الخبرة وقد تحتاج إلى أكثر من خبير'[4]، فيجب أن يكون الخبراء في مجال الأدلة الرقمية على وعي تام لأن أيّ خطأ في التفسير يؤدي إلى إتلاف أو محو الدليل الرقمي كحالة الخطأ في طريقة الحصول

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص. 26 .

[2] عبد الله حسين على محمود، مرجع سابق، ص.394، 395.

[3] مرجع نفسه، ص. 392.

[4] فايز محمد راجح غلاب، مرجع سابق، ص.363.

على الدليل الرقمي أو عدم تحريز الأدلة[1]، كما قد يتم إتلاف الأدلة بسبب خطأ الخبراء والجهة المجني عليها[2].

ثالثا-أنواع الخبرة في المجال المعلوماتي :

1-الخبرة الخاصة:

تعتبر الخبرة الفردية من أهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات والانترنت فالمؤسسات الكبرى المتخصصة في هذا مجال تعمل جاهدة على الاستعانة بأشخاص ثبتت كفاءتهم في مجال الحاسب الآلي والانترنت، فهناك من الدول تقوم بمحاولة التعرف على قراصنة الذين تحولوا مع مرور الزمن إلى رموز وطنية من جراء تحركاتهم عبر الشبكة الإلكترونية[3].

2-الجهات التعليمية:

يمكن مواجهة الجريمة المعلوماتية عن طريق المؤسسات التعليمية والتي تهدف بدورها إلى تطوير العلم والقضاء على المشكلات التي تواجه الإنسانية، حيث يتم تدعيمها ماديا ومعنويا حتى تكون أفضل سبيل للمواجهة، وأنشأت العديد من المؤسسات التعليمية منها دراسات الكمبيوتر في جامعة ستافرورد ومعهد التكنولوجيا في ماساشوستس والذي وفَر خبراء على درجة عالية من التفوق[4].

3-جهات الضبط القضائي:

قامت بعض الدول وأهمها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصة للخبرة في إجراء الخبرة على الانترنت، العابر نشاطها الإطار الدولي في هذا المجال المتمثل في منظمة الأنتربول.

---

(1) Compagnie national des experts de justice en information et techniques Associées, la preuve numérique à l'épreuve du litige, les acteurs du litige face à la preuve numérique (l'information numérique fait la preuve), Colloque du 13 avril 2010 à la première chambre de la cour d'appel de paris ; p.28. أنظر الرابط الإلكتروني:
http://www.cnejita.org/dac/collague 20100513 Actes.PDF

(2) ومثال من اشتراك الخطأ بين الخبراء والمجني عليه، ما وقع في إحدى جرائم المعلوماتية حيث قام أحد الأشخاص في إحدى الشركات بوضع قنبلة منطقية بنظام الحاسب الآلي، وقد تم التأكد أن الشركة قبل إبلاغ السلطات المختصة قامت باستدعاء خبير للتحقق من صحة وجود القنبلة وإبطالها، وقد اكتشف الخبير القنبلة وقام بإزالة البرنامج الموضوع لها، وعندما تولت الشرطة التحقيق وجدت أن إزالة القنبلة أدى إلى إتلاف أدلة وجودها، راجع فايز محمد راجح غلاب، مرجع سابق، ص. 363.

(3) عمر محمد أبو بكر بن يونس، مرجع سابق، ص.1035.

(4) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.299.

حيث أن آخر نشاط مؤسسي في هذا الإطار هو الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية **FBI** أطلق عليه المعمل الإقليمي الشرعي للحاسوب، وأصبح مقر خبرة عامة متعددة النواحي القضائية هدفه مكافحة التصعيد الخطير في الجرائم المعلوماتية من خلال التصنيف والتحليل للدليل الرقمي، وأهم دور يقوم به هذا المعمل هو التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها[1].

رابعا: مجالات الخبرة في الجرائم المعلوماتية:

أفرز التطور الهائل في مجال تكنولوجيا المعلومات على العديد من الأنشطة المستحدثة، منها العمليات المصرفية الإلكترونية، الإدارة الإلكترونية والتجارة الإلكترونية، مما يقتضي تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الإلكترونية المستخدمة في ارتكابها، من بين هذه الجرائم:

-الغش أثناء نقل البيانات أو بثها.

-التلاعب في البيانات أو في البرامج سواء الأساسية منها أو برامج التطبيقات[2].

الفرع الثاني

القواعد الفنية التي تحكم الخبرة القضائية في الجرائم المعلوماتية

تتمثل القواعد الفنية للخبرة أساسا في الوسائل الفنية التي يستعين بها الخبير المعلوماتي من أجل إظهار الحقيقة وتقدير عمله ودوره في العمل على حفظ الأدلة الناجمة عن الخبرة التقنية، والتي سنتناولها فيما يلي.

أولا-وسائل الخبير في اكتشاف الدليل الإلكتروني:

نتناول في هذا الإطار الوسائل المادية والإجرائية كالتالي:

1-الوسائل المادية:

وهي الأدوات الفنية للنظم المعلوماتية التي يمكن أن تستخدم في ارتكاب الجرائم، وأهمها ما يلي:

أ-عنوان برتوكول الانترنت IP والبـــريد الإلكتروني وبرامـــج المحادثـــة، ويقصد بعنوان الانترنـــت المسؤول عن تراسل كم من البيانات عبر شبكة الانترنت وتوجيهها إلى أهدافها ويشبه عنوان البـــريد

---

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص.1037،1038.

[2] علي محمود علي حموده، مرجع سابق، ص.30.

العادي حيث يسمح للشبكات بنقل الرسالة وهو يوجد بكل جهاز إلكتروني مرتبط بالانترنت ويتكون من أربعة أجزاء وهي المنطقة الجغرافية، مزود الخدمة، الحاسبات الآلية المرتبطة، والرابع يقوم بتعيين الحاسب الآلي الذي تم الاتصال به[1].

وتوجد أكثر من طريقة يمكن من خلالها معرفة العنوان الخاص بجهاز الكمبيوتر في حالة الاتصال المباشر، مثل ما يستخدم في حالة العمل على نظام تشغيل Windows، حيث يتم كتابة WINPCFG في أمر التشغيل فيظهر مربع حوار فيه عنوان **IP** على أنه عنوان الانترنت، وقد يتغير في كل اتصال شبكة الانترنت.

أما في حالة استخدام برامج المحادثات كأداة للجريمة، فإنه يجب تحديد هوية المتصل حتى ولو لم يدون معلوماته في خانة المرسل، وذلك بشرط أن تكون المعلومات التي وضعها أثناء إعداد بريد إلكتروني صحيحة.

ب-البروكسي Proxy ، يعمل البروكسي كوسيط بين الشبكة ومستخدميها وأيضا كمزود طلبا من المستخدم البحث عن صفحة ما ضمن ذاكرة Cache المحلية والمتوفرة، لذلك يتحقق البروكسي في حالة تنزيل الصفحة من قبل، وبالتالي يقوم بإرسالها إلى المستخدم دون حاجة الرجوع إلى الشبكة العالمية، أما إذا لم يتم تنزيلها فيتم إرسال طلب إلى الشبكة العالمية، وفي هذه الحالة يقوم البروكسي كمزود زبون ويستخدم أحد عناوين **IP**، كما يمكن لمزود البروكسي أن يحتفظ بتلك العمليات خاصة لإجراء الإثبات بواسطة فحص تلك العمليات المحفوظة به[2].

ج- نظام كشف الاختراق ، يرمز له بأحرف **IDS** وهذه البرامج تقوم بمراقبة وتحليل بعض العمليات التي تحدث على أجهزة الحاسب الآلي أو الشبكة، من أجل البحث عن إشارات تفيد وجود مشكلة في الحاسوب أو الشبكة، وذلك من خلال تحليل مجموعة من البيانات أثناء انتقالها عبرالشبكة ببعض ملفات التشغيل التي تختص بتسجيل الأحداث فور وقوعها في الحاسب الآلي أو الشبكة، ومقارنة النتائج بمجموعة الاعتداءات الواقعة على الأنظمة المعلوماتية والتي يطلق عليها مصطلح التوقيع، بالتالي إذا تم اكتشاف النظام لوجود توقيع من التوقيعات يقوم بإنذار مدير النظام بطرق عديدة وفورية، حيث يقوم نظام كشف الاختراق بتسجيل البيانات محل الاعتداء في سجلات الحاسوب الخاصة لهذا الغرض.

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.304.

[2] مرجع نفسه، ص.305.

2-الوسائل الإجرائية:

من بين الوسائل الإجرائية نجد ما يلي:

أ-**اختفاء الأثر**، إن المسجلات التي يتم نشرها في المواقع الخاصة بالمخترقين تشير دائما بنصائح مختلفة من بينها قم بمسح آثارك Cover your trachs وفي حالة عدم مسح المخترق لأثاره يقبض عليه، حيث يتقصى على الأثر بطرق عديدة سواء بواسطة البريد الإلكتروني الذي تم استقباله أو بتتبع أثر الجهاز الذي تم استخدامه للقيام بالاختراق، وحتى لو تمت عملية الاختراق بشكل صحيح وسليم إلا أنه يمكن القبض عليه كونه لم يقم بمسح أثاره.

ب-الإطلاع على عمليات التنظيم المعلوماتي وأسلوب حمايته، من المفروض على المحقق في حالة إجرائه للتحقيق في جريمة معلوماتية ما، أن يقوم بالإطلاع على النظام المعلوماتي ومكوناته من شبكات وبرامج، وعملياته كقاعدة المعطيات وإدارتها ومعرفة النظام والمستفيدين والإجراءات منها إجراء أمن العاملين، وكذلك عليه الإطلاع على أسلوب النسخ الاحتياطـــي والاستعانة ببرامج الحماية كمراقبة المستفيدين والبرامج وتسجيل الوقائع.

ج-الاستعانة بالذكاء الصناعي، من الممكن الاستعانة بالذكاء الصناعي في جمع الحقائق والأسباب والفرضيات، التي يستخلص منها النتائج عن طريق معاملات حسابية يتم تحليلها بالحاسب الآلي وفقا لبرامج صممت لأجل ذلك، حيث أن تقنيات الحاسب الآلي أثبتت نجاحها وتمكنها من جمع أدلة جنائية وتحليلها واستنتاج الحقائق منها[1].

ثانيا- عمل الخبير وأساليبه:

تقتصر مهمة الخبير على التحقيق في الدعوى وإبداء رأيه في المسائل الفنية التي يصعب على القاضي استنتاجها دون المسائل القانونية[2].

وعليه، لجمع الأدلة حول الجرائم السالفة الذكر بمعرفة الخبير المعلوماتي، يجب مراعاة القواعد الفنية المتعارف عليها في مجال الخبرة المعلوماتية، وبالتالي يمكن للخبير إتباع الخطوات التالية في عمله:

1-مرحلة ما قبل التشغيل والفحص:

يجب على الخبير أن يقوم بوضع نسخة أو نسخ مطابقة للأصل لوسائط التخـــزين المضبوطـــة

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص.308.

[2] محمد حسين منصور، الإثبات التقليدي والإلكتروني، د. ط.، دار الفكر الجامعي، الإسكندرية، 2006، ص. 254.

كالقرص الصلب للقيام بعملية الفحص المبدئي وحماية الأصل من الفقدان أو التلف، وعليه التأكد من صلاحية النظام للتشغيل ومدى مطابقة محتوى الأحراز المضبوطة أثناء التحقيق بما هو مدون عليها كما يقوم بتسجيل محتوى البيانات المضبوطة كالطرز والنوع...الخ.

2-مرحلة التشغيل والفحص:

يقوم الخبير في هذه المرحلة باستكمال تسجيل البيانات التي لم يتم ضبطها من خلال قراءة جهاز الحاسب الآلي، ويحدد أنواع البرمجيات كبرامج النظام، برامج التطبيقات وأيّ من البرامج له علاقة بموضوع الجريمة التي تحقق المعالجة فيها الصور في جرائم التزييف أو التعديل أو التلاعب...الخ مع إبراز إذا كانت مستندات أو معلومات لها دلالة بموضوع الجريمة كبصمات الأصابع في جرائم التزوير ووجود رسائل تهديد في جرائم القتل وغيرها، وكذلك ينبغي عليه اكتشاف المستندات أو النصوص المخبأة داخل الصور، وأن يقوم بتحويل الدليل الرقمي إلى مكونات مادية بواسطة طباعة الملفات أو تصوير محتواها أو وضعها وعاء حسب نوع البيانات المكونة، ويجب أن يقوم باسترجاع الملفات التي تم محوها على الأصل عن طريق استخدام أحد برامج استعادة البيانات بالنسبة للملفات والسجلات المعطلة أو التالفة وذلك باستخدام برنامج Eassy Recover 4 all Professional والعمل على تخزين السجلات أو البيانات والقيام بنسخ طبق الأصل من الأقراص أو الأسطوانات لفحصها.

3- مرحلة تحديد مدى ترابط الدليل المادي والدليل الرقمي:

يتم في هذه الخطوة فحص الدليل المادي المضبوط مع الدليل المستخرج من جهاز الحاسب الآلي والربط بينها ليصبح الدليل موثوق ويقيني حتى يتسنى قبوله أمام المحكمة.

4-تدوين النتائج وإعداد تقريره:

يقوم الخبير بتقديم تقرير موقعا منه لما توصل إليه من نتائج من بداية إجرائه للخبرة، وغالبا ما يرفق معه الملاحق الإيضاحية سواء كانت مصورة أو مسجلة وغيرها، ويقدم الملف إلى جهة التحقيق أو جهة الحكم[1].

ومن هنا فعلى الخبير الفني أن يستخدم الأساليب العلمية المتخصص فيها من أجل الوصول إلى الحقيقة، وهناك أسلوبين لعمل الخبير التقني:

الأول: القيام بتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها مثل التهديد أو النصب أو جرائم

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص. 35،36.

النسخ أو دعارة الأطفال، ثم القيام بتحليل رقمي لها من أجل معرفة كيفية برمجتها وتحديد عناصر حركتها وطريقة الوصول إلى معرفتها، ومن ثم الوصول إلى معرفة برتوكول الانترنت **IP** الذي نسب أو ارتبط بجهاز الكمبيوتر الذي صدر عنه هذه المواقع.

الثاني: تجميع وتحصيل مجموعة المواقع التي لا يمثل موضوعها جريمة بحد ذاتها، وإنما يؤدي متابعة موضوعها إلى ارتكاب الجرائم مثل المواقع التي تقوم بالمساعدة للتعرف على جرعات المخدرات أو المؤثرات العقلية أو كيفية إعداد القنابل وتخزينها[1].

ثالثا–دور الخبير التقني في حفظ الأدلة الإلكترونية:

يتطلب لحفظ الأدلة داخل جهاز الحاسوب معرفة دقيقة لصحة البيانات الواردة في الحاسب الآلي وهذا ما يستلزم من الخبير التقني ضرورة الكشف بداية على نطاق محتوى صحة حركة الحاسب الآلي من وجود شك في صحة الأدلة المستفادة، خاصة حالة وجود الخلل أو العطب مثل الفيروس.

ومثل هذا الاتجاه نجد التشريع الإنجليزي، حيث تتم عملية حفظ الأدلة داخل جهاز الحاسوب بأساليب عديدة منها استخدام الحفظ العادي وأهمها القيام بعمليات حجز الحاسوب على الدليل الموضوع فيه، ذلك أن الدليل الرقمي هو ملف يحتوي على معطيات رقمية تبين مظهرا معلوماتيا محددا غير قابل للتحويل إلاَ بقيام تعديلات أو تغييرات رقمية على البيانات المذكورة.

فعملية حفظ الأدلة الرقمية تتطلب من الخبير التقني القيام بمعرفة موقع الانترنت أو المعلومات التي تشكل الجريمة، كجرائم السب والقذف في غرف المناقشة أين يتم العودة إلى ذاكرة الخادم ليقوم بربط الغرف حتى يتم التوصل إلى تحديد موضوع السب والقذف وتاريخه، أما في حالة كون الجريمة من جرائم النشر عبر الانترنت، فيتم اللجوء مباشرة إلى ذاكرة الحاسب الآلي المستخدم، وبالتالي تستدعي عمليات حفظ الأدلة من الخبير أن يقوم باستخدام البرمجيات للقيام بحفظ الأدلة الرقمية كما أنه ملزم أن يقوم بعرض الأدلة على المحكمة أو جهات التحقيق[2].

الفرع الثالث

مدى كفاية النصوص التقليدية في معالجة المسائل المتعلقة بالخبرة المعلوماتية

باعتبار أن القاضي قد يستخدم خبير استشاري بشكل غير رسمي في المجال الرقمي، ذلك ما

---

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 1043، 1044.

[2] مرجع نفسه، ص.1045.

قد يشكل صعوبة ويعيق إجراءات التحقيق وأكثر من ذلك قد تكون وجها من أوجه البطلان، كون أن بعض القوانين تخول للمتهم دون سلطة التحقيق أو الاتهام الاستعانة بخبير استشاري، لأنه قد لا يجد القاضي خبيرا في مجال تكنولوجيا المعلومات ضمن قائمة جدول الخبراء، هذا ما يستدعي من المشرع التدخل من خلال تضمين نصوص قانونية التي تسمح بالاستعانة بالخبرة الاستشارية من طرف جهة التحقيق والاتهام في المجال المعلوماتي دون التقيد بخبراء الجدول المعتمدين[1].

ولقد نظم قانون الإجراءات الجزائية الجزائري نصوص خاصة بالأحكام المتعلقة بالخبرة بالنسبة للجريمة التقليدية من المادة **(143)** إلى المادة **(156)** [2]، ورغم عدم تضمين نصوص خاصة تتعلق بالخبرة الرقمية، وكذلك نقص الخبرة في مجال تكنولوجيا المعلومات، إلا أنه هناك إمكانية تطبيق الأحكام المتعلقة بالخبرة في الجرائم الناشئة عن الحاسب الآلي، فبات الأمر على القاضي أن يكون ملما بالأمور الفنية، باعتباره يشرف ويراقب أعمال الخبرة، كما أنه يحدد المواضيع التي تتطلب الاستعانة بالخبرة، غير أن هذا الأمر غير متوفر في الدول النامية، وبالتالي تدريب كوادر الأجهزة الضبطية والقضاة في مجال الخبرة الرقمية تكاد تكون ضرورة لا غنى عنها[3].

وهذه الحتمية أدت بالدولة الجزائرية بالعمل على استفادة الشرطة والدرك الوطني وغيرها من الأجهزة القائمة على تحقيق العدالة، إلى تلقي التدريب والتعليم في فرنسا، بلجيكا وكندا، وقد تم تكوين مركز وقاية ومكافحة الإجرام المعلوماتي ببوشاوي من طرف قيادة الدرك، ويتم إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي بموجب المرسوم الرئاسي رقم **(04-432)** المؤرخ في **20 ديسمبر 2004**[4]، ويشمل هذا المعهد على المصالح والأقسام والمخابر بموجب قرار مشترك مؤرخ في **14 أبريل 2007**، ومن بين مصالحه مصلحة الخبرات الخاصة بالدلائل التكنولوجيا، بحيث تضمنت المديرية العامة للأمني الوطن ومصالحها في بعض الولايات قسم خاص بالخبرة الرقمية، ويتكون من خبراء متخصصين في تحليل واستعادة البيانات المحذوفة وتتبع عنوان **IP**، ومعالجة الصور ومطابقتها

---

[1] عمر أبو بكر بن يونس، مرجع سابق، ص.892.

[2] راجع المواد من 143-156 من ق.إ.ج.ح.

[3] فايز محمد راجح غلاب، مرجع سابق، ص.369.

[4] مرجع نفسه، ص.370.

ومعرفة الصور التي تم تركيبها، وكذلك الخبرة المتعلقة برسائل الهاتف النقال[1]، وكما وضع المشرع نصوص خاصة لها علاقة بالخبرة الرقمية، ومن ذلك إمكانية السلطات المكلفة بالتفتيش الاستعانة بكل شخص له دراية بعمل المنظومة المعلوماتية من أجل مساعدتها في إنجاز مهمتها محل البحث[2]، وكما قام بإنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تكون مهمتها إنجاز الخبرات القضائية التي تطلبها السلطات والشرطة القضائية[3].

وعليه في الأخير يمكن القول أن الجرائم المعلوماتية هي جرائم ذو طبيعة غير مادية، هذا ما أدى بإجراءات التحقيق الجنائي فيها لا تزال محل خلاف فقهي وقضائي، وبالأخص إجراءات التفتيش والضبط عن بعد، والمعاينة وكذا غياب وجود الخبير المعلوماتي المتخصص في المجال الرقمي وغيرها من إجراءات التي تثير العديد من المشكلات التي تعيق التحقيق، باعتبار أن الدليل المراد استنباطه يكون خفيا غير مرئي وأكثر من ذلك فقدان الدليل لأثاره سواء بالتلاعب أو التغيير أو الحذف، لكون الجريمة المعلوماتية مجهولة لا تصل إلى علم سلطات التحقيق والاستدلال، وهذا راجع إلى عدم اكتساب المهارة والمعرفة وعدم الخضوع للتدريبات التي تسمح للقضاة وضباط الشرطة القضائية بمواجهة تقنيات الحاسب الإلكتروني المتطورة، وكذا عدم استعانتهم بخبراء مختصين في مجال التحقيق، وهذا ما ينعكس سلبا على نفسية المحقق والمجتمع وإيجابا على نفسية الجاني، كونه على ثقة بأن السلطات التحقيق المختصة غير قادرة على إيجاد الدليل ضده وهذا ما يشجعه أكثر على ارتكاب جرائم كثيرة وخطيرة، لذا فإن متابعة إجراءات التحقيق في مجال الجريمة المعلوماتية، تحتاج إلى الأمن المعلوماتي ولرجال الضبط القضائي والقضاة المتمكنون في الأمور الفنية، والتي لن يتسنى تحقيقها إلا عن طريق التدريب والتأهيل في المجال التقني المعلوماتي.

وكل هذه الأمور لا تؤدي إلى الكشف عن الحقيقة إلا بالحصول على الدليل الإلكتروني الرقمي، الذي يقوم عليه الإثبات الجنائي في الجرائم المعلوماتية للوصول إلى الحقيقة المطلقة، وبالتالي من المهم جدا التعرض إلى الدليل الرقمي والذي لناَ الحديث عنه في الفصل الثاني كما سيأتي.

---

[1] القرار الوزاري المؤرخ في 14 أبريل 2007 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، ج.ر.ع.36، الصادرة في 3 يونيو 2007.

[2] الفقرة الأخيرة من المادة 05 من قانون رقم(09-04).

[3] الفقرة(ب) من المادة 13 من قانون رقم(09-04).

الفصل الثاني

الدليل الرقمي وتقديره أمام القضاء الجزائي

يعرف الدليل على أنه الحجة والبرهان وهو ما يدفع به الخصم، ووسيلة لإثبات حق من الحقوق[1]، فالدليل الجنائي هو جوهر الإثبات سواء في مجال إثبات التهمة ونسبتها إلى المتهم أو إثبات عدم إمكانية إسنادها إليه، ويعد الدليل الجنائي ذو أهمية كبرى لأنه يناصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحوّل الشك إلى يقين باعتبار أن الحقيقة في معناها العام هي معرفة حقيقة الشيء بأن يكون أو لا يكون، والذي لا يتحقق إلاّ عن طريق الدليل المعبر عن هذه الحقيقة[2].

وإذا كانت الجرائم المعلوماتية ذو طبيعة خاصة، فإن هذا الأمر يؤثر مباشرة في أدلة إثباتها جنائيا، حيث أن الدليل الرقمي في الجرائم المعلوماتية يمتاز عن غيره بصعوبة فهمه، باعتباره يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل الطرق لضبطه، حتى يكون هذا الدليل الرقمي ذو أهمية بالنسبة لقضاة الحكم الذين غالبا ما يتخذونه دليل يرتكزون عليه في المسائل الفنية، وعليه فإن الدليل الرقمي ضروري للإثبات الجنائي في الجرائم المعلوماتية، وبه تتحدد مدى قدرة القاضي الجنائي للوصول إلى الحقيقة من خلاله لتكوين عقيدته والحكم بالإدانة أو البراءة، بالتالي هذا الأمر يحتاج إلى مناقشته والذي سنتعرض إليه في مبحثين على النحو التالي: : ماهية الدليل الرقمي كدليل إثبات في المواد الجنائية(المبحث الأول) وتقدير الدليل الرقمي أمام القضاء الجزائي(المبحث الثاني).

---

[1] سيدي محمد لبشير، مرجع سابق، ص.21.

[2] علي محمود علي حموده، مرجع سابق، ص.18.

المبحث الأول

ماهية الدليل الرقمي كدليل إثبات في المواد الجنائية

ترتكز عملية الإثبات الجنائي للجرائم المعلوماتية على الدليل الجنائي الرقمي، ذلك أنه الوسيلة الوحيدة والأساسية لإثبات هذا النوع من الجرائم، وهو محور اهتمام بحثنا لذا سنتناول في هذا المبحث مفهوم الدليل الرقمي(المطلب الأول)، محل ومراحل الدليل الرقمي في الإثبات الجنائي(المطلب الثاني).

المطلب الأول

مفهوم الدليل الرقمي

باعتبار أن الدليل الرقمي ذو أهمية بالغة في مجال الإثبات الجنائي للجرائم المعلوماتية، فإنه يجب التعرض إليه بتحديد مفهومه من خلال تعريفه وتعداد تقسيماته وخصائصه، وأنواع وأمثلة عنه فيما يلي.

الفرع الأول

تعريف الدليل الرقمي وتقسيماته

لقد تنوعت واختلفت تعريفات وتقسيمات الدليل الرقمي كما سنراه.

أولا- تعريف الدليل الرقمي:

يعرف البعض الدليل الرقمي على أنه: "الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهروبائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتباره أمام القضاء.

وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[1].

في حين عرفه الدكتور عمر محمد أبو بكر بن يونس على أنه:" الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة"، فيعد الدليل الرقمي الدليل المستعان بتقنية المعالجة الآلية للبيانات، والذي يؤدي بقاضي الموضوع إلى اقتناعه بثبوت ارتكاب الجريمة من شخص ما[2].

---

[1] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، د.ط.، دار الكتب القانونية، مصر، 2006، ص. 88.

[2] عمر محمد أبو بكر بن يونس، مرجع سابق، ص.969.

وكذلك وضع البعض الآخر تعريف للدليل الرقمي على أنه: "هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات أدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"[1].

إن مقدمات التعامل مع الدليل الرقمي تشير بكونه يتجاوب مع التطور الحاصل بسرعة فائقة حيث أنه بعدما كان الدليل الصامت والثابت يقدم ما يمكن الحصول منه على نسخ عن طريق الطباعة Print out، والذي يطلق عليه تسمية "مخرجات الحاسوب" مثل: الوثائق Document، والصور Pics...الخ فإن التطور اقتضى أن يكون هناك مظهر جديد للدليل الرقمي ذاته وهو المظهر التقني المعلوماتي الذي يتميز بالحركية والذكاء[2].

ثانيا- تقسيمات الدليل الرقمي:

للدليل الرقمي أشكال مختلفة، وقد قسمها البعض إلى الأقسام الأساسية التالية:

1- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها.

2-أدلة رقمية خاصة بالشبكة الدولية للمعلومات "الانترنت".

3-أدلة خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

بالتالي هذا التقسيم يتطابق مع تقسيم الجريمة عبر الحاسب الآلي[3].

وقد قررت وزارة العدل الأمريكية لسنة 2002 أن الدليل الرقمي يمكن تقسيمه كالتالي:

1-السجلات المحفوظة في الحاسب الآلي وتشمل الوثائق والملفات المكتوبة والمحفوظة كالبريد الإلكتروني وملفات معالجة الكلمات مثل Winword ورسائل وغرف المحادثات عبر الانترنت[4].

2-السجلات التي تم إنشاؤها وإعدادها بواسطة الحاسوب، وهي تعد مخرجات الحاسوب، والتي لم يشارك الأشخاص فيها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي files[5].

---

(1) عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص.13.

(2) عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 969.

(3) ممدوح عبد الحميد عبد المطلب، مرجع سابق،ص.88.

(4) عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص.14.

(5) خالد عياد الحلبي، مرجع سابق، ص. 234.

3-السجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤه عن طريق الحاسب الآلي، ومنها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيها مباشرة إلى برامج أوراق العمل، وبعد ذلك تتم معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها تلقائيا مثل:Excel.

الفرع الثاني

خصائص الدليل الرقمي

يمتاز الدليل الرقمي عن غيره من الأدلة الجنائية بعدد من الخصائص التالية:

1- تتكون الأدلة الرقمية من بيانات ومعلومات إلكترونية غير مرئية وغير ملموسة، بحيث يتطلب لإدراكها استخدام أجهزة ومعدات الحاسب الآلي (Hardware) واستعمال نظم برمجيات الحاسوب (Software)[1].

2- يعد الدليل الرقمي دليل علمي، بحيث يتطلب منه توافر مجال تقني للتعامل معه، لذلك فكل ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، بالتالي فالدليل العلمي يخضع لقاعدة ضرورة تعبيره عن الحقيقة، وهذا ما تضمنته قاعدة في القضاء المقارن التي تنص على ما يلي:" إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة".

3- يعد الدليل الرقمي من طبيعة تقنية وهذا ما يميزه عن الدليل التقليدي، من حيث أن التقنية لا تنتج سكينا يتم من خلاله معرفة القاتل أو اعترافا مكتوبا أو مالا قدم كرشوة أو بصمة أصبع، بل تنتج التقنية نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه، وهذا ما حذا به المشرع البلجيكي بمقتضى القانون الصادر في **28 نوفمبر 2000م**، بتعديل قانون التحقيق الجنائي من خلال إضافة المادة(**39**) التي أجازت ضبط الأدلة الرقمية مثل: نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية[2]، وعليه ما يميز الدليل الرقمي على أنواع الأدلة الأخرى أنه يمكن أن يستخرج نسخ من الدليل الرقمي مماثلة ومطابقة الأصل ولها نفس القيمة العلمية والثبوتية، وهذا ما يكفل وجود ضمانة قوية وفعّالة للحفاظ على الدليل ضد الفقدان والتلف والتغيير من خلال وضع نسخ طبق الأصل من الدليل[3].

---

[1] عبد الناصر محمد محمود فرغلي، محمد سيف سعيد المسماري، مرجع سابق، ص.14.

[2] عمر محمد أبو بكر بن يونس، مرجع سابق، ص.7.

[3] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص. 15.

4- صعوبة التخلص من الدليل الرقمي، وتعتبر هذه الخاصية من أهم مميـزات الدلـيل الرقـمي باعتبارها ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة، بحيث يقتضي الأمر مقارنة بين الدلـيل الرقمي والدليل الجيني الذي يطلق عليه الحمض النووي **DNA**، ذلك لاتحاد كل منهما في هذه الخاصية التي تتمثل في صعوبة التخلص منهما من جهة، ومن جهة أخرى من الممكـن إحـداث تعـديل فـي تكوينهما معا، وهذا ما يستوجب مقارنة الأدلة الرقمية بالأدلة التقليدية، حيث أن هذه الأخيرة تسـتمد قوتها في حالة التسريع بالحصول عليها، فمثلا بصمة الأصبع إذا ما طالت المدة بين سـاعة ارتكـاب الجريمة وبين الحصول عليها فتكون قابلة للشك، كما أن في الشهادة يجب التعرف على مـدى قـدرة الشاهد على التذكر حيث أن قبول شهادة تعتمد على مستوى الرجل العادي في التذكر الذي يعترف به القانون وهذا من ناحية، أما من الناحية أخرى فالأدلة المادية يمكن التخلص منها عن طريـق مسـح بصمة الأصبع من مكانها، كما أن في بعض الدول يتم التخلص من الشهود عن طريق القتل أو التهديد به، وكذلك يمكن التخلص من الأوراق والأشرطة المسجلة إذا كانت تحتوي على ارتكـاب أشـخاص لجرائم، وذلك عن طريق حرقها أو تمزيقها، وعليه فإن عملية التخلص من هذه الأدلة سهل جدا ومن المستحيل استرجاع الدليل المستمد إذا ما تم تدميره كلية،أما الحال بالنسبة للأدلة الرقمية فهـو لـيس كذلك، لأن موضوع التخلص من الدليل الرقمي باستعمال أو الاسـتعانة بخصـائص الـتخلص مـن المستندات في الحاسب الآلي والشبكة الإلكترونية لا تعتبر من العوائـق التـي تحيـل دون اسـترداد الملفات، حيث أنه تتوافر برمجيات من ذات الطبيعة الرقمية يمكن من خلالها استرجاع كامل الملفـات التي تم من قبل إلغاؤها أو محوها من الحاسب الآلي أو إظهارها، وهذا ما يعني صعوبة إخفاء الجاني لجريمته[1].

5- إمكانية توظيف نشاط الجاني لمحو أو إزالة الدليل من الحاسب الآلي كدليل إدانة ضده، لأن فعل الجاني بمحو الدليل يتم تسجيله في الحاسوب، والذي يمكن الحصول عليه لاحقا كدليل للإدانة.

6- تمتاز بعض الأدلة الرقمية بسعة تخزينية عالية، بحيث يمكن لقرص صغيرة تخزين مكتبة كاملة كما يمكن لآلة فيديو رقمية تخزين مئات الصور.

7- يمكّن الدليل الرقمي من تسجيل المعلومات عن الجاني ورصدها وتحليلها في الوقـت نفسـه، لأن الدليل الرقمي يمكن أن يقوم بتسجيل تحركات الأفراد وسلوكا تهم وعاداتهم وبعض الأمـور الخاصـة

---

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص.981، 982.

بهم لذلك فالبحث الجنائي عن الدليل الرقمي يكون بسهولة مقارنة مع الدليل المادي[1].

8- الدليل الرقمي هو مفهوم يحتوي التطور والتنوع، ذلك لأن هذا المصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقميا، بحيث يكون بين هذه البيانات والجريمة رابطة أو علاقة من نوع ما تلك التي تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة [2].

الفرع الثالث

أنواع وأمثلة الدليل الرقمي

للدليل الرقمي أنواع وأمثلة متعددة نذكر منها ما يأتي.

أولا- أنواع الدليل الرقمي:

يمكن تقسيم الأدلة الرقمية إلى الأنواع الأساسية التالية:

1-الورق ومخرجات الطابعات:

غالبا ما تترك الجرائم الواقعة على الأموال أو على الأشخاص أثار من الأوراق والمستندات بالغة الأهمية التي يتم حفظها في الحاسب الآلي، فالكثير ممن يقومون بطباعة المعلومات بهدف المراجعة أو التأكد من الشكل العام أو صحة المستند موضوع الجريمة، فالطابعات وأجهزة الحاسب الآلي ذات السرعة الفائقة تطبع الكثير من الأوراق في وقت يسير، لذلك يعد الورق من الأدلة الرقمية التي يتم من خلالها بحث وتفتيش مسرح الجريمة، وللورق أربعة أنواع هي[3]:

أ-المسودة التي يتم إعدادها بخط اليد مثل تصور للعملية التي يتم برمجيتها.

ب-أوراق تالفة والتي تتم طباعتها للتأكد من برمجة العملية، ومن ثم إلقاؤها في سلة المهملات.

ج-الأوراق التي تتم طباعتها والاحتفاظ بها لأغراض تفيد الجريمة.

د-الأوراق الأساسية والمحفوظة في الملفات العادية أو دفاتر الحسابات وخاصة التي يتم تزويرها من أجل تنفيذ الجريمة[4].

---

[1] ممدوح عبد الحميد عبد المطلب، مرجع سابق ، ص. 89.

[2] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 980، نقلا عن،

Eagham (Casey),Digital evidence and forensic science, Computer and the internet, computer crime- &s ted. Academic press. USAUK.

[3] عبد الله حسين على محمود، مرجع سابق، ص. 397.

[4] سيدي محمد لبشير، مرجع سابق، ص.71.

2-الأجهزة الإلكترونية، ومنها:

أ-الحاسب الآلي وملحقاته، لتحديد الجريمة على أنها جريمة معلوماتية مرتبطة بالمكان أو بالشخص يفترض وجود حاسب آلي، حيث بإمكان خبير الحاسب الآلي التعرف على الجهاز ومواصفاته مع تمييزه عن غيره من أجهزة الحاسب الآلي الأخرى، بالإضافة إلى كيفية تحديد أسلوب التعامل معه أثناء الضبط والتحريز[1].

ب-الطابعات، تقوم الطابعات باستخراج ما تم تحضيره لطباعته، وتختلف أنواعها من عادية وليــزرية، ملونة وغير ملونة، حيث غالبا تستخدم في مجال التقنية المعلوماتية.

ج-الموديم: هي الوسيلة التي يمكن من خلالها لأجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف، كما يقوم كذلك بإرسال الفاكس والرد على المكالمات الهاتفية، وتبادل البيانات وتعديلها، ويأخذ أشكال متنوعة مرتبطة بتطور تقنية المعلومات.

د-الهاتف النقال، يعتبر جهاز إلكتروني حجمه صغير يفيد التواصل بين الأشخاص عبر الهواء، وقد تطور في الآونة الأخيرة، فأصبح يتمتع بأشكال ومميزات أحدث أجهزة الحاسب الآلي اليوم، وأطلق عليه تسميات عدَة منها الجوال، والمحمول، والخلوي والنقال،...الخ[2].

3-وسائل التخزين، ومنها:

أ-القرص الثابت الداخل، يعد الوحدة الرئيسية التي يتم من خلالها تشغيل نظام الحاسب والبرامج والبيانات.

ب-الأقراص المدمجة (**CD**)، هي وحدات تخزين متنقلة تحتوي على معلومات، وتقوم بتخزين هذه المعلومات عليها وإعادة تسجيلها.

ج- ذاكرة فلاش (**USB**)، وهي سهلة النقل والتبادل وحجمها صغير تعمل على تخزين ونقل البيانات ولها قدرات تخزين وأحجام مختلفة ومتنوعة[3].

د-الأشرطة الممغنطة (**Magnetic Tapes**)، وهي وسيلة تستخدم غالبا في الحفظ الاحتياطي للبيانات والمعلومات وتوضع في مكان بعيد وآمن، وكما يقوم البعض بإيداعها لدى خزائن البنوك أو مراكز التوثيق الحكومية الأمنية.

---

[1] عبد الله حسين على محمود، ص. 398.

[2] سيدي محمد لبشير، مرجع سابق، ص. 71.

[3] مرجع نفسه، ص.72.

و- البطاقات الممغنطة وبطاقات الائتمان القديمة والمواد البلاستيكية المستخدمة في إنشاء تلك البطاقات، قد يمكن أن تكون قرائن للإثبات في الجرائم المعلوماتية[1].

4-البرامج، ومنها:

أ- برامج نظم التشغيل، أعدت هذه البرامج المصممة لتحديد تشغيل نظم الحاسب الآلي، والتي تقوم باستقبال وإخراج المعلومات والبيانات والتحكم في الذاكرة والتخزين وإدارة التطبيقات.

ب-برامج التطبيقات، تعتبر برامج مصممة أساسا لأداء وظيفة محددة كمعالجة النصوص، بالإضافة إلى إدارة قاعدة البيانات، ويتم تحميل مثل هذه البرامج في حالة الحاجة إليها[2].

ثانيا- أمثلة الدليل الرقمي:

يمكن أن نذكر كأمثلة عن الأدلة الرقمية ما يلي:

1- بروتوكول (TPC /IP)، يعتبر من أهم وأشهر البروتوكولات المستخدمة في شبكة الانترنت والاتصالات، كما يعد جزء أساسي من الانترنت ويتكون مما يلي:

-بروتوكول(User Datagsam Protocol/ UDP).

- بروتوكول(Transmission Control Protocol/ TCP) .

- بروتوكول(Internet Protocol/ IP) .

ومن مميزات هذه البروتوكولات، أنها تقوم معا بنقل المعلومات الخاصة بالمستخدم وفقا لنظام هيكلة تبادل المعلومات المعروف باسم (**TCP/ IP with OSI**)[3].

حيث يقوم بروتوكول (TCP) بتسليم واستقبال المعلومات المطلوب إرسالها أو إعادة إرسالها في حالة الضرورة، وبتنسيق من بروتوكول (UDP) الذي صمم من أجل مواجهة بعض التطبيقات التي لا تستخدم (TCP)، كما أن تطبيقات كلا من (UDP /TCP) أعدت أيضا لمواجهة المسائل المألوفة أثناء عملية تبادل المعلومات والتي تتمثل في إخفاء الهاردوير وتأخر المعلومات، واشتباك وازدحام الشبكات والأخطاء التي قد تتكرر أو تتالى، وبعد تقسيم المعلومات من حزمة معلوماتية (الباكت) من طرف (TCP)، يقوم بروتوكولIP بعنونة المعلومات المرفقة مع إضافة معلومات أخرى، فتصبح الباكت المحتوي على حزمة (TCP /IP)، وأثناء اتصال الحاسب الآلي بالانترنت يأخذ عنوان خاص يسمى

---

[1] عبد الله حسين علي محمود، مرجع سابق، ص. 399، 400.

[2] سيدي محمد لبشير، مرجع سابق، ص. 72.

[3] مرجع نفسه، ص.73.

IP Adresses وكل عنوان مكون من جزأين، الأول يتضمن أرقام الشبكة، والثاني يتعلق بأرقام مزود الخدمة[1].

2-الكوكيز(Cookies)، هي مجموعة من الملفات أو السجلات النصّية التي يرسلها الخادم (Server) عن طريق الاتصال به بواسطة القرص الصلب لحاسب المستخدم، حيث أنها تمكن من تسجيل عنوان (IP) الخاص بالحاسب الآلي، وتحديد موقعه الجغرافي ونظام التشغيل، والتاريخ وفترة الاتصال والصفحات التي تم اكتشافها، وكلمة المرور مع اسم المستخدم، وبالتالي تعد الكوكيز أداة يتم من خلالها جمع البيانات التعريفية الخاصة بالمستخدم، حيث لا يمكن لهذا الأخير الهروب منها لأن بدونها لا يستطيع تصفح الانترنت[2].

المطلب الثاني

محل ومراحل الدليل الرقمي في الإثبات الجنائي

إنَ الدليل الجنائي الرقمي هو جوهر الإثبات في الجرائم المعلوماتية، بالتالي فمحل الدليل الرقمي هو الجريمة المعلوماتية، ذلك أن عدم وجود جريمة معلوماتية يعني عدم وجود دليل رقمي يثبتها، أما في حالة ثبوت وقوع جريمة معلوماتية فتقوم عملية البحث عن الدليل الرقمي لإثباتها ونسبتها إلى المتهم المعلوماتي، لهذا تمر الأدلة الجنائية الرقمية في سيرها للإثبات كغيرها من الأدلة الجنائية الأخرى بعدة مراحل، وكل مرحلة من هذه المراحل مميزة عن غيرها، وسوف نتطرق إلى محل الدليل الرقمي ومراحله في الإثبات الجنائي في فرعين مستقلين، الفرع الأول يتمثل في محل الدليل الرقمي والفرع الثاني يتعلق بمراحل الدليل الرقمي في الإثبات الجنائي.

الفرع الأول

محل الدليل الرقمي

خلت معظم قوانين العقوبات على مستوى العالم من نصوص تجريم الأفعال الضارة التي تقع نتيجة الاستخدام غير المشروع للحاسب الآلي، سواء كان هذا الأخير أداة للجريمة المعلوماتية أو محلا لها[3]، لهذا سوف نتعرض إلى الإطار القانوني لهذه الجريمة وثم نحدد موقف المشرع الجزائري منها.

---

(1) ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص99-102.

(2) سيدي محمد لبشير، مرجع سابق، ص.73.

(3) ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص. 44.

أولا: الإطار القانوني للجرائم المعلوماتية:

باعتبار أن محل الدليل الرقمي هو الجريمة المعلوماتية والتي تعتبر جريمة مستحدثة، حيث أنها ظهرت تبعا للتطور التكنولوجي لوسائل الإعلام والاتصال، ارتأينا إلى التعريف بها وتبيان أهم المميزات التي خصت بها عن باقي الجرائم.

1-تعريف الجرائم المعلوماتية:

سبق وأن تم ذكر الجرائم المعلوماتية عموما، غير أن التعريفات الخاصة بها قد تعددت واختلفت الاتجاهات الفقهية من حيث ضيقها واتساعها دون التوصل إلى تعريف موحد لها، وهذا يعود لاختلاف الفقهاء في الظاهرة الإجرامية الناشئة عن الحاسب الآلي بين الذين ينظـــرون إليها من زاويـــة الـــتقنية، والذين يستندون إليها من منظور قانوني، ونظرا لصعوبة إيجاد تعريف جامع وشامل لجرائم الحاسب الآلي أدى بالبعض إلى القول أن :"الجريمة المعلوماتية تقاوم التعريف"[1].

ويمكن تقسيم الجريمة المعلوماتية إلى تعريفات تتعلق بالوسيلة المستخدمة ألا وهي الحاسب الآلي، وتعريفات تستند إلى موضوع الجريمة[2]الذي يشمل الأفعال غير المشروعة الموجهة ضد المال المعلوماتي[3].

ومن التعريفات التي تستند إلى وسيلة ارتكاب الجريمة، نجد تعريف الفقيه الألمـــاني (تيدمـــان) الذي عرف الجريمة المعلوماتية على أنها:" كل أشكال السلوك غير المشروع (أو الضـــار بالمجتمع) الذي يرتكب باستخدام الحاسب"[4]، وكذا تعريف الأستاذ (Mass) على أن الجريمة المعلوماتية هي كل الاعتداءات غير المشروعة التي ترتكب باستخدام المعلوماتية بغرض تحقيق الربح [5].

---

[1] قارة أمال، الجريمة المعلوماتية، رسالة لنيل ماجيستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، بن عكنون، 2002، ص. 17.

[2] أحمد خليفة الملط، الجرام المعلوماتية، د.ط.، دار الفكر الجامعي، الإسكندرية، 225، ص. 81.

[3] يقصد "بالمال المعلوماتي" الحاسب بكل مكوناته، ويتكون من عنصرين أساسيين هما الكيان المادي المتمثل في جهازي الإدخال والإخراج ووحدة التشغيل، والكيان المعنوي المتمثل في قيام الحاسب بوظائفه كمعالجة المعلومة المطلوبة مثلا.

[4] قارة أمال، مرجع سابق، ص.17، نقلا عن،

Tiedemann, Traude et autres délits d'affaires commis à l'aide d'ordinateurs éléctroniques. R.D.P.C. 1984 .n°7 ;61

[5] محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجـــرائم المعلومـــاتية، ط. 1، دار الثقـــافة للنشـــر والتـــوزيع، عمـــان، 2007، ص.8.

أما عن تعريفات الجريمة المعلوماتية التي تستند إلى موضوع الجريمة، فقد عرفها مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 م بأنها: كل فعل غير قانوني أو أخلاقي أو لم يتم التصريح به مرتبط بالمعالجة الآلية للبيانات أو بتحويلها[1]، وكما عرفها الأستاذ محمود أحمد عبابنة على أنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية"[2].

لذلك يمكن القول على أنه لا يوجد مصطلح موحد للدلالة على الجريمة المعلوماتية، فالبعض يطلق عليها تسمية جرائم إساءة استخدم الحاسب الآلي، والبعض الآخر يسميها جرائم الانترنت، أو جرائم التكنولوجيا الحديثة، أو جرائم المعالجة الآلية للمعطيات، كما أن هناك آخرون يطلقون عليها مصطلح جرائم الكمبيوتر، أو الجرائم الإلكترونية، أو الجرائم المعلوماتية[3]، وعموما جميع هذه المصطلحات ترتبط بالتقنية المعلوماتية عند ارتكابها.

كما يجب التفرقة بين الجرائم المعلوماتية بالمعنى الفني عن بقية الجرائم الأخرى، التي يستخدم فيها الحاسب الآلي عموما والانترنت خصوصا كأداة لارتكابها.

فجرائم الانترنت وشبكات المعلومات يقصد بها الدخول غير المشروع إلى الشبكات الخاصة كالبنوك والمؤسسات وكذا الأفراد، والقيام بالعبث في البيانات الرقمية التي تحتويها شبكة المعلومات مثل تغيير البيانات أو إتلافها أو محوها، امتلاك أدوات أو كلمات المرور السرية لتسهيل ارتكاب الجرائم التي تلحق أضرار بالبيانات والمعلومات ذاتها، وكذلك بالنسبة للبرامج والأجهزة التي تحتويها، بينما الجرائم التقليدية الأخرى كغسل الأموال، الإرهاب، الدعارة، تجارة المخدرات، والاستخدام غير المشروع لبطاقات الائتمانية، فيعتبر الانترنت أداة لارتكابها وليست ضمن جرائم الانترنت بالمعنى الفني وإن كان يطلق عليها الجرائم المعلوماتية[4].

وعليه، تعتبر الجرائم المعلوماتية مجموعة من الجرائم الجنائية التي ترتكب عن طريق شبكة

---

(1) نهلا عبد القادر المومني، الجرائم المعلوماتية، ط.1، دار الثقافة للنشر والتوزيع، عمان، 2008، ص. 49.

(2) محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط.1، دار الثقافة للنشر والتوزيع، عمان، 2009، ص.19.

(3) أحمد خليفة الملط، مرجع سابق، ص.96، نقلا عن، هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، د.ط، مكتبة الآلات الكتابية، مصر، 1995، ص.31.

(4) عرشوش سفيان، جرائم المساس بأنظمة الكمبيوتر والانترنيت، ملخص مذكرة التخرج ليسانس، المركز الجامعي خنشلة، معهد العلوم القانونية، 2006، ص.10.

الاتصال بصفة عامة، وعبر الشبكة الإلكترونية العالمية والأنظمة المعلوماتية بصفة خاصة[1].

2- خصائص الجرائم المعلوماتية:

تتميز الجرائم المعلوماتية بخصائص منها ما يتفق مع الجرائم التقليدية ومنها ما يختلف عنها ومن أهمها ما سيتم توضيحه:

أ- خطورة الجريمة المعلوماتية، ذلك أنها تمس مباشرة المؤسسات الاقتصادية من جراء تزايد الخسائر المالية مقارنة بالجرائم التقليدية، ونظرا لاختلاف سلوك هتين الجريمتين، فإن هذا ما يؤدي إلى سهولة ارتكاب جرائم الحاسب الآلي وصعوبة تحديد المشتبه بهم[2].

ب- الجرائم المعلوماتية هي الجرائم التي تتجاوز الحدود، حيث أنه يمكن عن طريق الحاسب الآلي اختراق حواسيب عن بعد بين الدول، بسبب اتساع نطاق المكاني وإمكانية ارتكاب هذا النوع من الجرائم في مناطق إقليمية مختلفة نظرا لارتباطها بتقنية المعلومات وشبكات الاتصال الواسعة، مثلا كأن يرتكب الجاني جريمته المتمثلة في غسل الأموال أو التزوير أو سرقة المعلومات وهو موجود في أوروبا، أما المجني عليه سواء كان الشخص طبيعي أو معنوي موجود في الولايات المتحدة الأمريكية، ولهذا فالجريمة المعلوماتية تتميز بأنها تتخطى حدود الدول[3].

ج-صعوبة الكشف وإثبات الجرائم المعلوماتية، إن الجريمة المعلوماتية تمثل اعتداء على برامج وبيانات الحاسب الآلي، سواء بالتغيير أو المحو أو التعديل كليا أو جزئيا في الملفات المخزنة داخل نظام الحاسب الآلي، ويقوم الجاني بهذه الأفعال بسرعة فائقة وفي مدة قصيرة لا تتعدى الثواني لذا يكون من الصعب اكتشاف الجريمة، وغالبا ما تكون للصدفة دور رئيسي في اكتشاف الجريمة الإلكترونية[4]، وهناك أيضا صعوبة تتعلق بإثبات الجريمة المعلوماتية، باعتبارها لا تترك آثار مادية ملموسة ولا أدلة كتابية، بالتالي تحتاج الجرائم المعلوماتية إلى دراية فنية وطرق خاصة لإثباتها مما يستلزم خبرة فنية من طرف القاضي ورجال الشرطة وأعوان الضبط القضائي من خلال التعليم والتأهيل لأساليب البحث والتحري في تقنية المعلومات لتجسيد الجهود المبذولة من طرف الدول بغية

---

(1) Lehir (Yves), Périllat- Amédé (Frédéric), les E.SC.I Enquêteurs spécialisé en 12 / 2008, SRPJ deToulouse,P.9.www.Ossir.org/resist /supports/cr/20081118/RESIST_2008-11-les- ESCI.PDF.

(2) محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط. 1، د.د.ن، د.ب.ن، 2007، ص.75.

(3) محمود أحمد عبابنة، مرجع سابق، ص. 34.

(4) عادل يوسف عبد النبي الشكري،" الجريمة المعلوماتية وأزمة الشرعية الجزائية "، ع. 7، كلية القانون، جامعة الكوفة، 2008، ص. 116.

مكافحة الجرائم المعلوماتية[1].

د- تتم الجريمة المعلوماتية أثناء عملية المعالجة الآلية للبيانات، حيث أنها لا تنتفي في أيَ مراحلها سواء أثناء إدخال البيانات، أو أثناء المعالجة، أو في مرحلة إخراج المعلومات[2].

و-يقوم بهذا النوع من الجرائم مجرمون يتمتعون بمعرفة وخبرة فنية عالية وأساليب احترافية[3] فالذكاء هو الركيزة الأساسية لارتكابها، بالإضافة إلى أن أهم دوافع الجاني لارتكاب جرائم الانترنت هو الربح المادي أو الانتقام أو في بعض الأحيان بدافع حب المغامرة واكتشاف إلى ما يمكن أن يتوصل إليه الذات[4]. لهذا فالجريمة المعلوماتية تختلف عن الجريمة التقليدية لأن الأولى جريمة من ذوي الياقات البيضاء، إذ أنها لا تحتاج إلى العنف أو سفك الدماء، وإنما كل ما تحتاج إليه قدرة عقلية ومعرفة بتكنولوجيا وتقنية المعلومات التي تؤهلهم إلى ارتكاب مثل هذا النوع من الجرائم[5].

ثانيا-الجرائم المعلوماتية في إطار القانون الجزائري:

نظرا إلى أن استخدام الحاسب الآلي وشبكة الانترنت قد يشكل خطرا باعتبار أن سوء استخدامها يتولد عنه ارتكاب جرائم يصعب إثباتها، مما أدى بالمشرع الجزائري إلى التدخل استنادا إلى مبدأ الشرعية الجنائية " لا جريمة ولا عقوبة إلاَ بنص"، حيث جرَم بعض صور الجريمة المعلوماتية وعاقب مرتكبيها ضمن القانون رقم **(15/04)** المعدل والمتمم للأمر رقم **(66/ 154)** المتضمن قانون العقوبات الجزائري، وذلك في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"[6].

وبالتالي يمكن تعريف نظام المعالجة الآلية للمعطيات بأنه مجموعة من المكونات المادية التي تشمل وحدتي الإدخال والإخراج وأجهزة التشغيل، والمكونات المعنوية التي تضم البرامج المستخدمة

---

[1] خالد ممدوح إبراهيم، الجريمة المعلوماتية، ط. 1، دار الفكر الجامعي، الإسكندرية، 2009، ص.79-81.

[2] عادل يوسف عبد النبي الشكري، مرجع سابق، ص. 115.

[3] قارة أمال، مرجع سابق، ص.24.

[4] خالد ممدوح إبراهيم، الجريمة المعلوماتية، مرجع سابق، ص.81.

[5] قارة أمال، مرجع سابق، ص.25.

[6] أنظر القسم السابع مكرر من القانون رقم **15/04** المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، ج.ر.ج.ج.**ع.71**، يعدل ويتمم الأمر رقم **66/ 156** المؤرخ في 18 ضفر عام 1386 الموافق 8 يونيو 1966، ج.ر.ج.ج.**ع.49**، المتضمن قانون العقوبات الجزائري.

لمعالجة البيانات والمرتبطة بشبكات الإلكترونية[1].

ولقد تضمنت المواد من (**394 مكرر**)إلى (**394 مكرر 7**) من قانون العقوبات الجزائري عدة صور للجرائم المعلوماتية، نوضحها فيما يلي:

1- جريمة الدخول أو البقاء عن طريق الغش في المنظومة المعالجة الآلية للبيانات:

يعرف الدخول غير المشروع على أنه إساءة استخدام الحاسب الآلي من طرف شخص غير مصرح له الدخول إليه، وذلك في سبيل الوصول إلى معلومات أو معطيات مخزنة للإطلاع عيها أو لمجرد التسلية[2].

ويعرف البقاء غير المشروع بأنه: " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام".

وجريمة الدخول أو البقاء غير المشروع في صورتها البسيطة وفقا للفقرة الأولى من المادة (**394 مكرر**) من قانون العقوبات الجزائري هي جريمة عمدية، والتي تقوم على القصد الجنائي العام المتمثل في العلم والإرادة ولا تستوجب قصدا جنائيا خاصا[3]، وفي حالة أن نتج عن الدخول أو البقاء غير المصرح به محو أو تعديل البيانات داخل النظام أو عدم قدرة النظام عن تأدية وظيفته، مع وجود علاقة سببية بين الدخول أو البقاء غير المشروع والنتيجة المحققة، ترتب على ذلك تشديد العقوبة لهذه الجريمة[4].

أماَ بالنسبة للعقوبات المقررة لهذه الجريمة، فيعاقب كل من يدخل أو يبقى داخل النظام المعالجة الآلية للمعطيات أو في جزء منه عن طريق الغش بالحبس من ثلاثة(**03**) أشهر إلى سنة(**01**) وبغرامة من **50.000** دج إلى **100.000** دج، فإذا ترتب عن الدخول أو البقاء غير المشروع تغيير أو حذف أو تعديل تضاعف العقوبة، أمَا إذا نتج عن الدخول أو البقاء غير المصرح به تخريب للنظام من جراء التغيير أو الحذف أو التعديل فتشدد العقوبة بالحبس من (**06**)أشهر إلى سنتين وبغرامة من**50.000** دج

---

(1) Bouder (Hadjira), Protection des systèmes d'information, aspects juridiques, Centre de recherche sur l'information Scientifique et Technique, p. 18.

انظر الرابط الإلكتروني: www.mptic.dz/fr/IMG/BOUDER.PDF.

(2) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د.ط.، دار الجامعة الجديدة، الإسكندرية، 2007، ص.111.

(3) جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، د.ط.، دار هومه، الجزائر، 2012، ص.111.

(4) مرجع نفسه، ص .113، 114.

إلى **150.000** دج[1].

2- جريمة التلاعب في نظام المعالجة الآلية للمعطيات:

نصت المادة (**394 مكرر$_1$**) من قانون العقوبات الجزائري على أنه: " يعاقب بالحبس من ستة **06** أشهر إلى ثلاث **03** سنوات وبغرامة من **500.000** دج إلى **2.000.000** دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[2].

وعليه، يبدو واضحا أن هدف الجاني في هذه الجريمة هو الوصول إلى نتائج أو معطيات غير تلك المرجوة من النظام المعلوماتي، كما يجدر الذكر أن المعلومات يقتصر التجريم فيها على البيانات التي تم معالجتها، ويتمثل السلوك الإجرامي في هذه الجريمة بكل من فعل الإدخال غير المشروع داخل نظام المعالجة الآلية للبيانات، فعل محو البيانات وفعل التعديل بطريقة غير مشروعة، ولا يشترط لقيام الركن المادي للجريمة أن تقع هذه الأفعال شاملة، بل يكفي قيام إحداها لقيام الجريمة[3].

ولقد حرص المشرع الجزائري على مكافحة وقمع الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من **1.000.000** دج إلى **5.000.000** دج على كل من يقوم عمدا وبنية التحايل على التعامل في معطيات صالحة لارتكاب الجريمة سواء كان بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق النظام المعلوماتي لارتكاب الجرائم المنصوص عليها في المواد (**394 مكرر**) و(**394 مكرر$_1$**)، كما تعاقب ذات المادة على التعامل في معطيات متحصلة من الجريمة بطريقة غير مشروعة سواء بالحيازة أو الإفشاء أو النشر أو استعمال المعطيات مهما كان الهدف منه من إحدى الجرائم المنصوص عليها في المادتين السالفتي الذكر[4].

وقد عزز المشرع الجزائري الحماية الجنائية لجرائم المتعلقة بأنظمة المعالجة الآلية للبيانات حيث أضاف أحكام مشتركة بين الجرائم المنصوص عليها من المواد (**394 مكرر**) إلى(**394 مكرر$_2$**) من نفس القانون.

---

[1] أنظر المادة 394 مكرر من ق.ع.ج.

[2] أنظر المادة 394 مكرر 1 من ق.ع.ج.

[3] جباري عبد المجيد، مرجع سابق، ص.116.

[4] أنظر المادة 394 مكرر 2 من ق.ع.ج.

فتضاعف العقوبة إذا ارتكبت تلك الجرائم على الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام مع عدم الإخلال بتطبيق عقوبات أشد، أما بالنسبة لعقوبة الشخص المعنوي المرتكب للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات فتضاعف الغرامة عن خمس مرات الحد الأقصى لما هو مقرر بالنسبة للشخص الطبيعي، كما قد نص أيضا المشرع الجزائري بالعقاب على الاتفاق الجنائي الذي يهدف إلى التحضير للجرائم الماسة بالأنظمة المعلوماتية، وعليه فقد خرج عن القاعدة العامة المتمثلة في أنه لا عقاب على الأعمال التحضيرية، وذلك رغبة من المشرع تقرير حماية وقائية لنظم المعالجة الآلية للمعطيات لما يشكله الاتفاق الجنائي من خطورة، وكذلك يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في القسم الخاص بجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات وذلك بالعقوبات المقررة للجنحة.[1].

بالإضافة إلى تقرير المشرع الجزائري لعقوبات تكميلية تتضمن وفقا للمادة (**394 مكرر6**) من نفس القانون ما يلي:

-مصادرة الأجهزة والبرامج وكل الوسائل المستخدمة لارتكاب الجريمة مع إغلاق المواقع التي تكون محلا للجريمة.

-إغلاق المحل أو مكان الاستغلال وذلك في حالة ارتكاب الجريمة بعلم مالكه.[2]

فضلا على أن القانون الجزائري استحدث نصوص خاصة تتعلق بالنظم المعلوماتية في القانون رقم(**09-04**) الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث قضت الفقرة الأولى من المادة (**02**) منه على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يقصد بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي حددت في قانون العقوبات وأيّ جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[3].

ومن تطبيقات الجرائم المعلوماتية في القانون الجزائري، ما قامت به مصالح الدرك الوطني بحيث عالجت خلال التسعة الأشهر الأخيرة **21** قضية متصلة بجرائم معلوماتية، يأتي في بدايتها قرصنة المواقع الإلكترونية والمساس بأنظمة البيانات وكذلك محاولات النصب والاحتيال عبر الشبكة

---

[1] انظر المواد 394 مكرر 3، 394 مكرر 4، 394 مكرر 5، 394مكرر7 من ق.ع.ج.

[2] أنظر المادة 394 مكرر 6 من ق.ع.ج.

[3]أنظر الفقرة الأولى من المادة 2 من قانون 09- 04 المؤرخ في 05 أوت 2009.

العالمية الانترنت، بالإضافة إلى قضايا الاعتداء على الحياة الفردية الخاصة عبر مواقع التواصل الاجتماعي والبريد الإلكتروني[1].

الفرع الثاني

مراحل الدليل الرقمي في الإثبات الجنائي

سبق وأن تم الذكر أن الدليل الرقمي يمر بعدة مراحل وهي: مرحلة التحريز، مرحلة التحليل، مرحلة التقديم والعرض، وأخيرا مرحلة القبول، والتي سيتم إيضاحها كما يلي.

أولا- مرحلة التحريز:

يتم في هذه المرحلة التحريز والاحتفاظ بالأدلة الموجودة عن طريق إرسالها إلى المختبر الجنائي بطريقة لا تمكنها من التلف أو الكسر أو الإفساد، كما يتم أيضا التقاط الصور الفوتوغرافية أو بواسطة الفيديو لجميع أثار الجريمة كالحواسب وملحقاتها والبصمات وكل الأشياء التي تفيد في إظهار الحقيقة، والتي تم العثور عليها في مسرح الجريمة المعلوماتية، وأثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أيّ نوع من البيانات يمكن من خلالها الحصول على دليل جنائي رقمي، وعليه الحفاظ على النظام الرقمي وكامل القيم الرقمية ليتم تحديد الضرورية منها لاستخلاص الدليل لاحقا، وكذلك يستلزم نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة إلى الحاسب الخاص بالمختبر الجنائي الرقمي للاعتماد عليها، بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه[2].

ثانيا- مرحلة التحليل:

يتم في هذه المرحلة القيام بالفحص والتحليل لجميع الآثار المرتبطة والمستمدة من مسرح الجريمة، ويشمل ذلك القيم الرقمية لتحديد نوع الدليل، حيث يتم الفحص في محتويات الوثائق والملفات والمسارات واستعادة المحتويات التي تم حذفها، ويجب أن يتم الفحص بالصيغة العلمية عن طريق استخدام البرامج والتطبيقات الخاصة بتحليل نظام الملفات والمسارات، بالإضافة إلى ذلك يمكن من خلال تحضير قائمة البيانات المحذوفة وعرض البيانات المخزنة على شكل (Format) للاستفادة منها

---

[1] محمد الفتاح خوخي، " جريمة إلكترونية خلال 9 أشهر "، جريدة الخبر، الجزائر يوم الأحد 17 مارس 2013، أنظر الرابط الإلكتروني:

http://www.elkhabar.com/ar/ nas/ 327408- html

[2] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص. 124.

والأمر المهم جدا في هذه المرحلة وجوب قيام الفحص والتحليل على نسخ مطابقة الأصل لعدم تغيير خصائص الملفات، حيث يتم الحفاظ بالنسخة الأصلية المضبوطة من أجل التحقيق والتدقيق على أن البيانات الموجودة مطابقة للأصل ولم يطرأ عليها أي تغيير أو حذف.

ويهدف من وراء قيام عملية الفحص والتحليل إلى استنباط ثلاثة أنواع من الأدلة:

-دليل الإدانة (Iculpatory Evidence)، ويعد الدليل المؤكد والمستند إلى وجود فكرة معينة على ارتكاب وإسناد الجريمة محل التحقيق.

-دليل البراءة (Exculpatory Evidence) ويعتبر الدليل الذي يخالف فكرة ارتكاب الجريمة موضوع التحقيق.

دليل محايد (Evidence Tampering)، هو الدليل غير المرتبط لا بالإدانة ولا بالبراءة، بل يستعان به في إثبات أنه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته أو الاستعانة به كدليل.[1]

ثالثا- مرحلة التقديم والعرض:

هي المرحلة التي يتم من خلالها تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة.

ويستلزم الأمر موثوقية الأدلة الجنائية الرقمية لضمان مصداقيتها، حيث أنه يمكن توثيق الأدلة الجنائية الرقمية بالعديد من الوسائل المختلفة منها التصوير الفوتوغرافي، التصوير بالفيديو والقيام بنسخ الملفات المخزنة في الأقراص أو في الحاسب الآلي، كما يستوجب أيضا تدوين التاريخ والوقت وتوقيع الشخص الذي قام بإجراء الحفظ عند حفظ الأدلة الرقمية، بالإضافة إلى اسم ونوع نظام التشغيل والمعلومات المسجلة في الملف المحفوظ وقسم البرنامج أو الأوامر التي استعملت في إعداد النسخ.

فالتوثيق يفيد تأكيد مصداقية الدليل وعدم القيام بتعديله أي تغييره، مثل شهادة الأفراد المسؤولين عن جمع الأدلة بمطابقة الأدلة التي قاموا بتحصيلها والحفاظ عليها مع تلك الأدلة المقدمة والمعروضة لجهة الحكم، كذلك يمكن الاستفادة من التوثيق في حالة إعادة تكوين مسرح الجريمة، باعتبار أن أجهزة الحاسب الآلي وملحقاتها تتشابه مما يصعب إعادة تنظيمها في حالة انعدام وجود توثيق فوتوغرافي أو

---

[1] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص. 125.

توثيق الفيديو سليم ومفصل يقوم بتحديد الأجزاء والمكونات بأوضاعها وحالتها الأصلية بدقة، وبالتالي يعتبر التوثيق من ضمن إجراءات حفظ الأدلة إلى غاية الانتهاء من إجراءات التحقيق والمحاكمة لاحتوائه على تحديد دقيق على الجهات التي تحتفظ بالأدلة، بالإضافة إلى إعداد رسالة التصنيف الحسابي والتي تستعمل لمضاهاة الأدلة الجنائية الرقمية الرسمية مع النسخ من أجل التأكد من صحتها وأنها لم تتعرض للتحريف أو التعديل، فهي تعتبر مجموعة من الأحرف والأرقام المركبة والمنظمة بصيغة حسابية خاصة تمثل كل نوع من البيانات الرقمية، ففي حالة إدخال ملف الدليل الرقمي على رسالة التصنيف تكون قراءة الملف مطابقة لقراءة النسخة الأصلية لنفس الملف بالأحرف والأرقام، أما في حالة تحريف أو تعديل في النسخة فنتيجة المضاهاة تكون قراءة مختلفة ومغايرة للنسخة الأصلية[1].

رابعا- مرحلة القبول:

إن أمر قبول الأدلة الجنائية الرقمية المستخرجة من الوسائل الإلكترونية في المحاكم يعتمد على المبادئ القانونية التي تنظم عملية الإثبات أمام تلك المحاكم، وبعبارة أخرى أن سلطة القاضي الجنائي في تقدير أدلة الإثبات تختلف من دولة إلى أخرى حسبما تخضع له قواعد الإثبات في كل دولة، حيث يتضح وجود نظامين للأدلة الإثباتية، نظام الإثبات المحدد أو المقيد وأطلق عليه أيضا نظام الأدلة القانونية أين تكون الأدلة فيه محصورة ومقيدة مسبقا من طرف المشرع، أما النظام الثاني هو نظام الأدلة الإقناعية والمسمى أيضا بحرية الاقتناع.

إذن فإن مرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوف إلى مدى توافر هذا الدليل في النصوص القانونية بالنسبة لنظام الإثبات المحدد، وإلى مدى اقتناع القاضي الجنائي بالدليل الرقمي بالنسبة لنظام الأدلة الإقناعية[2]، لذلك سنتناول هذا الأمر بالتفصيل في المبحث الثاني.

المبحث الثاني

تقدير الدليل الرقمي أمام القضاء الجزائي

تعد مرحلة المحاكمة من أهم إجراءات الدعوى باعتبارها مرحلة حاسمة، إذ تعتبر عملية تقدير الأدلة جوهر الحكم، وليس باستطاعة القاضي إدراكه والوصول إليه إلاَ بعد ممارسته لسلطته التقديرية للأدلة محل الوقائع، فيتوقف سلامة الحكم على سلامة تقدير الأدلة، ويعتبر الدليل الرقمي كباقي الأدلة

---

[1] سيدي محمد لبشير، مرجع سابق، ص. 87، 88.

[2] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص. 128،127.

يتم تقديره من طرف القاضي الجنائي، غير أنه لا يستطيع هذا الأخير أن يقوم بتقدير هذا الدليل إلاَ إذا كانت المحكمة المرفوع أمامها الدعوى صاحبة الاختصاص بالفصل في الجريمة المعلوماتية.

وعليه تواجه الجريمة المعلوماتية العديد من المشكلات المتمثلة في تحديد القانون الواجب التطبيق والمحكمة المختصة بالنظر في تلك الجرائم، سواء على النطاق الداخلي أو على المجال الخارجي، ذلك أن المجرم المعلوماتي لا يحتاج إلى الحركة من مكانه أمام جهاز حاسوبه، فبإمكانه أن يقترف الجريمة في بضع ثواني من مكان تواجده وارتكاب أفعاله الإجرامية وتحقيق نتائج تلك الأفعال في أكثر من دولة، لأن الانترنت لا يعترف بوجود حدود بين الدول، فهو إذن لا يتقيد بحدود جغرافية وسياسية[1]. وعلى ذلك سنتناول قبل كل شيء المشكلات التي يثيرها الاختصاص القضائي في الجريمة المعلوماتية في المطلب الأول ثم نأتي إلى سلطة القاضي الجنائي في تقدير الدليل الرقمي في المطلب الثاني.

المطلب الأول

مشكلات الاختصاص القضائي في الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية من الجرائم التي تثير مشكلة الاختصاص القضائي على المستوى المحلي أو الدولي، وتعني مشكلة الاختصاص المحلي في الجرائم المعلوماتية تنازع الاختصاص بين أكثر من جهة قضائية داخل إقليم الدولة، أما مشكلة الاختصاص الدولي تعني تنازع الاختصاص بين أكثر من دولة[2]، وهذا ما سيتم تناوله من خلال ما يأتي:

الفرع الأول

الاختصاص القضائي الداخلي

يسمى هذا النوع من الاختصاص بالاختصاص الداخلي أو الإقليمي، بحيث يختص القضاء الوطني في الفصل في الدعوى الجزائية دون سواه، كما يقوم بتحديد إطار جغرافي أو دائرة اختصاص مكاني تتحدد بمنطقة معينة من إقليم الدولة، لهذا ينقسم الاختصاص المكاني أثناء ارتكاب الجريمة إلى مكان وقوع الجريمة، أو مكان إقامة المتهم، أو مكان القبض على المتهم[3].

---

[1] أحمد عبد الكريم سلامة، "الانترنت والقانون الدولي الخاص"، بحث مقدم إلى مؤتمر القانون والانترنت الذي انعقد بجامعة الإمارات العربية المتحدة، من 1-3 مايو 2000، ج.3، ط.3، 2004، ص.38.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 374.

[3] حسني الجندي، شرح قانون الإجراءات الجزائية، د.ط.، د.د.ن، د.ب.ن، 1990، ص. 687.

وقد قضت المادتين **(37)** و**(329)** من قانون الإجراءات الجزائية الجزائري على أن الاختصاص القضائي المكاني يتطلب توافر حالة من الحالات التالية:

-أن يكون إقامة المتهم أو أحد شركائه المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، ويتحدد مكان الإقامة بوقت وقوع الجريمة.

-أن يكون القبض قد ألقي على أحد المتهمين أو المشتبه بهم في نطاق تلك الدائرة[1].

وتثار مشكلة الاختصاص القضائي المحلي بالنسبة لجرائم المعلوماتية في حالة ما إذا ارتكبت الجريمة في أكثر من نطاق اختصاص محلي داخل الإقليم الوطني للدولة، بسبب طبيعة الجريمة وشبكة المعلوماتية، فالجريمة في هذه الحالة سواء تمثلت بجريمة الدخول أو إتلاف بيانات الحاسب الآلي أو أنظمة المعالجة الآلية للمعطيات وغيرها، قد وقعت بكامل أركانها في نطاق اختصاص المحاكم الجزائرية.

والحل المناسب لهذه المشكلة هو تمديد الاختصاص القضائي داخل إقليم الدولة بما يتناسب وطبيعة الجريمة المرتكبة، إذ يمكن تطبيق أيّ قاعدة من قواعد الاختصاص سواء إقترفت بمكان وقوع الجريمة، أو بمحل إقامة المتهم أو المشتبه به، أو بمكان القبض عليه، فينعقد الاختصاص للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها، فإذا نظرت محكمة محل إقامة المتهم في قضية فتكون مختصة بالنظر فيها دون غيرها، ولها أن تمدد الاختصاص بشأن اتخاذ أي إجراء من إجراءات المحاكمة، بشرط أن يكون التمديد بموجب نص قانوني[2].

وهذا ما جعل القانون الجزائري يمدد الاختصاص القضائي بالنسبة لبعض الجرائم التي نصت عليها المواد **(37)**، **(47)**، **(80)** و**(329)** من قانون الإجراءات الجزائية الجزائري.

حيث تضمنت الفقرة الثانية من المادة **(37)** من هذا القانون على إجازة تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى في جرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كما أجازت المادة **(47)** من نفس القانون لقاضي التحقيق القيام بعملية تفتيش أو حجز ليلا أو نهارا في جرائم محددة، منها الجرائم الماسة بأنظمة المعالجة الآلية للبيانات، وذلك في أي مكان على امتداد التراب الوطني أو يأمر ضابط الشرطة القضائية المختص

---

[1] أنظر المادتين 37 و329 من ق.إ.ج.ج.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 375، 376.

بذلك، بالإضافة إلى نص المادة(**329–3**) من القانون السالف الذكر والتي سمحت بتمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى في بعض الجرائم من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]، ومن خلال النصوص القانونية السابقة يتضح أن التشريع الجزائري قد حسم المشكلة بالنسبة لتنازع الاختصاص القضائي بين الجهات داخل الإقليم الوطني للدولة، وهذا الاختصاص يتحدد من خلال ما يلي:

1–بنطاق ضرورة التحقيق، حيث نصت المادة (**80**) من هذا القانون على أنه يجوز لقاضي التحقيق أن يقوم بجميع إجراءات التحقيق في نطاق اختصاص المحاكم المجاورة لنطاق اختصاصه وفق الشروط التالية:

أ–ضرورة الانتقال خارج نطاق اختصاصه المكاني.

ب–إخطار وكيل الجمهورية بدائرة اختصاصه.

ج–إخطار وكيل الجمهورية بدائرة اختصاص المحكمة التي يستقبل إليها.

د–تبيان الأسباب التي جعلته يمدد دائرة اختصاصه المكاني في محضر المعاينة.

2–كما يحدد الاختصاص وفقا لجرائم أخرى باعتبارها تشكل خطورة على أمن المجتمع، منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بحيث يمكن لوكيل الجمهورية تمديد اختصاصه المحلي إلى دائرة اختصاص محاكم أخرى، وكما أن لقاضي التحقيق أن يقوم بإجراء معاينة أو تفتيش أو حجز على امتداد التراب الوطني، وكذلك يجوز تمديد اختصاص المحكمة إلى نطاق اختصاص محاكم أخرى[2]، كما سبق الذكر.

ولم يقتصر المشرع الجزائري تمديد الاختصاص القضائي على هذه الجرائم، بل أجاز تمديد الاختصاص والقيام ببعض الإجراءات عن بعد في حالة أن تطلب الأمر تفتيش وحجز المعطيات في المنظومة المعلوماتية عن بعد ، حيث نصت المادة (**05**) من قانون رقم (**09–04**) على أنه: "... إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك"[3].

---

[1] أنظر المواد 37، 47، 80، 329 من ق.إ.ج.ج.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 377، 378.

[3] أنظر الفقرة الثانية من المادة 05 من القانون رقم 09–04 المؤرخ في 2009/08/05.

الفرع الثاني

الاختصاص القضائي الدولي

يعد الاختصاص القضائي الدولي بالنسبة للجرائم المرتكبة في نطاق المعلوماتية أكثر مشكلة بما عليه الوضع على مستوى إقليم الدولة الواحدة، على أساس أن الدولة بإمكانها وضع حد للمسألة كما سبق الذكر، على خلاف مشكلة الاختصاص القضائي على المستوى الدولي، باعتبار أن هذه الجريمة عابرة للحدود، بالإضافة إلى اختلاف التشريعات والنظم القانونية من دولة لأخرى، فقد يحدث أن ترتكب الجريمة في إقليم دولة ما من قبل أجنبي، وفي هذه الحالة تخضع الجريمة لاختصاص الدولة الأولى استنادا إلى مبدأ الإقليمية، وكما تخضع لاختصاص الدولة الثانية على أساس مبدأ الشخصية وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية[1]، وهذا ما سيتم تفصيله فيما يلي:

أولا- الاختصاص القضائي الإقليمي:

تختص المحاكم الجزائية في الدولة بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيّا كانت صفة الشخص المتهم وبغض النظر عن جنسيته.

غير أن لهذا المبدأ- الإقليمية- استثناءات منها: عدم تطبيقه على رؤساء الدول ورجال السلك الدبلوماسي، إضافة إلى الاعتراف ببعض الأحكام الأجنبية بموجب نص قانوني أو معاهدة دولية.[2]

ويشترط القانون الجزائري لتطبيق مبدأ الإقليمية أن تكون الجريمة أو أحد الأفعال المكون لها قد تم ارتكابها في نطاق الإقليم الوطني للدولة، فيكفي لانعقاد الاختصاص للمحكمة الجزائرية أن ترتكب الجريمة بكامل أركانها في الجزائر أو أيّ فعل من الأفعال المكونة لها، ولا يهم بعد ذلك مكان وجود الجاني[3].

وذات المبدأ- الإقليمية- يطبق على الجرائم المعلوماتية خاصة منها المتركبة بواسطة الانترنت إلاَ أن هذا قد يثير مشكلة تنازع الاختصاص القضائي لأكثر من دولة، كما لو بث الجاني صور ذات

---

[1] جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 1998، ص. 73.

[2] حسني الجندي، مرجع سابق، ص.55.

[3] راجع الفقرة 1 من المادة 03 من ق.ع.ج. و المادة 586 من ق.إ.ج.ج.

الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة، لأن شبكة الانترنت ليس لها مقر في دولة معينة، ولهذا يستطيع الأشخاص من كل دول العالم تبادل الأفكار والمعلومات بكل حرية ولأجل ذلك فهي لا تخضع لرقابة أو سيطرة دولة معينة، مما يؤدي ذلك إلى عدم وجود قانون جنائي يحكمها بل على العكس تتعدد القوانين التي تطبق عليه بتعدد الدول التي ترتبط بها، باعتبار أن القانون الجنائي يتعلق بسيادة الدولة، وهنا تكمن المشكلة، وكذلك تعد إحدى مشكلات الاختصاص القضائي عدم فاعلية المحاكمة عن الجرائم المعلوماتية، نظرا لتدويل الجرائم المرتكبة بواسطة الانترنت، وهذا ما يجعل منعها والعقاب عليها أمرا احتماليا في ظل الوضع الراهن للأنظمة القانونية[1].

بالإضافة إلى أن من الصعوبات التي تؤدي إلى عدم إمكانية تطبيق الاختصاص القضائي القائم على مبدأ الإقليمية في مجال الجرائم المعلوماتية، حالة كون مزود الانترنت تابع لمزود آخر كائن في بلد آخر، أو يكون المزود الرئيسي موجود في دولة بينما المزودات الفرعية في أكثر من دولة، والسؤال الذي يطرح نفسه أيّ من قضاء تلك الدول يكون مختصا، وأيّ من القوانين يكون واجب التطبيق؟[2].

أمام هذه المشكلات استلزم الأمر ضرورة وجود تعاون دولي لإقامة حد لمثل هذه الصعوبات من خلال معاهدات ثنائية أو دولية بما يجعل قضاء الدولة التي بدأت في اتخاذ الإجراءات أو الدولة الأكثر تضررا من الجريمة المعلوماتية هي المختصة، إضافة إلى تفعيل التعاون الأمني بين مختلف المؤسسات الأمنية فيما بينها، أوعن طريق الأنتربول الدولي[3]، بهدف تمكن الأجهزة الأمنية من الحصول على البيانات والمعلومات المتعلقة بتلك الجرائم، وتحديد مكان المجرم في الوقت المطلوب[4].

---

[1] جميل عبد الباقي الصغير، مرجع سابق، ص.42. 58.

[2] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 917.

[3]الأنتربول " جهاز أنشئ سنة 1923 تحت اسم اللجنة الدولية للبوليس الجنائي، ثم تغير اسمه عام 1956 إلى المنظمة الدولية للبوليس الجنائي، وتضم هذه المنظمة 160 دولة من بينها الجزائر ومصر، وتهدف هذه المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة من بينها الجرائم المعلوماتية، راجع عائشة بن قارة مصطفى، حجَية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، د.ط.، دار الجامعة الجديدة، الإسكندرية، 2010، ص. 258.

[4] مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، ط. 1، دار الكتب والوثائق القومية المصرية، القاهرة، 2000، ص.63.

ثانيا- الاختصاص القضائي الشخصي:

إن الاختصاص القضائي القائم على مبدأ الشخصية يقتضي اختصاص الدولة التي يكون أحد أفرادها هو الجاني ويحمل جنسيتها أثناء ارتكابه جريمة في الخارج، وهذا ما يسمى بالاختصاص الايجابي، إلا أن بعض الدول لم تقتصر على جنسية الجاني بل أضافت جنسية المجني عليه كمعيار لتطبيق قضائها على الجريمة التي ارتكبت ضد أفرادها في الخارج وهذا ما يسمى بالاختصاص السلبي.[1].

ولقد أدرج المشرع الجزائري في المادتين **(582)** و**(583)** من القانون السالف الذكر على أنه يطبق النص الجزائي على كل من يحمل جنسية جزائرية، إذا توافرت فيه الشروط اللازمة منها:

-أن يكون الفعل مجرما في كلا من البلدين الجزائري والأجنبي الذي اقترف فيه الجريمة، وأن توصف الجريمة بجنابة أو جنحة وفقا للقانون الجزائري، وكذلك ضرورة عودة المتهم إلى الجزائر، وأن يكون قد حكم عليه بحكم نهائي في الخارج، وأن تثبت قضاؤه للعقوبة في حالة إدانته أو سقطت عنه العقوبة بالتقادم أو حصل العفو فيها، ويشترط أن يكون الجاني وقت ارتكابه الجريمة يحمل الجنسية الجزائرية وعليه يتم النظر في الجريمة المرتكبة من طرف المحكمة المختصة بموجب طلب من النيابة العامة بعد إخطارها من الشخص المضرور أو ببلاغ من سلطات القطر الذي ارتكبت فيه الجريمة.[2]

والجدير بالذكر أن القانون الجزائري لا يعرف الوجه السلبي للاختصاص القائم على مبدأ الشخصية، فجنسية المجني عليه ليست شرطا لتطبيق قضائه على الجريمة المرتكبة في الخارج ضد من يحمل جنسيتها، باستثناء أن تكون الجريمة المقترفة تحمل وصف جناية أو جنحة تكون قد ارتكبت على متن طائرة أجنبية وكان المجني عليه جزائري في حالة أن هبطت في الجزائر بعد وقوع الجناية أو الجنحة أو القبض على الجاني بالجزائر[3].

وبالتالي فالاختصاص القضائي القائم على مبدأ الشخصية يثير العديد من المشكلات في مجال الجريمة بشكل عام والجريمة المعلوماتية بشكل خاص، والتي نوردها فيما يلي:

-لا يطبق اختصاص قضاء الدولة للجريمة المرتكبة في الخارج من طرف من يحمل جنسيـــتها، إذا كان الفعل المجرم لا يحمل وصف جريمة في الدولة التي ارتكـــبت فيها، إذن فالاختصـــاص لا ينعقد

---

[1] فايز محمد راجح غلاب، مرجع سابق، ص.385.

[2] أنظر المادتين 582 و583 من ق.إ.ج.ج.

[3] أنظر الفقرة الثانية والثالثة من المادة 591 من ق.إ.ج.ج.

بالنسبة للمعلومات والصور التي تبث عن الخارج باعتبارها غير مجرمة في بلد المنشأ، مع أنها جريمة في الدول التي يصلها البث، وفي هذه الحالة عندما لا يكون القانون الوطني مختصا بالنظر في الدعوى فتثار المشكلة بالنسبة لمن أصابه الضرر من الجريمة، حيث يجب عليه الانتقال إلى الدولة التي ارتكبت فيها الجريمة لرفع دعواه أين تثار المشكلة بصورة أكبر كون الفعل غير معاقب عليه في هذه الدولة[1].

-إن تنفيذ العقوبات يصطدم بصعوبات كثيرة، ذلك أن العقاب على فعل وقع في الخارج لا يجد أساس له في ظل قلة الدول التي وقّعت على اتفاقية تسليم المجرمين مقارنة بالكم الهائل من الدول التي تتعامل بالانترنت، لذلك فمن الأصلح إيجاد قانون دولي جنائي على غرار القانون الدولي الخاص ليطبق على الجرائم الواقعة على الانترنت أو بواسطتها.[2]

ثالثا- الاختصاص القضائي العيني:

يقوم الاختصاص القضائي القائم على أساس مبدأ العينية بالنظر في جرائم معينة، وهي تلك التي تمس أمنها ومصالحها دون النظر إلى مرتكب الجريمة إذا كان يحمل جنسية الدولة أم لا، وبغض النظر إذا كان مقترفها متواجد في إقليمها أو خارجه[3]، وكما أن أغلب التشريعات تقر مبدأ الاختصاص القضائي العيني للفصل في أيّ قضية تتعلق بمصالحها وأمنها القومي ومن بين تلك التشريعات قانون العقوبات الفرنسي[3].

وقد نص القانون الجزائري على مبدأ العينية في المادة **(588)** من قانون الإجراءات الجزائية التي تضمنت جواز متابعة كل أجنبي قام بالمساس بأمن وسلامة الدولة الجزائرية، ولم يقتصر المشرع الجزائري على هذا النص، بل أضاف من خلال القانون الجديد رقم **(09-04)** الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والذي تضمن في إحدى مواده تمديد الاختصاص القضائي بالنسبة لهذا النوع من الجرائم حيث ورد النص كالتالي:" زيادة على قواعد الاختصاص المنصوص عليه في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف

---

[1] أحمد عبد الكريم سلامة، مرجع سابق، ص.38.

[2] جميل عبد الباقي الصغير، مرجع سابق، ص.51.

[3] فايز محمد راجح غلاب، مرجع سابق، ص. 388.

مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتجية للاقتصاد الوطني.[1]

ومن خلال النصوص السالفة الذكر يتضح أن المشرع الجزائري قد تضمن اختصاص القضاء الوطني في كل من جرائم تزييف النقود والأوراق المصرفية الوطنية إذا ارتكبت الواقعة الإجرامية في الخارج من طرف أجنبي، وكذلك الجرائم التي تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتجية للاقتصاد الوطني، فهذه الجرائم يمكن أن ترتكب بواسطة الانترنت، وذلك في حالة كون الموقع الذي ارتكبت من خلاله الواقعة الإجرامية يقع خارج إقليم الدولة[2]، ومن تلك الجرائم نجد جريمة تسليم أو إفشاء أسرار الدفاع وجريمة الخيانة والتجسس وجرائم التعدي على الدفاع الوطني أو الاقتصاد الوطني وغيرها من الجرائم الماسة بالأمن القومي للدولة.[3]

غير أن تطبيق الاختصاص القضائي القائم على أساس مبدأ العينية يثير العديد من المشكلات التي تعيق تنفيذه، وهي كالتالي:

-مشكلة تعارض الاختصاص بين مبدأي العينية والإقليمية، فهنا تثار مسألة تنازع الاختصاص ما بين الدولة التي ارتكبت فيها الواقعة الإجرامية وفقا لمبدأ الإقليمية، والدولة الأخرى التي تعتبر تلك الجريمة من الجرائم التي يختص بها قضاؤها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على جرمه مرتين.

-يعتبر كل من السلوك والنتيجة شرطي الجريمة في الجرائم المعلوماتية التي ترتكب عن طريق الشبكات، لذلك فكل من محاكم مكان السلوك الإجرامي ومكان تحقق النتيجة الإجرامية مختصة بالنظر في الواقعة الإجرامية[4]، فإذا تم البث مثلا لفيروس معين في مكان معين وتحققت النتيجة الإجرامية المتمثلة في تدمير المعلومات أو التلاعب بالبيانات أو تحويل أموال أو غير ذلك من النتائج في مكان آخر، فإن الاختصاص سيكون للمحكمتين الأولى مكان بث الفيروس والثانية مكان تحقق النتيجة بالإضافة إلى ارتباط مشكلات الاختصاص وتطبيق القانون بصعوبات تتعلق بامتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود في الجرائم المعلوماتية، وما يتطلبه ذلك إلى ضرورة تعاون دولي شامل لتحقيق التوازن بين مستلزمات المكافحة ووجوب حماية السيادة الوطنية[5].

---

[1] المادة 15 من القانون رقم 09-04 المؤرخ في 2009/08/05.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 390.

[3] أنظر المواد 61- 83 من ق.ع.ج.

[4] جميل عبد الباقي الصغير، مرجع سابق ، ص.63.

[5] فايز محمد راجح غلاب، مرجع سابق، ص. 391، 392.

ومن خلال ما تم إيضاحه فإن مشكلة الاختصاص القضائي أصبحت معقدة نظرا لعدم وجود اتفاق دولي ينظم المشكلة، ذلك في ظل ما تتمتع به شبكة المعلوماتية من فقدان السيطرة والرقابة عليها وعلى المعلومات المتداولة عبرها، بالتالي حبذا لو تم إعادة النظر بالنسبة للجرائم المعلوماتية، كما أنه لا مانع من تقرير نص يمكن من خلاله السماح لضباط الشرطة القضائية الانتقال عبر العالم الافتراضي للتعاون مع جهات ضبط دولية خارج مجال اختصاصه المكاني من أجل ضبط الجرائم ذات الطابع الرقمي[1].

المطلب الثاني

سلطة القاضي الجنائي في تقدير الدليل الرقمي

قبل أن يبدأ القاضي الجنائي في تقدير الدليل الجنائي بصفة عامة والدليل الرقمي بصفة خاصة لابد من قبوله أولا للتأكد من مدى صلاحيته وملائمته كدليل إثبات جنائي، ولقبول القاضي الجنائي لهذا الدليل في الإثبات لابد أن يستند على أساس، وهذا الأخير يختلف من نظام لآخر سواء كان نظام لاتيني أو نظام أنجلو سكسوني [2]، وعلى ضوء إختلاف هذين النظامين وجد نظام أخر يجمعهما ألا وهو النظام المختلط، وهذا ما سنتناوله من خلال فرعين:

شروط قبول الدليل الرقمي كدليل إثبات في المواد الجنائية (الفرع الأول)، أساس قبول الدليل الرقمي على ضوء أنظمة الإثبات الجنائية(الفرع الثاني).

الفرع الأول

شروط قبول الدليل الرقمي كدليل إثبات في المواد الجنائية

يتمتع القاضي الجنائي بسلطة واسعة في تقديره لأدلة الإثبات حتى وإن كان دليل رقمي فبإمكانه أن يتحرى عن الحقيقة عن طريق جمع الأدلة دون إلزامه بتفضيل مسبق لدليل معين، حتى وإن تم تحديد مسبق لنوع الأدلة التي لا يجوز الإثبات بغيرها أو كان الدليل دليلا علميا كالدليل الرقمي حيث وضع المشرع للأدلة الرقمية شروط تعد بمثابة صمام أمان تجاه انحراف القاضي عند ممارسته لها، وتضفي عليها المصداقية واقترابها من الحقيقة، وبالتالي قبولها كأدلة إثبات في المواد الجنائية[3].

---

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 823.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص.179،180.

[3] مرجع نفسه، ص.267،268.

فلقبول القاضي الجنائي بالدليل الرقمي وحجية الإثبات به يجب توافر شروط معينة، أولها ضرورة أن يتم الحصول على دليل رقمي مشروع ومقبول، وثانيها ضرورة مناقشة هذا الدليل الرقمي وثالثها ضرورة بلوغ الاقتناع القضائي درجة اليقين، وعلى ذلك سوف نتناول الشروط التي تحكم اقتناع القاضي الجنائي بالدليل الرقمي كما يلي:

أولا- شرط مشروعية الدليل الرقمي:

إن القاضي الجنائي يتمتع بسلطة تقدير الدليل الرقمي المقبول في الدعوى، حيث يشترط لمقبوليته في الدعوى أن يتم الحصول عليه بطرق مشروعة وفقا للأمانة والنزاهة، ذلك أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول، لأن محل الحرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة[1]، وعليه فمشروعية الدليل الرقمي تعد ضمانا كبيرا للحرية الفردية، إذ يترتب على استخدام وسائل غير مشروعة للحصول على الأدلة الرقمية بطلان الإجراءات وعدم صلاحيتها لأن تكون أدلة إدانة في المواد الجنائية، ومن أمثلة الطرق غير المشروعة استخدام الإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة الخاصة بالدخول إلى النظام والوصول إلى الأدلة المتحصلة من الوسائل الإلكترونية[2].

ثانيا- شرط مناقشة الدليل الرقمي:

من أهم القواعد في الإجراءات الجنائية أنه يجب على القاضي أن يبني حكمه على أدلـــة طرحت أمامه لمناقشة الدليل في الجلسة، ويترتب على ذلك أن يكون للدليل أصل ثابت في أوراق الدعـــوى وأن تمنح للخصوم فرصة الإطلاع عليه ومناقشته، وقد قضت المادة **(212-2)** من قانون الإجراءات الجزائية الجزائري على أنه:" لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معـــرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

ولا يختلف ذلك بالنسبة للدليل الرقمي، أيًا كان شكله سواء كانت بيانات معروضة على شاشة الحاسب الآلي، أو معلومات مخزنة على أقراص، أو أشرطة ممغنطة أو مستخرجة في شكل مطبوعات، فجميعها تكون محلا للمناقشة في حالة الأخذ بها كأدلة إثبات أمام المحكمة.

---

[1] عائشة بن قارة مصطفى، مرجع سابق، ص. 268.

[2] علي محمود علي حموده، مرجع سابق، ص. 38.

ويقوم مناقشة الدليل الرقمي على عنصران أساسيان، الأول يتمثل في إتاحة الفرصة للخصوم للإطلاع على الدليل الرقمي والرد عليه، وذلك من أجل احترام حقوق الدفاع وأن يتمكن الخصوم من مواجهة هذه الأدلة والرد عليها، ويتيح مبدأ المواجهة تجسيد ضمانات منها لزوم إحاطة المتهم علما بالتهمة المنسوبة إليه ومنحه الوقت الكافي لتحضير دفاعه والسماح له بالاستعانة بمحامي، ومن ناحية أخرى أثناء عملية المواجهة يسمح لكل طرف من الخصوم تقديم ما لديه من مستندات وسؤال الشهود والخبراء، حيث يمكن طلب اتخاذ أي إجراء يرى القاضي الجنائي أنه مناسبا لإظهار الحقيقة؛ أما العنصر الثاني يتمثل في أن يكون للدليل الرقمي أصل في أوراق الدعوى، وذلك حتى يكون اقتناع القاضي مبني على أساس، بالتالي ألزم المشرع تحرير محضر الجلسة لإثبات وقائع الدعوى الجنائية وأدلتها، وحتى يتمكن كل من قاضي الموضوع أو أحد من الخصوم الرجوع إلى هذا المحضر لتوضيح أي من الوقائع الثابتة به[1]، ولقد أدرج المشرع الجزائري مبدأ المواجهة وأحاطه بضمانات قانونية في المادتين(**100**) و(**101**) من قانون الإجراءات الجزائية[2].

وعليه يترتب من شرط مناقشة الدليل الرقمي أن يكون اقتناع القاضي أثناء إصدار الحكم مبني على عقيدته وليس على اقتناع غيره، فلا يجوز أن يبني اقتناعه استنادا إلى معلوماته الشخصية أو رأي غيره، لأن القناعة المتولدة لدى القاضي هي جزء من مناقشة الأدلة والتي عن طريقها تتضح قوة أو ضعف الأدلة، فيبني القاضي قناعته من خلال الأخذ بها أو باستبعادها[3].

---

[1] عائشة بن قارة مصطفى، مرجع سابق، ص. 271– 273.

[2] نص المادة 100 من ق.إ.ج.ج.: " يتحقق قاضي التحقيق حين مثول المتهم لديه لأول مرة من هويته ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر في عدم الإدلاء بأي إقرار وينوه عن ذلك التنبيه في المحضر فإذا أراد المتهم أن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور كما ينبغي للقاضي أن يوجه المتهم بأن له الحق في اختيار محام عنه فإن لم يختر له محاميا عين له القاضي محاميا من تلقاء نفسه إذا طلب منه ذلك وينوه عن ذلك بالمحضر كما ينبغي للقاضي علاوة على ذلك أن ينبه المتهم إلى وجوب إخطاره بكل تغيير يطرأ على عنوانه ويجوز للمتهم اختيار مواطن له في دائرة اختصاص المحكمة".

المادة 101 منه: " يجوز لقاضي التحقيق على الرغم من مقتضيات الأحكام المنصوص عليها في المادة 100 أن يقوم في الحال بإجراء استجوابات أو مواجهات تقتضيها حالة استعجال ناجمة عن وجود شاهد في خطر الموت أو وجود إمارات على وشك الاختفاء

ويجب أن تذكر في المحضر دواعي الاستعجال".

[3] فايز محمد راجح غلاب، مرجع سابق، ص. 413.

ثالثا- شرط بلوغ الاقتناع القضائي درجة اليقين:

يجب على القاضي أن يصدر الحكم عن اقتناع يقيني بالأدلة المتحصلة من الوسائل الإلكترونية فاليقين هو وجود حقيقة يستنتجها القاضي الجنائي بواسطة المعرفة الحسية بعيدا عن كل غموض أو احتمال وهذا عن طريق معاينة القاضي لهذه الوسائل وفحصها بالمعرفة الذهنية واستقراء النتائج ليتأكد من وجود الحقيقة[1]، فشرط اليقين في أحكام الإدانة هو شرط عام، حيث أنه سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة كالدليل الرقمي، لذلك لابد أن يكون الدليل الرقمي غير قابل للشك، إذ أن هذا الأخير يفسر لصالح المتهم استنادا إلى قاعدة أن الأصل في الإنسان البراءة، فيكفي أن يتشكك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة[2]، وذلك إعمالا بمبدأ تفسير الشك لصالح المتهم كما سبق ذكره، وهو ما أكدته المادة(**45**) من الدستور الجزائري[3].

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالمعرفة الحسية أو العقلية عن طريق التحليل والاستنتاج، فإن الجزم بوقوع الجريمة المعلوماتية ونسبتها إلى المتهم المعلوماتي تحتاج من القاضي نوع آخر من المعرفة، وهي المعرفة العلمية بالأمور المعلوماتية خصوصا أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات، ويؤدي الجهل في هذه الأمور إلى التشكيك في قيمة الدليل الرقمي، وبالتالي يقضي إلى الحكم بالبراءة ويستفيد من هذا الشك المتهم المعلوماتي مما يؤدي إلى إفلات المجرمين من تطبيق العدالة والقانون، ومن ثم يترتب على ثبوت التهمة بلوغ الاقتناع بالإدانة درجة اليقين من طرف القاضي الجنائي لأن الاقتناع ثمرة اليقين[4].

ويعتبر الرأي الغالب في الفقه الكندي مخرجات الحاسوب تتوفر على اليقين المنشود في الأحكام الجنائية، بالتالي هي من أحسن وأفضل الأدلة، كذلك نصت بعض القوانين الأمريكية على اعتبار أفضل الأدلة الممنوحة لإثبات البيانات والمعلومات هي النسخ المستخرجة من البيانات المخزنة في الحاسوب لذلك تعد أفضل الأدلة ويتحقق مبدأ اليقين فيها[5].

---

[1] علي محمود علي حموده، مرجع سابق، ص.37.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص.277.

[3] نصت المادة 45 من الدستور الجزائري على أن : " كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته، مع كل الضمانات التي يتطلبها القانون."

[4] عائشة بن قارة مصطفى، مرجع سابق، ص. 278، 279.

[5] علي حسن الطوالبه، مرجع سابق، ص.8.

الفرع الثاني

أساس قبول الدليل الرقمي على ضوء أنظمة الإثبات الجنائية

يخضع القاضي الجنائي لقبول الدليل الرقمي حسب طبيعة نظام الإثبات السائد في الدولة، وتنقسم هذه الأنظمة إلى النظام اللاتيني، النظام الأنجلوسكسوني، والنظام المختلط، والتي نتناولها فيما يلي:

أولا –النظام اللاتيني:

يطلق على هذا النظام بنظام الإثبات الحرَ، أو نظام الأدلة الإقناعية أو ما يعرف بحرية الإقناع حيث أن في هذا النظام المشرع لا يحدد أدلة الإثبات ووسائله، بل يترك الحرية للقاضي في تأسيس حكمه وفقا لاقتناعه الشخصي بأيّ من الأدلة المتوفرة أمامه وبدون أن يفرض عليه دليل معين، كما أن للقاضي الجنائي أن يقرر قبول أو رفض دليل بشرط أن يكون استنتاجه مطابقا للحقيقة ولا يخرج عن مقتضيات العقل والمنطق[1].

ومن التشريعات الأخذة بهذا المبدأ التشريع المصري والفرنسي، وكذا التشريع الجزائري[2]الذي كرّس مبدأ الاقتناع كأصل في نص المادة **(212–1)** التي نصت على أنه: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص"[3]، لذلك يتضح أن مبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع لفتح مجال لنوع من الأدلة العلمية التي يكتشفها العلم الحديث، وذلك لمواجهة الجرائم المستحدثة كبصمة الصوت، والبصمة الوراثية، والدليل الرقمي خاصة، وبالتالي فهذا الأخير شأنه شأن باقي الأدلة الأخرى[4].

ولقد تطور دور الإثبات العلمي مع ظهور الدليل الرقمي، مما جعل القاضي في هذا النظام يضطر للتعامل مع الأدلة المستحدثة باعتبارها ضرورية تؤدي إلى كشف أنواع جديدة من الجرائم في مقابل نقص الثقافة المعلوماتية، وأكثر من ذلك يزيد من نسبة هذا الاضطرار الصعوبات التي يثيرها هذا الدليل[5].

---

[1] سيدي محمد لبشير، مرجع سابق، ص.88، 89.

[2] عائشة بن قارة مصطفى، مرجع سابق، ص. 181.

[3] الفقرة الأولى من المادة 212 من ق.إ.ج.ج.

[4] عائشة بن قارة مصطفى، مرجع سابق، ص.183.

[5] مرجع نفسه، ص. 239.

ومن النتائج المترتبة على تطبيق هذا المبدأ، تمتع القاضي الجنائي بدور إيجابي في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الرقمي، أي أن القاضي[1] غير مقيد بالأدلة التي يقدمها له أطراف الدعوى، لأن من حقه بل من واجبه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات للتحقيق والتنقيب في الدعوى بحثا عن الأدلة اللازمة لتكوين قناعته على الوجه الصحيح، فلا يكتفي بما قدمه الخصوم من أدلة [2]، كما أن من مظاهر الدور الإيجابي للقاضي الجنائي في استخلاص الدليل الرقمي، توجيه أوامر إلى مزود الانترنت من أجل البحث والكشف عن الحقيقة، كعناوين المواقع الصفحات المطلع عليها من طرف المتهم، الملفات والحوارات التي شارك فيها، الرسائل التي أرسلها أو استقبلها وغيرها من المعلومات، وباستطاعته أيضا أن يأمر مشغل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وكما يمكن للقاضي أن يكلف مشغل النظام بحل رموز لبيانات مشفرة داخل ذاكرة الحاسب الآلي، وكذا أن يأمر بتفتيش نظم الحاسب الآلي عن طريق فحص نظام الاتصال بالانترنت وفحص مركبات الحاسب الآلي وملحقاته، إضافة إلى هذا فإن مرحلة قبول الدليل الرقمي تعد الخطوة التالية بعد البحث عن الدليل وتقديمه من طرف كل من سلطة الإدعاء والمتهم والقاضي، فالقاضي الجنائي أول ما يتأكد منه قبل قبوله للدليل هو مدى صحة ومشروعية الدليل ومصداقيته، وكل هذا قبل الوصول إلى المرحلة الأخيرة ألا وهي مرحلة تقدير الدليل المقبول، لأن القاضي الجنائي لا يقــدر إلا الدليل الرقمي المقبول، ولا يكون كذلك إلاَ إذا كان مشروعا[3].

ثانيا: النظام الأنجلوسكسوني:

يطلق على هذا النظام بنظام الإثبات المحدد أو نظام الأدلة القانونية، حيث تكون فيه الأدلة محصورة ومحددة مسبقا من طرف المشرع، فلا يجوز للقاضي أن يخرج عليها وأن يقوم ببناء الحــكم

---

[1] سواء كان قاضي حكم أو قاضي التحقيق لأن مسألة الإثبات قد تثار في أية مرحلة من مراحل الدعوى الجنائية، بل قد يمكن أن تثور في مرحلة الاستدلالات، راجع عائشة بن قارة مصطفى، مرجع سابق، ص. 192.

[2] يتميز دور القاضي المدني عن القاضي الجنائي، في أن القاضي المدني يتمحور عمله في قبول الأدلة المطروحة عليه من قبل المتعارضين بحيث لا يبادر بنفسه للتنقيب عن الحقيقة، لذلك فإن دور القاضي المدني سلبي مقارنة بالقاضي الجنائي الذي لا يكتفي بما يقدمه الخصوص، بل يكون من حقه ومن واجبه أن يتحرى ويبحث عن الحقيقة بالاستعانة بكل الطرق ووسائل الإثبات المتاحة له سواء نص عليها القانون أم لا، وهذا ما قضت به المادة 212 من ق.إ.ج.ج، عائشة بن قارة مصطفى، مرجع نفسه، ص. 189، 190.

[3] مرجع نفسه، ص. 193، 195.

على خلافها، لذلك ففي حالة توافر شروط الدليل على النحو الذي حدده وقيده المشرع يلزم القاضي الجنائي أن يؤسس حكمه على أساس هذا الدليل حتى وإن لم يكن مقتنعا به، كما أنه إذا ما لم تتوافر الشروط المطلوبة قانونا يكون القاضي ملزما ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الإدعاء، وحتى لو كان القاضي مقتنعا بثبوت الإدعاء[1]، ومن الدول المتأثرة بهذا النظام إنجلترا الولايات المتحدة الأمريكية، أستراليا وجنوب إفريقيا[2].

وتجدر الإشارة إلى أن الدليل في النظام الأنجلوسكسوني تحكمه قواعد خاصة لقبوله أمام المحاكم سواء تعلقت هذه القواعد بمضمون الأدلة من بينها قاعدة استبعاد شهادة السماع، أو تعلقت بكيفية تقديم الأدلة والتي تدعى بقاعدة الدليل الأفضل[3]، وما دام أن الدليل الرقمي يعد من قبل شهادة السماع، لكونه يتضمن أقوالا أو مواد قام بوضعها الإنسان في الحاسوب[4]، فإن هذا ما يطرح تساؤل حول موقع الدليل الرقمي من هذه القواعد، فهل يتم رفضه ومن ثم استبعاده كدليل إثبات جنائي، أم يتم قبوله، وعلى أيّ أساس يكون هذا القبول؟.

إن بعض التشريعات كالولايات المتحدة الأمريكية، إنجلترا، كندا، أستراليا، ترفض الشهادة السماعية في الإثبات الجنائي[5]، غير أن المشرع في الأنظمة الأنجلوسكسونية قد وضع قائمة من الاستثناءات على قاعدة شهادة السماع ومنها البيانات والمعلومات التي تستخرج من الكمبيوتر[6].

والحقيقة أن السبب في عدم الاعتماد على شهادة سماع كدليل في التشريعات التي تبنت النظام الأنجلوأمريكي، يرجع إلى عدم وجود الثقة في الشخص الذي أدلى بها خارج المحكمة، باعتباره لا يؤدي اليمين أمام المحكمة حتى يخضع لملاحظة القاضي أو المحلف وقت إدلائه أو كتابته، وكما لا يسمح للمتهم بممارسة حقوقه الدستورية خاصة منها حق المتهم في المواجهة، مع ذلك هناك حالات استثنائية أين يعتد بشهادة سماع كدليل إثبات في الدعوى الجنائية، ومن بين هذه الاستثناءات البيانات

---

(1) سيدي محمد لبشير، مرجع سابق، ص.88.

(2) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، د.ط.، دار الجامعة الجديدة، الإسكندرية، 2007، ص. 387.

(3) عائشة بن قارة مصطفى، مرجع سابق، ص. 196.

(4) عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 960.

(5) شهادة السماع هي: الشهادة التي يكون الشاهد الذي يدلي بها قد نقل إلى سمعه أن أمرا حدث، فهو لم يشارك أو يشاهد بإحدى حواسه في الواقعة التي تنظرها المحكمة في الجلسة، عمر أبو بكر بن يونس، مرجع نفسه، ص. 958.

(6) عائشة بن قارة مصطفى، مرجع سابق، ص. 198.

والمعلومات التي يتم الحصول عليها من جهاز الحاسوب، لذلك فإن الدليل الإلكتروني يدخل ضمن مجموعة الحالات الاستثنائية عن قاعدة شهادة سماع، ليصبح هذا الدليل مقبولا في الإثبات الجنائي[1].

ويلاحظ أن المشرع الإنجليزي وإن قبل الدليل الإلكتروني في الإثبات الجنائي على أساس أنه استثناء من قاعدة شهادة السماع، إلا أن القضاء الإنجليزي قد قبل هذا الدليل على أساس أنه شهادة مباشرة، ويتبين ذلك من خلال قضية (R.V. Wood) حيث سرقت بعض المعادن التي تم العثور عليها في حيازة المتهم، وكانت تركيبة المادة الكيماوية لهذه المعادن مسجلة في جهاز الحاسوب للمجني عليه وقد قدمت الورقة المستخرجة من الكمبيوتر كدليل إثبات، والسؤال المطروح في هذه القضية هل تعتبر الورقة المستخرجة من جهاز الحاسوب دليلا سماعيا؟، فأجابت المحكمة على أن الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة وتصلح كدليل إثبات، فهي ليست من قبيل الشهادة السماعية[2] كما قضت أيضا محكمة الاستئناف في إنجلترا بقبول الدليل الناتج عن الكمبيوتر في قضية (R.V. Pettingreme) التي اعتبرته شهادة مباشرة وليست سماعية، وتتلخص وقائع هذه القضية أنه وجد لدى حيازة متهم الذي قام بالسطو على البنك أرقام النقود المسروقة والتي كانت مسجلة في كمبيوتر البنك في إنجلترا، حيث أخذت المحكمة من مخرجات الحاسب الآلي الورقية كدليل إثبات مباشر وليست من الأدلة السماعية[3].

وقد تغيرت قاعدة الدليل الأفضل[4] مع ظهور المستندات الإلكترونية والتي قضت في نص المادة **(1002)**من قانون الإثبات الأمريكي بأن حجيّة الكتـــابة والصورة والتسجيل رهن بتقديم الأصل إلا إذا نص على خلاف ذلك، غير أنه في مجال الدليل الرقمـــي فقد قام المشرع المقارن بحسم هذه المســـألة لصالح الدليل الرقمي إذ أن المادة **(1001–1)** من قانون الإثبـــات الأمريكـــي تم تطويرها لكي تشمل الدليل الرقمي، حيث سمحت بالاعتراف بالمواد المكتوبة والمسجـــلة والإلكتـــرونية لكي تحظى بنفس حظوظ الأدلة الأخرى أمام المحاكم، لذلك قام المشـــرع الأمريكي باستعمـــال مدلول أشمـــل للكـــتابة

---

[1] رمزي رياض عوض، حماية المتهم في النظام الأنجلوأمريكي، د.ط، دار النهضة العربية، القاهرة، 1998، ص.34.

[2] شيماء عبد الغاني محمد عطا الله، مرجع سابق، ص.391.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص.204.

[4] يقصد بالدليل الأفضل أنه من أجل إثبات كتابة أو سجل أو صورة، فإن أصل الصورة أو السجل أو الكتابة يكون مطلوبا، كاستناد أحد أطراف الدعوى إلى عدة دعائم فيستوجب عليه أن يختار ويقدم أفضل نموذج لكي يكون دليلا للإثبات، عائشة بن قارة مصطفى، مرجع نفسه، ص. 204.

والتسجيلات ليشمل كل من الحروف أو الكلمات أو الأرقام أو ما يعادلها سواء مكتوبة على يد، أو منسوخة على الأدلة الكتابية، أو اتخذت شكل نبضات مغناطيسية والميكانيكية والإلكترونية، أو أي شكل آخر من تجميع المعلومات، لأجل ذلك تعد الكتابة الموجودة داخل الكمبيوتر في صورة كهرومغناطيسية من قبيل النسخة الأصلية، بالتالي فالمحررات الإلكترونية تعد أصلية، وكما وسع القانون الأمريكي من الدليل الرقمي في نص المادة **(1001-3)** والتي تضمنت أن الدليل الرقمي المستخرج من الطابعة يعد مقبولا كدليل أصلي كامل دون داع لجلب الحاسوب إلى المحكمة للتأكد من أصالة الدليل، وأبعد من ذلك فقد اعترف المشرع الأمريكي بالنسخة طبق الأصل الفورية الصادرة عن الحاسوب في نص المادة **(1001-4)** من قانون الإثبات الأمريكي، واستثناءا قيد المشرع قاعدة قبول النسخة المطابقة للأصل كأصل في حالة ما إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل لكي تحل محل الأصل أو إذا أثير حولها تساؤل جدي يتعلق بأصالتها[1].

ثالثا- النظام المختلط:

لقد حاول هذا النظام التوفيق بين النظامين اللاتيني والأنجلوسكسوني مع تلافي سلبيات كل من النظامين، والمتمثلة في إمكانية تعسف القاضي أثناء استعماله للسلطة التقديرية في الاقتناع بالدليل من عدمه في النظام اللاتيني، وكما أن القاضي في النظام الأنجلوسكسوني يكون دوره سلبيا ومقيدا في مسألة الإثبات لتقييده بالأدلة القانونية[2].

ويقوم هذا النظام بالجمع بين النظامين، وذلك عن طريق تحديد القانون لأدلة معينة للإثبات في بعض الجرائم من خلال تقييد سلطة القاضي في الإثبات، ومثال ذلك منح حجية للمحاضر المحررة في بعض المخالفات بالنسبة لما ورد فيها إلى أن يثبت العكس، وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة، ولقد أخذ المشرع الجزائري بمبدأ حرية الإثبات كأصل في المادة **(212)** من قانون الإجراءات الجزائية، إلاَ أنه يتضح في هذه المادة من خلال عبارة "ما عدا الأحوال التي ينص فيها القانون على غير ذلك " أن المشرع الجزائري استثناء أخذ بمبدأ الأدلة القانونية، حيث أن هناك بعض من الجرائم قد قيد المشرع إثباتها بنصوص خاصة كجريمة الزنا المعاقب عليها في نص المادة **(339)** من قانون العقوبات الجزائري[3]، والتي لا يمكن إثباتها إلاَ بالطرق التي أوردها المشرع على

---

[1] عمر محمد أبو بكر بن يونس، مرجع سابق، ص. 988، 989.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 405.

[3] أنظر المادة 212 من ق.إ.ج.ج. و المادة 339 من ق.ع.ج.

سبيل الحصر في نص المادة **(341)** من نفس القانون[1]، ونفس الشيء بالنسبة للمشرع المصري الذي نص أيضا على وسائل إثبات محددة لإثبات جريمة الزنا.

أما بالنسبة للأدلة الرقمية فقد قضى البعض أن السجلات الإلكترونية تتميز بكونها غير مرئية في ذاتها، بالتالي لا يمكن إسنادها كدليل في المحكمة، إلاَ في حالة تحويلها إلى أدلة مرئية ومقروءة عن طريق مخرجات الطباعة، فتكون مقبولة سواء كانت هي الأصل أو نسخة من الأصل[2].

ولقد اعتبرت بعض التشريعات منها التشريع الفرنسي أن الكتابة الإلكترونية لديها نفس القوة الإلزامية كالكتابة على الورق[3]، وهذا ما حذا به المشرع الجزائري بحيث جعل طريقة الإثبات بالكتابة مقبولة مهما كانت الوسيلة التي تتضمنها وكذا طرق إرسالها، وكما سوى بين الكتابة في الشكل الإلكتروني بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تتضمن سلامتها[4].

وتجدر الإشارة إلى أن القيود التي أوردها المشرع على حرية القاضي في الاقتناع، لا يقصد منها اعتبار أن المتهم مرتكب الجريمة التي نص على إعطائها وسائل إثبات ذو حجية، بل يعفي القاضي من إعادة التحقيق فيها ويظل للقاضي سلطة تقدير هذه الأدلة ليستخلص منها اقتناعه، وكما يبقى المتهم متمتعا بمبدأ افتراض براءته إلى أن يثبت عكس ذلك[5].

من خلال كل هذا يتبين أن ظهور الدليل الرقمي سيغير كثيرا من طرق الإثبات الجنائية بالنسبة للجرائم التي تقع على ملفات ومستندات رقمية، خصوصا أن الدليل الرقمي ذو طبيعة تقنية ويصعب التخلص منه، و في مقابل ذلك فإن محل الدليل الرقمي ألا وهو الجرائم المعلوماتية يتجاوز مداها أحيانا حدود الدولة أو القارات، مما يثير مشـــكلات في قواعد القـــانون الجنائي (الموضوعي والإجرائي) من

---

[1] تثبت جريمة الزنا في القانون الجزائري، إما بناء على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس، وإما بالإقرار الوارد في رسائل أو مستندات صادرة عن المتهم أو بإقرار قضائي.

[2] فايز محمد راجح غلاب، مرجع سابق، ص. 405.

[3] Compagnie National des experts de justice en informatique et techniques associées, op. cit , P.18.

[4] أنظر المواد 323 مكرر، 323 مكرر1 من الأمر 58/75 المؤرخ في 20 رمضان 1395 الموافق ل 26 سبتمبر 1975، المتضمن القانون المدني، ج.ر.ج.ج.ع. 78 الصادرة في 30 سبتمبر 1975، المعدل والمتمم بالقانون رقم 05/07 المؤرخ في 13 مايو 2007. ج.ر.ج.ج.ع. 31 الصادرة في 13 مايو 2007.

[5] علي محمود علي حموده، مرجع سابق، ص. 38.

حيث تنازع الاختصاص القضائي سواء داخليا أو دوليا والتي سبق إيضاحها، بحيث تكون الجرائم المعلوماتية خارج أيّة رقابة أو سيطرة جهة معينة مما يؤدي إلى عدم إمكانية خضوعها لقانون جنائي معين، بالتالي فالأمر يحتاج إلى إبرام اتفاقيات دولية تعمل على التعاون الدولي في المجال القضائي والشرطي لمواجهة مشكلات الاختصاص القضائي الناجمة عن الجرائم المعلوماتية، من ثم فإن عند تحديد الاختصاص في الجريمة المعلوماتية لدولة معينة وتحـــريك الدعوى فيها ومباشرة كل الإجراءات اللازمة للتحقيق إلى أن يتم الحصول على الدليل الرقمي لإثباتها، تأتي بعد ذلك مشكلة مدى قبول الدليل الرقمي ومصداقيته، فلقبول الدليل الرقمي كدليل إثبات أمام المحاكم يجب أن يتوفر على شروط معينة والتي من دونها لا يمكن قبوله، وكما أيضا تتحدد السلطة التقديرية للقاضي الجنائي في قبول الدليل الرقمي من عدمه وفقا لنظام الإثبات السائد في تلك الدولة المختصة بالنظر في الدعوى، كذلك يمكن القول أن التطور العلمي قد يؤثر على نظام الاقتناع القضائي في الكثير من المسائل الفنية التي نتجت عن ثورة المعلومات، مما يزيد من دور الخبرة في المسائل الجنائية بالنظر إلى الكثير من الجرائم التي ترتكب عبر الأنظمة الحاسوبية والانترنت والتي تعتبر من طبيعة فنية بحتة، غير أن السلطة التقديرية للقاضي الجنائي تكون لازمة وضرورية لتنقية الدليل الرقمي من الخطأ والغش حتى تتحول الحقيقة العلمية إلى حقيقة قضائية .

خاتمة

بعد أن فرغنا بحمد الله وتوفيقه من دراستنا لموضوع "الإثبات الجنائي في الجرائم المعلوماتية" فلا ريب أن هذه الجرائم أصبحت تشكل نمطا خطيرا في وقتنا الحالي، نظرا لكون الإثبات فيها صعب المنال، لاعتبار أدلتها الرقمية خفية غير مرئية، وقد حاولنا قدر الإمكان بحث مختلف جوانبه والمشكلات التي أثارها، لذلك يجدر بنا الحال من خلال هذه الدراسة إبراز أهم ما توصلنا إليه.

إذن يتضح أن الجرائم المعلوماتية كانت ومازلت محلا للخلاف الفقهي والقضائي، بالنظر إلى قيمة المعلومات وطبيعتها غير المادية وكذلك من حيث إجراءات التحقيق من التفتيش والضبط الذي قد يكون حتى عن بعد، وطبيعة الأدلة الناتجة عنها، وتعديها للحدود الجغرافية، ومدى شرعية الحصول على الأدلة الناتجة عنها والعمل بها، وتحديد نطاق الاختصاص المكاني المحلي والدولي والقانون الواجب التطبيق، ومدى كفاية النصوص التقليدية الموضوعية والإجرائية لمواجهتها، خاصة في ظل الدول التي لازالت لم تعدل بعد قوانينها ولم تصدر بعد قوانين حديثة لمواجهتها، لذلك فإن الإثبات الجنائي في الجرائم المعلوماتية يتطلب من رجال الضبط القضائي والقضاة أن يكونوا ملمين بالتدابير والإجراءات اللازمة لتأمين مسرح الجريمة المعلوماتية، وضبط وتحريز الآثار الجنائية الرقمية ونقلها بالطريقة العلمية الصحيحة، وهذا ما يستلزم التعاون الكامل بين كل من رجال الضبط القضائي وقاضي التحقيق والخبير، من أجل نجاح عملية ضبط الجريمة وتحريز ونقل الأدلة إلى المخبر وتحليلها ثم تقديمها في شكل ينفي أو يثبت إدانة المتهم، ويؤدي إلى اقتناع القاضي بالحكم الذي أصدره، لأن التعامل مع الدليل الجنائي الرقمي يحتاج إلى معرفة بأصوله وإلى مختبرات رقمية مجهزة بأنواع الأجهزة اللازمة.

ومن هنا يتبين أن أجهزة تحقيق العدالة مازالت بحاجة إلى التدريب الفني والتقني للتعامل مع الجرائم المعلوماتية وتكييفها التكييف القانوني السليم، على خلاف مجرمي التقنية الرقمية الذين يتابعون كل جديد يطرأ على المجال التقني الرقمي ليطوّروا من وسائلهم وأساليبهم الإجرامية، فضلا عن مشكلة تنازع الاختصاص بصدد هذه الجرائم باعتبار أن شبكة الانترنت ليس لها حدود معينة جغرافيا وسياسيا، مما يؤدي إلى وجود فراغ تشريعي في القانون الواجب التطبيق وعدم إمكانية إثبات التهم ضد مرتكبي جرائم الحاسب والانترنت والقبض عليهم ومحاكمتهم، وحتى في حالة إيجاد الحلول من الناحية القانونية كتطبيق القوانين التقليدية على الجرائم المعلوماتية، وذلك بتكييف جرائم السرقة بواسطة الحاسوب إلى جرائم السرقة التقليدية مثلا إلا أن هذه الحلول تضل تصطدم بعقبات عملية

بالنظر إلى الإجراءات المعقدة والطويلة التي يلزم إتباعها لمحاكمة الجاني الذي ارتكب أيّا من هذه الجرائم، ومن العوائق أيضا تنفيذ الأحكام الصادرة عن المحاكم الأجنبية ومن ذلك مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين، وكذلك عدم جواز تسليم المجرمين، بالإضافة إلى عدم وصول التعاون الدولي في مكافحة وضبط جرائم المعلوماتية إلى المستوى المطلوب بسبب عدم وجود تشريعات لمواجهة هذه الجرائم في دول معينة، كما أن الفعل المجرّم في دولة معينة قد يعد مباحا في دولة أخرى.

كما نلاحظ من خلال هذه الدراسة أن الإبقاء على سلطة القاضي الجنائي التقديرية في تقديره لهذه الأدلة العلمية والفنية على الرغم من علو شأنها ضرورية وحتمية لضمان تنقية الأدلة من الأخطاء وجعل الحقيقة العلمية حقيقة قضائية، ويظل القاضي هو الذي يحدد هذه الحقيقة لأن من خلال هذه السلطة يستطيع أن يفسر الشك لصالح المتهم، وكذا استبعاد الأدلة الإلكترونية التي يتم الحصول عليها بطرق غير مشروعة.

أما بخصوص التشريع الجزائري، فإن الإثبات الجنائي في مجال الجرائم المعلوماتية لا يزال قاصرا، بحيث لم يتضمن الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن القانون رقم(09-04) لسنة 2009، ، كما لم ينص على صدور إذن التفتيش مقتصرا على تفتيش الحاسوب، فإذا كان هذا الأخير متواجدا في أحد المساكن يتعين توافر شروط تفتيش المساكن، أما إذا كان الحاسوب في حيازة شخص خارج مسكنه أو كان في سيارته في الخارج، فإنه يكفي توافر شروط تفتيش الأشخاص، وبالنسبة لهذا الأخير فإن المشرع الجزائري لم يتطرق إليه إلا في حالة التلبس بجناية أو جنحة باعتبار القبض يجيز التفتيش وكذا في التحقيق الجمركي، إضافة إلى هذا فإن المشرع لم يتطرق في قانون رقم(09-04) لسنة 2009 إلى كل من الاعتراف والشهادة والاستجواب في مجال الجريمة المعلوماتية.

ومن خلال هذه النتائج نخلص إلى التوصيات التالية:

- من الأولى على المشرع الجزائري تضمين الاستثناء الخاص بوقت التفتيش والأشخاص المطلوب حضورهم ضمن القانون رقم(09-04) لسنة 2009، طالما أن المشرع قد وسع في هذا القانون من صلاحيات سلطات الاستدلال والتحقيق حيال مكافحة الجرائم المعلوماتية، كما أن من الأولى النص على صدور إذن التفتيش مقتصرا على تفتيش الحاسوب، فإذا كان هذا الأخير متواجدا في أحد المساكن يتعين توافر شروط تفتيش المساكن، أما إذا كان الحاسوب في

حيازة شخص خارج مسكنه أو كان في سيارته في الخارج، فإنه يكفي توافر شروط تفتيش الأشخاص، وأكثر من ذلك على المشرع إدراج تفتيش الأشخاص وتحديد كيفية وشروط إجرائه ضمن قانون الإجراءات الجزائية، كذلك عليه إدراج كل من إجراء الاعتراف والشهادة والاستجواب ضمن قانون رقم (09-04) من أجل وضع إمكانية للقاضي الاعتماد عليها للفصل في الدعوى، بالرغم من أن لهذه الإجراءات دور ضئيل في مجال المعلوماتية.

- دعوة المشرع الجزائري إلى إضافة عبارة "المعطيات المعلوماتية" في المادة**(81)** من قانون الإجراءات الجزائية ليتضح صياغة المادة كالتالي:" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية، يكون كشفها مفيدا لإظهار الحقيقة "، وكذا دعوته إلى تعديل نص المادة **(61)** من نفس القانون وذلك بإلغاء عبارة "ضبط" واستبدالها بعبارة "قبض"، لأن هذا الأخير يكون للأشخاص والضبط يكون للأشياء.
- وجوب الاهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم المعلوماتية.
- التطوير المستمر لأدوات التحليل كأدوات نسخ محتويات الأقراص وتخزين البيانات.
- توعية بشكل دائم عن مخاطر الجرائم المعلوماتية وأساليب المجرمين في ارتكابها عن طريق وسائل الإعلام.
- ينبغي على الدول التي لم تجرّم بعد الاستخدام غير المشروع للحاسب الآلي، أن تسارع إلى سن القوانين اللازمة لتجريم هذا النمط من الجرائم العابرة للحدود.
- ضرورة التعاون الدولي لمواجهة الجرائم المعلوماتية، وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرّم صور هذه الجرائم.
- إنشاء وحدات أمنية متخصصة في مكافحة الجرائم المعلوماتية وضبطها.
- وأخيرا تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ عنها في كلية الحقوق والشرطة والمعاهد القضائية، بحيث يشترط في المتقدمين إليه أن يكونوا حاصلين على مؤهل جامعي في علوم الحاسوب والشبكات.

وهكذا يكون البحث قد اكتمل بحمد الله، فإن كان فيه الحسن والصواب فهو من الله سبحانه وتعالى، وإن كان فيه النقص فهو منا، ولما لا ونحن بشر نجتهد ونخطأ ونصيب، فإن أصبنا فأجرنا على الله وإن أخطأنا فندعوه ألاّ يحرمنا أجر المجتهدين.

تم بحمد الله.

قائمة المراجع

أولا–الكتب:

1.أحمد خليفة الملط، الجرائم المعلوماتية، دون طبعة، دار الفكر الجامعي، الإسكندرية،2005.

2. جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دون طبعة ، دار هومه، الجزائر، 2012.

3. جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دون طبعة، دار النهضة العربية، القاهرة، 1998.

4. حسني الجندي، شرح قانون الإجراءات الجزائية، دون طبعة، دون دار النشر، دون بلد النشر، 1990.

5. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، طبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2011.

6. خالد ممدوح إبراهيم، الجريمة المعلوماتية، طبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.

7. _____، فن التحقيق الجنائي في الجرائم الإلكترونية، طبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.

8. رمزي رياض عوض، حماية المتهم في النظام الأنجلوأمريكي، دون طبعة، دار النهضة العربية، القاهرة، 1998.

9. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2007.

10. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دون طبعة، دار الجامعة الجديدة، الإسكندرية، دون سنة النشر.

11. عائشة بن قارة مصطفى، حجَية الدليل الإلكتروني في الإثبات الجنائي في القانون الجزائري والقانون المقارن، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2010.

12. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دون طبعة ، دار الكتب القانونية، مصر، 2007.

13. عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، طبعة الثانية، دار النهضة العربية، القاهرة، 2001.

14. عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، طبعة الثانية، منشورات الحلبي الحقوقية، بيروت– لبنان، 2007.

15. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجرائم المعلوماتية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2007.

16. محمد حسين منصور، الإثبات التقليدي والإلكتروني، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2006.

17. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دون طبعة، دار الجامعة الجديدة، الإسكندرية، 2007.

18. محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، طبعة الأولى، دون دار النشر، دون بلد النشر، 2007.

19. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.

20. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، طبعة الأولى، دار الكتب والوثائق القومية المصرية، القاهرة، 2000.

21. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دون طبعة، دار الكتب القانونية، مصر، 2006.

22. نبيلة هبه هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2007.

23. نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008 .

24. هلالي عبد الله احمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة، طبعة الأولى، دار النهضة العربية، القاهرة، 1997.

ثانيا–النصوص القانونية:

أ–النصوص التشريعية:

1. الأمر رقم (66–155)، يتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06–28، المؤرخ في20/ 12/ 2006، جريدة رسمية عدد 84 مؤرخة في 24/ 12/2006.

2. الأمر رقم (66–156) المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966،جريدة رسمية جمهورية جزائرية عدد 49 الصادرة في 11–06–1966، المعدل بالمرسوم التنفيذي رقم (04–15) المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، جريدة رسمية عدد 71، المعدل والمتمم بالقانون رقم 06–23 المؤرخ في 20–12–2006، جريدة رسمية عدد 84 الصادرة في 24–12–2006، المتضمن قانون العقوبات الجزائري.

3. قانون رقم (98–10) المؤرخ في 22 غشت 1998، يتضمن قانون الجمارك المعدل والمتمم.

4. قانون رقم (08–19) المؤرخ في 15–11–2008، جريدة رسمية عدد 63 المؤرخة في 16–11–2008، يتضمن الدستور الجزائري المعدل والمتمم.

5. قانون رقم(09ـــ04) المؤرخ في 5/ 8/ 2009، يتضمن قانون الوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47، الصادرة في 16/ 08/ 2009.

ب–النصوص التنظيمية:

1. قرار وزاري مؤرخ في 14 أبريل 2007 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، جريدة رسمية عدد 36، الصادرة في 3 يونيو 2007.

ثالثا–الرسائل والمذكرات:

1. أحمد بلال، الحماية الجنائية لبرامج الحاسب الآلي، رسالة للحصول على درجة الماجستير في العلوم الجنائية، كلية الحقوق، جامعة القاهرة، 2007.

2. سيدي محمد لبشير، دور الدليل الرقمي في إثبات الجرائم المعلوماتية، دراسة تحليليـــة تطبـــيقية، رسالة ماجستير في العلوم الشرطية تخصص التحقيق والبحث الجنائي، كلية الدراسات العليا ،جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

3.عرشوش سفيان، جرائم المساس بأنظمة الكمبيوتر والانترنيت، ملخص مذكرة التخـــرج لـــيسانس، المركز الجامعي خنشلة، معهد العلوم القانونية، 2006.

4. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة الدكتوراه، كلية الحقوق، جامعة عين الشمس، 2004.

5. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، فرع القانون الجنائي والعلوم الجنائية، كلية الحقــوق، جامعة الجزائر (1) ، 2010– 2011.

6. قارة أمال، الجريمة المعلوماتية، رسالة لنيل الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، بن عكنون، 2002.

7. مخلوفي عبد الوهاب، التجارة الإلكترونية عبر الانترنت، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقــوق، كليــة الحقــوق والعلوم السياسية، قسم الحقــوق، جــامعة الحــاج لــخضر، باتنــة، 2011.

رابعا–المقالات:

1. أحمد عبد الكريم سلامة،"الانترنت والقانون الدولي الخاص"، بحث مقدم إلى مؤتمر القانون والانترنت الذي انعقد بجامعة الإمارات العــربية المتحــدة، من 1–3 مايو 2000، جــزء3، طــبعة 3، 2004.

2. جاسم خريبط خلف، "الضبط القضائي في جــرائم الانترنــت"، مجلة جامعة ذي قار، مجــلة 4، ع.4، البصرة،2009.

3. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية"، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العرابية للعلوم الأمنية، الرياض، 2007.

4. عادل يوسف عبد النبي الشكري،" الجريمة المعلوماتية وأزمة الشرعية الجزائية "، ع. 7، كلية القانون، جامعة الكوفة، 2008.

5. علي محمود علي حموده، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر أكاديمية شرطة دبي، مركز البحوث والدراسات، ع.1، دبي– الإمارات العربية المتحدة– 26–28 نيسان 2003.

6. موسى مسعود أرحومة، "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية"، المؤتمر المغاربي الأولى حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 28،29- 09-2009.

خامسا-المقالات العلمية الإلكترونية:

أ- باللغة العربية:

1. عمرو حسين عباس، "بحث في أدلة الإثبات الجنائي و الجرائم الإلكترونية" (المعلوماتية)، بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة من 26 – 27/ 04 /2008، مقر جامعة الدول العربية، ص. 16، أنظر الموقع الإلكتروني:
www.arabip.center.com/public/events/papers/paper 2-4. pdf.

2. على حسن الطوالبه، "مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي"، دراسة مقارنة بحث منشور على شبكة الانترنت على موقع التالي:
www.policeme.gouv bh/reports/2011/Aprill/634383168746341670.pdf.

3. محمد الفتاح خوخي، " جريمة إلكترونية خلال 9 أشهر "، جريدة الخبر، الجزائر يوم الأحد 17 مارس 2013.
http://www.elkhabar.com/ar/ nas/ 327408- html.

ب- باللغة الفرنسية:

1. Bouder (Hadjira), Protection des systèmes d'information, aspects juridiques, Centre de recherche sur l'information Scientifique et Technique, p. 18.
www.mptic.dz/fr/IMG/BOUDER.PDF.

2. Compagnie national des experts de justice en information et techniques Associées, la preuve numérique à l'épreuve du litige, les acteurs du litige face à la preuve numérique (l'information numérique fait la preuve), Colloque du 13 avril 2010 à la première chambre de la cour d'appel de paris ; p.28.
http://www.cnejita.org/dac/collague 20100513 Actes.PDF.

3. Lehir (Yves), Périllat- Amédé (Frédéric), les E.SC.I Enquêteurs spécialisé en 12 / 2008, SRPJ de Toulouse, P.9.
www.Ossir.org/resist/ supports/cr/20081118/RESIST_2008-11-les- ESCI.PDF.

الفهـــــــرس