جامعة أكلي محند أولحاج –البويـــــــرة-
كلية الحقوق والعلوم السياسيـــــة
قسم القانون العـــــام

أساليب البحث والتحري في الجرائم المعلوماتية

• إعداد الطالبة:
غرباوي نادية

• إشراف الأستاذ:
د/طيبي مقران

لجنة المناقشة:

- الأستاذ يوسف أوتفات رئيسا
- الأستاذ طبيبي أمقران مشرفا ومقررا
- الأستاذة أيت بن اعمر صونيا ممتحنا

السنة الجامعية
2017/ 2016

شكر وعرفان

قال تعالى "و لئن شكرتم لأزيدنكم"

الحمد لله علام الغيوب ..والحمد لله حفاظا نصيرا تطمئن القلوب ..الحمد لله الذي كان لنا عونا معينا و حفاظا نصيرا.. و ما توفيقنا إلا من الله رب العالمين .

أتقدم بتشكراتي الخالصة إلى من ساعدني في إتمام هذا العمل المتواضع ..

واخص بالذكر المشرف على هاته المذكرة الأستاذ طيبي مقران الذي لم يبخل علي بتعليماته وتوجيهاته و نصائحه القيمة.. كما أتقدم بالشكر الجزيل..إلى كل من قدم لي يد العون سواء من قريب أو بعيد من زملائي و اخص بالذكر السيد سعدون علي و السيد اسعيداني عبد الحق كما لا أنسى الدكتور عادل يوسف الذي أفادني كثيرا في انجاز هذا البحث.

غرباوي نادية

الإهداء

إلى نبض قلبي و نور عيني ..إلى الذي علمني معنى الحياة فأمسك بيدي و حملني على صفحات الدنيا و أوصلني إلى بر الآمان و لم يبخل علي بحبه و عطفه وحنانه أقول لك أبي العزيز "رحمك الله و جعلك في اعلي الجنان"

إلى ينبوع الحنان و الحب و الكرم..إلى من علمتني الصمود مهما تبدلت الظروف "أمي" أطال الله في عمرها....

إلى..إخوتي و أخواتي ..

إلى كل أهلي و أقاربي دون استثناء و كل واحد باسمه

الى كل زميلاتي و زملائي بدون استثناء

إلى كل إنسان عزيز على قلبي

إلى كل الأساتذة الأعزاء.. دمتم ذخرا لهذه الوطن

الى الدكتور عادل يوسف الذي افادني كثيرا لانجاز هذا البحث

إلى كل هؤلاء أهدي ثمرة جهدي المتواضع.

غرباوي نادية

قائمة المختصرات

قائمة المختصرات باللغة الأجنبية LISTE OF ABBREVIATIONS	قائمة المختصرات باللغة العربية
IDS : Intrusion Détection Système	**ج.ر : الجريدة الرسمية**
IP : Internet Protocol	**ق.ع.ج : قانون العقوبات الجزائري**
TCP : Transmission Control	**ق.إ.ج.ج : قانون الإجراءات الجزائية الجزائري**
ARP : Adresse Résolution Protocol	**د.ط : دون طبعة**
NET STAT : Network Statistics	**د.س.ن : دون سنة نشر**
HIPPA : Health Insurance Portability and Accountability Act	**د.ب.ن : دون بلد نشر**
ISACA : Information Systems Audit and Control Association	**ص : صفحة**
COBIT : Control Objectives for Information and related- Technology	

مقدمـــة

مقدمة:

عرفت الجريمة من بدء البشرية فهي قديمة قدم الوجود الإنساني، فالإنسان باعتباره شخص اجتماعي تحكم حياته رابطة مع أفراد مجتمعه في شتى مجالات الحياة، و بما أن تركيبة الإنسان هي مزيج من الخير و الشر و نظرا لفطرته في إشباع حاجاته و رغباته و الظروف الحياتية و ما يتمخض عنها من صراعات لا زالت تعاني منها البشرية إلى اليوم ينتج عنها ارتكاب شتى أنواع الجرائم.

إن مجال الجريمة متطور على الدوام بتطور الحياة و أساليبها و ظروفها، فالجرائم التي كانت ترتكب في بداية العصور الأولى غير تلك التي ارتكبت في العصور التي ما بعدها لاختلاف نمط الحياة و حاجات الإنسان، ففي الماضي كان يسعى إلى ضمان بقاءه عن طريق الصراع من اجل البقاء، و بعد التطور الحاصل في المجتمعات تطورت تطلعات الإنسان بتطور مجالات الحياة و كذلك بتطور و اختلاف الزمان و المكان.

فعندما يتعارض المجتمع مع ما يريده الإنسان، فهذا يولد لديه إحساس بالرغبة في الانتقام و دافع للحصول على الكمال و الحياة الوفيرة و كما أن للجانب التربوي و تنشئة الإنسان و بعده عن الوازع الديني لها دور كبير في اضطراب سلوكه، فالجانب الأخلاقي للفرد هو من يوجه سلوكه للوجهة الصحيحة.

في الماضي كانت ترتكب جرائم تقليدية معهودة وضعت لها قوانين و قواعد تحكمها كما سلط المشرع لها عقوبات ملائمة لطبيعتها و جسامتها كجرائم السرقة و القتل و التهريب و الاختطاف على سبيل المثال، و كان المشرع قد عالج هذه الجرائم بنصوص تجريمية و أخرى إجرائية من اجل الوصول لكشف الحقائق و معاقبة الجاني.

و اليوم بعد تطور مفهوم الجريمة و أساليب ارتكابها، تولدت نوعية من الجرائم حديثة العهد مثل الجرائم الإرهابية و الجرائم المنظمة العابرة للحدود و الجرائم المعلوماتية التي لها خاصية تجعلها تتطبع بخصوصية المجرم الذي أصبح يطلق عليه بالمجرم المعلوماتي، لان مرتكبيها هم من فئات مميزة ممن لهم دراية و علم بالتقنيات الحديثة و تولدت لديهم فكرة عن كيفية ارتكاب الجريمة و كيفية إخفاء أثرها لإبعاد الشبهة عنهم.

لقد ساعد المجرم المعلوماتي في ارتكاب الجريمة طبيعة البيئة الرقمية التي ارتكبت فيها و طابعها المادي و المعنوي، لأنها قد تطبعت بتطبع الواقع التكنولوجي و التقني الذي مكن المجرم من التفنن في الأعمال الإجرامية إلى ابعد الحدود مستعينا في ذلك بمختلف الوسائل العلمية و التكنولوجية التي لها طابع خاص، من بينها نظم الإعلام الآلي والشبكات العنكبوتية التي حولت العالم إلى قرية صغيرة شملت استعمالاتها مختلف نشاطات الإنسان التجارية إلى مجالات التعليم و الترفيه مما أدى إلى بروز أثارها في مجال الاتصالات و تبادل الأفكار نتج عنها عدة أنشطة إجرامية عابرة للحدود .

لقد أثار البحث عن هذه الجرائم مشاكل و صعوبات في استخلاص الأدلة التي تثبت وقوعها و تدين مرتكبها، كونها تختلف عن الأدلة التقليدية في الجرائم العادية من حيث خصائصها و أنواعها و سبل جمعها ووسط ارتكابها وحتى صفات مرتكبيها، كما يثير الدليل الالكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي و فقدان الآثار التقليدية للجريمة المعلوماتية، بالإضافة إلى صعوبات متعلقة بسلطات الاستدلال و التحقيق من حيث إحجامهم عن الإبلاغ حرصا على ثقة العملاء أو لصعوبة اكتشافها من قبل الأشخاص العاديين، فضلا عن نقص خبرة سلطات الاستدلال و التحقيق .

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين متعودة على التعامل مع الجريمة بصورها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات أو آثار أقدام أو بقع دم أو محررات مزورة فإن المشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها، فهي لا تخلف أي آثار مادية محسوسة كما أن هذه الجريمة تتم في الخفاء، فكثيرا ما يعمد المجرم المعلوماتي إلى إخفاء نشاطه الإجرامي عن طريق تلاعبه بالبيانات والذي غالبا ما يتحقق في غفلة من المجني عليه فضلا عن سهولة تدمير الدليل ومحوه من مسرح الجريمة مما يعقد أمر كشفها وتحديد مرتكبها.

و على ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي.

كذلك يثير تساؤلات عديدة حول مشروعية وجود الدليل الالكتروني و مشروعية الحصول عليه وأدلة الإدانة ذات نوعية مختلفة، فهي معنوية الطبيعة كسجلات الحاسوب ومعلومات الدخول والاشتراك والنفاذ والبرمجيات، وقد أثارت أمام القضاء مشكلات من حيث مدى قبولها وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبات التقليدية.

إذن فإن البعد الإجرائي لجرائم الحاسوب والإنترنت ينطوي على تحديات ومشكلات عناوينها الرئيسة، الحاجة إلى سرعة الكشف خشية ضياع الدليل، وخصوصية قواعد التفتيش و الضبط الملائمة لهذه الجرائم، وقانونية وحجية أدلة جرائم الحاسوب والإنترنت، والحاجة إلى تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي.

كل هذا سنتناوله خلال تقسيمنا لهذا البحث ففي الفصل الأول تناولنا فيه الطبيعة الخاصة للتحقيق في هذا النوع من الجرائم كذا القائمين به و ما يميزهم من سمات تختلف عن المحقق العادي و ذكرنا أجهزة التحقيق في الجرائم المستحدثة بما فيها الجرائم المعلوماتية و ما يميزها.

و في الفصل الثاني تطرقنا إلى القواعد العامة للتحقيق في الجرائم المعلوماتية كجريمة عادية لها مسرح تقليدي التي نص عليها قانون الإجراءات الجزائية و كذا القواعد الخاصة بهذا النوع من الجرائم التي نص عليها قانون 04/09[1] المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 المتضمن بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال .

و قد اتبعت في هذا البحث عدة مناهج منها المنهج الوصفي و يتجلى من خلال وصف طبيعة التحقيق و الإجراءات و كذا السمات المميزة لرجال التحقيق و الأجهزة المختصة و المنهج التحليلي من خلال تحليلي و تفصيلي لإجراءات التفتيش و الضبط و التفاصيل المميزة للدليل الرقمي، كذلك المنهج المقارن حيث استخدمت هذا المنهج نظرا للطبيعة العالمية للجرائم المعلوماتية حيث بينت المعالجة التشريعية لها في النظم المقارنة و ما هي الوسائل التي استعملتها في معالجة هذا النوع من الجرائم.

---

[1] قانون 04/09 المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 المتضمن بمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الاتصال.

تظهر أهمية هذه الدراسة من خلال ارتباطها الوثيق والمباشر بظاهرة جديدة، وهي الجرائم الالكترونية التي بدأت في الظهور والانتشار حاليًا،حيث تعتبر من المواضيع الشائكة التي بدأت تشغل فكر فقهاء القانون الجنائي، وتتطلب أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مسائل الإثبات الجنائي،خاصة مسألة قبول وحجية الدليل الالكتروني حيث كانت من المسائل الهامة التي تعرضت لها المؤتمرات الدولية.

وتكمن أهمية هذه الدراسة في إلقاء الضوء على خصوصية إجراءات التحقيق في الجرائم المعلوماتية، وسنحاول من خلال الدراسة التعرف على القواعد العامة لتفتيش نظم الحاسوب والإنترنت للصول للدليل، وكذلك التعرف على نوعية الدليل و طبيعته الخاصة في مثل هذا النوع من الجرائم و المشاكل المتعلق به كونه ذو طابع مادي و معنوي في آن واحد و الذي يختلف باختلاف البيئة التي ارتكبت فيها الجريمة باعتبار أن مسرح الجريمة مسرح رقمي.

تسعى هذه الدراسة لتحقيق هدف أساسي يتمثل في التعرف على كافة الجوانب المتعلقة بإجراءات التحقيق و التحري في نظم الحاسب الآلي والإنترنت و طبيعتها الخاصة المختلفة عن القواعد الإجرائية التقليدية، و كذا بيان نوعية رجال التحقيق المؤهلون و الملمون بدراية كافية عن التقنيات المعلوماتية و توضيح أهمية الاستعانة بهم للوصول للدليل كما تهدف كذلك إلى إعطاء نظرة عن طبيعة الدليل الرقمي وطبيعته الناتجة عن البيئة التي ترتكب فيها الجريمة.

تأثرت الجريمة بالتقدم العلمي والتكنولوجي المعاصر، وبرزت أساليب إجرامية بتقنيات لم تكن معروفة من قبل، وطوعت التقنيات الحديثة لارتكاب الجريمة في مراحلها المختلفة من تخطيط وإعداد وتنفيذ وتضليل وتمويه للإفلات من العدالة، فاستخدمت الأجهزة والأدوات والتقنيات الحديثة في ارتكاب الجرائم التي تميزت بالعنف.

ومن الطبيعي أن يصاحب التقدم العلمي ظهور أنماط من الجريمة لم تتضمنها التشريعات العقابية القائمة، وتبدو النصوص الجزائية قاصرة عن ملاحقتها، ذلك أن التشريع وليد الحاجة لذا لم تتطرق التشريعات العربية إلى الجرائم المعلوماتية إلا نادرا، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية لم تتعدّ العقد الواحد، وإن كان دخوله إليها قد بدأ قبل ذلك بفترة طويلة نسبيًا.

وتكمن صعوبة التعامل مع الجرائم المعلوماتية في صعوبة إجراء التفتيش القانوني، فإذ كانت الجريمة واقعة على المكونات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة على برامج الحاسب وبياناته، فإن الصعوبات تبرز على اعتبار أنه بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر، وعلى اعتبار أن التفتيش عن هذه البيانات يستوجب الكشف عن الرقم السري إلى ملفات البيانات وهذا الرقم السري يعرفه المتهم ولا يمكن إجباره على البوح به و من هذا المنطلق أطرح الإشكالية التالية:

– ما هي طبيعة القواعد الإجرائية للتحقيق في نطاق الجرائم المعلوماتية؟

الفصل الأول

الإطار النظري للتحقيق الجنائي في نطاق الجرائم المعلوماتية

يعد البحث و التحقيق الجنائي من أهم و أدق الأعمال التي تؤدي إلى تكليل جهود الأجهزة الشرطية بالنجاح، ومفهوم التحقيق لا يقتصر فقط على القيام ببعض الأعمال و الإجراءات بل يتطلب خصائص و قدرات معينة و كذا وسائل وتقنيات معينة للوصول للحقيقة لاسيما إذا تعلق الأمر بنوعية خاصة و جديدة من الجرائم و هي الجرائم المعلوماتية وبالتالي فإجراءات التحقيق فيها لها كذلك مفهوم خاص و أساليب خاصة.

إن مسالة البحث و التحقيق في جرائم الكمبيوتر مسألة في غاية الأهمية و الصعوبة و لاسيما لاعتبارات التكوين العلمي و التدريبي و الخبرات المكتسبة لرجال القانون والعدالة الجنائية و حداثة هذه الجرائم و تقنياتها العالية التي تتطلب من القائمين بالبحث و التحقيق إلمام كاف بها، فلا يكفي أن يتمتع رجال القانون بالخلفية القانونية والشرطية فقط و إنما يجب أن يتمتع أيضا بخبرة فنية في هذا المجال.

ولقد كان للتزايد المستمر للجرائم المعلوماتية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الجرائم مهمتها التحري عن جرائم العالم الافتراضي وكشف النقاب عنها، وقد حملت هذه الأجهزة تسميات مختلفة منها شرطة الانترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات ولا يقتصر دور هذه الأجهزة على المستوى الداخلي فقط، بل هناك أجهزة متخصصة على المستوى الدولي و الاقليمي.

المبحث الأول

ماهية التحقيق الجنائي في الجرائم المعلوماتية

إن طبيعة الجرائم المستحدثة تفرض خصوصية لطبيعة التحقيق كي تتلائم و مجريات التحري و الكشف عن الجرائم و الوصول للأدلة الجنائية كما تفرض سمات خاصة و قدرات مختلفة لرجال القضاء و التحقيق، لان رجال التحقيق التقليديين غير متمكنين في التحقيق في هذا النوع من الجرائم لجهلهم للعديد من خفاياها و تقنياتها لأن الجريمة اليوم لا تعدمجرد سرقة أو قتل أو خطف بل جرائم لها طابع علمي و تقني مختلف تماما عن الجرائم المعهودة.

بالإضافة إلى إمكانية ارتكاب هذه الجرائم عن طريق الحاسوب فهناك أيضا جرائم مستحدثة أصبحت ترتكب بوسائل جديدة و تقنيات الحاسوب، وإذ كان التحقيق عموما يعتمد على ذكاء المحقق و فطنته وقوة ملاحظته وسرعة البديهة لديه و أن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطوير الأساليب و تكليف جهات مختصة لممارسته، من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة الرقمية.

المطلب الأول

مفهوم التحقيق الجنائي في نطاق الجرائم المعلوماتية

التحقيق الجنائي كنشاط قانوني يتعلق بإجراءات ضبط الجرائم و البحث عن مرتكبيها يختلف مفهومه عن مفهوم التحقيق إذا تعلق الأمر بنوع أخر من الجرائم و التي تعتبر ذات طابع مستحدث من بينها الجرائم المعلوماتية، و هذا التميز سيدفعنا إلى توضيح أهم النقاط التي تكشف لنا هذا الطابع المختلف لإجراءاته و ما يميزه من ذاتية.

الفرع الأول: تعريف و خصائص التحقيق الجنائي في الجرائم المعلوماتية

لقد تعددت تعريفات رجال الفقه فمنهم من عرفه بأنه العلم الذي يرشد المحقق إلى كيفية السير في التحقيق من بدايته إلى نهايته و يعلمه كيف يكتشف الجرائم الغامضة بتتبع اثر الجاني إذا فر من و جه القضاء للقبض عليه و ينال ما يستحق من جزاء[1]

أولا: تعريف التحقيق الجنائي في الجرائم المعلوماتية

أ- تعريف التحقيق الجنائي بشكل عام

عرف البعض التحقيق الجنائي بأنه مجموعة الأعمال و الإجراءات المشروعة التي يتخذها الباحث الجنائي في مجال كشف الجرائم و التعرف على الجناة و ضبطه و إقامة الأدلة قبلهم[2].

---

(1) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، طبعة أولى، مطابع الشرطة-شارع المرور- مصر 2008 صفحة 165- صفحة 166

(2) ممدوح عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دون طبعة، دار الكتب القانونية مصر 2006، ص 29.

كما عرفه البعض انه نشاط إجرائي تباشره سلطة قضائية مختصة للتحقيق في مدى صحة الاتهام الموجه بشأن واقعة جنائية معروضة عليها، و التحقيق الابتدائي مرحلة لاحقة لإجراءات جمع الاستدلال أو البحث التمهيدي الذي يباشره الضبط القضائي و تسبق مرحلة المحاكمة التي تقوم بها جهات الحكم[1].

و عليه فان التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة حيث تنص المادة 68 الفقرة 01 من قانون الإجراءات الجزائية "يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام و أدلة النفي".

و تنص الفقرة الثانية من نفس المادة "و تحرر نسخة عن هذه الإجراءات و كذلك عن جميع الأوراق و يؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة يطابقها للأصل و ذلك مع مراعاة ما أشير إليه في الفقرة من هذه المادة و ترقم و تجرد جميع أوراق الملف بمعرفة كاتب التحقيق أولا بأول حسب تحريرها أو ورودها لقاضي التحقيق"[2].

ب: تعريف التحقيق الجنائي في نطاق الجرائم المعلوماتية

يمكن تعريف التحقيق الجنائي في الجرائم المعلوماتية بأنه عمل قانوني يقوم به رجال الضبط القضائي المختصين في ضبط الجرائم المعلوماتية الرقمية من فاعل و دليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل[3] و هو إجراء من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة لما لهمن أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على

---

[1] عبد الله اوهايبية، شرح قانون الإجراءات الجزائية (التحري و التحقيق)، طبعة ثانية، دار هومة، الجزائر، 2004، ص 308 و ما بعدها.

[2] المادة رقم 68 الفقر 01 من قانون الإجراءات الجزائية (أمر رقم 66-155 المؤرخ في 08 يونيو 1966، يتضمن قانون الإجراءات الجزائية المعدل و المتمم جريدة رسمية رقم 49 سنة 1966) .

[3] مصطفى محمد موسى، المرجع السابق، ص 166.

مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة و التحقيق يمر بمرحلتين، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي، فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي حيث تنص المادة 12 فقرة 03 [1] من قانون الإجراءات الجزائية "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات" والمرحلة الثانية تدخل في اختصاص قاضي التحقيق بناء على نص المادة 38 من نفس القانون[2].

ثانيا: خصائص التحقيق في الجرائم المعلوماتية

هناك تشابه كبير بين التحقيق في جرائم الحاسوب والإنترنت وبين التحقيق في الجرائم الأخرى، فهي جميعًا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع وتحليل الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة الستة المشهورة لدى المحققين، إلا أن جرائم الحاسوب والإنترنت تتميز عن غيرها من الجرائم من أهم ما يميزها:

- العدد الكبير من السجلات التي يجب الإطلاع عليها، مثل الكتيبات الخاصة بأجهزة الحاسوب Computer Manuals**، ملفات تسجيل العمليات الحاسوبية** Log Files **بالإضافة إلى الإطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها.**

- أن التحقيق في الكثير من مراحله، سيجري في بيئة رقمية، من خلال التعامل مع الحواسيب والشبكات و وسائط التخزين ووسائل الاتصال.... الخ[3].

---

[1] المادة رقم 12 الفقرة 03 من قانون الإجراءات الجزائية ، مرجع سابق

[2] جاء في نص المادة "يناط بقاضي التحقيق إجراءات البحث والتحري..."

[3] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت- بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، تخصص القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية كلية الدراسات العليا-قسم العلوم الشرطية، الرياض، 2004، ص 63.

-هو عمل أمني تتولاه أجهزة متخصصة بالتنسيق والتعاون مع المؤسسات الخاصة التي تتولى تقديم خدمات الإنترنت ومتابعة الأمن على شبكاتها المتنوعة وهو عمل قانوني لان قانون الإجراءات الجزائية حدده كواجب للبحث و الكشف عن حقيقة الجرائم ومرتكبيها سواء بأنفسهم أو بوساطة مساعديهم أو مرؤوسيهم وتجمع الأدلة والقرائن التي تنفى التهمة أو تثبت وقوعها ونسبتها إلى فاعله، ويتم تنفيذها إما بأساليب علنية أو بالاتصال المباشر مع الأشخاص

المشتبه فيهم والمتهم والمجني عليه والشهود و الجهات ومقدمي خدمات الإنترنت وهو النطاق الشخصي التي يتم جمع البيانات والمعلومات منهم بشأن موضوع التحري، إما بأساليب سرية كالتخفي وانتحال الصفة حتى يأنس الجاني و يأنس جانبهم وليتمكنوا من أداء واجبهم، مادامت ردة الجاني حرة غير مقيدة [1].

و التحقيق في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده حتى ولو كانت المضبوطات هي مجرد حاسب لشخص واحد، لذلك فإنه يفضل أن يتعاون عدة محققين يمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص في إنجاز التحقيق والعثور على الأدلة، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب و الانترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.

الفرع الثاني: عناصر التحقيق الجنائي في الجرائم المعلوماتية

إن التعرض إلى موضوع فن وأصول التحقيق الجنائي في الجرائم المعلوماتية يقتضي التعرض إلي المبادئ الأساسية للتحقيق فيها و هو ما يتطلب عرض العناصر الأساسية للتحقيق، ونقصد بعناصر التحقيق تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها [2].

---

[1] مصطفى محمد موسى، قواعد و إجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية و التخطيط لها، كلية التدريب قسم البرامج التدريبية، الرياض، 2012، ص04.

[2] سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية- قسم الحقوق- جامعة الحاج لخضر، باتنة،2013/2012 ص 111- ص 112 .

العنصر الأول: استظهار الركن المادي للجريمة

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية و اتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل الكمبيوتر ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف Hosting Server**، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.**

العنصر الثاني: استظهار الركن المعنوي للجريمة

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد حدد المشرع الأمريكي الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي [1].

العنصر الثالث: تحديد وقت ومكان ارتكاب الجريمة المعلوماتية

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة ، فعل سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server احد البنوك في الأمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يثير مشكلة أخرى وهي مكان ارتكاب الجريمة المعلوماتية ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود[2].

---

[1] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، منشور على الرابط الالكتروني التالي:

http://www.4shared.com/account/home.jsp

[2] علي عدنان الفيل، إجراءات التحري و جمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) دون طبعة، المكتب الجامعي الحديث، 2012،ون بلد نشر، صفحة 67 .

العنصر الرابع: علانية التحقيق في الجريمة

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقتصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما أن فيها اطمئنانا للجمهور على أن الإجراءات تسير في طريق طبيعية، و العلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة، ففي الابتدائي تعتبر العلانية نسبية أي قاصرة على الخصوم في الدعوى الجنائية، والعلانية في التحقيق النهائي – أو مرحلة المحاكمة هي علانية مطلقة بمعني أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة.

على أن المشرع يجيز في المرحلتين – التحقيق الابتدائي والتحقيق النهائي – مباشرة الإجراءات في غير علانية، فيصدر القرار بجعله سرياً، ولما كان هذا استثناء يأتي على قاعدة عامة أصلية كان من المنطقي أن نرى المشرع يحدد الأحوال التي يجوز فيها جعل التحقيق سرياً، وهذه على كل حال رخصة لا يحسن الالتجاء إليها إلا عند الضرورة [1].

الفرع الثالث: وسائل التحقيق في الجرائم المعلوماتية

للجرائم المعلوماتية طابعها الخاص المميز لها، فان التحقيق فيها يحتاج إلى معرفة تامة و إدراك لوسائل وقوع الجريمة و بالتالي حل لغزها و الوصول للجاني عند القيام بالتحقيق[2].

---

[1] خالد ممدوح، مرجع سابق.

[2] محمد بن نصير محمد السرحاني، مرجع سابق.

في جريمة ما فانه يجب على المحقق الالتزام بقوانين و تشريع و لوائح مفسرة، و قواعد فنية تحقق الشرعية و سهولة الوصول إلى الجاني، لكن كيف يتم إثبات جريمة الكومبيوتر؟ هذا هو السؤال الذي يحدد الإطار الذي سوف يعمل فيه مأمور الضبطية القضائية.

و سبقت الإشارة إلى أن فريق التحقيق في جرائم الحاسوب والإنترنت قد يجد نفسه يفتش عن الأدلة الرقمية داخل المسرح السيبراني للجريمة وسط كم هائل من البيانات، الأمر الذي يعد عائقا قد يحول دون استخراج الأدلة، إلا أنه يوجد العديد من البرمجيات التي يمكن أن تلعب دورًا كبيرًا في مساعدة فريق التحقيق على جمع الأدلة بشكل أسرع وأكثر و توجد ثمة وسائل تساعد على ذلك أهمها:

أولا: الوسائل المادية: هي الأدوات الفنية التي غالبا ما تستخدم في بنية نظم المعلومات و التي يمكن باستخدامها تنفيذ أساليب و إجراءات التحقيق المختلفة و التي تثبت وقوع الجريمة و تساعد على تحديد شخصية مرتكبها و من أهمها:.

1-عناوين IP، و البريد الالكتروني و برامج المحادثة: عنوان الانترنت هو المسؤول عن تراسل حزم البيانات عبر شبكة الانترنت و توجيهها إلى أهدافها و هو يشبه إلى حد كبير عنوان البريد العادي وفي حالة وجود أية مشكلة أو أية أعمال تخريبية فان أول ما يجب أن يقوم به المحق هو البحث عن رقم الجهاز و تحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال الغير القانونية.

و يمكن لمزود خدمة الانترنت أن يراقب المشترك كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة و برامج خاصة لذلك [1].

2- نظام جرة العسل HONEY POT[2]: هو نظام حاسوبي مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية و يعتمد على خداع من يقوم بالهجوم و إعطاءه انطباعا خاطئا بسهولة الاعتداء على هذا النظام

---

[1] حول ذلك انظر: سليمان بن مهجع العنزي، وسائل التحقق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية- كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض، 2003، ص 99 .

[2] هى " سيرفر لجذب اهتمام المهاجمين sacrificial Server " يوضع بأسلوب مناسب ليجذب اهتمام المهاجمين ... جرة العسل honey pot ليس له أى قيمة فى مجال العمل ما عدا أنه ينذر المنظمة بوقوع هجوم . يمكن لجرة العسل honey pot أن يستعمل أي من (host-based IDS - network-based IDS) .

بهدف إغراءه و بمهاجمته ليتم منعه من الاعتداء على أي جهاز أخر في الشبكة في الوقت الذي يتم جمع اكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء و تحليلها و بالتالي اتخاذ إجراء وقائي فعال.

3- البروكسي PROXY: مزودات البروكسي مستخدمة عالميا و على نطاق واسع لتسريع التعامل مع الانترنت و لأداء بعض الوظائف الأمنية الهامة[1].

وأحيانًا يشار إليه ببوابة التطبيقات Application Gateway وهو نوع خاص من البرمجيات التي تؤمن الاتصال بواسطة بروتوكول الإنترنت بين الشبكة الداخلية المحمية والعالم الخارجي أي شبكة الإنترنت.

4-الجدار الناري FIREWALL : وتقوم هذه البرامج أثناء توليها لهذه المهمة بتوثيق عمليات الاتصال الخارجة والداخلة وإنشاء سجلات Logs توضح مصدر و وجهة كل اتصال منها بحيث تحفظ هذه السجلات على شكل ملفات حاسوبية يمكن الرجوع لها وقراءتها في أي وقت[2].

5- برامج التتبع: تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم و تقديم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، و يحتوي هذا البيان على اسم الحدث و تاريخ حدوثه و عنوان IP التي تمت من خلاله عملية الاختراق، و اسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق و أرقام مداخلها و مخارجها على شبكة الانترنت و معلومات أخرى[3].

6 نظام كشف الاختراق INSTRUSION DETECION SYSTEME: و يرمز له اختصارا بالحرفIDS وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري

---

[1] ممدوح عبد المطلب ، مرجع سابق، ص 83.

[2]محمد بن نصير السرحاني ، مرجع سابق ص 86-ص 87.

[3] هناك العديد من هذه البرمجيات بعضها تأتي على شكل أدوات مضمنه بأنظمة التشغيل مثل أداة Trace route لبيئة يونيكس وأداة Tracer لبيئة نوافذ مايكروسوفت XP/ NT/2000 ، والبعض الآخر يأتي على شكل برامج ذات واجهة رسومية مثل برنامجيNeotrace Pro و Visual route والتي تظهر خارطة للعالم توضح فيها خط سير الاتصال الشبكي وصولا إلى المصدر وذلك باستخدام العنوان الشبكي IP Address أو أسم النطاق،Domain Name وتعطي معلومات عن العنوان الشبكي للحاسوب الذي جرى الاختراق بواسطته، ومعلومات عن مزود الخدمة الذي تتبع له الشبكة التي ورد منها الاتصال الحاسوبي وهذه المعلومات قد تساعد في التعرف على الفاعل.

حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة.

7- برمجيات استعراض الصور: وهذا النوع من البرمجيات لا يختص بالتحقيق في جرائم الحاسوب والانترنت فقط بل يمكن أن يستعمله المستخدم العادي أيضًا حيث تقوم بعرض الصور الرقمية على شاشة الحاسوب ويمكن أن تقدم هذه البرمجيات خدمة جيدة للمحققين من خلال تمكينهم من مشاهدة واستعراض الصور الرقمية المخزنة داخل الحواسيب أو وسائط التخزين الخارجية، حيث تبرز الحاجة لهذه البرمجيات في جرائم حيازة ونشر مواد وصور ذات طابع إباحي (1).

8- أدوات تدقيق و مراجعة العمليات الحاسوبية AUDITING TOOLS: و هي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات و نظام تشغيل حاسوب معين و تسجيلها في ملفات خاصة يطلق عليها LOGS و الكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل المختلفة و بعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل[2].

9- أدوات الضبط: هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية منها على سبيل المثال برامج الحماية و أدوات المراجعة و أدوات مراقبة المستخدمين للشبكة و برامج التصنت على الشبكة و التقارير التي تنتجها نظم امن البيانات ومراجعة قاعدة البيانات و برامج النسخ الاحتياطي[3].

10- أدوات فحص و مراقبة الشبكات: و تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل و معرفة العمليات التي تتعرض لها و من هذه الادواة أداة ARP-برنامج VISUAL TPUT5.2 -أداةTRACER-أداةNET STAT[4].

---

(1) هناك برامج كثيرة تنتمي لهذه الفئة، من أشهرها برنامجي ThumsPlus وACDSee.

(2) ومن الامثلة على هذه الادوات لبيئة بيونيكس SYSLOGD لبيئة النوافذ و اداة EVENT VIEWER

(3) سليمان بن مهجع العنزي، مرجع سابق، ص 101.

(4) وضاف أدوات فحص و مراقبة الشبكات :

- **ARP: تحديد مكان الحاسب الالي فزيائيا على الشبكة**
- **VISUAL ROUT 5.2 a :يلتقط اي عملية فحص التقطت ضد الشبكة**
- **TRACER : رسم مسار بين جهازين و تسمح لرؤية المسار الذي اتخذه IP من مضيف الى اخر**
- **NET STAT: هي اداة لفحص حالة الاتصال الحالي للبروتوكول TCP/IP_**

ثانيا الوسائل الإجرائية

يقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة و المحددة و المتغيرة و الغير المحددة التي تثبت وقوع الجريمة و تحدد شخصية مرتكبها و منها:

1-اقتفاء الأثر: من اخطر ما يخشاه مجرم المعلوماتية تقصي أثره أثناء ارتكابه للجريمة فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح أثارك COVER YOUR TRACKS فلو لم يقم المخترق بمسح أثاره فمؤكد سوف يتم القبض عليه حتى و إن كانت عملية الاختراق تمت بشكل سليم، و يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد الكتروني أو بتتبع اثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[1].

2 - الاطلاع على عمليات النظام المعلوماتي و أسلوب حمايته[2].

ينبغي على المحقق وهو بصدد التحقيق في الجرائم المعلوماتية كالجرائم المتعلقة الانترنت أن يطلع على النظام المعلوماتي و مكوناته من شبكات و تطبيقات و خدمات تقدم للعملاء كما ينبغي عليه الاطلاع على عمليات النظام المعلوماتي كقاعدة البيانات و إدارتها و خطة تأمينها و معرفة مواد النظام و المستفيدين و الملفات و الإجراءات و تصنيف الموارد العامة، و مدى مزامنة الأجهزة، و مدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، و مدى توزيع الصلاحيات للمستفيدين وإجراءات أمن العاملين وأسلوب النسخ الاحتياطي والاستعانة ببرامج الحماية كمراقبة المستفيدين والموارد و البرامج التي تعالج البيانات و تسجل وقائع و حالات فشل الدخول إلى النظام، بالاظافة إلى معرفة نوعية برامج الحماية و أسلوب عمله و الاستفادة من التقارير التي تنتجها نظم أمن البيانات و تقارير جدران الحماية[3].

---

(1) علي عدنان الفيل، مرجع سابق ص 76- ص 77.

(2) أصبحت النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات، حيث أصبح من المهم الحفاظ على أمن المعلومات بعناصره الرئيسية الثلاث: السرية و الصوابية والاستمرارية وعلى المستوى العالمي يبرز نظام الايزو للاعتماد و التقييم و التقييس لضمان أمن المعلومات، كما يوجد نظام HIPAA في الولايات المتحدة الأمريكية لضمان أمن المعلومات الصحية ونظام COBIT من ISACA لأمن المعلومات.

(3) علي عدنان الفيل، المرجع نفسه، ص 77- ص 78.

3-الاستعانة بالذكاء الصناعي: أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية و تحليلها و استنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الصناعي في حصر الحقائق و الاحتمالات و الأسباب و الفرضيات و من ثم استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج صممت لهذا الغرض[1] .

المطلب الثاني

ماهية المحقق الجنائي في الجرائم المعلوماتية

ان خصوصية الجريمة المعلوماتية و حداثتها تتطلب كما سبق و أن ذكرنا قواعد إجرائية خاصة في التحقيق لذا فان المختصين بالتحقيق في هذا النوع من الجرائم يختلفون عن أولائك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها وهذا ما سنتطرق إليه في المطلب الموالي.

الفرع الأول: مفهوم المحقق الجنائي في الجرائم المعلوماتية.

أولا: تعريف المحقق الجنائي في الجرائم المعلوماتية

1-تعريف المحقق الجنائي بشكل عام

المحقق الجنائي هو احد أفراد سلطة إنفاذ القوانين المكلف لاتخاذ جميع الإجراءات القانونية الإدارية و الفنية المؤدية إلى كشف الجريمة و التعرف على الجناة و إلقاء القبض و جمع الأدلة و معاونة المتضررين من الجريمة[2].

---

[1] هو سلوك وخصائص معينة تتسم بها البرامج الحاسوبية تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها، من أهم هذه الخاصيات القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة.

[2] عبد الله بن حسين آل حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية، جامعة نايف العربية للعلوم الأمنية-قسم العلوم الشرطية-رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، الرياض، 2014، ص 20.

2- تعريف المحقق الجنائي في الجرائم المعلوماتية

هو رجل البحث الذي يقف على الحد الفاصل بين جهاز مكافحة الجريمة وبين المتحري عنه، سواء كان شخصاً أو أشخاص، ويقوم بعمله بوساطة أو بدون التقانات الإلكترونية وملحقاته سواء سلكية أو لاسلكية عبر شبكة الإنترنت لتحقيق غرض محدد متمثل في البيانات والمعلومات التعريفية أو التوضيحية للحد من الجريمة أو ضبطها لتحقيق الأمن أو لأي سبب آخر و إفراغ النتيجة في وثيقة سواء كانت محضرا أو تقريرا أو مذكرة فحص شكوى من مجهول أو معلوم[1].

ثانيا: خصائص المحقق الجنائي في الجرائم المعلوماتية

إذا كان من السهولة و اليسر و لفترة طويلة سبقت الثورة العلمية و التكنولوجية التي يشهدها العالم بكافة إرجائه خلال العقود الثلاثة الماضية و التي أدت إلى تغيير الكثير من المفاهيم و الأساليب و الدوافع أن يتمكن الباحث الجنائي من التعرف على كيفية وقوع الجريمة و ترتيب إحداثها و الوصول إلى مرتكبها فان الأمر الآن في ظل تطور الأساليب الإجرامية أصبح أمرا صعبا و معقدا[2].

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجهه و معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والإنترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل على اعتبار أن جهله بأساليب ارتكاب الجريمة

---

(1) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 05.

(2) انظر صلاح الدين عبد الحميد، المحاكاة الحاسوبية، بحث غير منشور، مكتبة الباحث، دون بلد نشر، 2003، ص 22

(3) جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، د.ط، دار النهضة العربية، القاهرة، 2002،ص 115.

المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن فيها البيانات[1] و التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق.

ويجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب و الأنترنت يمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهم أن يستعينوا بخبراء في مجال الحاسوب و الأنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة[2] تدل على وقوعها وتخزينها في الأقراص المعدة لذلك ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكروويف[3]حتى لا تتلف محتوياتها.

و يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت، وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات و اعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك.

---

[1]عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، 2003، ص 612.

[2] أشعة المايكروويف هي جزء من الأشعة الكهرومغناطيسية ذات طول موجي طويل يقاس بالسنتمتر في المدى من 0.3 إلى 30 سنتمتر تنتج هذه الأشعة في الطبيعة عندما يمر تيار كهربي من خلال موصل وهي تشبه موجات التلفزيون والراديو والجوال تستخدم في الاتصالات ونقل المعلومات وأجهزة الاستشعار عن بعد و أجهزة الرادار.

الفرع الثاني: تأهيل وتدريب المحقق المعلوماتي:

تنبأ المؤتمرون بمناسبة انعقاد المؤتمر الثاني للرابطة الدولية للقانون الجنائي الذي عقد في أمستردام عام2000 بحدوث نقلة جوهرية على أساليب ارتكاب الجريمة خلال عقد من الزمان بسبب دخول عنصر تقنية الحاسب الآلي والإنترنت في الحياة مما قد يجعل موظفي نظام العدالة الجنائية عاجزين عن التعامل معها بمهاراتهم الشرطية والقانونية التقليدية.

ونبه المؤتمرون آنذاك إلى ضرورة إعداد رجال قانون لديهم المهارة المعلوماتية التي تمكنهم من التعامل مع الجريمة الرقمية بمهارات رقمية، لتقى أكثر من500 عالمًا وخبيرًا ومهنيًا في مجال علم الإجرام والعدالة الجنائية في ندوة التي نظمتها جامعة استكهولم ليطرحوا بحوثًا حول أنماطًا معقدة من الجرائم الرقمية مما يتطلب معاملة رقمية من حيث منعها واكتشافها والتحقيق فيها وقد ركز عدد من الباحثين على المحصلة النهائية لإجراءات العدالة الجنائية، أي النطق بالحكم في الجرائم الرقمية و وضح في هذا السياق عوامل عديدة قد تؤثر سلبًا على دور القضاء الجنائي التقليدي.

في ضوء هذه المؤشرات تبرز أمام موظفي نظام العدالة الجنائية تحديات كبيرة ينبغي التغلب عليها حتى لا تضار العدالة وتضيع الحقوق ومن تلك التحديات[1] و في الكثير من بلدان العالم تعتد الدورات التدريبية المتخصصة لرجال الشرطة و أعضاء النيابة العامة سواء في مراكز تابعة لوزارة الداخلية أو في المراكز المتخصصة التابعة لوزارة العدل كما هو الحال في أمريكا و بريطانيا و كندا، و عند الحديث عن المهارات الفنية التي ينبغي أن يكتسبها المحقق في الجرائم المعلوماتية فإننا لا نقصد بها المهارات التقليدية التي يجب أن يتمتع بها كل محقق فهي مهارات يفترض بداهة توافرها فيه، فمهارات التعامل مع مسرح الجريمة و التحفظ على الأدلة و مناقشة الشهود و غيرها تعتبر من أساسيات التحقيق.

و عليه فان التركيز هنا سينصب على المهارات التي تتسم بالجدة و الحداثة و تعتبر إفراز للتطور الإنساني في مجال تقنية الاتصالات و الحوسبة و أمرا مستجدا في من يتعامل مع هذه الجرائم المستحدثة [2] و ذلك من خلال بالإسراع في أن يطور رجال البحث الجنائي

---

[1] محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الالي و شبكات الانترنت، حلقة علمية، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، القاهرة، 2008، ص 33-ص 34.

[2] علي عدنان الفيل، مرجع سابق، ص 21-ص 22.

وسائلهم البحثية وقدراتهم العلمية، وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب والنظم المعلوماتية ولكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي إتخاذها[1]على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة.

وإذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في الجرائم المعلوماتية، فالتقدم المتواصل في تكنولوجيا الحاسب الآلي و الأنترنت يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة مجرمي المعلوماتية.

ويرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعاة عناصر أساسية تتمثل في شخص المتدرب ومنهج الدورة التدريبية وصفة وأسلوب التدريب[2].

و تتم تهيئة المحقق الجنائي و تكوينه علميا و مهنيا على الأعمال الجنائية الإدارية و الأمنية في الكليات الأمنية حيت يتم تأهيلهم و تزويدهم بالعلوم الجنائية و الأمنية و الإدارية و الشرعية و القانونية[3].

الفرع الثالث: أنواع المحققين في الجرائم المعلوماتية

توكل مهمة التحقيق في الجرائم المعلوماتية عبر إلى نوعين من المتخصصين :

النوع الأول: يمثلون الخبرة الفنية و هم النخبة المتخصصة في مجال الحاسب الآلي و شبكاته، يتم الاستعانة بهم في جميع مراحل ضبط جرائم الحاسوب و اكتشافها و التحقيق

---

(1) سعيداني نعيم، مرجع سابق ص، 118 .

(2) هشام محمد فريد رستم، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون و الحاسب الآلي و الانترنت، ، كلية الشريعة و القانون– العين– الامارات، من 01 الى03 مايو 2000، ص 115 .

(3) عبد الله بن حسين آل حجراف القحطاني، مرجع سابق، ص 22.

مع المتهمين فيها، و كذلك في تقديم الأدلة الجنائية أمام الادعاء و المحاكم الجنائية و شرح أبعاد الجريمة و أسلوب ارتكابها بالعدد الذي يحقق العدالة[1] يجمع بين المعرفة بعلوم الحاسبة الالكترونية و الشبكات و بين الإلمام بإجراءات التحقيق الجنائي و أساليبه و كيفية التعامل مع مسرح الجريمة ويكون مسؤولا عن رفع و تحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة التي لا تؤثر على سلامة الدليل و صلاحيته لإقامة الدعوى و العرض على المحكمة و هم:

– محقق جنائي :شخص أو أكثر بحسب ظروف الحادث، لديه خبرة ومعرفة بأساليب التحقيق وإجراءاته، مع إلمامه بطبيعة جرائم الحاسوب والإنترنت وكيفية التعامل مع الأدلة الجنائية الرقمية، ويتولى التفتيش عن الأدلة وأخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة[2].

خبير حاسوب وشبكات: شخص أو أكثر بحسب ظروف الحادث، لديه خبرة ومعرفة في علوم الحاسوب والشبكات مع إلمامه بإجراءات التحقيق الجنائي وأساليبه وكيفية التعامل مع مسرح الجريمة، يكون مسؤولا عن رفع وتحريز الأدلة الجنائية الرقمية، بالطريقة المناسبة فنيًا التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى والعرض في المحكمة) .

– خبير مدقق حسابات: متخصص في المراجعة المحاسبية و على درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة في المؤسسات المصرفية و الآليات المختلفة التي يتم بواسطتها تبادل النقد الالكتروني و يعمل مع خبير الحاسبة الالكترونية و الشبكات على تحديد أسلوب الجريمة و ما إذا كان هناك تلاعب في الأنظمة المتضررة بالإضافة إلى تقدير الخسائر المادية الناتجة عن الجريمة[3].

– خبير تصوير فوتوغرافي: يتولى تصوير مسرح الجريمة كما هو متبع في جميع الجرائم بالتصوير الفوتوغرافي و الفيديو.

---

(1) مصطفى محمد موسى، مرجع سابق، ص 254.

(2) علي عدنان الفيل، مرجع سابق، ص 17–ص 18.

(3) محمد بن نصير محمد السرحاني، مرجع سابق، ص 77 و ما بعدها .

- خبير بصمات: يتولى رفع البصمات من مسرح الجريمة كإجراء عام في معظم الجرائم مع التركيز على المكونات المادية للحاسبات الالكترونية و الشبكات المتضررة أو المشتبه بوجود صلة لها بالجريمة، خاصة لوحة المفاتيح و الماوس (الفارة) و ذلك بعد اتخاذ الاحتياطات الفنية اللازمة من قبل خبير الحاسبة الالكترونية.

- خبير رسم تخطيطي: يقوم بعمل رسم تخطيطي لمسرح الجريمة بطريقة فنية دقيقة مستخدما مقياسا مناسبا للرسم، بما يوضح تقسيماته وأماكن تواجد الأدلة والأشخاص فيه[1].

النوع الثاني: يمثلون الكفاءة المهنية و هم المتخصصون في مجال التحقيق الجنائي لأخذ أقوال الشهود و استجواب المتهمين يعتمد على قواعد مهنية و قدرات لا تتوافر في خبراء الحاسب الآلي فطريقة توجيه الأسئلة و ترتيب أولوياتها و استنتاج الحقائق من الطريقة التي يتحدث بها المتهم و قراءة لغة الجسد لديه، أمور مهنية لا يوفيها حقها إلا المحققون الذين لديهم خبرة و معرفة علمية يطلقونها لذلك يجب الجمع بين التحقيق الجنائي في جرائم الحاسب الآلي وشبكاته بين النوعين الخبرة الفنية و الكفاءة المهنية للقيام بإجراءات التحقيق مع الأشخاص من ذوي العلاقة بالجريمة الالكترونية الرقمية[2].

المبحث الثاني

أجهزة التحقيق في الجرائم المعلوماتية

إنه بالنظر إلى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية كجريمة مستحدثة تختلف عن الجريمة التقليدية ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة إلى أن تعهد بمسألة البحث والتحري عن هذا النوع من الجرائم لأجهزة متخصصة، لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام، يجمع جهاز التحقيق بصفة عامة و جهاز التحقيق الجنائي في الجرائم الالكترونية

---

(1) علي عدنان الفيل، مرجع سابق، ص 18.

(2) المحقق الجنائي يكون شخص أو أكثر بحسب ظروف الجريمة يتولى التفتيش عن الأدلة و اخذ إفادة الأشخاص ذوي العلاقة في مسرح الجريمة.

بصفة خاصة بين العلانية و السرية في أدائه و في علاقته التبادلية مع الأجهزة الأخرى سواء محلية أو أجنبية عامة أو خاصة و كذا مع الناس بمختلف تركيباتهم و نظمهم الاجتماعية و الثقافية و الدينية و الاقتصادية و الجنائية و السياسية.

المطلب الأول

طبيعة جهاز التحقيق في الجرائم المعلوماتية

يتكون هذا الجهاز من أفراد بمختلف مستوياتهم التنظيمية و إمكانيات تقنية من أجل الحد من الجريمة عامة و الالكترونية خاصة و ضبطها و في هذا المطلب سنتطرق لتعريف بجهاز التحقيق في الجرائم المعلوماتية عن طريق بيان بعض أساسياته و الخصائص المميزة له كجهاز تحقيق في نوع جديد من الجرائم و هي الجرائم المعلوماتية.

الفرع الأول: مفهوم جهاز التحقيق

لم يتفق الفكر الإداري حتى الآن على تعريف للأجهزة فهناك من يهتم بهيكل الجهاز و يرى أن المنظمة هي عبارة عن هيكل يتكون من العلاقات، القوة، الأهداف، الأدوار الأنشطة والاتصالات أو العوامل الأخرى التي عادة ما توجد عندما تعمل مجموعة من الأفراد مع بعضها أما المهتمون بالعلاقات الإنسانية فذهبوا إلى أن المنظمة عبارة عن مجموعة من الأفراد ذوي أهداف مشتركة، أما المدرسة الحديثة –فترى أن المنظمة عبارة عن المراحل أو الوظائف المهيكلة التي فيها يتصل الأفراد ببعضهم البعض من أجل أهداف معينة[1].

أولا: تعريف جهاز التحقيق

جهاز التحقيق في الجرائم المعلوماتية هو عبارة عن الوظائف المتخصصة الكترونيا و قانونيا و التي يصدر بها قرار إداري و تشغل بنوعين من الأفراد (ضباط ضباط صف)[2] و المدنيين و قد حملت هذه الأجهزة عدة تسميات مختلفة من بيها شرطة الانترنت أو فرقـــة

---

[1] راجع في ذلك رمضان بدر احمد حامد، إدارة المنظمات، اتجاه شرطي، طبعة اولى، دار القلم الكويتي ، دون بلد نشر 1983، ص 28 و ما بعدها.

[2] رتبة ضابط صف في الجيش الشعبي الوطني هو: رقيب، رقيب أول– مساعد، مساعد أول، منشور على الرابط التالي: http://www.ingdz.net/vb/showthread.php?t=69555

التحري عن الجرائم المعلوماتية الرقمية و نظمها و برامجها و شبكاتها، و قد قسمت الأجهزة التي تتولى التحقيق في الجرائم المعلوماتية إلى ثلاثة أنواع:

-النوع الأول: أجهزة الأمن العام و تختص بالتحقيق في جرائم الاعتداء على النفس و المال

-النوع الثاني: أجهزة تختص بالتحقيق في الجرائم المخلة بأمن الدولة و تنقسم إلى:

أ- أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل و تتولاها أجهزة متخصصة مثل مباحث امن الدولة في مصر، فرنسا و الكويت .

ب- أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج و تتولاها أجهزة متخصصة في المخابرات العامة في مصر (1).

-النوع الثالث: جهاز التحقيق في الجرائم المعلوماتية و هذا النوع من الأجهزة لم ينشأ بعد في كل في كل الدول العربية و إن كانت بعض الدول قد أنشأته منذ أن استخدمت الحاسب الآلي و شبكات المعلومات .

ثانيا: خصائص جهاز التحقيق: من خصائص جهاز التحقيق في الجرائم المعلوماتية انه:

- إدارة متخصصة و وظائفها يحكمها مبدأ التخصص و التمييز القائم على تطبيق المعرفة في سرعة و سرية.

- إن وظائفها صدر بها قرار إداري يحدد هيكلها التنظيمي و اختصاصاتها.

- أنها جهاز بشري يتصل أفراده ببعض وفق قواعد أمن المنشأة (أمن الأفراد و المعلومات و وسائل الاتصال و التنقل) بهدف تحقيق أهداف الجهاز(الحد من الجريمة و ضبطها و ضبط الدليل الالكتروني) و أهدافهم التي من أجلها التحقوا و استمروا في الجهاز و هي الحصول على المميزات المالية و الوضع الاجتماعي المتميز.

الفرع الثاني:عناصر فاعلية جهاز التحقيق

الدولة الآمنة الكترونيا هي التي لديها جهاز تحقيق جنائي الكتروني سريع في المعرفة و تطبيقها لجمع المعلومات و تحليلها و الوصول إلى الدليل الالكتروني في الجريمة الالكترونية للإدانة و البراءة و هذا ما سنتطرق إليه في هذا الفرع.

---

(1) مصطفى محمد موسى، مرجع سابق، ص 287.

أولا: المعرفة الالكترونية

المعرفة الالكترونية هي سر تقدم جهاز التحقيق الجنائي الالكتروني في الألفية الثالثة فالتنمية الالكترونية لها متطلبات كمية خاصة مثل الموارد البشرية ممثلة في رجل الأمن و الادعاء و القضاء و المشرع و الموارد المالية و هناك متطلبات نوعية مثل المعرفة العلمية الالكترونية الرقمية و في أجهزة الدول النامية تمثل المتطلبات الكمية بشكل عام حوالي 80% أما المتطلبات النوعية فلا تزيد عن 20 % والعكس صحيح في أجهزة الدول المتقدمة مثل ألمانيا و الولايات المتحدة الأمريكية و انجلترا فمظاهر تخلف المعرفة الأمنية الالكترونية تتمثل في أن نسبة الأمية الالكترونية العالية و انخفاض نسبة التعليم الأمني المهني الالكتروني و المتخصص في مكافحة الجريمة عامة و التحقيق الجنائي خاصة [1].

بالنسبة لمعايير المعرفة الالكترونية يمكن أن يصنف جهاز التحقيق الالكتروني بأن لديه معرفة الكترونية بتطبيق المعايير التالية:

- القدرة على الخلق و الابتكار.

- القدرة على اندماج أجهزة مكافحة الجريمة الكترونيا بفاعلية التحقيق الجنائي الالكتروني و مسايرة التطور الالكتروني.

و على الأجهزة العربية لمكافحة الجريمة[2] أن تختار ما يسمى بالالكترونيات الرقمية الملائمة و هي التي تتلائم مع ظروفها و عاداتها و تقاليدها وواقعها الأمني (المجرم و الجريمة والأمن و القضاء)، و هذا لا يعني الالكترونية البسيطة وحدها و إنما أيضا تتضمن التكنولوجيا المتقدمة حسب الاحتياجات الأمنية التي تشمل على سبيل المثال أمن البيئة و الأمن الغذائي و الأمن المائي و الطاقة و تغطية جميع الاحتياجات الضرورية مع مواكبة التقدم الإنساني و تتكون منظومة العلم الأمني والتكنولوجيا من مكونين:

- منتجوا العلوم الأمنية و القانونية ممثلو في المفكرين (أعضاء هيئات التدريس في كليات الشرطة و الحقوق الأمنية مثل الدارسين و مستخدمي التكنولوجيا و هم رجال

---

[1] مصطفى محمد موسى، المرجع نفسه، ص 289- ص 290.

[2] علي حبيش، المعرفة التكنولوجية سلعة القرن القادم (تحقيق محي يوسف جريدة الأهرام، الجمعة 1998/11/13) ص 19.

نقلا عن مصطفى موسى نفس المرجع، ص 289 و ما بعدها .

مكافحة الجريمة و الناس). و يلعب المفكرين الأمنيين دورا في المعرفة الأمنية منها التواصل الوثيق بين البحث العلمي و اعتبارات للحفاظ عليه و استمراره و إعداد بحوث أساسية في مجال البحوث التطبيقية الالكترونية المستندة إلى معرفة علمية مما يتطلب الإنفاق على هذه البحوث[1].

ثانيا السرعة الالكترونية

يقصد بالسرعة الالكترونية في مجال التحقيق الجنائي سرعة دوران البيانات و المعلومات و من خلال شبكة الاتصالات السلكية و اللاسلكية الالكترونية و الرقمية المعلوماتية، فامن الغد سيعتمد على السرعة الالكترونية سرعة اتخاذ القرارات (أمنيا و ادعائيا و قضائيا) سرعة خروج الأفكار الالكترونية الأمنية الجديدة لمواجهة الجريمة الالكترونية الرقمية.

و السؤال الآن ما هو المصير الذي ينتظر أجهزة مكافحة الجريمة الأقل تقدما الكترونيا؟

و يمكن القول أن العلم ينتقل بسرعة خارقة من العالمية إلى العولمة و نعني بذلك انه نتيجة لثورة الاتصالات و خصوصا ذيوع استخدام شبكة الانترنت فانه تنشأ شبكات معلومات علمية كونية يسهم في إمدادها بالنتائج العلمية العلماء في كل مكان و تكون متاحة لأي باحث علمي في العالم و تكون مسرحا للأساليب الالكترونية لشياطين الإنس.

بالإضافة إلى ذلك و نظرا لان الاتصال بين العلماء نتيجة استخدام المؤتمرات الفضائية عن طريق الانترنت و الاتصال من خلال البريد الالكتروني و الانضمام إلى جماعات النقاش فان الاتصال السريع و الفوري و المستمر بين العلماء يؤدي إلى حالة جديدة من التراكم المعرفي و العلمي غير المسبوق، لذلك ليس من وسيلة إلا بتحويل مجتمعاتنا لتصبح مجتمعات معلوماتية عامة بما فيها من أجهزة مكافحة الجريمة[2] ويتطلب جهاز التحقيق الجنائي الالكتروني كي يكون بسرعة البرق نظاما عصبيا رقميا[3]

---

(1) مصطفى موسى، نفس المرجع، ص 290- ص 291.

(2) مصطفى محمد موسى، مرجع سابق، ص289-299

(3) نجح بيل جيتس رئيس شركة مايكروسوفت العالمية للبرمجيات بالتبشير بحلول عصر جديد قوامه النظام العصبي الرقمي digital nervous system الذي سيكون بلا شك عنواناً لثورة اجتماعية شاملة بدأت بوادرها الأولى تتجسّد في الأساليب الرقمية المتكاملة لطرق أداء الشركات والمؤسسات الصناعية والاجتماعية بدون استثناء، ويستأثر بيل جيتس وحده بفضل إرساء الأسس النظرية والعملية للنظام العصبي الرقمي فهو الذي وضع هذا المصطلح أصلاً، وهو الذي يسعى الآن إلى نقله إلى حيّز التطبيق العملي من خلال البحوث الجادة والاستثمارات الهائلة التي وظّفتها مايكروسوفت في هذا الإطار، أنظر الرابط التالي:

http://www.shakwmakw.com/vb/showthread.php?t=47578&s=

و يجب أن تكون وضيفة التكنولوجيا الرقمية و شبكاتها مثل وضيفة الجهاز العصبي البيولوجي داخل جسم الكائن الحي فالجهاز العصبي البيولوجي هو شبكة اتصالات فائقة الحساسية و السرعة بجسم الكائن الحي يقوم بإثارة استجاباته و سلوكياته تجاه ما يدور حوله يجعله يتفاعل بسرعة مطلقة مع الخطر و الاحتياجات و الفرص أو مع الآخرين و يعطيه المعلومات التي يحتاجها، حينما يقوم بتامل الموضوعات الأمنية و تحديد الاختيارات و يجعله دائما متيقظا متنبها لمعظم الأشياء المهمة و يقوم باستبعاد المعلومات عير المهمة بالنسبة له.

إن مراحل تحويل جهاز التحقيق الجنائي إلى جهاز ذو نظام عصبي يمر بمراحل منها:

- **المعرفة بالعمل الالكتروني الرقمي.**
- **تنفيذ و أداء الأعمال الالكترونية الرقمية.**
- **هذه المرحلة خاصة بالشرطة و الادعاء و القضاء و الدفاع و التشريع.**

ثالثا: السرية الالكترونية

يقصد بالسرية الالكترونية في مجال التحقيق الجنائي في الجرائم الالكترونية الأخبار و المعلومات المتعلقة بالتدابير و الإجراءات التي تتخذ لكشف الجرائم الالكترونية الرقمية أو تحقيقها أو محاكمة مرتكبيها، فإفشاء المعلومات المتعلقة لهذه الجرائم، أو نقلها فيه ما يفيد منه الجناة أو بعضهم في الفرار من وجه القضاء أو العمل على تضييع الأدلة و إفسادها لذلك كان لإضفاء السرية على إخبار تدابير الكشف عن هذه الجرائم أو تحقيقها أو محاكمة مرتكبيها لحصر نطاق هذه الجرائم و عدم إفلات الجناة فيها من القصاص و يتناول التعريف السابق ثلاثة أنواع من الأخبار و المعلومات يجب أن تكون سرية و هي:

- **المعلومات المتعلقة بالتدابير و الإجراءات الماسة بأمن الدولة كجمع الاستدلالات و التحقيق الإداري الذي يسبق تحريك الدعوى و تقديم بلاغ على ارتكاب هذه الجرائم.**
- **الأخبار و المعلومات المتعلقة بالتحقيق في إحدى الجرائم الالكترونية الرقمية كما هو الشأن في المعلومات المتصلة لتحريك الدعوى و الأمر بالقبض على احد الجناة الالكترونيين أو التفتيش لشخصه أو مسكنه أو حاسوبه الرقمي ، المعلومات المتعلقة باستجواب المتهمين أو أقوال الشهود أثناء التحقيق، إجراءات المعاينة و المواجهة و قرار الاتهام أو الأمر بالا وجه لإقامة الدعوى لما تتضمنه هذه القرارات عادة من تفصيلات أو معلومات مستمدة من التحقيق.**

- المعلومات المتعلقة بالمحاكمة في إحدى الجرائم الالكترونية بما فيذلك المرافعات و التحقيق النهائي، و يجوز للمحكمة التي تتولى المحاكمة أن تأذن بإذاعة ما تراه من مجرياتها.
- الأشياء والديسكات و الاسطوانات الليزر و غيرها من المكاتبات و المحررات و الوثائق و الرسوم و الخرائط و التصميمات و الصور و غيرها سواء كانت ورقية أم رقمية من الأشياء التي يجب لمصلحة البلاد أن لا يعلمها بها إلا من يناط بهم حفظها أو استعمالها و التي يجب أن تبقى سرا [1].

المطلب الثاني

أجهزة التحقيق على المستويين الداخلي والدولي و الاقليمي

بتطور أساليب الجريمة في الآونة الأخيرة و ظهور الجرائم المستحدثة لم تعهدها من قبل أصبح من غير الممكن مواجهتها بالأساليب الإجرائية المعتادة، حيث لم تعد إجراءات التحقيق التقليدية ملائمة لهذا النوع من الجرائم من بينها الجرائم المعلوماتية التي تعد من الجرائم العابرة للحدود الإقليمي للدولة، و المحقق التقليدي لم يعد يمكنه التعامل مع هذه الجرائم لما تنقصه من مهارات تقنية و كفاءة لمواجهته و عجز الأساليب الإجرائية التقليدية للتحقيق فيها خصوصا أن هذه الجريمة عابرة للقارات و قد تمتد أثرها إلى أجهزة المعلوماتية الأخرى في إقليم أخر لذا تم التفكير في إنشاء أجهزة متخصصة لمثل هذا النوع من الجرائم سواء على المستوى الوطني أو الدولي و هذه الخطوة لم تخطوها كل البلدان العربية و سنتطرق فيما يلي إلى هذه الأجهزة خاصيتها و أساليبها في مكافحة الجريمة المعلوماتية.

الفرع الأول: أجهزة التحقيق على المستوى الداخلي

تم إنشاء العديد من أجهزة التحقيق في العديد من الدول العربية و الأجنبية كما أنشات أجهزة دولية للتعاون فيما بين الدول لمواجهة هذه الجرائم و في هذا الفرع سأتناول هذه الأجهزة في الجزائر و الدول الأجنبية.

أولا: أجهزة التحقيق في الجزائر: لقد أولت الجزائر أهمية و عناية بتطوير أجهزة التحقق لديها ومن اجل مواجهة الجريمة المعلوماتية لذا فقد أنشات هيئات و أجهزة خاصة من اجل

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، ص 06 و ما بعدها.

التحقيق الجنائي فيها من بينها الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال التي نصت عليها المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 [1] و تحدد تشكيلة الهيئة و تنظيمها وكيفيات سيرها عن طريق التنظيم وللهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها و هما:

1- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و ذلك بتوعية مستعملي تكنولوجيا الإعلام و خطورة الجرائم التي يمكن أن يكونوا ضحاياها من أهمها جرائم التجسس و المؤسسات الرئيسية أو الجهات الحكومية.

2- مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال هما نوعان:

أ- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات بشأن الجرائم المعلوماتية بما في ذلك تجميع الخبرات القضائية م 14 ف/ ب من قانون 04/09 لتنشيط و تنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين و المشتركين في ارتكابها.

- القيام بإذن من السلطات القضائية بجميع إجراءات التحري دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون .

- تقديم مساعدة لمصالح الأمن و الدرك الوطني و جميع الإدارات و مصالح الدولة الوطنية.

- التدخل تلقائيا بعد موافقة السلطات كما نصت المادة 04 فقرة 02 من قانون 04/09 من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.

ب- تبادل مع نظيراتها في الخارج قصد جمع المعطيات المفيدة في التعرف على الجناة و تحديد مكان تواجدهم[2].

بالنسبة لجهاز الشرطة فقد انشات المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية "لشاطوناف" بالجزائر العاصمة و مخبرين جهويين لكل من "قسنطينة...

---

[1] تنص المادة على" تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته يحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق التنظيم القانون **04/09** المؤرخ في **05** أوت **2009** الجريدة الرسمية العدد **47**، ص **08**

[2] احمد مسعود مريم، **آليات مكافحة تكنولوجيات الإعلام و الاتصال في ضوء القانون رقم 04/09 ، مذكرة مقدمة لنيل شهادة الماجستير جامعة قاصدي مرباح –ورقلة– كلية الحقوق–تخصص قانون جنائي، 2013/2012**، ص **46**.

و وهران"، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر[1].

أما على مستوى الدرك الوطني فيوجد بالمعهد الوطني للأدلة الجنائية و علم الإجرام "ببوشاوي" التابع للقيادة العامة للدرك الوطني قسم الإعلام و الإلكترونيك المختص بالتحقيق في الجرائم المعلوماتية و مكافحتها "ببئر مراد رايس" هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في البيوت والبنوك كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى و كذا إنشاء معهد خاص بعلم الإجراء لتطوير مستوى التعامل مع الجريمة، و قد قدم عدة خبراء مداخلات في الملتقى الذي يتعلق بتطوير أساليب الجريمة[2].

ثانيا: أجهزة التحقيق في الدول الأجنبية

على غرار الجزائر ذهبت عدة تشريعات إلى الاهتمام بالجرائم العابرة للحدود و التحري فيها باعتبار خاصيتها المستحدثة و انشات عدة مراكز لمكافحتها من بين هذه الدول:

1- السويد:

أنشأت السويد أول مركز شرطة في العالم لبلدية" كرامفورس" الريفية بالسويد و يمكن للأهالي رفع الشكاوى و تسديد الغرامات عن طرق موقع الكتروني على الشبكة ثم تزويده بالصوت و الصورة ليستطيع متلقي البلاغ مشاهدة المبلغ مما يتيح قدرا اكبر من المصداقية كما يحد من البلاغات الكيدية و الكاذبة. و يعتبر هذا المركز الافتراضي مقدمة لشبكة مراكز افتراضية ستنتشر في السويد و تتيح للمواطنين إمكانية الاتصال برجال الشرطة في حالة الضرورة لتقديم المعلومات، و يساعد هذا المركز على تخفيف الضغط على مراكز الشرطة التقليدية[3].

2- الولايات المتحدة الأمريكية.

---

(1) سعيداني نعيم، مرجع سابق، ص 107 .

(2) http://www.al-fadjr.com/ar/index.php?news=71333?print

(3) مصطفى محمد موسى، التحقيق الجنائي في الجريمة الالكترونية، مرجع سابق، ص 323.

قامت الولايات المتحدة الأمريكية عدة مراكز لمكافحة الجريمة المعلوماتية منها شرطة الواب web police **و يعتبر نقطة مراقبة على الانترنت و تلقي الشكاوى من مستخدمي الشبكة و ملاحقة الجناة و القراصنة و تقديمهم للمحاكمة منهم:**

-مركز تلقي الشكاوى IC3: [1] تم إنشاؤه من طرف مكتب التحقيقات الفدرالي FBI (2) **عام 2000 و عام 2003 تم برمجة مراكز الشكاوى و الاحتيال عبر الانترنت المعروف بـ IFCC[3] مع هذا المركز يعمل بطريقة تشاركية يقوم بتلقي الشكاوى عبر موقعه على الانترنت خلال ملأ استمارة الكترونية من طرف الشاكي ثم يقوم المختصون بتحليل الشكاوى و ربطها بالشكاوى الأخرى المستلمة من قبل.**

- المركز الوطني للحماية البنية التحتية التابع للمباحث الفدرالية الأمريكية: قد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات و الاعتداءات عبر الانترنت و على رأسها شبكات الاتصالات كما انشات قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية ويختص بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها و كذا نيابة جرائم الحاسوب و الاتصالات CTC[4].

3- الصين: أسست شرطة إقليم "انهوى" الجنوبي الشرقي وحدة شرطة متخصصة لمراقبة شبكة الانترنت و تخطط 20 مدينة و مقاطعة أخرى لإقامة وحدات مماثلة وسبب إنشاء هذه الوحدة و التخطيط لإنشاء غيرها إلى أن 16.9 مليون صيني يستخدمون الانترنت و يقضون متوسط حوالي 16.5 ساعة أسبوعيا أمام الشبكة، كما توجد أكثر من 270 موقع صيني على الانترنت و ذلك وفق تقرير نشر عام 2000 [5] و تسمى هذه الوحدة القوة المضادة للهكرة تختص برقابة المعلومات و التي تسمح لمواطنيها بالدخول عبر الانترنت.

4- بريطانيا: قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة

---

(1) اختصار لـ: INTERNET CRIME COMPLAINT CENTER

(2) افتتاح مكتب التحقيقات الفدرالي FBI موقعا على شبكة الانترنت لتلقي بلاغات الاحتيال عبر الانترنت و يمكن الوصول إليه على العنوان التالي:WWW.IFVVFBI.GOV.

(3) اختصار لكلمة : INTERNET FRAUDECOMPLAINT CENTER

(4) إختصار لـ :COMPUTER AND TELECOMMUNICATION COORDINATTO-

(5) مصطفى محمد موسى، مرجع سابق، ص 326.

المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام2001 .

5- فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية و نذكر من هذه الأجهزة:

- القسم الوطني لقمع جرائم المساس بالأموال والأشخاص: ويتكون هذا القسم من محققين مختصين في التحقيق بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997[1].

-المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات و الاتصالات: ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في 2000/05/15.

ثالثا: الدول العربية:

- مصر: انشات وزارة الداخلية في الحكومة المصرية جهازا متخصصا للتحقيق في الجرائم الالكترونية تحت مسمى إدارة مكافحة جرائم الحاسبات و شبكة المعلومات استنادا للقرار الوزاري رقم 02، كما تم إنشاء إدارة للبحث تخضع للإشراف المباشر لمدير الإدارة العامة و تشرف عليه فنيا مصلحة الأمن العام، اختصاصات الإدارة مكافحة و ضبط الجرائم التي تقع باستخدام الحاسبات على نظم شبكة المعلومات و قواعد البيانات كالتخريبات و الفيروسات و الاختراقات و اتخاذ الإجراءات القانونية حيالها بالاشتراك مع الأجهزة المختصة بذلك كما انشات أقسام المكافحة جغرافيا و هي وحدات مكافحة جرائم شبكات المعلومات بالأجهزة التي تنهض بأعمال البحث حسب مكانها الجغرافي بعد استكمال مقوماتها البشرية و المادية على أن تخضع للإشراف الفني الفدرالي لإدارة مكافحة جرائم الحاسبات و شبكات المعلومات بالإدارة العامة للمعلومات و التوثيق كما تم إنشاء فرق تدريبية للضباط و أمناء الشرطة و المدنين العملين في مجال الحاسبات[2].

---

[1] سعيداني نعيم، مرجع سابق، ص 105.

[2] مصطفى محمد موسى، مرجع سابق، ص 310.

-المملكة العربية السعودية: حيث صدر في عام 1428 نظام مكافحة الجرائم المعلوماتية ووضع العقوبات لمرتكبيها وأسند هذا النظام إلى وزارة الداخلية مسؤولية تنفيذ هذا النظام والذي يهدف إلى وضع معايير قانونية وتنظيمية لمكافحة جرائم المعلومات والحاسب الآلي والإنترنت من خلال تحديد الجرائم ذات الصلة واتخاذ إجراءات تأديبية مقابل كل جريمة أو انتهاك[1].

ألقت أجهزة الأمن في المملكة العربية السعودية على«هكر» يقوم بابتزاز بصور يحصل عليها من خلال عمليات اختراق إلكترونية(كمين، 2010 م) كما أوضحت دراسة أجرتها شركة الخليج للحاسبات أن دول الخليج العربية تعتبر أحد الأهداف الرئيسة للجرائم الإلكترونية[2].

الفرع الثاني: أجهزة التحقيق على المستوى الدولي و الاقليمي

أولا: أجهزة التحقيق على المستوى الدولي: كما سبق و أن ذكرنا فان تطور الجريمة المعلوماتية و انتشارها عالميا أدى إلى التفكير في إنشاء أجهزة للتحقيق و الكشف عن هذه الجرائم التي أصبحت تتعدى النطاق المكاني باعتبارها عابرة للحدود و بالتالي قد يمتد أثرها إلى إقليم آخر و مما يصعب التحقيق فيها و العثور على الدليل فقد يضطر الأمر إلى التفتيش في نظم أخرى متواجدة في دولة أخرى .

لذا فقد تم الاتفاق على ضرورة تدعيم التعاون الدولية من اجل مواجهة هذه الجريمة و التحقيق فيها فتم إنشاء المنظمة الدولية للشرطة الجنائية الانتربول الدولي و هي اختصار لكلمة الشرطة الدولية (بالإنجليزية International Police) والاسم الكامل لها هو منظمة شرطة الجرائم الدولية (بالإنجليزية International Criminal Police Organisation.هو اكبر منظمة شرطية دولية أنشئت عام 1923، مكونة من قوات الشرطة تظم 190 دولة[3] مقرها الرئيسي "ليون" فرنسا و بها ابرع لغات رسمية هي العربية-الانجليزية-الفرنسية-الاسبانية، فهي مكونة من الجمعية العامة-المكاتب المركزية

---

[1] فيصل حسن حامد، التحديات التي تواجه الأجهزة الأمنية في المملكة العربية السعودية، المجلة العربية للدراسات الأمنية و التدريب، العدد 63 الرياض، 2015، ص 174.

[2] فيصل حسن حامد، المرجع نفسه، ص 173.

[3] انتسبت الجزائر إلى منظمة الشرطة الدولية عام 1963

الوطنية –المستشارون– لجنة ضبط ملفات الانتربول يتبادل أعضاء الشرطة الدولية المعلومات عن المجرمين الدوليين و يتعاونون فيما بينهم لمكافحة الجرائم المنظمة[1].

يسهل الانتربول تبادل المساعدة على أوسع نطاق ممكن بين جميع السلطات إنفاذ القوانين الجنائية و يضمن قدرة الشرطة في التواصل فيما بينها بشكل مأمون في العالم اجمع، كم يتيح إمكانية الاطلاع على البيانات و المعلومات الشرطية من جميع أنحاء العالم و تقديم الدعم العلماني في مجالات إجرام محددة ذات أولوية [2].

يقوم برنامج الانتربول بمكافحة الجرائم المعلوماتية على التدريب و العمليات، يعمل على مواكبة التهديدات الناشئة و يهدف إلى تعزيز تبادل المعلومات بين الدول الأعضاء عن طريق الفرقة العاملة و المؤتمرات الإقليمية، توفير دورات تدريبية لوضع معايير مهنية و تنسيق العمليات الدولية، إعداد قائمة عالمية بأسماء ضباط الاتصال و وضعها بتصرف المحققين في مجال الإجرام المعلوماتي على مدار الساعة مساعدة البلدان الأعضاء على التحقيق في الهجمات و الجرائم عن طريق توفير خدمات في مجال التحقيق و قواعد البيانات و إقامة شراكة مع المنظمات الدولية الأخرى.

و كانت منظمة الانتربول التي تعمل في مجال التعاون بين قوات الشرطة أول منظمة دولية تضع هيكلا للمساعدة المتبادلة [3].

2- أجهزة التحقيق على المستوى الإقليمي:

–المركز الأروبي للجريمة المعلوماتية: هي وكالة تطبيق القانون الأوربية، وظيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوربي في مجالات مكافحة الجرائم الدولية الكبيرة والإرهاب من بينها الجرائم المعلوماتية، تمتلك الوكالة أكثر من 700 موظف في مقرها الرئيسي الكائن في لاهاي في هولندا، وهي تعمل بشكل وثيق

---

(1) تتمثل مهمة الانتربول في تمكين أجهزة الشرطة في العالم من العمل معا لمنع الجريمة و مكافحتها و تزود المنظمة هذه الأجهزة بالدعم التقني و الميداني بفضل بنية تحتية دولية متطورة لمساعدتها على مواجهة التحديات المتنامية في مجال مكافحة أشكال الجريمة الناشئة.

(2) منشور على الموقع التالي بتاريخ 11ماي2013 www.alfetn.org/t10835-topic,.

(3) برنامج تعزيز حكم قانون في بعض الدول العربية–مشروع تحديث النيابة العامة، أعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية من 19 إلى 20 يونيو 2007 .

مع أجهزة أمن دول الاتحاد الأوربي ودول من خارج الاتحاد كأستراليا وكندا والولايات المتحدة الأمريكية و النرويج، لا يمتلك ضباط اليوروبول صلاحيات مباشرة للإيقاف والاعتقال ولكنهم يقومون بدعم ضباط الأمن العاديين بالقيام بمهام جمع المعلومات وتحليلها وتوزيعها إضافة لتنسيق المهمات المشتركة، وتستفيد أجهزة الأمن المستقلة لدول الاتحاد بدورها من خدمات الوكالة موظفو اليوروبول يأتون من فروع أمنية مختلفة بما في ذلك أجهزة الشرطة العادية وشرطة الحدود وشرطة الجمارك وغيرها[1] .

– الأوروجست Eurojust: هو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 و ينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الإتحاد الأوروبي، ويعد الأروجست وحدة للتعاون القضائي، مهمته الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات وله من الصلاحيات ما يؤهله لفتح تحقيقات ومباشرة متابعات جزائية [2].

– الافريبول AFRIPOL أو منظمة الشرطة الجنائية الإفريقية: هي منظمة تسهل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية، الإرهاب، المخدرات و الاتجار بالأسلحة في إفريقيا، أنشئت في 13 ديسمبر 2015 في الجزائر خلال المؤتمر الإقليمي الأفريقي بدعوى من اللواء عبد الغني هامل، مكونة من قوات الشرطة لـ 41 دولة،مقرها الرئيسي في أعالي بن عكنون بالعاصمة الجزائرية لها خمس لغات و هي: (العربية، الانجليزية الفرنسية، الاسبانية و البرتغالية) [3]

و أوضح اللواء هامل في ندوة صحفية أن هذه الآلية "ستشجع التعاون الشرطي الإقليمي و تعمل على تقريب وجهات النظر بين رؤساء الشرطة في مجال تقييم التهديدات و تحديد السياسات و تعزيز القدرات المؤسساتية الشرطية في ميدان التكوين و الشرطة العلمية وإدارة

---

(1) wwwhttps://ar.wikipedia.org/wiki/

(2) سعيداني نعيم ، مرجع سابق، ص 108.

(3) (https://ar.wikipedia.org/wiki/

أجهزة الشرطة التي تقوم على احترام حقوق الإنسان و العدل و المساواة و كذا تبادل الممارسات السليمة."

كما أكد ان الجزائر ستلتمس من لجنة الاتحاد الأفريقي في غضون الآجال المناسبة إدراج المشروع المتعلق بإنشاء الأفريبول في جدول الأعمال الخاصة بالقمة القادمة لرؤساء دول و حكومات الاتحاد الإفريقي المزمع عقدها في شهر يونيو 2014 بمالابو بغينيا الاستوائية [1].

---

(1) **تاريخ النشر: الثلاثاء 12 فبراير 2014 سا 5:37 http://www.elkhabar.com/ar/index.php?news=385641**

الفصل الثاني

استنباط الدليل الرقمي في الجرائم المعلوماتية

إن التحقيق هو إجراء من أهم الإجراءات التي تُتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

و الثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا،مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي و المرحلة الثانية تدخل في اختصاص قاضي التحقيق و الحاصل أنه مع ظهور الجرائم المعلوماتية التي تمثل ضربا من ضروب الذكاء الإجرامي، و التي باتت تتخذ أنماطا جديدة أصبح لا يجدي معها إتباع الطرق التقليدية في تحصيل الدليل لإثباتها لما تثيره طبيعتها غير المادية من إشكالات، وما تؤديه التقنية الحديثة من دور في الوصول إلى الدليل الرقمي.

وقد تطرقت إلى الخصوصية المميزة للدليل الرقمي الذي لم يعد يتسم بالطابع المادي فحسب بل يتخذ كذلك شكلا معنويا من خلال البرامج التي يتميز بها نظم المعلوماتية و إبراز المشاكل القانونية التي أفرزها ظهور المعلوماتية وتطبيقهاعلى طبيعة الإجراءات الخاصة بملاحقة الجناة.

المبحث الأول

طبيعة الدليل الرقمي في الجرائم المعلوماتية

من القواعد المستقرة في مجال الإثبات الجنائي أن القاضي لا يمكنه أن يقضي بعلمه الشخصي فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة، ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته و لهذه الأهمية التي يتمتع بها الدليل عموماً حظي باهتمام المشرع في مختلف الأنظمة القانونية من حيث تحديد شروط مشروعيته وتقدير قيمته الإثباتية، مع اختلاف النظم القانونية في الاتجاه الذي تتبناه بين موسع ومضيق.

ونتيجة للتطور العلمي وانتشار التقنية الرقمية في التعاملات اليومية، أصبحت تستعمل تلك التقنية كوسيلة لارتكاب الجرائم تارة ، وكموضوع للجريمة تارة أخرى ، وبذلك اختلف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي و هو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية أو ما يسمى بالأدلة الإلكترونية ولذا فإن ذلك يثير التساؤل حول قبول الدليل الرقمي في إثبات الوقائع الجنائية ، لاسيما إذا علمنا مقدار التطور في مجال تقنية المعلومات على نحو يتيح العبث بالمخرجات الرقمية بما يجعل مضمونها مخالفاً للحقيقة دون أن يتسنى لغير المتخصص إدراك ذلك ، فهل مفهوم اليقين الذي يجب أن يتمتع به الدليل الجنائي يتعارض وهذه الطبيعة الخاصة للدلـيل الرقمـي ؟

المطلب الأول

ماهية الدليل الرقمي

إن تقييم أي نظام قانوني لا يمكن أن يصل إلى نتائج صحيحة إلا إذا توافر لدى المقوم تصوراً واضحاً لذلك النظام ، إذ الحكم على الشئ فرع عن تصوره ، ولذا فإننا إذ نتطلع في هذه الورقة إلى دراسة نظام الأدلة الرقمية إن جاز التعبير نعتقد أنه من الواجب تناول هذا النوع من الأدلة بالتعريف ليتسنى فهم ماهيته لنتمكن في النهاية من الحكم عليه، ولذلك فإننا في هذا المطلب سنتناول مفهوم بالدليل الرقمي .

الفرع الأول: مفهوم الدليل الرقمي.

أولا: تعريف الدليل الرقمي

عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 بأنه المعلومات ذات القيمة المحتملة و المخزنة أو المنقولة في صورة رقمية و كان قد عرفته في مارس 2000 بأنه المعلومات المخزنة أو المنقولة و التي يمكن الاعتماد عليها أمام المحكمة[1].

كما يعرف الدليل الالكتروني بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج و تطبيقات وتكنولوجيا خاصة وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 213.

النصوص المكتوبة أو الصور أو الأصوات و الأشكال و الرسوم وذلك من أجل الربط بين الجريمة و المجرم و المجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ و تطبيق القانون[1].

كما عرف بأنه الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة باستعماله تكنولوجيات الإعلام والاتصال[2].

كما عرفه البعض الأخر بأنه الدليل المأخوذ من أجهزة الحاسب الآلي و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة و يتم تقديمها فيشكل دليل يمكن اعتماده أمام القضاء في حين عرفه البعض الأخر بأنه الدليل الذي يجد له أساسا في العالم الافتراضي و يقود إلى الجريمة.

ثانيا: خصائص الدليل الرقمي

يمتاز الدليل الرقمي عن الدليل المأخوذ من مسرح الجريمة المعتاد بما يلي:

- **طريق نسخ الدليل الرقمي من أجهزة الكمبيوتر تقلل من مخاطر إتلاف الدليل الأصلي.**
- **استخدام التطبيقات و البرامج الصحيحة يكون من السهولة تحديد ما إذا ما كان الدليل الرقمي قد تم العبث به أو تعديله و ذلك لإمكانية مقارنته بالأصل.**
- **الصعوبة النسبية لتحطيم أو محو الدليل فيمكن للدليل الرقمي ان يعاد تظهيره من خلال الكمبيوتر دسك نشاط الجاني لمحو الدليل يسجل أيضا حيث يتم تسجيلها في الكمبيوتر و يمكن استخلاصها لاحقا لاستخدامها كدليل إدانة ضده.**
- **الاتساع العالمي لمسرح الدليل الرقمي حيث يمكن لمستغلي الدليل من تبادل المعرفة الرقمية بسرعة عالية في مناطق مختلفة من العالم مما يسهم في الاستدلال على الجناة بسرعة اقل نسبيا.**

---

[1] ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 88.

[2] احمد مسعود مريم، مرجع سابق، ص 69.

- **امتيازه بالسعة التخزينية العالية كما يمكن من خلاله رصد المعلومات عن الجاني و تحليلها في ذات الوقت[1].**
- **الطبيعة التقنية والفنية، وكيفية معنوية للأدلة الجنائية الالكترونية لا تدرك بالحواس العادية ويتطلب إدراكها الاستعانة بأجهزة ومعدات و نظم الحاسبة الآلية [2]**

(HARD WARE-SOFT WARE)، فالدليل الالكتروني وكما أسلفنا عبارة عن مجالات مغناطيسية كهربائية، ومن ثم فإن ترجمة الدليل الالكتروني وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل بل أن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيئة التي يمكن الاستدلال بها على معلومة معينة .

- **الأدلة الرقمية أدلة علمية لما كانت التقنية ابنة العلم فكذلك يعد جميع ما ينشأ عن التقنية سببا في تقرير أن الأدلة الجنائية الالكترونية هي أدلة علمية يرجع إلى أنها تستمد مما يصنعه أهل العلوم التقنية من آراء واستنتاجات علمية على ضوء ما يتم الوصول إليه من برامج وأجهزة وبرامج تقنية، والدليل الالكتروني يعد من طائفة ما يعرف بالأدلة المستمدة من الآلة [3].**
- **كما إن المعلومة الرقمية غير ثابتة، إذ يمكنها أن تظهر على شكل حركي يصعب بذلك إيجادها و هي سهلة النسخ فالموسوعة العالمية هي صور يمكن نسخها في دقيقة تقريبا بواسطة USB.**
- **غنية كميا لأنه يقدر بأنه 100 مليار حزمة إلكترونية تحول يومياً عبر العالم، كما أنَّ الأنظمة الرقمية هي كثيرة إلى أبعد الحدود.**

---

(1) مصطفى محمد موسى، المرجع السابق، ص 217-218.

(2) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية- دراسة تطبيقية مقارنة-المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي جامعة نايف العربية للعلوم الأمنية الرياض، ص 14 .

(3) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقد في 2009/10/28، لأكاديمية الدراسات العليا، طرابلس.

- غنية نوعيا أكثر من الأوراق ومثال ذلك ميزات أو بيانات تعريف ملف معلوماتي ليس هناك ما يعادلها في عالم الكتابة.

- المعلومة الرقمية عطوبة سواء عن طريق الخطأ أو عمدا [1].

الفرع الثاني: أنواع الدليل الرقمي

تختلف الجريمة المعلوماتية عن الجريمة التقليدية فالأولى تتم في بيئة غير مادية عبر نظام حاسب آلي أو شبكة المعلومات الدولية(الانترنت) حيث يمكن للجان عن طريق (نبضات إلكترونية رقمية)لا ترى أن يعبث في بيانات الحاسب أو برامجه وذلك في وقت قياسي قد يكون جزءًا من الثانية[2] كما يمكن محوها في زمن قياسي كذلك قبل أن تصل يد العدالة إليه مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الالكترونية على الدليل المتوافر، و وفقا لما قررته وزارة العدل الأمريكية سنة 2002 فأن الدليل الالكتروني يمكن تقسيمه إلى ثلاث مجموعات:[3].

1-السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت.

2-السجلات التي تم إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الآلي ATM .

3-السجلات: التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل مثلExcel ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها، يلاحظ أن التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصل إليه، وفي كل الأحوال يظل الدليل المستمد منه

---

(1) نبيل عبد المنعم جاد، جرائم الحاسب الآلي، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي – مطبعة بندسمال، دبي،2005، ص 12.

(2) خالد ممدوح إبراهيم، الدليل الرقمي في الجرائم الالكترونية، بحث منشور على الموقع الالكتروني الآتي:
WWW.F-LOW.NET/LAW/THREADS/ 19223 تاريخ زيارة الموقع 2016/08/15

(3) عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الإنترنت – ندوة الدليل الرقمي – بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من05 -08 مارس2006، ص05.

رقميا، حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسسا على طابع افتراضي مبناه أهمية الدليل الرقمي ذاته وضرورته إلا أنه لكي يحدث تواصل بين القانون وبين الدليل المذكور-نتيجة لنقص توافر الإمكانيات الرقمية في المحاكم -فإنه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلا أصليا، كذلك قسم الدليل الجنائي الالكتروني لقسمين:

أولا : الأدلة التي أعدت لتكون وسيلة أثبات

أ -السجلات التي تم إنشاؤها بواسطة الحاسوب تلقائيا وتعتبر هذه السجلات من مخرجات الحاسوب التي لم يساهم الأفراد في إنشائها, مثل سجلات الهاتف وفواتير البطاقة البنكية[1].

ب- السجلات التي تم حفظ جزء منها بالإدخال وجزء تم إنشاؤه بواسطة الحاسوب مثل رسائل غرف المحادثة المتبادلة على الانترنت و رسائل البريد الالكتروني.

ثانيا: أدلة لم تعد لتكون وسيلة أثبات

وهذا النوع من الدليل الالكتروني نشأ من دون أرادة الفرد وله أثر يتركه الجاني دون أني كون راغبا في وجوده و يسمى بالبصمة الالكترونية وتتجسد في الآثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسل منه أو التي يستقبلها وكافة الاتصالات التي تمتمن خلال الحاسوب و شبكة الانترنت [2].

الفرع الثالث: وسائل جمع و توثيق الدليل الرقمي

تسهم معرفة علوم الحاسب و الأدلة الجنائية و تحليل السلوك في جمع الأدلة الالكترونية الرقمية و عادة ما توجد الأدلة الرقمية في مخرجات الطابعة و التقارير و الرسوم و في أجهزة الكمبيوتر و ملحقاته و في الأقراص المرنة و الصلبة و أشرطة تخزين المعلومات و في أجهزة المودم و البرامج و أجهزة التصوير و مواقع الويب و البريد الالكتروني و لذلك تستخدم عدة طرق و أدوات تسهم في جمع الأدلة الرقمية و هي:

---

[1] خالد عياد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، ط.1، دار الثقافة للنشر و التوزيع عمان 2011، ص 234 .

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، د.ط، دار الكتب القانونية، مصر 2007 ص 64 .

أولا: وسائل جمع الدليل الرقمي

أ-برنامج معالجة الملفات

و هو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضغوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها [1]

ب-برنامج النسخ

وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر و هو برنامج مفيد للحصول على التوازي أو على التوالي و هو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها [2].

ج-قرص بدء تشغيل الكمبيوتر

و هو قرص يمكن المحقق من تشغيل الكمبيوتر إذا كان نظام التشغيل فيه محميا بكلمة مرور ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة Double space **فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.**

د-برامج كشف الدسك

و يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد، ونسخة خاصة بالشرطة[3].

ر- برامج الاتصالات و هو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

---

[1] مصطفى محمد موسى، مرجع سابق ص 220 .

[2] هدى طالب علي، الإثبات الجنائي في جرائم الانترنت و الاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق جامعة النهرين، بغداد، 2012، ص 123 .

[3] مصطفى محمد موسى، المرجع نفسه ص 219-220 .

هذه أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها الخبراء في هذا المجال نظرا لعلمية و دقة هذه الأدلة.

ثانيا: وسائل توثيق الدليل الرقمي

الأدلة الجنائية الرقمية مثل غيرها من الأدلة المادية تحتاج إلى التوثيق والتأمين وبالقدر الذي يكفل لها المصداقية ويبعد عنها العيوب ,وذلك لأسباب عدة منها.

1- التوثيق الذي يحفظ الأدلة الرقمية في شكلها الأصلي تستعمل لعرض وتأكيد مصداقية الدليل وعدم تعرضه لتحريف أو تعديل، فالصورة المسجلة- بالفيديو- مثلا يمكن الاستعانة بها في تأكيد مدى صحة المناقشة الحية عن طريق مطابقة النص الرقمي مع النص المصور على الشاشة.

2- الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة. والتوثيق هو الأسلوب الوحيد الذي يمكن المحققين من القيام بهذا الدور أمام القضاء، و يعتبر فشل المحققين في التمييز بين أصل الدليل وصورته أمام القضاء سببا في بطلان الدليل .

3- من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة إذ أن تشابه أجهزة الحاسوب وملحقاتها يجعل من الصعب إعادة ترتيبها دون توثيق سليم ومفصل حدد الأجزاء والملحقات و أوضاعها الأصلية بدقة.

4- يشكل التوثيق جزء من عمليات حفظ الأدلة الالكترونية حتى انتهاء إجراءات التحقيق والتوثيق يشمل تحديدا دقيقا للجهات التي تحتفظ بالأدلة وقنوات تداولها والتي ينبغي حصرها في نطاق محدود قدر الإمكان[1].

عند توثيق الدليل الرقمي يجب التأكد من أين، كيف، متى، وبواسطة من تم ضبط الدليل وتأمينه؟ كما انه من الضروري توثيق الأدلة الالكترونية بعدة طرق كالتصوير الفوتوغرافي التصوير وطباعة نسخ من الملفات المخزنة في جهاز الحاسوب أو المحفوظة في الأقراص

---

[1] يتكون نظام المعلومات الإدارية في عملية تحريز المضبوطات من العناصر التالية

- وحدة الإرسال و يتولاها مأمور الضبط القضائي المختص بالتفتيش وضبط الواقعة

- قنوات تدفق معلومات الحرز و يمثلها محضر الضبط و كارت الحرز

- وحدة الاستقبال ويمثلها وكيل النيابة العامة.

وعند حفظ الأدلة الالكترونية على الأقراص والشرائط يجب تدوين البيانات التالية على كل منها[1]:

-التاريخ والوقت .

- توقيع الشخص الذي قام بإعداد النسخة .

- رسم او نوع نظام التشغيل

- رسم البرنامج أو الأوامر المستعملة لإعداد النسخ

- المعلومات المضمنة في الملف المحفوظ

المطلب الثاني

القيمة القانونية للدليل الرقمي

إن مجرد وجود دليل يثبت الجريمة وينسبها إلى شخص معين لا يمكن التعويل عليه لإصدار الحكم بالإدانة، إذ يلزم أن يكون لهذا الدليل قيمة قانونية وهذه القيمة للدليل الالكتروني يتوقف على مسألتين رئيسيتين الأولى مشروعية وجود الدليل الالكتروني والثانية مشروعية الحصول على الدليل الالكتروني و هذا ما سنتناوله في هذا المطلب.

الفرع الأول: مشروعية الدليل الرقمي

أولا: مشروعية وجود الدليل الرقمي:

يقصد بمشروعية وجود الدليل أن يكون الدليل معترف به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه لتكوين عقيدته للحكم بالإدانة، ويمكن القول إن النظم القانونية تخلف في موقفها من الأدلة التي تُقبل كأساس للحكم بالإدانة بحسب الاتجاه الذي تتبناه ، فهناك اتجاهان رئيسان، الأول نظام الأدلة القانونية ، والثاني نظام الإثبات الحر .

1- نظام الأدلة القانونية:

وفقاً لهذا النظام فإن المشرع هو الذي يحدد حصراً الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات ، كما يحدد القيمة الاقناعية لكل دليل ، بحيث يقتصر دور القاضي على

---

[1] محمد أمين البشري، الأدلة الجنائية الرقمية مفهومها ودوره افي الإثبات، المجلة العربية للدراسات الأمنية والتدريب، الرياض المجلد 17، العدد 33، 2004، ص 121 .

مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات ، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ينتمي هذا النظام للنظم ذات الثقافة الأنجلوسكسونية، مثل المملكة المتحدة " بريطانيا " والولايات المتحدة الأمريكية فرنسا[1] ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته للنصوص القانونية لذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر إعتناقا له[2].

2- نظام الإثبات الحر

يسود الإثبات الحر في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه ، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبنى هذه القناعة على أي دليل وإن لم يكن منصوص عليه بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات ، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع والقاضي هو الذي يختار من بين ما يُطرح عليه ما يراه صالحاً للوصول إلى الحقيقة وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توافر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل انحصار دور المشرع[3].

وعليه فإنه في مثل هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود على اعتبار أن المشرع لا يعهد عنه سياسة النص على قائمة لأدلة الإثبات، ولذلك فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى اقتناع القاضي به إذا كان هذا النوع من الأدلة

---

(1) سعيداني نعيم، مرجع سابق، ص 209

(2) طارق محمد الجملي، مرجع سابق.

يمكن إخضاعه لتقدير القضائي، إذن وفقا لهذا النظام فإن الأصل في الأدلة مشروعية وجودها، فالدليل الرقمي سيكون مشروعاً من حيث الوجود استصحاباً للأصل [1].

ثانيا: مشروعية الحصول على الدليل الرقمي: يشترط لقبول الدليل الجنائي عموماً كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة ، وذلك يقتضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن، ونحن هنا إذ نبحث مشروعية الدليل الرقمي فإننا سنقتصر على ما يثيره جمع هذا الدليل من إشكاليات قانونية بالنظر إلى طبيعته الخاصة .

و لذا فإن الإشكاليات العامة لجمع الأدلة والتي بدورها لا تقتصر على الدليل الرقمي لن تكون محلاً للبحث الراهن اختصاراً للوقت ولانعدام خصوصيتها بالنسبة لموضوع الدراسة، و في إطار مشروعية الأدلة الرقمية نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أم في مجال التنقيب في الجرائم المعلوماتية.

ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ومن بينها الأدلة الرقمية بطريقة شرعية ونزيهة، وقد قضي في هولندا أنه إذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية.

ومن قبيل الأدلة غير المشروعة الحصول على دليل رقمي من خلال إجراء مراقبة الاتصالات دون أن يكون محل الإذن من السلطة القضائية المختصة أو اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدي إلى المساس بالحياة الخاصة للغير أو ممارسة الإكراه المادي أو المعنوي في مواجهة المشتبه فيه من أجل فك شفرة نظام من النظم

---

[1] هدى طالب علي، مرجع سابق، ص 132.

المعلوماتية أو التحريض على ارتكاب الجريمة عن طرف الضبطية، ويعد من الطرق غير المشروعة أيضا استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية[1].

الفرع الثاني: حجية الدليل الرقمي

لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات [2] ففي ظل النظم القانونية التي تعتمد النظام اللاتيني في الإثبات كالنظام القانوني الليبي و اللبناني و الفرنسي فإن القاضي يملك سلطة واسعة في تقييم الدليل من حيث قيمته التدليلية، فللقاضي قبول الدليل أو رفضه وهو يعتمد في ذلك على مدى اقتناعه الشخصي بذلك الدليل ففي فرنسا فان حجية مخرجات الحاسوب ليست ملحة و عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة، و يدرس الفقه الفرنسي هذه الحجية تحت نطاق قبول الأدلة الناشئة عن الآلة و الأدلة العلمية مثل أجهزة التصوير و أشرطة التسجيل و التصنت[3].

أما النظام الانجلوساكسوني فيرى أن المشرع هو الذي يحدد أدلة الإثبات و يقدر قيمتها الاقناعية في طليعة هذه الدول بريطانيا الولايات المتحدة الأمريكية، فبريطانيا أصدرت قانون إساءة استخدام الحاسوب عام 1990 الذي لم يتناول الأدلة الناتجة عن الحاسوب[4].

أما الاتجاه المختلط فيجمع بين النظامين اللاتيني و الانجلوساكسوني فيعتمد على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الأخر أو يشترط في الدليل شروطا في بعض الأحوال أو يعطي القاضي الحرية في تقدير الأدلة القانونية مثل القانون الإجرائي الياباني حيث يقرر الفقه الياباني أن السجلات الالكترومغناطيسية تكون غير مرئية في حد ذاتها و لذا لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صورة مرئية و مقروءة عن طريق مخرجات الطباعة.

---

[1] سعيداني نعيم، مرجع سابق، ص 210 و ما بعدها.

[2] هلالي عبد الإله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، د. ط، دار النهضة العربية، القاهرة 1999، ص 42.

[3] قضت محكمة النقض الفرنسية " أن أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي.

[4] لقد صدر تشريع الإثبات بالحاسوب في إنكلترا عام 1983 م، وقد ركز بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه والتي تزود بشهادة شفوية تكون مقبولة و التي يتم تقديرها من قبل المحكمة المختصة .

أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل، وإنما بعوامل مستقلة عنه، ولكنها تؤثر في مصداقيته، ولكن هل يمكن التثبت من سلامة الدليل الرقمي من حيث العيوب؟ و بكلمة أوضح هل من الممكن أن يضفى على الدليل الرقمي اليقين من خلال إخضاعه للتقييم الفني الذي يمكِّن من تفادي تلك العيوب التي تشوبه وما موقف القاضي الجنائي من هذا الدليل إذا ما خضع لمثل ذلك التقييم؟ [1].

-وسائل تقييم الدليل الرقمي:

سوف نتناول وسائل تقييم الدليل الرقمي من حيث سلامته من العبث، ثم وسائل تقييمه من حيث سلامة الإجراءات المتبعة للحصول عليه من الناحية الفنية وذلك على النحو الآتي:

أولاً :تقييم الدليل الرقمي من حيث سلامته من العبث:

يمكن التأكد من سلامة الدليل الرقمي من العبث بعدة طرق نذكر منها:

1- يلعب علم الكمبيوتر دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون وهيئة الدليل الرقمي وهذه العلوم يستعان بها في كشف مدى التلاعب بمضمون هذا الدليل وتبدو فكرة التحليل التناظري الرقمي من الوسائل المهمة للكشف عن مصداقية الدليل الرقمي ومن خلالها تتم مقارنة الدليل الرقمي المقدم للقاضي بالأصل المدرج بالآلة الرقمية، ومن خلال ذلك يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.

2-حتى في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي أو في حالة أن العبث قد وقع على النسخة الأصلية، ففي الإمكان التأكد من سلامة الدليل الرقمي من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات[2].

---

[1] مثلما يخضع الدليل الرقمي لقواعد معينة تحكم طرق الحصول عليه، فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية وذلك يرجع للطبيعية الفنية لهذا الدليل، عليه فهناك وسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه .

[2] ممدوح عبد الحميد عبد المطلب و زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من 10-12-2003/05م ،المجلد الخامس، ص 2241 إلى ما بعدها.

3- هناك نوع من الأدلة الرقمية يسمى بالدليل المحايد، وهو دليل لا علاقة له بموضوع الجريمة ولكنه يساهم في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول تعديل أو تغيير في النظام الكمبيوتري.

ثانيا: تقييم الدليل الرقمي من حيث السلامة الفنية

سبق الحديث على أن الدليل الرقمي يتم الحصول عليه بإتباع جملة من الإجراءات الفنية والتي من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، الأمر الذي يحتم إخضاعها إلى اختبارات كوسيلة للتأكد من سلامة هذه الإجراءات من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ويتبع في ذلك مجموعة من الخطوات أهمها إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كلا المعطيات المتعلقة بالدليل الرقمي وفي ذات الوقت لم نضف إليها أي بيان جديد، وهو ما قد يعطي للنتائج المقدمة مصداقية في التدليل على الواقع ويتمثل هذان الاختباران في:

- اختبار السلبيات الزائفة ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي وأنه لم يتم إغفال معطيات مهمة، أما الاختبار الثاني والذي يعرف باختبار الإيجابيات الزائفة فمفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لاختبار يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة.

-الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية والبحوث المنشورة في مجال تقنية المعلومات الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي وفي المقابل بينت تلك الدراسات أيضا الأدوات المشكوك في كفاءتها وهو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[1].

---

[1] سعيداني نعيم، مرجع سابق، ص 218 .

المطلب الثالث

مشاكل الإثبات بالدليل الرقمي

إن إثبات الجريمة من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل لإثباتها و بالتالي فهي تتطلب خبرة فنية عالية و اعتماد أسلوب واضح لتحقيق و لا كن قبل هذا يجب أن نبين نوعية الدليل في هذه الجرائم.

لا يترك المجرم المعلوماتي أو الإلكتروني في الكثير من الأحيان آثار تقودنا إليه من أجل معاقبته، و هذا راجع لكون أن الجريمة مسرحها الشبكة العنكبوتية التي توصف بأنها عالم افتراضي، فكيف لعالم افتراضي أن يبقى على الأثر لحين اكتشافه فبدون أي شعور قد تتعرض للسرقة أو تخترق المواضع دون ترك أي دليل مادي.

الفرع الأول: مشاكل تتعلق بالدليل الرقمي

أولا: عدم ظهور الدليل المادي

كما وضحنا سابقا أن الجريمة المعلوماتية تتم ببيئة لا علاقة لها بالورق أو المحررات فعن طريق "كليك" (clique) بسيط يمكن تغيير الكير من المعلومات في وقت قصير، فيصعب استخلاص الدليل المادي لهذه الجريمة، لأنه في عالم غير واقعي، فهناك الكثير من المواقع التي تحث على الإرهاب و الانتحار و لا يعرف حتى مالكها الحقيقي، لذا فإنه لابد من وضع أجهزة مراقبة و برامج من أجل تفادي الاختراق القرصنة و تأهيل المحققين لتعامل مع المجرمين[1] الذين يتمتعون بمؤهلات عالية فالدليل في الجريمة التقليدية مرئي على العكس من الجريمة المعلوماتية التي تتم دون رؤية لدليل الإدانة ، وحتى في حالة وجود الدليل فان للجاني طمسه أو محوه، فغالبية الجرائم المعلوماتية تكتشف مصادفة وليس بالإبلاغ عنها [2]، ومن مبررات عدم ظهور الدليل المادي هو أننا نتعامل مع معلومة–هذه المعلومة–هي الوسيلة لاقتراف الجريمة المعلومة التي كانت في أصل فكرة جسدت في قالب فني.

---

(1) droit7.blogspot.com/2013/11/blog-post_3422.html

(2) في دراسة مسحية تمت من قبل لجنة التدقيق في انكلترا في شأن الاحتيال المعلوماتي و إساءة استعمال الحاسب شملت 6000 من المؤسسات التجارية وشركات القطاع الخاص تعتمد على الحاسب الآلي في انجاز أعمالها تبين أن ما يقارب من نصف حالات الاحتيال التي تمت ضد هذه المؤسسات و الشركات قد اكتشفت مصادفة و كبدتها خسائر قدرت بنحو 2,5 مليون جنيه استرليني.

و قد أكدت إحصائيات أمريكية أن الموظفين العاملين بالمؤسسات التي تعتمد على نظام المعلوماتية هم أنفسهم الذين يقومون باختراق أجهزة المؤسسات و الاختلاس لدرايتهم بالثغرات الأمنية الموجودة و التعامل معها و بالتالي عدم إمكانية ظهور الدليل المادي و يعمل المجرم المعلوماتي على التخطيط الجيد من أجل عدم ترك دليل مادي، حتى و إن تركه فإنه بإمكانه العودة و محوه قبل وصول أيدي العدالة إليه [1].

ثانيا: سهولة إخفاء الدليل الرقمي

في الجريمة العادية عادة يترك السارق المختلس أو القاتل آثار مادية[2] يمكن أن تستدل بها سلطات التحقيق من أجل إدانة المجرم، و بما أن الجريمة الالكترونية هي جريمة متخصصة فحتى المجرم المعلوماتي أو الالكتروني له طبيعة خاصة ففي الكثير من الأحيان يمكنه محو ما قام به أو مسح آثار الجريمة سواء عند نشر الفيروس أو الاختلاس أو الخرق الآلي أو التسلل إلى الموقع، ومن الأسباب التي تساهم في تعذر الحصول على أثار تقليدية تخلف الجريمة المعلوماتية أن الجاني نفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا، وحتى لو تم ضبطه فقد يرجع هذه الجريمة إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة [3].

ثالثا: إعاقة الوصول إلى الدليل:

جناة الجرائم الإلكترونية من المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو الاستثارة وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، ولذلك نجد أنهم وهم يرتكبون الجرائم الإلكترونية يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة كشف سرتهم وإزالة حجب الشر التي اصطنعوها بأيديهم.

---

(1) droit7.blogspot.com/2013/11/blog-post_3422.html

(2) و نقصد بالأدلة و عدم رؤيتها وعدم تركها للأثر هي تلك الأدلة التي تقودنا إلى الجاني لمعاقبته و ليس الآثار التي يفهم منها التأثيرات الانحلال الخلقي للشباب، مثلا عند نشر الفيروس فآثاره مدمرة بينها تعطيل الأجهزة و عند تشويه المعلومات على الموقع فلذلك آثاره و لكن ليست هي الآثار المقصودة بل المقصود هو الدليل الذي يقودنا إلى المجرم.

(3) غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر و الانترنت، المنعقد في الفترة من 01 الى2000/02/03 بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة، ص 04.

وكمثال لذلك نجد أنهم قد يستخدمون التشفير[1] وكلمات السر التي تمكنهم من إخفاء الأدلة التي قد تكون قائمة ضدهم وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم أن يفهم مقصودها، وقد يقوم هؤلاء أيضا بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها صعبا جدا وليس بِخافٍ كذلك أن هؤلاء الجناة قد يستخدمون الوسائل الإلكترونية المختلفة لإعاقة الوصول إليهم، فقد يستخدمون البريد الإلكتروني في إصدار تكليفاتهم بارتكاب جرائم القتل والاغتيالات والتخريب دون أن يتمكن أحد من تحديد أماكنهم أو تسجيل هذه التكليفات على النحو الذي كان يحدث في الاتصالات السلكية واللاسلكية.

كذلك فإن مرتكبي جرائم الإنترنت يصعب ملاحقتهم لاستحالة تحديد هويتهم سواء عند قيامهم ببث المعلومات على الشبكة أو عند تلقيهم لها، لأنهم في الغالب يستخدمون أسماء مستعارة أو يدخلون إلى الشبكة ليس عن طريق أبواب حاسباتهم الآلية وإنما عن طريق مقاهي الإنترنت أيضا فإنه يلاحظ أن ملاحقة جرائم الإنترنت قد تتعلق ببيانات تكون مخزنة في داخل دولة أجنبية بواسطة شبكة الاتصال عن بعد، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة. ولعل هذا الأمر يكشف لنا عن أهمية التعاون القضائي الدولي في مجال الإنابة القضائية خاصة في مجال الجرائم العابرة للقارات والتي منها تلك الجرائم التي تقع بسبب ثورة الاتصالات عن بعد[2].

رابعا: صعوبة فهم الدليل الرقمي:

لا شك في أن طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل فنية لا يقوى على فهمها إلا الخبير المتخصص، بعكس الدليل القولي فإن الكثير ممن يتصلون به يسهل عليهم فهم مضمونه وإدراك حقيقته، وإذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الإلكترونية قد يتحصل من عمليات فنية معقدة عن طريق التلاعب في نبضات وذبذبات الكترونية وعمليات أخرى غير مرئية، فإن الوصول إليه وفهم مضمونه قد يكون في

---

[1] التشفير هو العلم الرياضي للرموز و الشيفرات و الرسائل السرية حيث استدم الناس التشفير عبر التاريخ لتبادل رسائل لا يمكن قراءتها (على ما يأملون) من قبل أي كان ما عدى الشخص المقصود لتلقي الرسالة، منشور على الرابط التالي:
https://ssd.eff.org/ar/module/

[2] غنام محمد غنام، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي منشور على الموقع التالي:
http://www.f-law.net/law/threads/11333 بتاريخ 2008/03/05

غاية الصعوبة فالطبيعة و تثار مشكلات عديدة في الإثبات الجنائي، ومثال ذلك أن إثبات التدليس الذي قد يقع على نظام المعالجة الآلية للمعلومات يتطلب تمكين مأمور الضبط القضائي أو سلطة التحقيق من جميع المعطيات الضرورية التي تساعد على إجراء التحريات والتحقق من صحتها للتأكد عما إذا كانت هناك جريمة قد وقعت أم لا، ومثل هذا الأمر يتطلب إعادة عرض كافة العمليات الآلية التي تمت لأجل الكشف عن هذا التدليس.

وقد يستعصى هذا الأمر على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة كذلك فإن الكثير من العمليات الآلية للبيانات التي قد يقوم بها الحاسب الآلي بطريقة آلية دون الحاجة إلى عمليات إدخال كما هو الحال في احتساب الفائدة على الإيداعات البنكية والتي تقيد آليا بأرصدة حسابات العملاء على ضوء الشروط المتفق عليها مسبقا والمخزنة في برنامج الحاسب، قد يكون من السهل اختراقها وارتكاب جرائم تزوير واستيلاء تقع عليها عن طريق إدخال بيانات غير معتمدة في نظام الحاسب أو إجراء تعديلات في برامجه أو القيام بالتلاعب في البيانات المخزنة[1].

وبالنظر إلى أن طبيعة هذه العمليات يصعب أن تخلف وراءها آثار مادية ملموسة تكشف عنها، فإن ذلك سيزيد من صعوبة عمل المحققين الذين يعملون في حقل الجرائم التي تتمخض عن هذه العمليات الإلكترونية، فقد يستعصى عليهم فهم الأدلة المتحصلة عن هذه الوسائل بسبب تعقيدها وصعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات.

أيضا فإن فهم الدليل الموصل إلى إثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية قد يزداد صعوبة، في تلك الحالات التي يتصل فيها الحاسب الآلي بشبكة الاتصالات العالمية، ففي مثل هذه الحالات فإن فهم مثل هذا الدليل يحتاج إلى خبرة فنية وقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل السبل لضبطه.

و بالنظر إلى أهمية الخبرة في فك غموض الجرائم التي تقع بالوسائل الإلكترونية، فإن ذلك يكشف لنا عن الأهمية المتزايدة لتدريب الخبراء القضائيين على تقنيات الحاسبات الآلية لتمكينهم من القيام بمهامهم في المسائل الإلكترونية الدقيقة وإعداد تقاريرهم الفنية فيها

---

[1] غنام محمد غنام، المرجع نفسه.

والتي تكون ذات أهمية بالنسبة لقضاء الحكم الذي غالبا ما يتخذ منها سندا يرتكن إليه في المسائل الفنية البحتة [1].

الفرع الثاني: مشاكـل الاستــدلال

كما ذكرنا سابقا فإن مشاكل إثبات الجرائم الالكترونية أنها تترك أثر كما يصعب الاحتفاظ بالآثار، بحيث تعتمد على التقنيات العالية حيث يصعب الاستدلال فيها و مع صعوبة إثباتها إلا أن ما يزيد الوضع سوءا هو الإحجام عن الإبلاغ و أيضا نقص الخبرة في هذا المجال

أولا : عدم الإبلاغ

إن عدم الإبلاغ من طرف الأشخاص الذين شاهدوا المجرم عند قيامه بالجريمة هو ما زاد في عدم اكتشاف الجريمة، ومن أسبابه نجد :

-عدم إبلاغ الشركات وخصوصا التجارية منها بعمليات الخرق التي يقوم بها المجرم المعلوماتي، هذا الإبلاغ يتسرب إلى المجرم المعلوماتي و بالتالي تكشف الثغرات الأمنية في النظام المعلوماتي، نقص الغطاء تشريعي لهذه السلوكيات، و قد يحدث أن يبلغ عن سلوكيات مشبوهة للمجرمين المعلوماتيين و لكن في الكثير من الأحيان لا يمكن اكتشاف الشخص الذي قام بالسلوك الإجرامي، فمثلا جريمة نشر فيروس في الكثير من الأحيان لا يمكن اكتشاف الشخص الذي قام بنشره. و مما يزيد من مشكل عدم الإبلاغ ما يلي :

- المعرفة المتأخر من أن الجهاز أصيب بفيروس عن طريق الشبكة

- تحويل الشبكة لساحة من المعارك بين الدول مما أصبحت المعاملات التجارية غنيمة سهلة للاختراق [2] .

---

[1] إن فهم الأدلة الفنية التي تتحصل من الوسائل الإلكترونية يتطلب أيضا تدريب جهات الضبط القضائي والتحقيق والقضاء على فهم طبيعة المعطيات التي تقع عليها الجرائم الإلكترونية، والعمل على إلمامهم بمكونات الحاسب الآلية وكيفية عملها ومعرفة اللغة التي تتعامل بها، والتي تعتمد على المختصرات خاصة وان الجرائم التي تقع باستخدام الوسائل الإلكترونية في الغالب ما تعتمد على رموز تكون معروفة عند أهل العلم والخبرة . ولقد جاء في توصيات المجلس الأوروبي الصادر في سنتي 1985 و 1995 بما يفيد ضرورة استحداث دوائر جديدة تضطلع بمواجهة جرائم الحاسب الآلي وتزويدها بالموظفين الأكفاء ذوي الخبرة والدراية العلمية بالإضافة إلى توفير الأجهزة والمعدات التقنية اللازمة لذلك .

[2] و على ضوء هذه الصعوبات عرضت بعض الاقتراحات على لجنة خبراء مجلس أوربا و لكن قوبل هذا الاقتراح بالرفض لأن الشركة التي تم التسلل لموقعها تصبح هي الجانية و ليست المجني عليها. و من الصعوبات التي تواجه الإبلاغ أيضا هو عدم وجود شبكة دولية فعلية للتبادل المعلوماتي .

– ضخامة الأضرار حيث أن الفيروس ليس مقيد برقعة جغرافية معينة.

ثانيا : نقص الخبـرة

إن صعوبة اكتشاف الجريمة بالدرجة الأولي مرده إلى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر و الانترنت و الطرف الآخر قراصنة محتلون و منحلون أخلاقيا يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية و قد وصل

اسم النخبة أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء [1]، و من العوامل المساعدة في نقص الخبرة في الجرائم المعلوماتية هي :

– عدم تخصيص أموال من أجل التأهيل الجيد للمحققين و كذا حداثة الجريمة و خصوصيتها التي لم يعتد عليها رجال الشرطة، مما جعلهم قاصرين في مواجهتها.

– ضخامة المعلومات على الشبكة و انتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق.

– الإنترنت بيئة خصبة للسلوك الإجرامي .

– التطور السريع للتقنية الحديثة و عدم وجود هيئات قضائية مختصة .

– وجود مواقع على الشبكة تسهل عملية إرسال البريد الالكتروني دون الحاجة إلى ذكر البيانات

و يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة و المهارات للمتخصصين لوضع مناهج مدروسة للتدريب على التحقيق مع مراعاة خصوصية التطور التقني السريع دون إهمال التعاون الدولي في مثل هذه الحالات.

ثالثا: عدم وجود تعاون دولي

في ظل الصراعات الحاصلة، يصعب إيجاد تعاون دولي حقيقي لمكافحة وكشف الجريمة الإلكترونية، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين و تتحقق النتيجة في بلد أخر كقيام مجموعة من المجرمين بتشويه معلومات معينة وليس بالضرورة أن ينتج هذا السلوك وأثاره في بلد المجرمين، فما هو محضور في الجزائر من الناحية الأخلاقية مباح في دول أخرى.

---

[1] نلاحظ أن عملية سن التشريعات أبطأ من عملية الإجرام و هذا في العالم كله دون استثناء

و التطور السريع للجريمة و المعالجة البطيئة للحالات، ساعد المجرم المعلوماتي على الاستفادة من هذه العقبات للعبث والتخريب [1].

المبحث الثاني

القواعد الإجرائية لاستنباط الدليل الرقمي

إن الجرائم المعلوماتية إلى جانب طابعها الافتراضي تعد كغيرها من الجرائم الأخرى لها جانب تقليدي من خلال الأجهزة المادية كالحاسوب و الطابعات و غيرها ممن يمكن التعامل معهم كمسرح مادي للجريمة فلا يمكن الاستغناء عن الإجراءات العامة للتحقيق و التي تطبق في كل الجرائم التقليدية و المستحدثة على حد سواء كالمعاينة من طرف ضابط الشرطة القضائية و جمع الاستدلالات و تفتيش نظم الحاسب المادية و ضبط الدليل .

و لكن إلى جانب ذلك يثار إشكال فيما يخص الطبيعة الخاصة للجريمة و طابعها الافتراضي و مكوناتها المعنوية التي لا يمكن أن يطبق عليها القواعد العامة فحسب لان طبيعتها تتطلب تقنيات جديدة للبحث عن الجاني و الوصول للدليل الذي له طابع خاص لذا سنتناول في المطلب الأول القواعد الإجرائية العامة للتحقيق والمطلب الثاني القواعد الإجرائية الخاصة و التي جاء بها قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها [2] .

---

[1] تنشأ ضرورة وجود توافق دولي محكم في مجال الحق في المعلومات على وجه الخصوص من سهولة حركة المعلومات في أنظمة تقنية المعلومات حيث يرجع لهذه السهولة في حركة المعلومات بأنه بالامكان ارتكاب جريمة عن طريق حاسب آلي موجود في دولة معينة بينما يتحقق نجاح هذا النشاط الإجرامي في دولة أخرى، وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال والذي يعتبر ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقنية نظم المعلومات ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات. وفي مجال الإجراءات فإن التوافق بين مختلف سلطات التدخل الوطنية سيكون هاما من أجل التيسير دون عقبة لطلب المساعدة القانونية الوطنية، أنه قد تلتمس إحدى الدول المساعدة القضائية من دولة أخرى بحيث يمكن لهذه الأخيرة أن تباشر التدابير التي تكون طبقا لقوانينها الخاصة

[2] قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

المطلب الأول

القواعد الإجرائية العامة لاستنباط الدليل الرقمي

على الرغم من وجود اختلاف بين إجراءات التحقيق في الجرائم المعلوماتية و إجراءات التحقيق في الجرائم الأخرى، فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة و التفتيش و الاستجواب بالإضافة إلى جميع الأدلة، كما تشترك في كونها تسعى للإجابة على الأسئلة المشهورة لدى المحقق بهدف كشف الحقيقة بمساعدة الخبرة و الشهادة التي تقود المحقق لضبط الدليل الرقمي، وتعتبر مرحلة ضبط الدليل النتيجة التي تعقب إجراءات البحث و التفتيش عن الدليل والتي سنحاول دراستها في هذا المطلب.

الفرع الأول: المعاينة.

يقصد بالمعاينة مشاهدة و إثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها و هي من إجراءات التحقيق الابتدائي و يجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق، و تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لبيان مدى صحتها في الإثبات فليس الحال كذلك بالنسبة للجرائم المعلوماتية، حيث نادرا ما يتخلف عن ارتكابها آثار مادية و قد تطول الفترة الزمنية بين وقوع الجريمة و اكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها[1].

وينبغي التعامل مع مسرح الجريمة الإلكترونية على أنه مسرحان:

1- مسرح تقليدي: ويقع خارج بيئة الحاسوب والانترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية يترك فيها الجاني آثار كالبصمات،أو وسائط تخزين رقمية[2] و يتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه[3].

---

(1) هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتب الآلات الحديثة، د.ط، مصر، 2002، ص 39.

(2) بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسة القانونية، العدد الأول 2013، ص 68.

(3) يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون-تخصص القانون الدولي للأعمال جامعة مولود معمري-تيزي وزو-كلية الحقوق و العلوم السياسية، 2013، ص84 .

2- مسرح افتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله[1] و التعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية[2].

و عند تلقي بلاغ عن وقوع إحدى الجرائم المعلوماتية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، و يرى الفقه الجنائي ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية مثل تصوير الحاسب و الأجهزة الطرفية و إخطار الفريق الذي يتولى المعاينة والذي يعد خطة موضوعية بالرسومات، كما عليه إثبات حالة التوصيلات والكابلات ليتمكن من إجراء المقارنة عند العرض على المحكمة مع ضرورة عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل التأكد من خلو المحيط من أي قوى مغناطيسية قد تتسبب في محو البيانات، كما يجب أن يتم التحفظ على محتويات سلة المهملات التي قد تكون ذات صلة بالجريمة، ومن الضروري أن تتم المعاينة من طرف المحققين ذوي الكفاءة العلمية و الخبرة الفنية في مجال المعلوماتية و أن تتم وفق مبدأ المشروعية [3].

الفرع الثاني: التفتيش و ضبط الدليل الرقمي

يهدف التفتيش إلى البحث عن الحقيقة في مستودع السر وهو من أهم إجراءات التحقيق في كشف الحقيقة، و غالبا ما يسفر عن أدلة مادية، و يباشر إما على شخص المتهم و أما على مسكنه[4] و إذا كان لتفتيش الأشياء المادية للحاسب لا تثير إشكالية فما مدى خضوع البرامج و المعلومات كمكونات معنوية للتفتيش، و هذا يتطلب منا البحث في مسالة المحل الذي ينصب عليه هذا الإجراء.

---

(1) جميل عبد الباقي صغير، الجوانب الإجرائية للانترنت، د.ط ، دار الفكر العربي، القاهرة، 2001، ص 28.

(2) محمد بن نصير السرحاني، مرجع سابق، ص 77.

(3) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 20117، ص 17

(4) سعيداني نعيم، مرجع سابق، ص 144 .

أولا: التفتيش

1-إجراءات التفتيش في المنظومة المعلوماتية

أ-تفتيش منظومة الحاسب الآلي المادية

إن الدخول للمكونات المادية للحاسب بحثا عن ما يتصل بجريمة معلوماتية للكشف عن مرتكبيها لا خلاف فيه بين الفقهاء طالما تم وفقا للإجراءات القانونية المقررة، فان كانت في مكان خاص كمسكن المتهم كان لها حكمه فلا يجوز تفتيشها إلا في حالات يجوز فيها تفتيش مسكنه بنفس الضمانات المقررة قانونا في التشريعات المختلفة و إن كانت في مكان عام كالمقاهي الشوارع كان لها حكمه [1]

إلا أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية القانون06-22 [2] استثنى بموجب المادة 45 و كذا الفقرة 02 من المادة 47 و الفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند التفتيش بخصوص جرائم المعلوماتية، أي أن المشرع لا يشترط حضور الشخص المشتبه فيه عند تفتيش مسكنه، و انه يجوز القيام بذلك في كل ساعة من ساعات الليل أو النهار و دون الحاجة إلى رضا صاحب الشأن[3] و قد نص المشرع الجزائري في المادة 44 من ق.إ.ج أن التفتيش يرد على أشياء و هي كلمة تنصرف في الأرجح على المكونات المادية [4] و بالتالي لا يوجد مانع قانوني أن ينصب التفتيش على المكونات المادية للحاسوب و ملحقاته و معداته.

ب- تفتيش مكونات الحاسب الآلي المعنوية

إذا كانت المكونات المادية للحاسوب صالحة للتفتيش كمحل فان امتداد ذلك إلى مكونات غير مادية هو محل جدل كبير حول مدى صلاحيتها أن تكون محل للبحث عن الأدلة المادية لتقديمها للمحكمة المختصة كدليل إدانة، لذا يثور الشك في ما إذا كان البحث عن الأدلة في

---

(1) طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي في النظام القانوني لحماية المعلوماتية دون طبعة، دار الجامعة الجديدة، مصر، ص 397 .

(2) قانون 06-22 المتضمن تعديل قانون الإجراءات الجزائية (الامر 66-155 المؤرخ في 08 يونيو 1966، يتضمن قانون

الإجراءات الجزائية المعدل و المتمم- الجريدة الرسمية رقم 49 سنة 1966).

(3) انظر المواد: 45، 47، 64 من قانون الإجراءات الجزائية.

(4) و في نفس القول تنصرف ما جاءت به المادة 64 من نفس القانون بنصها "لا يجوز تفتيش المساكن...ضبط الأشياء

الحاسوب نوعا من التفتيش باعتبارها ليس لها مظهر مادي[1]، فنجد القانون اليوناني في المادة 251 تعطي سلطة التحقيق إمكانية القيام بأي شيء يكون ضروري لجمع و حماية الدليل و يفسر الفقه اليوناني عبارة "أي شيء" تشمل البرامج و البيانات المعالجة الكترونيا[2] وهناك جانب من التشريعات الإجرائية قد حدد الهدف من التفتيش في البحث عن الأشياء و ضبطها هذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس لا يمتد في نطاق شموله إلى الكيانات المنطقية، و قد عملت الدول التي تأخذ بهذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية، و يتضح موقف المشرع الجزائري من خلال قانون 09-04 حيث نص في المادة 05 [3] على جواز تفتيش المنظومة المعلوماتية، و كذلك المشرع الفرنسي الذي قام بتعديل النصوص التي تحكم التفتيش و أضاف عبارة"المعطيات المعلوماتية" و قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي أخر أو في بلد أخر و نميز هنا بين احتمالين:

الاحتمال الأول: اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان أخر داخل الدولة: يثار هنا التساؤل عن مدى امتداد الحق في التفتيش إذا تبين إن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بنهاية طرفية في مكان أخر مملوك لشخص غير المتهم.

---

[1] عبد العظيم وزير، شرح قانون العقوبات القسم الخاص جرائم الاعتداء على الأموال الطبعة الأولى، دار النهضة العربية القاهرة، 1993 ، ص 40 .

[2] على النقيض من ذلك إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فان المفهوم المادي لا ينطبق على برامج و بيانات الحاسب الآلي غير المحسوسة ، يقترح هذا الرأي في مواجهة القصور التشريعي ضرورة أن تضاف إلى هذه الغاية التفتيشية عبارة (مواد معالجة آليا) لتصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني البحث عن الأدلة أو أي مادة معالجة بواسطة الحاسب الآلي.

[3] " تنص على انه يجوز للسلطات القانونية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها و كذا منظومة تخزين معلوماتية.

يرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 163 من قانون الإجراءات الألماني [1].

و يعتبر المشرع الجزائري من بين هذه التشريعات حيث نص في الفقرة الثانية من المادة 05 من قانون 09-04 [2] إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة بذلك. و المشرع الفرنسي قد حسم هذه المسالة بتعديله قانون الإجراءات الجزائية بموجب القانون 2003/239 المتعلق بالأمن الداخلي الصادر في 18 /2003/03 المادة 17 أجازت لضباط الشرطة القضائية أو تحت مسؤولياتهم الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي فيها التفتيش عن المعطيات التي تهم التحقيق و المخزنة في النظام المذكور أو في نظام أخر بما أن هذه المعطيات يتم الدخول إليها أو نكون متاحة انطلاقا من النظام الرئيس [3] .

الاحتمال الثاني: اتصال حاسب المشتبه فيه بحاسب آخر أو نهاية طرفية موجودة في مكان أخر خارج الدولة: يتم تخزين بياناته في أنظمة معلوماتية خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة [4] في هذه الحالة فان امتداد الإذن بالتفتيش إلى خارج إقليم الدولة التي صدر من جهتها المختصة الإذن و دخول في إقليم دولة أخرى و التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك الدولة بسيادتها لذا لا بد من أن يتم التفتيش في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد أو

---

(1) تصبح المادة على النحو التالي" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء مادية أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة.

(2) المادة 05 من قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 05 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال.

(3) تنص المادة 2/17 من القسم الرابع على انه من حق السلطة القائمة بتفتيش الكمبيوتر المتواجدة بدائرة اختصاصها أن تقوم في حالة الاستعجال بمد نطاق التفتيش إلى جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الأصلي محل التفتيش.

(4) عبد الله حليس علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات ، بحث منشور على موقع:
www.arablawinfo.com

يعقد بين الدول المعنية، و هذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الالكتروني [1] بموجب المادة 5/ف3 من القانون 04/09.

ثانيا: ضوابط التفتيش

- الضوابط الشكلية للتفتيش

إن القواعد الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات الفردية ولعل أبرز هذه الشروط هي:

-إجراء التفتيش بحضور أشخاص معينين في القانون

إن من التشريعات المقارنة من أوجب حضور عملية التفتيش الذي تجريه الضبطية القضائية المشتبه فيه أو شهود و أوجبت تشريعات أخرى حضور أشخاص معينين في القانون وأجازت في أحوال أخرى إجراء التفتيش دون حضور أحد، وهناك تشريعات سكتت تماما عن التعرض لهذا الشرط[2] والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء، و المشرع الفرنسي استوجب في الفقرة الأولى من المادة 57 من قانون الإجراءات الجنائية حضور صاحب المسكن وعدم حضوره يترتب عليه البطلان.

غير أن المشرع الجزائري بموجب المادة 45 من القانون رقم 06 - 22 المؤرخ في 20 ديسمبر 2006 استثنى إجراء الحضور لبعض الأشخاص إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه اوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات .

- محضر تفتيش نظم الحاسب الآلي

التفتيش من أعمال التحقيق لذا ينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر عموما والتي

---

[1] محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية –محور القانون الجنائي – بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية من 26 إلى 28 افريل، دبي، 2003، ص 350.

[2] سعيداني نعيم، مرجع سابق، ص 152.

تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[1].

- الميعاد الزمني لإجراء التفتيش في البيئة الرقمية:

حرصت التشريعات الإجرائية على حضر تفتيش المنازل وما في حكمها في وقت معين فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساء، أما بالنسبة لتشريعات الدول الانجلسكسونية كالقانون الانجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين والمشرع الجزائري ذهب إلى حضر تفتيش المساكن وما في حكمها في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساء و استثناء يصح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد 342 إلى348 [2]من قانون العقوبات المرتكبة في أماكن معينة أو في حالة رضا صاحب المسكن صراحة وفي نطاق التفتيش المتعلق بالجرائم المعلوماتية فإن الاستثناء الوارد بالفقرة الثالثة من المادة 47 ق.إ.ج[3] المعلوماتية حيث جاء في نصها".... عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ... فإنه يجوز إجراء التفتيش...في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص."

- الإذن بالتفتيش: لم ينص المشرع في القانون 04/09 صراحة على وجوب استصدار الإذن بتفتيش نظم المعلوماتية في حالة التحريات المتعلقة بالجرائم المتلبس بها أو التحريات الأولية لكن بالرجوع إلى الفقرة 05 التي نصت على انه "يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية ..." أي أن قيام ضباط

---

[1] عبد الله هلالي، تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة، طبعة أولى، دار النهضة العربية مصر، ص 77.

[2] جاءت المواد من 342 الى 348 في القسم السابع من الفصل الثاني من قانون العقوبات تتضمن تحريض القصر على الفسق و الدعارة.

[3] المادة 47 **من قانون الإجراءات الجزائية المعدل و المتمم (الأمر 66-155 المؤرخ في 08 يونيو 1966- الجريدة الرسمية رقم 49 سنة 1966).**

الشرطة القضائية بالتفتيش يكون بناء على قواعد قانون الإجراءات الجزائية التي تفرض أن يتم التفتيش المساكن على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق[1].

– تحديد مجال الإذن بالتفتيش أورد المشرع الجزائري على تطلب شرط التحديد لصحة الإذن بالتفتيش إذ نصت المادة 44 " ... يجب أن يتعين الإذن بالتفتيش بيان وصف الجرم وعنوان – الأماكن التي يتم زيارتها وتفتيشها وذلك تحت طائلة البطلان" [2] إلا انه وفي نطاق تفتيش الأنظمة المعلوماتية فان المادة المطلوبة قد تختلط بكميات من البيانات الأخرى التي لا تناسب الموضوع قيد التحقيق لذلك فإنه لا يستقيم الأمر مع مبدأ الخصوصية، كما أن ضبط النظام برمته قد يسبب خسارة ، ويثير إمتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه يرى البعض في هذه الحالة عدم امتداد البحث لديه إلا في حالتي التلبس أو رضائه بالتفتيش[3] و يثور التساؤل حول ما إذا كان كل ملف يلزم إذن قضائي مستقل عن الأخر[4] و المشرع الجزائري كأغلب التشريعات لا يقدم حلا لهذه المسألة، و في الولايات المتحدة الأمريكية وجد تضارب بين الأحكام القضائية بخصوص هذه المسألة ففي ما اعتبرت بعض الأحكام أن جهاز الحاسوب بما يحتويه من ملفات ومعلومات صندوقا واحدا ولا يستوجب تفتيشه إلا إذنا واحدا فقط، اعتبرت على خلاف ذلك أحكام أخرى أن كل ملف في الحاسوب يتطلب إذنا خاصا لتفتيشه [5]و من الدول التي حددت مجال الإذن بالتفتيش الولايات المتحدة وكندا[6].

---

(1) احمد مسعود مريم،- مرجع سابق، ص 90 .

(2) المادة 44 من قانون الإجراءات الجزائية المعدل و المتمم .

(3) التحقيق الجنائي الالكتروني، مقالة منشورة على موقع مدونة المحترف، 2010، 09:41 :www.th3professional.com

(4) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، د.ط، دار الجامعة الجديدة، 2007، ص 292.

(5) تسبيب الحكم على أساس أن الكومبيوتر يحتوي على الكثير من الملفات، وإذا كان أجيز لضابط الشرطة القضائية فتح الملفات الأخرى الموجودة داخل جهاز الحاسوب فإن ذلك سوف يؤدي بالفعل إلى الاعتداء على الحياة الخاصة للفرد.

(6)حيث نصتا على أن يكون إذن التفتيش متضمنا:

–البحث عن أدلة متحصلة من كيان الحاسب المنطقي والتي يدخل فيها برامج التطبيق و نظم التشغيل.

–البيانات المستخدمة بواسطة برنامج الكومبيوتر.

–السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.

–السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

- محل التفتيش

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سر و محل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال. وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجود فيه فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا لاسيما اشتراط الإذن بالتفتيش من السلطات القضائية المختصة وهو ما نصت عليه المادة 44 من قانون الإجراءات الجزائية[1].

2-الضوابط الموضوعية للتفتيش

1-السبب:

أ- وقوع جريمة معلوماتية :

ضرورة وقوع جريمة من الجرائم المعلوماتية التي نص عليها المشرع في نصوص التجريم والعقاب، كما هو الحاصل في التشريع الجزائري الذي أدرج فصلا خاصا- الفصل السابع -في قانون العقوبات لجرائم الاعتداء على نظم المعالجة الآلية للمعطيات ذلك أن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية غير مشروعة وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29 يونيو1990[2] .

ب- ضرورة الاشتباه في شخص معين:

لا يكفي لقيام سبب التفتيش وقوع جريمة معلوماتية بل لا بد أن يكون هناك اتهام موجه ضد شخص معين أو أن تتوافر دلائل كافية تدعو للاعتقاد بارتكابه للجريمة حتى يمكن انتهاك

---

(1) تنص المادة على: "أنه لا يجوز لضباط الشرطة القضائية الدخول إلى المساكن وإجراء التفتيش إلا بإذن مكتوب من وكيل الجمهورية أو من قاضي التحقيق، وهذه الضمانة خاصة بجميع الجرائم بما فيها الجرائم المعلوماتية، أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة فإن أغلب التشريعات تجيز لرجال الضبطية دخول المحلات العامة المفتوحة للجمهور كمقاهي الأنترنت من أجل مراقبتها و التأكد من احترامها للأخلاق والآداب العامة بكل سهولة دون حاجة لإذن بالتفتيش

(2) و في فرنسا صدر قانون رقم 19/88 في 05 يناير 1988 وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور قانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994 .

حق الخصوصية لديه وتفتيش حاسوبه وبرامجه الخاصة ويمكن الاستدلال على ذلك بما نصت عليه المادة 46 ق.إ.ج، ومن الدلائل المستمدة من القرائن التي تنبئ عن ارتكاب الشخص لجريمة معلوماتية وأن يتم تحديد هوية الحاسوب وكان يخص شخصا بعينه[1].

ج-توافر قرائن لدى المتهم تفيد في كشف الحقيقة

يجب توافر أمارات وقرائن قوية على وجود أشياء في كشف الحقيقة لدى المشتبه فيه أو غيره[2] ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

إلا أنه وبالرجوع إلى نص المادة 05[3] من القانون 09-04 نجد أن المشرع قد أجاز إمكانية اللجوء إلى إجراء تفتيش النظام المعلوماتي للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرتها المادة الرابعة من نفس القانون، وهو الأمر الذي يفهم صراحة بقراءة نص المادتين معا.

ثانيا: ضبط الدليل الرقمي

تعتبر مرحلة ضبط الدليل هي النتيجة التي تعقب إجراءات البحث و التفتيش عن الدليل و لقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط، لكن في مجال الجرائم المعلوماتية لإثبات هذا النوع من الجرائم فان الدليل ليس كالدليل التقليدي فالبيئة الافتراضية لا تنتج سكينا أو سلاحا ناريا وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي فما مدى صلاحية هذا النوع من الدليل لأن يكون محلا للضبط؟والتحفظ على هذه الأدلة، ويؤدي بطلان التفتيش إلى بطلان الضبط[4] و لقد اختلفت والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والتي لا تصلح بطبيعتها محلا لوضع اليد، وانقسمت في ذلك إلى اتجاهين:

---

(1) تنص على "لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية ويحوزون أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش ...."

(2) سعيداني نعيم، مرجع سابق، ص 154.

(3) تنص على:" يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية....الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها..."

(4) محمد سعيد نمور، أصول الإجراءات الجزائية-شرح لقانون أصول المحاكمات الجزائية- طبعة أولى- دار الثقافة للنشر والتوزيع، الأردن، 2005 ، ص359.-

الاتجاه الأول: يرى أصحابه أنه لا يمكن تصور إجراء الضبط على الكيانات المنطقية للحاسوب لانتفاء الكيان المادي عنها، وبالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لانتفاء الطابع المادي عن هذه البيانات في حال تجردها عن الدعامة المادية[1] ومن التشريعات التي أخذت هذا الاتجاه قانون الإجراءات الجنائية الألماني.

-الاتجاه الثاني :يرى أنصار انه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الجريمة و بيان الحقيقة فان هذا المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها[2].

و المشرع الجزائري يرى إمكانية حجز المعلومة و من ثمة و طبقا لأحكام المادة 06 من القانون 09-04 عندما يتوصل المحققون أثناء إجراء التفتيش في منظومة معلوماتية إلى وجود معطيات تفيد التحقيق يمكنهم حجزها برمتها بعد نسخها على دعامة مادية كطبعها على الورق أو ضبطها على الشاشة لتسهيل قراءتها و التعامل معها. و إلى جانب المشرع الجزائري نجد الفقه الفرنسي ذهب إلى الاعتراف بان للبرنامج كيانا ماديا ملموسا يتمثل في نبضات الكترونية أو إشارات الكترونية مغناطيسية أو ممغنطة .

- محل الضبط:

يختلف الضبط في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل و ذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية و التي تكون في هيئة رموز و نبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسيب التي تحفظها، أما الثاني فيرد على أشياء مادية[3]

1-ضبط المكونات المادية للمعلوماتية:

لا يثير ضبط المكونات المادية للحاسب أية صعوبات في التنفيذ أو مشكلات و بالتالي يمكن ضبط الوحدات المعلوماتية الآتية:

---

[2]عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، د.ط، منشأة المعارف، الإسكندرية، ص358 .

[2]طارق ابراهيم الدسوقي عطية، مرجع سابق، ص 442.

بوعناد فاطمة زهرة، مرجع سابق، ص 69 .

– وحدة المدخلات، وحدة الذاكرة الرئيسية، وحدة الحساب و المنطق، وحدة التحكم و وحدة المخرجات[1]، و السبب في ذلك أن الضبط لم يرد–حسب الأصل–على أشياء معنوية، إنما ورد على أشياء مادية و هي المكونات المادية للحاسب.

2– ضبط المكونات المعنوية للمعلوماتية:

لا شك أن ذلك يثير صعوبات عديدة بالنظر إلى طبيعة محل الجريمة[2] وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم ضبط جهاز الكومبيوتر وملحقاته، ولأجهزة الكومبيوتر أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه والتعرف على مواصفاته بسرعة منها ضبط المعدات المستعملة في شبكة الانترنت وأهمها المودم (MODEM)، وسائط التخزين المتحركة كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة والأشرطة المغناطيسية، ضبط البرمجياتSoftware' ضبط البريد الإلكتروني والذي يحتوي على برامج متخصصة لكتابة و إرسال واستعراض وتخزين الرسائل الإلكترونية.

الفرع الثالث: الاستعانة بالخبرة و الشهادة

أولا: الاستعانة بالخبرة

إذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق و القاضي فهي اوجب في مجال الجرائم المعلوماتية حيث تتعلق بمسائل فنية أية في التعقيد و محل الجريمة فيها غير مادي و التطور في أساليب ارتكابها سريع و متلاحق و لا يكشف غموضها إلا متخصص و على درجة كبيرة من التميز في مجال تخصصه.

1– أهمية الاستعانة بالخبرة و شروط صحتها

إن أهمية الاستعانة بالخبير في الجرائم المعلوماتية تظهر عند غيابه فقد تعجز الشرطة في كشف الجريمة أو تدمر الدليل بسبب الجهل أو الإهمال في التعامل معه و الخبير لا يشترط فيه كفاءته فحسب بل يضاف إليها سنوات من أعمال الخبرة في مجاله[3].

---

(1) طارق ابراهيم الدسوقي عطية، مرجع سابق، ص 449.

(2) زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، د.ط، دار الهدى للطباعة و النشر و التوزيع، الجزائر **2011**، ص **210** و ما بعدها .

(3) علي عدنان الفيل، مرجع سابق، ص 27 و ما بعدها.

ومن الشروط التي درجت أغلب التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة فأما ما يتعلق بالخبير فأنه يشترط:

أ- اختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا: و قد نصت المادة 144[1] من قانون الإجراءات الجزائية على ذلك بقولها ":يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة" وإذا لم يتضمن الجدول من الخبراء المتخصصين في مجال الخبرة فإنه يجوز لجهات التحقيق بصفة استثنائية اختيار خبراء ليسوا مقيدين في الجدول.

ب- حلف اليمين القانونية: حيث يجب لصحة تقرير الخبير أداء اليمين لحمل الخبير على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها،سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولذلك لا يغني عن هذا الإجراء أية ضمانة أخرى من الضمانات[2].

وقد أوجب المشرع الجزائري بنص المادة 145 من ق.إ.ج [3] أن يحلف الخبير اليمين القانونية قبل أداء مهمته و إذا اذا كان مقيدا في الجدول لا يجدد حلفه مرة أخرى.

ج- تقرير الخبير و ميعاده و شكله: بعد انتهاء الخبير من أبحاثه وفحوصاته، يعد تقريرا يضمنه خلاصة ما توصل إليه من نتائج، و يشترط أن يقوم الخبير بإيداع تقرير خبرته خلال المدة المحددة له و إلا جاز للقاضي استبداله بغيره ما لم يقدم الخبير طلبا بتمديد هذه المهلة وذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذ تعلق الأمر بالجريمة المعلوماتية فقد أوجبت المادة 87 من قانون الإجراءات الجنائية المصري والمادة 98 من الإجراءات الجزائية الاتحادي الإماراتي على المحقق أن يحدد ميعاداً للخبير ليقدم تقريره فيه وللقاضي أن يستبدل به غيره إذا لم يقدم التقرير في الموعد المحدد له ولا يترتب على عدم تحديد الموعد أي بطلان.

---

(1) المادة 144 من قانون الإجراءات الجزائية المعدل و المتمم.

(2) احمد ابو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود و القصاص، د.ط، المركز العربي للدراسات الأمنية و التدريب، الرياض، 1993، ص 377.

(3) تنص على" يحلف الخبير المقيد لأول مرة بالجدول الخاص بالجدول القضائي يمينا أمام ذلك المجلس بالصيغة الأتي بيانها: اقسم بالله العظيم بان أقوم بإبداء مهمتي كخبير على خير وجه و بكل إخلاص و أن ابدي رأيي بكل نزاهة و استقلال...."

2- متطلبات أعمال الخبرة في الجرائم المعلوماتية

تتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظم الحاسبات الآلية كما تتنوع شبكات الاتصال بينها، مما أن تدقق جهات التحقيق والمحاكمة عند اختيارها للخبير و يمكن تحديد هذه الخبرة في الموضوعات الآتية:

أ- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية، والأجهزة الطرفية الملحقه به، وكلمات المرور أو السر و أكواد التشفير.

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

ج- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة. وعلاوة على ما تقدم يرى الباحثان أن الخبير المعلوماتي يجب أن يكون لديه العلم والخبرة والمهارة التي تمكنه من أداء مهمته على الوجه الأمثل .

3- مدى حجية تقرير الخبير في الجرائم المعلوماتية

الخبرة شأنها شأن باقي أدلة الإثبات تخضع حجيتها لتقدير القاضي ومدى تأثير أعمال الخبرة في الاقتناع الذاتي للقاضي، وسنعرض في هذا المطلب لتقدير تقرير الخبير ومدى تأثيره في الاقتناع الذاتي للقضائي و لما كانت المحكمة ملزمة بالإحالة إلى رأي الخبرة الفنية وأخذ الرأي فيما يتعلق بمسألة فنية إلا أن محكمة الموضوع لها كامل السلطة في تقدير القوة التدليلية لعناصر الدعوى المطروحة على بساط البحث وهي الخبير الأعلى في كل ما تستطيع هي أن تفصل فيه بنفسها ما دامت المسألة المطروحة ليست من المسائل الفنية البحتة التي لا تستطيع المحكمة أن تشق طريقها لإبداء الرأي فيها، فإن ما استخلصته المحكمة من مطالعتها للعقد موضوع الاتهام لا يحتاج إلى خبرة في تقديره لأن اختلاف المواد يمكن تبينه بالعين المجردة. وتجدر الإشارة إلى أنه وإن كان من المقرر أن تملك المحكمة سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز لها تفنيدها إلا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع [1].

---

[1] عبد الناصر محمد محمود فرغلي-محمد عبيد سيف سعيد المسماري، المرجع السابق، ص 29 .

وقد ذهبت المحكمة الاتحادية الإماراتية العليا بدولة الإمارات العربية المتحدة إلى أنه:

" ...و إن كان من المقرر– في قضاء هذه المحكمة – أن لمحكمة الموضوع سلطة تحصيل فهم الواقع في الدعوى وأدلة الاتهام فيها وصحة نسبة الواقعة إلى المتهم وتقدير الأدلة المعروضة على بساط البحث ومنها تقارير الخبرة الفنية، إلا أن ذلك مشروط بأن يكون تقديرها سائغا ويكفي لحمل قضاء الحكم ، كما أنه من المقرر– في قضاء هذه المحكمة –أنه لا يسوغ للمحكمة أن تستند في دحض ما قال به الخبير الفني إلى معلوماتها شخصية بل يتعين عليها إذا ما ساورها الشك فيما قرره الخبير في هذا الشأن أن تستجلي حقيقة الأمر بالاستعانة بغيره من أهل الخبرة لأنها من المسائل الفنية البحتة التي لا يصح للمحكمة أن تحل نفسها محل أهل الخبرة "[1].

4-الإقرار بحجية الوسائل الالكترونية في الإثبات

تكاد تجمع كافة النظم القانونية، في الوقت الراهن على حجية الملفات المخزنة في النظم، لذا و في بعض التشريعات الانجلوسكسونية فان الالتزام بالتعاون يتسع فقط لمجرد إصدار الأمر بإحضار الشهود أو بعض المستندات و لكن لإلزام الغير بتقديم المساعدة للسلطة القضائية عن طريق تقديم الأدلة و المساعدة للوصول إليها [2].

ثانيا: الاستعانة بالشهادة

الشهادة في مجال الجريمة المعلوماتية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية، وأمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية وله أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه.

---

[2] الطعن رقم 370 لسنة 22 قضائية – جلسة 1 /6 /2002، والطعن رقم 373 لسنة 22 قضائية – جلسة 01 /06 /2002 مجموعة الأحكام صادرة عن المحكمة الاتحادية الإماراتية من دوائر المواد الجزائية والشرعية – الطبعة الأولى، المكتب الفني 1425 – 2004 م .

[2] و من ذلك القانون الانجليزي الصادر عام 1984 في شان البوليس و الأدلة الجنائية، و يعطى المحققين الحق في أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المختزنة في الحاسب الآلي أو الاطلاع عليها أو قراءتها، و تسمح لبعض التشريعات بالاستفادة بالشهود كخبراء او كمعاونين للقضاء من تلقاء أنفسهم.

1- تعريف الشاهد المعلوماتي

والشاهد في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول في نظام المعالجة الآلية للبيانات، و يطلق عليه اسم الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي[1] و هو بهذا المفهوم قد يكون واحدا من عدة طوائف أهمها:

أ- مشغلوا الحاسب الآلي: ممن لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به [2].

ب- المبرمجون: و هم المتخصصون في كتابة البرامج و يمكن تقسيمهم إلى فئتين:

- الفئة الأولي : هم مخططو برامج التطبيقات[3] .

- الفئة الثانية:هم مخططو برامج النظم [4].

2- التزامات الشاهد المعلوماتي: و يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن البحث عن أدلة الجريمة بداخله، و السؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات و الإفصاح عن كلمات المرور و الشفرات؟ هناك اتجاهان في هذا الصدد:

-الاتجاه الأول: و يميل إلى هذا الاتجاه الفقه الجنائي الألماني حيث يرى عدم التزام الشاهد يطبع البيانات المخزنة في ذاكرة الحاسبة على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[5].

-الاتجاه الثاني: يرى أنصاره أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات آو الإفصاح عن كلمة المرور آو الشفرات الخاصة بالبرامج المختلفة، و من ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهاداتهم و الإفصاح عن كلمات

---

(1) هلالي عبد الاله أحمد، التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة، د. ط – دار النهضة العربية، القاهرة 2000، ص23.

(2) محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، د.ط، مطابع المكتب المصري الحديث، القاهرة 1991، ص 25

(3) علي عدنان الفيل، مرجع سابق، ص 62.

(4) عبد الناصر محمد محمود فرغلي- محمد عبيد سيف سعيد المسماري، مرجع سابق، ص 21.

(5) علي عدنان الفيل، مرجع سابق، ص 63 و ما بعدها.

المرور السرية ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق و المحاكمة[1].

المطلب الثاني

القواعد الإجرائية الخاصة لاستنباط الدليل الرقمي

إن القواعد الإجرائية التقليدية للتحقيق في الجرائم المعلوماتية هي قواعد عامة لا بد منها و لا يخلو أي تحقيق من اللجوء إليها إلا أنها و أمام الثورة المعلوماتية لا يمكن أن تكون الإجراءات الوحيدة التي تقود المحقق إلى العثور على الدليل لما تميز به هذه الجرائم المستحدثة من خاصية تختلف عن الجرائم العادية ومن ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية ما جاء به في القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية الأمر 156/66 خلال إجرائي التسرب و اعتراض المراسلات ثم من خلال القانون04/09 استحداث اجرائين آخرين وهما المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير.

الفرع الأول: التسرب

تعتبر الجريمة المعلوماتية من بين الجرائم التي يمكن فيها اللجوء إلى إجراء التسرب إذا اقتضت ذلك الضرورات التحري أو التحقيق بشأنها هو تقنية حديثة في التحري و التحقق عن بعض أنواع الجرائم الواردة على سبيل الحصر في القانون، استحدثه المشرع الجزائري بمقتضى تعديل قانون الإجراءات الجزائية في 2006 .

و التسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك، ويمكن تجسيد عملية التسرب في الجرائم الالكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة و يحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم [2].

---

[1] عوض محمد عوض، المبادىء العامة في قانون الاجراءات الجنائية، د.ط، دار المطبوعات الجامعي، 2012، ص 404.

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

و تظم أحكامه بموجب المواد من 65 مكرر 11 إلى 65 مكرر 18 منه.

و قد ورد تعريف التسرب في المادة 65 مكرر 12[1] من ق. إ.ج التي يفهم منها ان عملية التسرب تتمثل في اقتراف ضابط الشرطة أو عون الشرطة القضائية لتنظيم اجرامي بما يمكنه من معرفة نشاط غير مشروع و تحديد دور كل عنصر من عناصره[2].

أولا: شروط التسرب

المشرع الجزائري في هذا الصدد كما أعطى لسلطات التحقيق إمكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، فمن ناحية أخرى لم يفتح الباب على مصراعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

1- الشروط الشكلية

تنحصر الشروط الشكلية للتسرب في الإذن و ما يجب أن يتضمنه فلا يمكن أن يباشر ضابط الشرطة القضائية عملية التسرب بمفرده دون إذن من قبل الجهات القضائية و هذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية، و يجب أن يكون الإذن مكتوبا و إلا كان الإجراء باطلا[3] كما يجب ان يتضمن ذكر هوية الضابط الذي تتم على يديه عملية التسرب و تحديد المدة المطلوبة في عملية التسرب و التي لا يتجاوز إجراء التسرب 04 أشهر تحدد حسب المقتضيات.

2- الشروط الموضوعية

الأول يتمثل في تحديد نوع الجريمة والتي يجب أن لا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 5[4] أما الشرط الموضوعي الثاني فهو أن يكون الإذن

---

[1] تنص على"يقصد بالتسرب هو قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة بإيهامهم انه فاعل معهم أو شريك لهم أو خاف"

[2] حزيط محمد، مذكرات في قانون الإجراءات الجزائية، ط 8، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2013 ص 115 .

[3] انظر المادة 65 مكرر 15 من ق ا ج ج.

[4] سبعة أنواع وهي: جرائم المخدرات، الجريمة المنظمة العابرة للوطنية، جرائم تبيض الأموال، الجرائم الإرهابية، جرائم الفساد الجرائم المتعلقة بالتشريع الخاص بالصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

بالتسرب مسبباً، فمن خلال التسبيب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن، لذلك فكان لزاماً عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[1].

ثانيا: طرق التسرب في مجال الجريمة المعلوماتية: يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أوصفات هيآت مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام الهاكر للموقع[2].

من اجل القيام بعملية التسرب فقد أجاز المشرع استعمال أساليب و طرق خاصة أتاحت بدورها إمكانية اللجوء إلى استخدام عدد الوسائل و التقنيات هي في الأصل ليست مسموح بها قانونا لأنها تعتبر مساسا لمبدأ حرمة الحياة الخاصة غير انه لكل قاعدة استثناء و هو ما فعله المشرع الجزائري عندما تدخل بواسطة القواعد الإجرائية ليقيد أحيانا هذه الحرمة للحياة الخاصة.

الفرع الثاني: اعتراض المراسلات

استحدث المشرع الجزائري بموجب القانون رقم 06-22 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وقد ضمنه ستة مواد من المادة 65 مكرر إلى المادة 65 مكرر 10 [3] وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه، و تتمثل في اعتراض كل المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية التي يقصد بها التنصت التيليفوني و هي تقنية يتم من خلالها

---

(1) انظر المادة 65 مكرر 15 ق ا ج ج .

(2) سعيداني نعيم، مرجع سابق، ص 177.

(3) المواد من 65 إلفى 65 مكرر 10 من ق.إ.ج.ج، مرجع سابق

الاعتراض عن طريق ربط خط هاتفي لشخص ما مع اللجوء إلى تسجيل المكالمات في أشرطة ممغنطة[1].

شروط اعتراض المراسلات

1- ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ :طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء[2] وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الاعتراض وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا، و عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية اعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها[3].

2-تحديد طبيعة المراسلة ومدة الاعتراض : وهذا ما يفهم صراحة من نص المادة 65 مكرر7 التي نصت على أنه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها، كما أن المشرع قد أستوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق [4].

---

(1) شيخ ناجية، أساليب البحث و التحري المستحدثة في قانون رقم 06-22 المعدل و المتمم لقانون الاجراءات الجزائية، المجلة النقدية للعلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 294 .

(2) انظر المادة 65 مكرر 05 من ق.إ.ج

(3) انظر المادة 65 مكرر 09 ق ا ج ج .

وهي نفس المدة التي حددها المشرع الفرنسي في المادة 100 من قانون الإجراءات الجزائية الفرنسي، وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/21 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وذلك في الفقرة" و "من المادة الأولى منه والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الوصول إليها وهو ما أكده المشرع الجزائري بموجب المادة 10من الفصل الرابع من القانون 04/09المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها تحت عنوان" التزامات مقدمي الخدمات".

الفرع الثالث: مراقبة الاتصالات

ذهب رأي إلى تعريف مراقبة الاتصالات الالكترونية بأنها تعمد الاتصال و التسجيل و محلها المحادثات الخاصة سواء كانت مباشرة آو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية و اللاسلكية .

أما المشرع الجزائري فلم يتطرق إلى تحديد ما المقصود بمراقبة الاتصالات الالكترونية مكتف بذلك تحديد مفهوم الاتصالات الالكترونية فحسب، غير أن الفقه قد تصدى إلى هذه المهمة حيث عرف إجراء المراقبة الالكترونية على انه مراقبة شبكة الاتصالات، أو هو عمل قانوني الذي يقوم به المراقب باستخدام التقنية الالكترونية لجمع المعطيات و معلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته يرتبط بالزمن لتحقيق غرض أمني غرض أخر و الملاحظ أن التقنية هنا هي التقنية الالكترونية التي هي مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة [1] .

كما عرفه المشرع الأمريكي بأنه " عملية استماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز الكتروني أو أي جهاز أخر [2] .

أولا: تعريف مراقبة الاتصالات

لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الالكترونية ولكن بعض التشريعات قد عرفته مثل التشريع الأمريكي والكندي، فقد عرفها المشرع الأمريكي بأنها عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز الكتروني أو أي جهاز آخر المادة 2510-4 من قانون الاتصالات الفدرالي الأمريكي لسنة 1968 و طبقا لقانون الاتصالات الالكترونية لسنة 1986 أصبح التعريف المذكور يتسع ليشمل الاتصالات الالكترونية الأخرى [3].

و قد تبنى المشرع الجزائري مراقبة الاتصالات كإجراء خاص لعمليات الوقاية من جرائم محددة و هي الأعمال الموصوفة بجرائم الإرهاب و التخريب أو الجرائم الماسة بأمن الدولة أو كإجراء الأولي تقتضيه التحريات و التحقيقات القضائية و هذا الإجراء ليس جديد فقد

---

[1] مصطفى موسى، المراقبة الالكترونية عبر شبكة الانترنت-دراسة مقارنة بين المراقبة الأمنية التقليدية، دار الكتب و الوثائق القومية المصرية، ط 1، مصر، 2000، ص 25.

نصت عليه المادة 65 إلى 65 مكرر 10 من قانون الإجراءات الجزائية فصل متعلق باعتراض المراسلات و تسجيل الأصوات[1].

ومن الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الرقمي فقط، بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء فإنه يمكن كذلك تطويع هذه التقنية لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة ويعتبر تكريس المشرع لإجراء المراقبة الإلكترونية للاتصالات خطوة جريئة منه على اعتبار أن هذا الإجراء يعد من أخطر الإجراءات في إطار النظام الإجرائي عبر العالم الافتراضي لكونه يمس مباشرة خصوصيات الإنسان، وذلك بالرغم من أن البعض من الفقه يرى أن المراقبة لا تزال محل نظر في القانون من حيث ضرورة الالتزام بما هو مقرر في القوانين والضمانات الدستورية للحق في الخصوصية.

ثانيا: حالات اللُّجوء إلى مراقبة الاتصالات

يمكن اللُّجوء إلى المراقبة الالكترونية إذا توافرت إحدى الحالات التالية:

01- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة التي نص عليها القانون04/09 و المراقبة الوقائية كمبدأ عام لا تطبق على متابعة قضائية لجريمة مرتكبة، ولكن تخص كشف خطر أو تهديد لأمن الدول، وتشمل البحث عن المعلومات السياسية، الاقتصادية والعسكرية، وعليه فإن هذه الجرائم لم ترتكب ولكن المشرع سمح في إطار الوقاية من هذه الجرائم بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات يُحتمل تورطهم مستقبلاً بالقيام بالأفعال الموصوفة جرائم إرهاب

---

(1) انظر المادة 04-أ من قانون 04/09 المتعلق بمكافحة الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال.

أوتخريب أو الجرائم الماسة بأمن الدولة غير أن هذا الإجراء لا يُمنح إلاّ بشروط خاصة حددها المشرع بنص المادة 4 فقرة 3 من القانون09 - 04[1].

ولقد شدد المشرع في الفقرة الأخيرة من المادة 04 [2] بأن الترتيبات التقنية الموضوعة لمراقبة الاتصالات الالكترونية في هذه الحالة هي موجهة حصار لتجميع وتسجيل معطيات ذات صلة بالوقاية من تلك الأفعال ومكافحتها، وذلك تحت "طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني واحتمال اكتشاف جريمة قبل وقوعها وخاصة بنوع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو احتمال ضئيل، فما يُعرف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أنها صعبة الاكتشاف ولا يتم اكتشافها أحيانا إلا مُصادفة، فكيف عن هذا الاحتمال الوارد في نص المادة 4 فقرة "ب" من القانون 09-04 و ان كان هذا الأمر يدخل أيضا في إطار الوقاية من هذه الجرائم.

3- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى مراقبة الاتصالات الالكترونية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[3].

وتترتب ع على المراقبة السرية للاتصالات عموما ومن ضمنها الاتصالات الالكترونية في الغالب، تسجيل محتوى تلك الاتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها في ما بعد لإثبات الجريمة الواقعة، ولكن تختلف نوعية التسجيل هنا بحسب ما

---

[1] تنص المادة 4 فقرة 03 " يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه في الحالات الآتية.....لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية".

[2] جاء في الفقرة الأخيرة من المادة 4 ق ا ج انه "تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع و تسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية و الاعتداء على أمن الدولة و مكافحتها، و ذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة بالغير"

[3] انظر المادة 16-17-من قانون 09-04 المتعلق بمكافحة الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال .

إذا كانت المحادثة الالكترونية المراقبة هي عبارة عن اتصال صوتي فقط، أو اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون في الثاني تسجيل صوتي مرئي، وما ينبغي الإشارة إليه أن المراقبة السرية الالكترونية للاتصالات الالكترونية، ومن ضمنها المحادثات الهاتفية، لا يمكن اعتبارها نوعا من أنواع التفتيش، وذلك لأن المراقبة الالكترونية ترد عن البيانات الالكترونية المتحركة والتي تتجسد هنا بالاتصالات الالكترونية حال إجرائها دون تلك التي انتهت وخزنت، في حين التفتيش إنما يرد فقط على البيانات الالكترونية الساكنة أو المخزنة والتي تتجسد هنا بالاتصالات الالكترونية التي تمت وخزنت[1].

الفرع الرابع: مساعدات مزودي الخدمات

مزود الخدمة هو كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أوجهة خاصة وقد يقدم خدماته للجمهور أو مجموعة من المستخدمين الذين يشكلون مجموعة مغلقة [2].

وقد عرف المشرع الجزائري مزود الخدمة بموجب الفقرة 06 من المادة الثانية من القانون 04/09 انه:

- **التعريف الاول: كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.**
- **التعريف الثاني: أي كيان آخر يقوم بمعالجة أوت خزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.**

---

[1] رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية–دراسة مقارنة– د.ط، المكتب الجامعي الحديث الإسكندرية، 2013، ص 192.

[2] وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/21 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وذلك في الفقرة" و "من المادة الأولى منه والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الوصول إليها وهو ما أكده المشرع الجزائري بموجب المادة 10من الفصل الرابع من القانون 04/09المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تحت عنوان" التزامات مقدمي الخدمات".

وقد ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين في انتظار اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره.

وما تجدر الإشارة إليه في هذا الإطار أنه ليس أي معطيات معلوماتية محل اعتبار من المشرع، بل حصر المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة في المعطيات المتعلقة بحركة السير معطيات المرور[1].

وقد رتب المشرع الجزائري مسؤولية إدارية وأخرى جزائية على تقاعس مزودي الخدمة عن حفظ المعطيات المذكورة، لإمكانية أن يشكل هذا التقصير عرقلة للسير العادي للتحريات القضائية.

واسترشادا بما ذكر فإن مزودي لخدمة الانترنت يعتبرون مصدرا لجهات البحث والتحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في نفس الوقت بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها[2].

---

[1] انظر المادة 2 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[2] وقد حصر المشرع معطيات المرور التي ألزم في المادة 11 مزودي الخدمة بحفظها في:

- **المعطيات التي تسمح بالتعرف على مستعملي الخدمة.**
- **المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.**
- **الخصائص التقنية وكذا تاريخ ووقت ومدة الإتصال.**
- **المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.**
- **المعطيات التي تسمح بالتعرف على المرسل إليه الات60ال وكذا عناوين المواقع المطلع عليها.**

خاتمـــــــة

خاتمة:

خاتمة البحث ليست تلخيصا لما ورد فيه، فهذا مبين بين دفتيه، ولكنها إبراز لأهم النتائج التي توصل إليها وبيان لأهم المقترحات التي يرنو إليها، فإذا كان موضوع هذا البحث قد تناول طبيعة التحقيق في الجرائم المعلوماتية و القواعد الإجرائية المتبعة للوصول إلى الدليل فإنه يكون بذلك قد تناول مشكلة من المشكلات التي أفرزتها ثورة الاتصالات عن بعد، فهذه الثورة كما نعلم على قدر ما أسعدت البشرية ويسرت لها سبل الحياة، فقد أتعستها بهذه النوعية الجديدة من الجرائم التي ساهمت هذه الثورة في ارتكابها والتي تتميز بطبيعة فنية وعلمية معقدة، ويتصف مرتكبيها بطبيعة ذكية ماكرة.

إن ثورة الاتصالات عن بعد قد غيرت الكثير من المفاهيم التقليدية التي كانت تسير دفة الحياة قبل بزوغ نجمها، فبدأنا نسمع عن العمليات المصرفية الإلكترونية، وعن النقود الإلكترونية، وعن المستندات الإلكترونية، وعن الحكومة التوقيعات الإلكترونيين.

ولا شك في أن ظهور هذه العمليات الإلكترونية الجديدة ووجوب حمايتها جنائيا من صور الإعتداء المتطورة التي قد تقع عليها بالوسائل الإلكترونية المتطورة، قد أظهر أن هناك قصورا كبيرا في النصوص الجنائية الموضوعية والإجرائية، بحيث أن هذه النصوص قد أصبحت عاجزة عن حماية المصالح والقيم التي افرزتها ثورة الاتصالات عن بعد و ظهور هذا النوع الجديد من الجرائم قد أظهر مدى الحاجة الماسة إلى تطوير وسائل الإثبات الجنائي بحيث تستطيع إثبات هذه الجرائم الفنية والتي يرتكبها جناة يغلب عليهم الإحتراف ويتصفون بالذكاء، فلا يوجد شك في وجود صعوبة كبيرة في إثبات الجرائم الإلكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفائه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها، كما وان هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر في رجال الشرطة والمحققين والقضاة.

و هكذا من الصعب إثبات الجرائم التي تقع على العمليات الإلكترونية بالوسائل الإلكترونية بالنظر إلى الطبيعة الفنية المعقدة لهذه الجرائم واتصاف مرتكبيها بالذكاء والاحتراف، وهو ما يؤدي إلى ضرورة الاجتهاد لإيجاد الحلول لها و هذا ما جعلنا نسلط الضوء على طبيعة إثبات

هذه الجرائم وطرق الحصول على الأدلة التي تثبتها وصور الأدلة المتحصلة منها وسلطة القاضي بالنسبة لتقدير هذه الأدلة.

وقد تبين أن هناك قصورا واضحا في الكثير من التشريعات الجنائية الموضوعية والإجرائية العربية في مواجهة ظاهرة الجرائم التي تقع بالوسائل الإلكترونية أو على هذه الوسائل فما زال الكثير منها يخضع هذه الجرائم للنصوص التقليدية وهو ما قد يترتب عليه الاعتداء على مبدأ شرعية الجرائم والعقوبات، أو إفلات الكثير من الجناة من العقاب و مازال الكثير منها يقف في حمايته للحريات الشخصية وحرمة الحياة الخاصة من الوسائل الإلكترونية عند النصوص التقليدية التي تنص –فقط– على حماية هذه الحريات من وسائل الاتصال التقليدية

فعلى الرغم من انتشار الوسائل الإلكترونية في هذه الدول، إلا أن الكثير من تشريعاتها لم تمسها يد التعديل لكي تقوى على حماية المصالح المستجدة التي أفرزتها هذه الوسائل .

و قد ازداد الإثبات بالخبرة والقرائن بالنسبة لهذا النوع الجديد من الجرائم الذي جاءت به ثورة الاتصالات عن بعد، وهو ما يستوجب الاهتمام بالخبراء وتأهيلهم التأهيل العلمي الصحيح الذي يمكنهم من القيام بأعمال الخبرة.

كما أن هناك صعوبة تكتنف الدليل الجنائي بالنسبة للجرائم الإلكترونية سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلى عمليات فنية وعلمية وحسابية معقدة، كما وأن طبيعته قد تكون غير مرئية، كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه وقد يتم ذلك طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة أو التالفة، أن تكون كذلك واقعا وفعلا.

توصيـــــات

انتهيت من هذا البحث على ضرورة التأكيد على بعض النقاط من خلال عدة توصيات و هي:

- **ضرورة وضع تشريعات فيكل الدول تتتسق مع الأحكام القانونية الدولية في مجال مواجهة هذه الجرائم، وتنظيم الأحكام الإجرائية الخاصة بمواجتها.**
- **إعداد برامج أمن المعلومات من خلال إعداد خطط التدريب المختلفة مع تعيين المتخصصين في كل جهة لتتولى مسؤولية الأمن المعلوماتي.**
- **وضع ضوابط لمقاهي الانترنت وحصر المترددين عليها وعمل قاعدة بيانات لهم حتى يسهل متابعتهم منح سلطات التحقيق الصلاحية القانونية والتدريب العملي اللازم لاختراق نظام الحاسوب وضبط ما يحتويه من بيانات مخزنة.**
- **ضرورة التعاون الدولي لمواجهة مشاكل صور السلوك المنحرف المتمثل في جرائم الكمبيوتر والانترنت، وذلك بعقد المزيد من الإتفاقيات الثنائية والجماعية.**

نماذج قضايا تم ضبطها في مجال جرائم الانترنت

القضية الأولى: الهكر

"الهاكر" هو الشخص الذي يستمتع بتعلم لغات البرمجة و أنظمة التشغيل الجديدة و هو الشخص الذي يستمتع بعمل البرامج أكثر من تشغيل هذه البرامج، و الذي يؤمن بوجود أشخاص أخرين يستطيعون القرصنة، خبير بلغة برمجة ما أو نظام تشغيل معين.

1- الهاكرز في الدول العربية:

للأسف الشديد كثير من الناس في الدول العربية يرون أن الهاكرز هم أبطال بالرغم من العالم كله غير نظرته للهاكرز بعد خبر القبض على "ميتنيك"، فمنذ دخول الانترنت للدول العربية عام 1996 و الناس يبحثون عن طرق القرصنة الجديدة و كثير من الناس تعرضوا لمثل هذه المشكلة.

آخر الإحصائيات ذكرت أن هناك 80% من المستخدمين العرب أجهزتهم تحتوي على ملف "الباتش" و الذي يسهل عمل الهاكرز و يجدون أن هناك فرق بين ما يسمى الهاكرز أو الكراكز و لكن الاسمان هما لشخص واحد وهو القرصان الفرق البسيط بينهما هو الهاكرز 95 من عمله يقوم به في فضاء الانترنت أما الكراكز أو سارق البرامج يقوم بعمله في أغلب الأحيان دون الحاجة للاتصال بالشبكة فهو يقوم بفك شفرة البرامج فقط

2- الهاكرز في الولايات المتحدة الأمريكية:

قبل البدء في الحديث عن الهاكرز في الولايات المتحدة الأمريكية و قصة قرصنة جديدة نيويورك تايمز، نتحدث عن (كيفين ميتنيك)[1] أشهر هاكر في التاريخ قام بسرقات كبيرة عبر استخدام الانترنت و الكومبيوتر، حتى القبض عليه في Digital Equipment company حيث استطاع أن يخترق الكمبيوتر الخاصة بالشركة التي يعمل بها و تقرر سجنه لمدة عام

---

[1] راجع قضية كيفن ميتنيك لدى طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي في النظام القانوني لحماية المعلوماتية د.ط، دار الجامعة الجديدة، مصر، 2009، ص 553 و ما بعدها

من أشهر جرائمه سرقة الأرقام الخاصة بـ 20000 بطاقة ائتمان و التي كانت أخر جريمة له حتى القبض عليه بعدها و تم سجنه لمدة عام و لكن إلى الآن لم يخرج من السجن لان FBI يرون بان "كيفن" هذا خطير و لا توجد شبكة لا يستطيع اختراقها.

كان يستخدم خبرته كضابط سابق في البحرية الأمريكية للتحكم بشبكة الهاتف و تضليل مطارديه حيث كان يستخدم مقاسم الهاتف الرقمية و برع في الدخول إلى بدلات مؤسسة الهاتف المحلية و تمكن من الحصول على مكالمات هاتفية مجانية و تطور الأمر إلى الاستماع إلى مكالمات الآخرين، و قد دخل 1981 مع اثنان من أصدقاءه خلسة إلى المركز الرئيسي لشركة الهاتف في مدينة لوس انجلوس و وصلوا إلى الغرفة التي تحتوي على الكمبيوتر الذي يدير عمليات الاتصال ، و اخذوا كتب التشغيل الخاصة به وقوائم وسجلات تتضمن مفاتيح السر لإقفال الأبواب في تسعة مراكز أساسية تابعة لشركة الهاتف في المدينة، و عندما حققت الشرطة المحلية في الأمر ، لم تتمكن من كشف الفاعل ، و بعد سنة أبلغت عنهم فتاة من أعضاء المجموعة للشرطة الذين سارعوا لاعتقال الشبان الثلاثة و حكم على "كيفن" بقضاء ثلاثة أشهر سجن الإحداث بتهمة السرقة و تدمير بيانات عبر شبكة كمبيوتر، كما قضت المحكمة بوضعه بعد ذلك تحت المراقبة في لوس انجلوس و من جهته حاول مركز الخدمة الاجتماعية تقديم العون له و الاستفادة منها بشكل شرعي لكن النتيجة جاءت سلبية، إذ سعى كيفن إلى تعلم أمور مختصرة و حيل تساعده علة ممارسة هوايته باختراق شبكات الكمبيوتر و هذا ما قاده من انزلاق إلى آخر حيث اعتقل ثانية عام 1983 من قبل شرطة جامعة شمال كاليفورنيا بعد ضبطه يحاول استخدام كمبيوتر الجامعة لاختراق شبكة ARPA NET للوصول من خلالها إلى البنتاجون و حكمت المحكمة عليه بستة شهور تدريب إصلاحية للإحداث في كاليفورنيا.

أدين كيفن مرة أخرى بسرقة برامج من إحدى شركات البرمجيات في كاليفورنيا عن طريق الشبكة و تمكنت الشرطة من اكتشاف ذلك بتتبع خط الهاتف الذي تمت عن طريقه العملية والذي أوصلها إلى الشقة التي يعيش فيه، وضع تحت المراقبة 36 شهرا.

و في عام 1988 حاول "كيفن" مع صديقه الدخول إلى مخابر شركة "ديجيتال" التي اكتشف المسؤولون فيها تلك المحاولات لكنهم فشلوا ، فاستعانوا بالشرطة المحلية و مكتب التحقيقات الفدرالي الذين عملا بالتعاون مع خبراء "ديجيتال" على تتبع مصادر محاولات

الاختراق بدون التوصل إلى نتيجة لان "كيفن" قد اتخذ احتياطات ذكية لمنع اكتشافه و ذلك باستخدام جهاز كمبيوتر الأول يحاول عن طريقه اختراق شبكة ديجيتال و الحصول على نظام تشغيل و الثاني يراقب مركز مؤسسة الهاتف و يتتبع المحاولات الرامية لاكتشافه، و كان بإمكان مكتب التحقيقات الفدرالي اكتشافه بسهولة من خلال تتبع الهاتف الذي يتصل منه ولكن اختراقه لشبكة الهاتف مكنه من العبث ببدالتها و تضليل المحققين ، و هذا ما حدث عندما توجهوا مسرعين إلى الشقة التي توصلوا إلى أن محاولات الاختراق تجري بواسطة الهاتف الموجود فيها ليكتشفوا أنهم كانوا مضللين و تم إلقاء القبض عليه. لكن لم يتقيد "ميتنيك" غير بسنة السجن؛ حيث انتقل بعدها بمدة قصيرة إلى لاس فيجاس، وعمل مبرمجاً بسيطاً لكنه لم يلبث أن عاد أوائل عام 1992 إلى سان فرانسيسكو بعد وفاة شقيقه إثر تناوله جرعة زائدة من الهيروين.

في ديسمبر من العام 1992 تلقى قسم شرطة بكاليفورنيا اتصالاً عبر الكمبيوتر، يطلب فيه صاحبه الحصول على نسخ من شهادات رخص القيادة للمتعاونين مع الشرطة. واستخدم المتصل شفرة تظهر أنه مخول قانونياً بالاطلاع على تلك الوثائق، وطلب إرسالها بالفاكس إلى عنوان في إحدى ضواحي لوس أنجلوس.

و بفحص رقم الطالب تبين أنه محل يقدم خدمة الفاكس والتصوير، وتقرر إرسال المطلوب لكنهم أرسلوا بعض رجال الأمن لتقصي الأمر، وهناك وجدوه يخرج من المحل حاملاً الأوراق وعندما شعر بهم، ركض هارباً عبر إحدى الحدائق القريبة مخلفاً وراءه الأوراق. وبفحص الأوراق وجد أنها تحمل بصمات "كيفين".

جعلت هذه الحادثة وما كتبته الصحف من كيفين لصاً ذكياً، ومثيراً للإعجاب، بل إن أحد الصحفيين –ويدعى ماركوف– جعل أخبار كيفين شغله الشاغل، وأخذ يتلقط كل كبيرة وصغيرة عنه، ما دفع مكتب التحقيقات الفيدرالي إلى تعيينه مستشارها في عمليات مطاردة "كيفين".

القضية الثانية

- **قضية جستين بترسن[1]**

متقد الذكاء يخترق اعقد الشبكات بحثا عن المال كان هدفه الأول شبكة وكالة TRW لخدمات بطاقات الائتمان حيث تمكن من اختراقها و سرقة بيانات لمجموعة بطاقات الائتمان من كمبيوتراتها و اتبع ذلك بالنفاذ إلى خطوط شركة Telnet و سرقة بيانات منها كما اخترق شبكة "باسيفيك بيل" الهاتفية و سيطر على خطوط الهاتف المتجهة نحو إحدى محطات الراديو المحلية، كما طور عمله بالحصول على بطاقات ائتمان فعلية لأشخاص كان يلتقط أسماءهم من دليل الهاتف.

و حينما شعر جستين أن مكتب التحقيقات الفدرالي قد اشتبه به و بدا بمراقبته تم اعتقاله لكن مسؤولون من مكتب التحقيقات الفدرالي طلبوا منه العمل معهم و وافق حيث انصب عمله على ملاحقة الهاكرز الذين يمكن أن يسببوا مشاكل للمؤسسات التجارية و السلطات، و لم يتردد في تقديم أية معلومات أو وثائق كان يتحصل عليها من أشهر من يقومون بعمليات الاختراق و منهم صديقه، بكنه بعدها واصل أعماله من اختراقات و سرقات، طارده مكتب التحقيقات الفدرالي و قبض عليه بـ 14 شهرا سجنا و 03 سنوات تحت المراقبة أطلق سراحه عام 1997

القضية الثالثة:

- **قضية فيروس ميليسا[1]:**

القي القبض على "ديفيد سميث" بتهمة برمجة ونشر فيروس الكومبيوتر "ميليسا"، لكن إلقاء القبض لم يطلق مشاعر قوية مماثلة لتلك التي أثارها الفيروس في نفوس ملايين مستخدمي الكومبيوتر. ويرجح الخبراء أن فيروس "ميليسا" أصاب مليون جهاز فقط. وهذا يقل كثيراً عن واحد في المائة من عدد الأجهزة الموجودة في العالم. وذكر الخبراء أن الاحتياطات ضد الوباء أدت إلى حوادث عطل أكثر مما أحدثه الفيروس نفسه وتمنى

---

(1) طالع قضية جستين بترسن نقلا عن ممدوح عبد المطلب، مرجع سابق، ص، 240 و ما بعدها .

(2) انظر قضية ديفيد سميث على الموقع التالي: http://daharchives.alhayat.com/issue_archive/Hayat%20INT/ **نشر بتاريخ 4 1999/4/1**

بعضهم على هدي قوله تعالى "و عسى أن تكرهوا شيئاً وهو خير لكم" أن يساعد درس "ميليسا" على التحول إلى طرق أكثر اقتصادية لإرسال البريد الالكتروني.

لم تُعلن لحد الآن تفاصيل عن شخصية ديفيد سميث المتهم في قضية إطلاق فيروس "ميليسا"، لكن ترددت أنباء تقول أن "ميلسيا" هو اسم صديقته. و رغم الاسم الجميل فقد أثار أطلاق الفيروس الذعر الكبير بسبب قدرته على الاستنساخ الذاتي والانتقال عبر شبكة الانترنت إلى أجهزة الكومبيوتر حول العالم. ويكمن الفيروس داخل وثيقة ملحقة برسالة مرسلة بالبريد الالكتروني الذي يستخدم برامج "مايكروسوفت" "وورد 97" أو "وورد 2000" تحمل الرسالة عبارة بالانجليزية تقول "الموضوع: رسالة مهمة من...و هذه الوثيقة التي طلبتها...لا تطلع عليها أحداً".

وتعود خطورة الفيروس إلى استخدامه لعناوين معروفة لمتلقي الرسالة الذي يفاجأ حال فتحه ملحق الرسالة بقائمة عناوين مواقع إباحية في الانترنت تهاجم بريده الالكتروني وتلتقط أول 50 عنوان محفوظ في دفتر عناوين الانترنت الخاصة.

وتستنسخ الرسالة نفسها عبر العناوين الخمسين منتقلة إلى أجهزة كومبيوتر أخرى...وهكذا تنشأ متوالية هندسية، تخنق شبكة البريد الالكتروني.

و يُقدر عدد أجهزة الكومبيوتر التي تلقت الرسائل بنحو مليون، ويقل هذا الرقم عن واحد في المائة من عدد الأجهزة الموجودة في العالم. ذكرت ذلك صحيفة "غارديان" البريطانية التي قالت أن اكتظاظ شبكة البريد الالكتروني برسائل التحذير من الفيروس كان أشد مما فعله الفيروس نفسه، وعبر محرر الكومبيوتر في الصحيفة البريطانية عن الأمل في التحول عن إرسال ملاحق للرسائل إلى تضمينها كنص بسيط ضمن الرسائل نفسها. ومع أن من المستبعد حدوث ذلك فانه يمكن أن يحرر مساحات كبيرة جداً من خطوط حمل البريد الالكتروني ويخفف العبء عن صناديق البريد. فرسائل النص البسيط تقل عن عُشر حجم ملفات "وورد". ومن الأفضل لخطوط المعلومات الفورية تسلم 100 ملف حجم 4 كيلو K4 يومياً بدلاً عن ملف واحد يضم لوغو الشركات الملون الذي يمكن أن يحتل 500 كيلو K500.

بدا رجال الشرطة التنقيب عن نطاق واسع عن مبتكر هذا الفيروس في عالم غامض مليء بالهاكرز و مطلقي الفيروسات و استنفرت وحدة الجرائم الافتراضية في الشرطة الفدرالية

إلى أن الكثير من الشكوك انتابتهم في جدوى تحرياتهم، خاصة و أن الجريمة تميل إلى أن تكون افتراضية لا جوانب واقعية أبدا فيها. و أفضت عمليات البحث إلى إن المشتبه فيه يطلق على نفسه اسم « Sky Roket » انطلقت أعماله من شبكة "أمريكا اون لاين" http://www.aol.com و هذا الاسم محرف عن صاروخ الفضاء و هو اسم تجاري شائع لبعض التجهيزات والألعاب علاوة على استخدامه ككناية عن سرعة الانطلاق و التحليق الصاعق.

و قد استطاعت شركة .Network Associates Inc المتخصصة في أنظمة الكمبيوتر أن تتحقق من العلاقة بين "فيروس مليسا" و "سكاي روكت" و بين العديد من الفيروسات التي ظهرت خلال أكثر من عام و عند التحقيق في الأمر تبين أن "سكاي روكت" هو احد مستخدمي شبكة "أمريكا اون لاين" و أن هذا الاسم تم السطو عليه سابقا من قبل احد الهاكرز الذين يتقنون كسر كلمات السر للحصول على الخدمات مجانا، أو لتغطية بعض نشاطاتهم غير المشروعة على الشبكة، و أكد المحققون المتعاونون من Network Associates أن المالك الحقيقي لعنوان سكا يروكن بريء من هذه التهمة بيد أن الشخص الذي ينتحل شخصيته هو من ابتكر الفيروس، و تابع المحققون اقتفاء اثر "سكاي روكت" ليتبين أن هذا الاسم استخدم لأول مرة انطلاقا من النرويج ضمن منتدى يعالج مواقع إباحية.

و حرصت الشرطة الفدرالية كتمان تفاصيل ما توصلت إليه لكن كان من الواضح أنها حصلت على مساعدة قيمة من شبكة "أمريكا اون لاين" ، ثم بدأت بتضييق الخناق لا على الفاعل بمعونة احد الوشاة، وبالاقتفاء العكسي لمسيرة الفيروس و بتحليل طريقة صنعه.

و تم اعتقال ديفيد سميث عام 1990 في نيوجرسي يتهمه تخريب أنظمة الاتصالات العامة و التأمر و السطو على خدمات الكمبيوتر .

مضبوطات المصنفات الفنية لعام 2006

إحصاءات مضبوطات المصنفات الفنية بمصر عام 2006 لاستخلاص النتائج و معرفة المؤشرات موضحين الجداول محل التحليل .

رقم	الحاسب الالي(عدد القضايا 6294)	بث القنوات الفضائية (عدد القضايا 7933)	
864	جهاز حاسب ألي بمشتملاته	2903	جهاز ريسيفر
1397	وحدة معالجة مركزية	1	كارت فك شفرات قنواتART
784	هارديسك 157 جهاز نسخ اسطوانات	5106	كامة
7686	اسطوانة ليزر CD مقلدة لبرامج حاسب و العاب و	499	مكبر إشارة
7	افلام	5140	موزع إشارة 304 بوستر، 1478 ريموت
4444	برنامج حاسب ألي محمل على أجهزة مقلدة	716	مثبت إرسال
25	جهاز مسح كروت الذاكرة للتليفون المحمول	1	كامة لفك شفرة القنوات الفضائية الجنسية
1	جهاز حاسب ألي عالي التقنية يستخدم في تصميم	1	كارت فك شفرة القنوات الفضائية الجنسية
	المحررات و المستندات الحكومية و صور كثيرة من	4	منقي صوت و صورة، 100 منظم للإشارة
	الأختام و الاكلاشيهات	7	جهاز تحكم، 1 كاميرا مراقبة، 1 جهاز فك شفرات
50	إيصال سحب مقيد بوزارة الداخلية–الإدارة العامة	1	
1	للمرور		
	جهاز دي لينك لربط أجهزة الكمبيوتر بالشبكة الدولية		
1	للانترنت.		
7	وحدة اتصال 1جهاز بروجكتور، 4 وحدة إضاءة		
16	سماعة 295 كابل توصيل لتحميل التليفونات		
	المحمولة بالنغمات، جهاز توصيل لاسلكي ، محول		

[1] تقرير الأمن العام لعام 2006، مصلحة الأمن العام، وزارة الداخلية المصرية، ص 867 نقلا عن مصطفى محمد موسى التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 407.

2- جدول إحصائي تحليلي لبعض المضبوطات في قضايا المطبوعات لعام 2006 [1]

المطبوعات عدد القضايا 564	
41785	مصحف شريف بدون ترخيص من مجمع البحوث الإسلامية
15561	كتاب جامعي مقلد 9490 مذكرة مناهج جامعية مقلدة
13698	كناب ديني مقلد و منسوخ 2541 كتاب بدون رقم إيداع
3879	ملصق ديني 37 ولاعة مطبوع عليها صور جنسية
18990	غلاف مصحف شريف بدون بصمة ذهبية
1127	كروت و أغلفة دون الحصول على تصريح
2432	نسخة من كتب خارجية لمناهج تعليمية لمراحل التعليم الأساسي بدون تصريح بين وزارة التربية و التعليم
	مرجع علمي خاص بكلية الطب معد للتصوير منه
1	مرجع علمي مقلد و منسوخ بأسلوب التصوير العلمي
12	نسخة من كتاب حقوق الإنسان معد للتصوير منه
1	نتيجة إجمالية لعام 2007 9000غلاف مقلد و منسوخ
9000	

جدول إحصائي تحليلي بمضبوطات قضايا المصنفات السمعية و البصرية لعام 2006[2]

المخل بالآداب العامة(عدد القضايا 26)		المصنفات الفنية (عدد القضايا 592)	
721	اسطوانة ليزر مخلة بالآداب العامة لمشاهد جنسية	9637	شريط فيديو لأفلام مقلدة و منسوخة
260	فاضحة	42859	اسطوانة ليزر CD أفلام ماستر
	شريط فيديو مخل بالآداب العامة لمشاهد جنسية فاضحة	3	وحدات معالجة مركزية مثبت بأحدها عدد 3 هارد ديسك بالوصلات
		1	لوحة مفاتيح 2 طابعة 1 ماوس 3 محزل كهربائي
			جهاز نسخ اسطوانات مثبت بأحدهما عدد 6
		2	وحدات نسخ، 2 جهاز مشغل اسطوانات

جدول إحصائي تحليلي بمضبوطات قضايا العلامات و البيانات التجارية و المنشأ الجغرافي و النماذج الصناعية

نوعية القضايا	عدد القضايا
العلامات و البيانات التجارية	381
المنشأ الجغرافي	46
النماذج الصناعية	44
الإجمالي	**471**

---

(1) تقرير الأمن العام لعام 2006 ، نفس المرجع، ص 868 نقلا عن مصطفى محمد موسى، نفس المرجع ، 408.

(2) تقرير الأمن العام ، نفس المرجع، ص 866 ، نقلا عن مصطفى محمد موسى، ص 408.

قائمة المراجع

أ-الكتب

- **كتب عامة:**

1. حزيط محمد، مذكرات في قانون الإجراءات الجزائية، طبعة ثامنة، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2013.
2. عبد الله اوهايبية، شرح قانون الإجراءات الجزائية (التحري و التحقيق)، طبعة ثانية، دار هومة، الجزائر، 2004.
3. عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، طبعة أولى، دار المطبوعات الجامعية ، 2012.
4. محمد سعيد نمور، أصول الإجراءات الجزائية-شرح لقانون أصول المحاكمات الجزائية- طبعة أولى- دار الثقافة للنشر والتوزيع الأردن ،2005.

- **كتب متخصصة:**

1.احمد ابو القاسم الدليل الجنائي المادي ودوره في إثبات جرائم الحدود و القصاص المركز العربي للدراسات الأمنية والتدريب بالرياض-عام1993.

2. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة دار النهضة العربية القاهرة 2002.

3. خالد عياد الحلبي ،إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت، طبعة أولى دار الثقافة للنشر والتوزيع، عمان 2011.

4.خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، 2010.

5. زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دون طبعة، دار الهدى للطباعة و النشر و التوزيع، الجزائر،2011.

6. رشاد خالد عمر، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية، د.ط-دراسة مقارنة-المكتب الجامعي الحديث مصر، 2013.

7. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، دون بلد نشر،2007.
8. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي في النظام القانوني لحماية المعلوماتية دون طبعة، دار الجامعة الجديدة، مصر، 2009.
9. عبد العظيم وزير، شرح قانون العقوبات (القسم الخاص)، جرائم الاعتداء على الأموال، طبعة أولى، دار النهضة، العربية، القاهرة، 1993 .
10. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر و الانترنت، طبعة أولى، دار الفكر الجامعي، مصر 2006.
11. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون دراسة مقارنة–منشأة المعارف، الإسكندرية، دون سنة نشر.
12. علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)، دون طبعة، المكتب الجامعي الحديث، دون بلد نشر، 2012.
13. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، مطابع المكتب المصري الحديث، دون طبعة، القاهرة، 1991.
14. مصطفى محمد موسى:
– التحقيق الجنائي في الجرائم الالكترونية، طبعة اولى، مطابع الشرطة– شارع المرور– مصر، 2008.
– قواعد و إجراءات البحث الجنائي لكشف غموض الجرائم المعلوماتية و التخطيط لها، كلية التدريب، قسم البرامج التدريبية، الرياض، 2012.
– المراقبة الالكترونية عبر شبكة الانترنت–دراسة مقارنة بين المراقبة الأمنية التقليدية دون طبعة، دار الكتب و الوثائق القومية المصرية، مصر، 2000.
1. ممدوح عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دون طبعة، دار الكتب القانونية، مصر 2006.
2. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية دون طبعة، مكتبة الآلات الحديثة، مصر،2000.

3. هلالي عبد الاله احمد:

- حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، دون طبعة، دون دار نشر، دون بلد نشر،1999.

- التزام الشاهد بالإعلام في الجرائم المعلوماتية – دراسة مقارنة- دون طبعة، دار النهضة العربية، القاهرة، 2000.

- تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة طبعة أولى، دار النهضة العربية مصر، د.سنة نشر.

4. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، طبعة أولى دار المطبوعات الجامعية، مصر،2009.

ب-رسائل جامعية

1. احمد مسعود مريم، آليات مكافحة تكنولوجيا الإعلام و الاتصال في ضوء القانون قم 04/09، مذكرة مقدمة لنيل شهادة الماجستير جامعة قاصدي مرباح –ورقلة- كلية الحقوق-تخصص قانون جنائي، 2013/2012.

2. سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية-تخصص علوم جنائية-جامعة الحاج لخضر--باتنة –كلية الحقوق و العلوم السياسية-قسم الحقوق-2013/2012 .

3. سليمان بن مهجع العنزي، وسائل التحقق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية-كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية، الرياض،2003.

4. عبد الله بن حسين ال حجراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية، جامعة نايف العربية للعلوم الأمنية، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، الرياض 2014.

5. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت- بحث مقدم استكمالا لمتطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية-تخصص القيادة الامنية، جامعة نايف العربية للعلوم الامنية-كلية الدراسات العليا-قسم العلوم الشرطية، الرياض، 2004.

6. هدى طالب علي، الاثبات الجنائي في جرائم الانترنت و الاختصاص القضائي بها، رسالة ماجستير، كلية الحقوق جامعة النهرين، 2012.
7. يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون-تخصص القانون الدولي للأعمال-جامعة مولود معمري-تيزي وزو-كلية الحقوق و العلوم السياسية، 2013 .

ج- مؤتمرات

1. طارق محمد الجملي،الدليل الرقمي في مجال الاثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقد في 2009/10/28 لأكاديمية الدراسات العليا طرابلس.
2. عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي2003 .
3. عبد الناصر محمد محمود فرغلي-محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية-دراسة تطبيقية مقارنة-المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، جامعة نايف العربية للعلوم الأمنية الرياض 2007.
4. عمر محمد بن بونس، مذكرات في الإثبات الجنائي عبر الإنترنت – ندوة الدليل الرقمي- بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من05 -08 مارس2006.
5. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر و الانترنت، المنعقد في الفترة من الى02/03 2000 بكلية الشريعة والقانون بدولة الإمارات العربية المتحدة.
6. محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية، محور القانون الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية من 26 إلى 28 افريل، دبي، 2003.
7. ممدوح عبد الحميد عبد المطلب و زبيدة محمد قاسم، عبد الله عبد العزيز، أنموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر الأعمال المصرفية والإلكترونية، نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة وغرفة تجارة وصناعة دبي، في الفترة من 10-12-2003/05، المجلد الخامس.

8. نبيل عبد المنعم جاد، جرائم الحاسب الآلي، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بندسمال دبي،2005.
9. هشام محمد فريد رستم، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون و الحاسب الآلي و الانترنت، ، كلية الشريعة و القانون- العين- الإمارات، من 01 الى03 مايو 2000.

د- مقالات:

1. بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مقالة منشورة في مجلة الندوة للدراسة القانونية، العدد الأول، 2013.
2. شيخ ناجية، أساليب البحث و التحري المستحدثة في قانون رقم 22/06 المعدل و المتمم بقانون الاجراءات الجزائية، المجلة النقدية للعلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013 .
3. علي حبيش، المعرفة التكنولوجية سلعة القرن القادم(تحقيق محي يوسف جريدة الاهرام الجمعة 1998/11/13).
4. فيصل حسن حامد، التحديات التي تواجه الأجهزة الأمنية في المملكة العربية السعودية مقالة منشورة في المجلة العربية للدراسات الأمنية و التدريب، العدد 63 الرياض،2015
5. محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي و شبكات الانترنت حلقة علمية، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، القاهرة، 2008.

ر- نصوص قانونية:

1- أمر رقم 66-155 مؤرخ في08 يونيو 1966، يتضمن قانون الإجراءات الجزائية المعدل و المتمم (جريدة رسمية رقم 49 مؤرخة في 1966/06/11).
2- أمر رقم 66-156 المؤرخ في 08 يوليو سنة 1966 المتضمن قانون العقوبات(جريدة رسمية رقم 49 مؤرخة في 1966/06/11).
3- قانون 09-04 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

مواقع الكترونية:

1. التحقيق الجنائي المعلوماتي، مقالة منشورة على موقع مدونة المحترف:

www.th3professional.com.201009:41

2.غنام محمد غنام، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي

تاريخ زيارة الموقع: http://www.f-law.net/law/threads/11333

بتاريخ 2008/03/05

3- خالد ممدوح ابراهيم:

- الدليل الرقمي في الجرائم الالكتروني، منشور على الموقع الالكتروني الآتي:

تاريخ زيارة الموقع 2016./08/05 19223 WWW.F-LOW.NET/LAW/TH

- فن التحقيق الجنائي في الجرائم المعلوماتية، منشور على الرابط الالكتروني التالي:

4- http://www.4shared.com/account/home.jsp

5- www.droit7.blogspot.com/2013/11/blog-post-3422.html

6- www://ar.wikipedia.org/wiki

7- http://www.elkhabar.com/ar/index.php بتاريخ 2014/02/12

8- https://ssd.eff.org/ar/module سا5:37

فهرس