جامعة سعد دحلب بالبليدة

كلية الحقوق

قسم القانون العام

مذكـــرة ماجستيـــر

تخصص: العلوم الجنائية و الإجرامية

إثبـــــات الجرائـــــم المعلوماتيـــــة

من طرف

ثـــامر أمـــال

أمام اللجنة المشكلة من :

د/ جبارصلاح الدين	أستاذ محاضر،أ، جـــامعة البليدة	رئيســـــا
أ.د/ سعيـــد يوسف	أستاذ التعليم العالي،أ، جامعة البليدة	مشرفا ومقررا
د/ خليـــل عمرو	أستاذ محاضر،أ، جـامعة البليـــدة	عضوا مناقشا
د/رامـــي حليـــم	أستاذ محاضر،ب، جامعة البليـــدة	عضوا مناقشا
أ/ناشف فريـــد	أستاذ مساعد،أ، جـــامعة البليـــدة	عضوا مناقشا

البليدة ، جوان، 2012

ملخـــــــص

أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات و تدفقها في السنوات الأخيرة، ثورة الكترونية تطبق الآن في جميع مناحي الحياة ،و أضحى من الصعوبة بمكان الاستغناء عن خدماتها اللامحدودة،بحيث نستطيع أن نقول بثقة بأنه لم يعد هناك شأن يتصل بالحياة الإنسانية إلا و طاله نصيب من هذا التطور التكنولوجي المثير.

و على الجانب الأخر من هذا الوجه المشرق،واكب هذا التقدم تقدما مناظرا له قادته العقلية البشرية الإجرامية مستغلة على وجه غير مشروع المخترعات العلمية و ما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية و استحداث صور أخرى من الجرائم ارتبطت ارتباطا وثيقا بالتقنية المعلوماتية ،عرفت هذه الجرائم بالجرائم المعلوماتية.

إن ظهور الجرائم المعلوماتية بما يميزها من طبيعة خاصة سواء من حيث محلها أو أسلوب ارتكابها وحتى من حيث مرتكبيها ،أدى إلى ظهور العديد من المشكلات ،كان من أبرزها القصور الذي اعترى لفترة طويلة القوانين الجنائية الموضوعية التي وضعت نصوصها في ظروف تختلف عن الظروف التي خلفتها ثورة المعلومات.و لم يتوقف الأمر عند هذا الحد، فسرعان ما انتقل هذا القصور إلى القوانين الجنائية الإجرائية ،خاصة مجال الإثبات الجنائي كونه أحد أهم مواضيعها .

فالطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية تركت أثارا واضحة في إثباتها، حيث أفرزت جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في العديد من الصعوبات التي أصبحت تشكل عائقا كبيرا أمام أجهزة العدالة الجنائية خاصة في ظل غياب المعرفة التقنية لدى هذه الأخيرة ، الأمر الذي أدى في الكثير من الأحيان إلى عدم اكتشاف العديد من الجرائم المعلوماتية في زمن ارتكابها و عدم الوصول إلى مرتكبيها ،وحتى تعذر إقامة الدليل اللازم لإثباتها.

أمام هذا الوضع، أصبح الأمر يستدعي و بشدة إعادة النظر في وسائل الإثبات التقليدية و تطويرها بما يواكب التطور في أساليب ارتكاب الجرائم المعلوماتية ،فضلا عن ضرورة وضع الخطط و البرامج الإستراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع المستحدث من الجرائم.

شـــــكـــــر

إن قلت شكرا فشكري لن يوفيكم

حقا سعيتم فكان سعيكم مشكورا

الشكر جزيل الشكر و العرفان لله الذي لا يطيب الليل إلا بشكره ،و لا يطيب النهار إلا بطاعته ، و لا تطيب اللحظات إلا بذكره ،و لا تطيب الآخرة إلا بعفوه،و لا تطيب الجنة إلا برؤيته جل جلاله.

الشكر جزيل الشكر و العرفان إليكم أساتذتي الكرام، يا من أشعلتم شمعة في دروب علمنا ، و وقفتم على المنابر لتنيروا دروبنا ،يا من لم تبخلوا علينا بحرف يزيد من حصيلة فكرنا.

الشكر جزيل الشكر إليكم أستاذي الفاضل"سعيد يوسف"، يا من فضلتم علي بوقتكم و جهدكم و فكركم و توجيهكم و نصحكم ،و شكري لكم لن يوفي سعيكم، فأدامكم الله نفعا لنا و منبر فخر في خدمة علمنا.

الفهرس

مـــــقدمـــــــة

لقد أنعم الله على الإنسان بنعمتي العقل و العلم ، فعن طريقهما بدأ يطور أسلوب معيشته، فبعد أن كان يعيش عصر الصيد و يعتمد على الرعي و الترحال، بدأ يعرف الزراعة و حياة الاستقرار، ثم دخل عصر الثورة الصناعية، بظهور الآلة و الصناعات المختلفة التي غيرت خريطة البشرية و قلبت موازين المجتمع الإنساني رأسا على عقب.

و لم تقف رحلة الإنسان في تطوره عند العيش في ظل الثورة الصناعية، فإذا كان القرن التاسع عشر جعل كل اهتمامه منصبا على الطاقة و تنمية مصادرها المتنوعة، فإن القرن العشرين شهد ميلاد ثورة جديدة تلت الثورة الصناعية و فاقتها أهمية ، سميت بالثورة المعلوماتية. انطلقت هذه الأخيرة منذ ميلاد الحاسوب الآلي ، و تفجرت بظهور الشبكة الدولية للاتصالات.

فقد نشأ عن اجتماع تكنولوجيا الاتصالات و تكنولوجيا الحاسوب الآلي ثورة حقيقة في المعلومات، بحيث أدت ثورة الاتصالات إلى تراكم مذهل في المعرفة و حصيلة هائلة في المعلومات تعجز الوسائل البشرية عن ملاحقتها و فهرستها واستخلاصها و تصنيفها ومعالجتها و الاستفادة منها و السيطرة على تدفقها من مصادر متباينة، و جاءت تكنولوجيا الحاسوب الآلي لتقدم خدمة جليلة للإنسان بما يملكه هذا الاختراع الثوري من دقة و سرعة في جمع المعلومات و تحليلها و معالجتها و توزيعها و استرجاعها في وقت قصير [1] ص06، الأمر الذي أدى إلى انتشاره و تسلله إلى كل بيت و إلى كل نشاط تمارسه المؤسسات و الإدارات و الهيئات و الشركات العامة و الخاصة، بحيث نستطيع أن نقول بثقة أنه لم يعد هناك شأن يتصل بالحياة الإنسانية إلا و طاله نصيب من هذا التطور التكنولوجي المثير.

ورغم ما حققه هذا التطور التكنولوجي من ايجابيات شملت مختلف مناحي الحياة الاقتصادية و الاجتماعية و السياسية، إلا أن الأمر لم يخل من السلبيات، حيث واكب هذا التطور تطورا مناظرا له، قادته العقلية البشرية الإجرامية مستغلة على نحو غير مشروع ما أفرزه هذا التطور من تقنيات معلوماتية، لارتكاب العديد من الجرائم التقليدية و استحداث صور أخرى لم تكن معروفة من قبل، ارتبطت ارتباطا وثيقا بهذه التقنية،والتي تزايدت معدلاتها في الآونة الأخيرة على وجه الخصوص، بصورة أدت إلى بزوغ فجر ظاهرة إجرامية جديدة عرفت بالإجرام المعلوماتي.

هذا الإجرام الذي قال عنه البعض [2] ص514، أنه يعد أحد الأوجه العديدة للتعدي على التقنية في مجال الأعمال و الإدارة، و ليس المقصود به مجرد مشكلة نظرية بحتة في مجتمع مستقبلي تحكمه المعلوماتية، بل إن الإجرام المعلوماتي هو حقيقة اجتماعية مادية بحتة تشغل ذهن كثير من الفقهاء ، حيث بات هذا الأخير يشكل تهديدا كبيرا للأفراد في خصوصياتهم و ممتلكاتهم، و الشركات في كيانها المادي و الاقتصادي، و حتى الدول في أمنها و استقرارها، ضاربا عرض الحائط كل الاعتبارات.

إن مجيء هذا النوع المستحدث من الإجرام و ما صاحبه من خسائر فادحة و مخاطر جسيمة، جعل القانون الجنائي في مأزق كبير، حيث أصبحت النصوص القانونية غير كافية و قاصرة و عاجزة عن توفير الحماية الكافية، فضلا عن عدم قدرتها على الانطباق على ما ينجم عن هذا الإجرام من تهديد للأفراد و المؤسسات و الدول، خاصة في ظل مبدأ الشرعية الذي يقضي بأن "لا جريمة و لا عقوبة إلا بقانون"، وفي ظل مبدأ حظر القياس بالنسبة للنصوص الجنائية الموضوعية . الأمر الذي نجم عنه فراغ تشريعي اعترى العديد من التشريعات، خاصة العربية منها التي ظنت أنها في منأى عن هذا النوع من الإجرام، غير أن السنوات الأخيرة أثبتت عكس ذلك، حيث عرف هذا الإجرام انتشارا واسعا في منطقتنا العربية، و ذلك نتيجة التوسع المفرط في استخدام التكنولوجيات الحديثة في شتى الميادين، و ظهور الاقتصاد العالمي الجديد المبني على ثورة الاتصالات و المعلومات، و ازدياد حجم المبادلات و المعاملات و العلاقات عبر الشبكات الداخلية منها و العالمية .

إدراكا لمخاطر هذا النوع المستحدث من الإجرام، وأمام قصور القوانين الجنائية بما تتضمنه من نصوص تجريم تقليدية لمواجهته، كان لا بد على الدول خاصة العربية منها من التحرك جاهدة للخروج من هذا المأزق، محاولة سد الفراغ الذي يعتري قوانينها في هذا المجال، خاصة و أن خطر الإجرام المعلوماتي المحتمل في البيئة العربية قد يكون كبيرا إذا لم تتم مواجهته بالمستوى المطلوب . و هو بالفعل ما ذهبت إليه العديد من الدول العربية، حيث منها من اتجهت إلى وضع قوانين و تشريعات خاصة بهذا النوع من الإجرام كالمشرع السعودي حيث استحدث نظاما خاصا سمي " نظام مكافحة الجرائم المعلوماتية "، و منها من فضلت العمل على جبهة قوانينها الداخلية و تعديلها من أجل ضمان الحماية القانونية الفعالة ضد هذا الإجرام، و ذلك من خلال ضم ما يشكله هذا الإجرام من اعتداءات إلى نصوص القسم الخاص في قوانينها العقابية، و هو ذات ما ذهب إليه المشرع الجزائري، حيث أضاف بموجب القانون رقم 04-15المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات، للفصل الثالث من

الباب الثاني من الكتاب الثالث قسما سابعا مكررا تحت عنوان" جرائم المساس بأنظمة المعالجة الآلية للمعطيات".

إن القصور الذي اعترى لفترة طويلة القوانين الجنائية الموضوعية، سرعان ما انتقل إلى القوانين الجنائية الإجرائية، خاصة مجال الإثبات الجنائي كونه أحد أهم مواضيعها، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبة كبيرة في إثباتها، بينما و أمام ما يتسم به الإجرام المعلوماتي من طبيعة خاصة، أصبحت هذه النصوص تقف عاجزة عن ملاحقة مقترفيه و إثبات ما ينجم عنه من اعتداءات، الأمر الذي أدى في كثير من الأحيان إلى نتائج خطيرة، كون الإثبات يتعلق بمصالح جوهرية للمجتمع ككل من جهة و بحرية الإنسان و كرامته من جهة أخرى، فأساس توقيع العقوبة على أي متهم هو إثبات إدانته بإقامة الأدلة التي تثبت وقوع الجريمة و نسبتها إليه، و بدون هذا الإثبات فإن حق الدولة في العقاب يتجرد من أي قيمة له و يصبح هو و العدم سواء، فكما يقول بوزا " فإن البحث عن الأدلة يعد إحدى المشاكل الأساسية للإجراءات الجزائية، و بدون الدليل لا يتم الإسناد و تطبيق الجزاء، و يحتفظ هذا البحث على الدوام بأهميته مهما طرأ على القانون الجزائي من تطور".[3] ص02

ولقد تعاظم دور الإثبات خاصة في ظل ما أفرزته ثورة المعلومات و الاتصالات من سلوكيات منحرفة اجتماعيا لم تكن موجودة في الماضي، حيث و مع التطور التقني في أساليب ارتكاب الجرائم أصبح مطلوبا من سلطات إنفاذ القانون أن تتعامل مع نوع مستحدث من الأدلة في مجال الإثبات الجنائي سواء من حيث كم البيانات المدونة في جهاز الحاسوب الآلي و كيفية إثباتها، أو سواء من حيث وسيلة إثباتها، لا سيما و أن هذه السلطات في الوقت الحالي غير مؤهلة للقيام بهذا الدور، و هي ثغرة يعتمد عليها المجرم المعلوماتي الذي يعكس أعلى درجات المهارة في فنون التعامل مع الحاسوب الآلي، الأمر الذي أصبح يستدعي و بشدة إعادة النظر في وسائل الإثبات التقليدية و تطويرها بما يواكب التطور في أساليب ارتكاب هذه الجرائم، فضلا عن ضرورة وضع الخطط و البرامج الإستراتيجية لتحديث أجهزة العدالة الجنائية و تطويرها من حيث كوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم.

و من هنا تجلت لنا أهمية موضوعنا و حاجته من ثم إلى بحث المشكلات المتعلقة به محاولة للوصول إلى إيجاد الحلول المناسبة له، رغم ما يكتنف هذا الموضوع من صعوبات في

ظل التطور المتسارع لتكنولوجيا المعلومات و التجدد المستمر لها، و في ظل الغموض الذي يحيط به و عدم وضوح معالمه حتى على المشتغلين بالقضاء لقلة القضايا التي عرضت عليهم، خاصة في بلداننا العربية، التي لم تبدأ التعامل مع هذا النوع من الجرائم إلا حديثا، فموضوع كموضوع إثبات الجرائم المعلوماتية لم يتخذ في الواقع العربي بعد، البعد الذي اتخذه في الغرب. غير أنه و في الوقت الذي شكل لنا كل هذا صعوبة من صعوبات البحث في هذا الموضوع، شكل لنا عاملا محفزا للكتابة فيه، لعلنا نبسط ما صعب منه، و نوضح ما غمض منه ونرسم معالم ما لا معالم له.

فنتيجة للوضع العام، و عدم استقرار العلم في مجال التقنيات المعلوماتية، التي لا تزال في تطور مستمر، فإن أنشطة إثبات الجرائم المعلوماتية لم تحظ بعد بالاستقرار على النحو الذي حظيت به أنشطة الإثبات في الجرائم التقليدية، الأمر الذي أدى إلى عدم توفر المعايير القياسية لما يعد صائبا و غير صائب في هذا المجال، وكل هذا يفرض واقعا واضحا هو عجز النظم و القواعد السائدة عن استيعاب الواقع، خاصة في ظل غياب المعرفة و الخبرة الفنية اللازمة لدى سلطات إنفاذ القانون التي لا زالت غير قادرة على التعامل مع هذا النوع المستحدث من الجرائم.

و عليه و بناء على ما تقدم، ارتأى لنا أن نتبع منهجا تحليليا وصفيا ،قمنا من خلاله بسبر المسائل الفنية و القانونية ذات الصلة بإثبات الجرائم المعلوماتية، وحاولنا إلقاء نظرة على المستجدات في هذا المجال في ضوء ما وصلت إليه الدراسات الجنائية المتخصصة من تطور على مستوى السنوات الأخيرة، و وقفنا من خلال هذه الدراسة على التحديات التي تواجه إثبات هذا النمط المستجد من الجرائم، لعلنا نساهم و لو بشيء بسيط في وضع الخطوط العريضة للتعرف على كيفية إثبات الجرائم المعلوماتية .

ولهذا الغرض، رأينا أن نتناول موضوع دراستنا ضمن فصلين كالتالي:

في الفصل الأول سلطنا الضوء على خصوصية إثبات الجرائم المعلوماتية و ذلك من خلال تقسيمه إلى ثلاثة مباحث، تناولنا في المبحث الأول مفهوم الجرائم المعلوماتية، و خصصنا المبحث الثاني للحديث عن الطبيعة الخاصة لهذه الجرائم، أما المبحث الثالث فتطرقنا فيه إلى أثر الطبيعة الخاصة بالجرائم المعلوماتية في الإثبات الجنائي.

أما الفصل الثاني فعالجنا من خلاله مراحل إثبات الجرائم المعلوماتية، و قسمناه هو الأخر إلى ثلاث مباحث، تناولنا في المبحث الأول مرحلة جمع الاستدلالات في الجرائم المعلوماتية، ثم تناولنا في المبحث الثاني مرحلة التحقيق في هذه الجرائم، و من ثم تطرقنا في المبحث الثالث إلى مرحلة المحاكمة في الجرائم المعلوماتية .

الفصل 1
خصوصية إثبات الجرائم المعلوماتية

أدى التقدم العلمي الحاصل في مجال تقنية المعلومات وتدفقها في السنوات الأخيرة و كذا الانتشار المطرد لأجهزة الحاسوب الآلي، إلى ظهور نوع جديد من الجرائم لم تكن موجودة من قبل، ارتبطت ارتباطا وثيقا بتكنولوجيا المعلومات و الاتصالات، عرفت بالعديد من التسميات من بينها تسمية الجرائم المعلوماتية، بحيث لم يتفق الفقهاء إلى حد اليوم على مسمى موحد لهذا النوع من الجرائم، و التي تعد أحد أهم ثمار التقدم السريع في المجالات العلمية سواء اقتصرت على الحاسوب أو تعدته إلى الانترنت . اتسمت هذه الجرائم بطبيعة خاصة ميزتها عن غيرها من الجرائم التقليدية، فهي تتم في بيئة رقمية لا علاقة لها بالأوراق أو الأجسام أو الأشياء أو غيرها من ماديات الطبيعة، كما أنها تشكل نوعا جديدا من الجرائم التي لا تعترف لا بالمكان و لا بالزمان، ضاربة عرض الحائط جميع الحواجز و الحدود، ومرتكبوها لهم من الذكاء و المهارة التقنية العالية و المعرفة الفنية في مجال المعلوماتية، ما يمكنهم من اقتراف جرائمهم دون ترك سبيل الاهتداء إليهم، وذلك لاستخدامهم طرق و أساليب تقنية عالية الكفاءة يصعب اكتشافها.

إن ما يميز هذه الجرائم من طبيعة خاصة ترك آثارا واضحة على إثباتها، حيث انتقل الإثبات فيها من نطاق ما هو ملموس و محسوس إلى نطاق ما هو افتراضي و رقمي، فلم تعد هناك آثار تقليدية يمكن اعتمادها في إثبات ما يقع من جرائم معلوماتية، و إنما أصبح الإثبات فيها يعتمد على أرقام و بيانات و معلومات قد تتغير و تمحى من السجلات المخزنة في الحواسب الآلية، والتي ليس لها أي أثر خارجي ملموس [4] ص25، و على ذلك تم الانتقال من مرحلة التعامل مع أدلة مادية إلى مرحلة التعامل مع نوع جديد من الأدلة ذات الطبيعة غير المرئية، السهلة المحو و كذا التدمير، و تحول بذلك مسرح الجريمة المعلوماتية من مسرح تقليدي يمكن العثور فيه على العديد من الأدلة التي تثبت ما يقع عليه من جرائم، إلى مسرح افتراضي يصعب الحصول فيه على مثل هذه الأدلة، ليس هذا فحسب، و إنما اتسع هذا المسرح ليتخطى إقليم الدولة الواحدة إلى دول أخرى لا يمكن تمديد إجراءات الضبط و التفتيش إليها، إلا بوجود اتفاقيات أو معاهدات تسمح بذلك، كما أن السرعة التي ترتكب بها الجريمة بحيث قد لا تستغرق أكثر من عدد من الثواني ، قد تعقد من عملية إثباتها . فضلا عن هذا فإن ما تلم به أجهزة

العدالة الجنائية من معرفة بالقواعد القانونية الواجب إتباعها في إثبات الجرائم بصفة عامة، أصبح لا يكفي لوحده لإثبات الجرائم المعلوماتية.

إن كل هذا يدعو إلى القول أن إثبات هذا النوع من الجرائم يكتسي خصوصية تميزه عن إثبات غيره من الجرائم التقليدية، و تتجسد هذه الخصوصية بصفة أساسية في ما يكتنف هذا الإثبات من صعوبات في مجال هذه الجرائم. وهذا ما سنحاول التطرق إليه من خلال هذا الفصل، و حتى نكون منطقيين ومنهجيين في عرض أفكارنا، ارتأينا تقسيمه إلى ثلاثة مباحث، نتطرق في المبحث الأول إلى مفهوم الجرائم المعلوماتية، و من ثم نتناول في المبحث الثاني الطبيعة الخاصة لهذه الجرائم، لنصل في المبحث الثالث إلى الحديث عما تتركه هذه الطبيعة الخاصة من أثر في إثبات الجرائم المعلوماتية.

1.1. مفهـــــوم الجرائـم المعلوماتيـة

تعد الجرائم المعلوماتية من الجرائم الحديثة نسبيا، و التي ظهرت بظهور تكنولوجيا حديثة هي تكنولوجيا المعلومات و الاتصالات، وهي بلا جدال جرائم ضربت بقوة، و تنامت بسرعة فائقة في ظل الانفتاح العالمي و ارتباط الأسواق الدولية بعضها ببعض، فأصبحت تشكل خطرا يهدد الأفراد في ممتلكاتهم و خصوصياتهم، و المؤسسات في كيانها المادي و الاقتصادي، وحتى الحكومات في أمنها و سيادتها . و نظرا لجسامة أخطار هذه الجرائم و فداحة خسائرها و سرعة انتشارها من جهة، و حداثتها النسبية من جهة أخرى، أصبحت موضوع اهتمام بالغ من قبل العديد من الفقهاء و رجال القانون، سعيا منهم لفهم هذه الظاهرة وإبراز موضوعها و تحديد أنواعها، مما يتيح المجال لرفع الغموض عنها و الالتباس حولها، و ذلك من أجل توعية أفضل بمخاطرها . فسلامة التعامل مع أي ظاهرة مستحدثة يقتضي أولا و قبل كل شيء إيضاح معالمها و تحديد ماهيتها،و هذا ما سنحاول التطرق إليه في هذا المبحث من خلال تقسيمه إلى ثلاثة مطالب، نتناول في المطلب الأول تعريف الجرائم المعلوماتية ، ثم نتطرق في المطلب الثاني إلى موضوعها ثم نخصص المطلب الثالث للحديث على أهم أنواعها.

1.1.1. تعريـــــف الجرائـم المعلوماتيـة

تعتبر الجرائم المعلوماتية من الأنماط المستحدثة التي رافقت التطور التكنولوجي الحديث، فهي لم تحظ بعد بالاستقرار على النحو الذي حظيت به نظيراتها من الجرائم التقليدية، الأمر الذي أدى إلى وجود اختلافات جوهرية بين شراح القانون بصفة عامة و القانون الجنائي بصفة خاصة، سواء من حيث المصطلحات المستخدمة للتعبير عنها، أو من حيث التعريفات التي وضعت لها.

1.1.1.1. تعدد المصطلحات الدالة على الجرائم المعلوماتية

إن أول ما يلفت انتباه الباحث في ظاهرة الجرائم المعلوماتية هو تنوع المصطلحات الدالة عليها، فقد تناولت الدراسات هذه الظاهرة بعدد ليس بالقليل من المصطلحات، و هذا راجع للتطور المستمر و اللامتناهي لتكنولوجيا المعلومات والاتصالات، و التي تعد بيئة هذه الظاهرة المستحدثة.

فهناك من استعمل مصطلح "الاحتيال المعلوماتي"، و هناك من أطلق عليها تسمية "الجرائم التي يساعد على ارتكابها الحاسوب الآلي"، و يفضل البعض استعمال عبارة التعسف في

استعمال الحاسوب الآلي أو إساءة استعمال الحاسوب الآلي للدلالة على هذه الظاهرة، على أساس أن هذه المصطلحات أشمل و أوسع، لأنها تشمل إلى جانب الجرائم كافة الصور التي تنطوي على إساءة استخدام الحاسوب الآلي دون أن تصل إلى درجة السلوك الإجرام [5]ص27. و هناك من فضل استعمال مصطلح جرائم نظم المعلومات[6] ص82 و ذلك لسببين أساسيين، الأول كون أن هذا المصطلح يعبر عن محل الأنشطة الإجرامية و يمكنه أن يتواكب مع التطورات المستحدثة في مجال المعلوماتية و وظيفتها في الحياة الاجتماعية دون أن يتم حصرها في نطاق وسيلة معينة، و الثاني كون المصطلحات الأخرى تربط نفسها بأداة و وسيلة ارتكاب الأنشطة الإجرامية أو تحصرها في نطاق نوع معين، مما يؤدي إلى تجدد ظهور المشاكل القانونية في تطبيق النصوص على الواقع . و ليس بعيدا عن هذا المصطلح أطلق عليها البعض مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

و في ظل التقدم التكنولوجي يفضل البعض استخدام مصطلح " جرائم التكنولوجيا الحديثة " على أساس أنها جرائم تكنولوجيا باعتبارها مرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسب وغيرها من أجهزة تقنية قد تظهر في المستقبل، و هي حديثة نظرا لحداثتها النسبية من ناحية وارتباطها الوثيق بما قد يظهر من أجهزة حديثة قد تكون ذات طاقة تخزينية و سرعة فائقة و مرونة في التشغيل.[7] ص 33

و من جانبنا، فإننا نميل مع البعض إلى استخدام مصطلح الجرائم المعلوماتية للدلالة على الجرائم المتعلقة بالحاسوب الآلي و الانترنت، و ذلك كون هذا المصطلح يشمل جميع جوانب المعلوماتية سواء من الناحية الاجتماعية أو الاقتصادية أو القانونية، فضلا على اشتماله جميع التقنيات المستعملة في التعامل مع المعلومات، الحالية منها و المستقبلية.

و يمكن القول أنه مهما تعددت المصطلحات المستخدمة للدلالة على الجرائم المعلوماتية، إلا أنه لابد من مراعاة اعتبارات هامة عند اختيار المصطلح الدال عليها، وتتمثل هذه الاعتبارات فيما يلي: [6] ص15

- اختيار المصطلح يتعين أن يزاوج بين البعدين التقني و القانوني .
- دقة اختيار المصطلح، حيث يتعين أن ينطلق من أهمية التمييز بين المصطلحات المنتمية لما يعرف بأخلاقيات التقنية أو أخلاقيات الحاسوب و الأنترنت، و بين ما يعرف بإجرام التقنية أو جرائم الحاسوب.

◆أن يكون المصطلح قادرا على أن يعبر بقدر الإمكان عن حدود محله، فيكون شاملا لما يعبر عنه.

2.1.1.1. تعدد التعريفات الدالة على الجرائم المعلوماتية

تعددت الجهود المبذولة من قبل المهتمين بدراسة هذا النمط المستحدث من الجرائم لوضع تعريف للجرائم المعلوماتية، إلا أن محاولاتهم في وضع تعريف جامع مانع لها، باءت بالفشل، حتى قيل أن هذه الجرائم تقاوم التعريف[5] ص28، كما ذهب البعض إلى التشكيك في إمكانية وضع تعريف يحدد مفهوم الجريمة المعلوماتية، و ارجعوا صعوبة ذلك إلى أمرين هما: [6] ص 91

◆الخشية من حصر نطاق الجريمة داخل إطار يضر بها، و ذلك لأن الطبيعة الفنية للجريمة المعلوماتية تفرض صعوبة في حصرها داخل إطار قانوني تجريمي محدد و واضح .

◆وجود بعد دولي للجريمة المعلوماتية، يستوجب أن يكون التعريف متفق عليه على نطاق واسع حتى يمكن العمل من خلاله، و تنسيق التعاون فيما بين الدول في المجالات المتعلقة بالإجرام المعلوماتي.

و قد تناولت العديد من الدراسات ما جاء من تعريفات مختلفة للجرائم المعلوماتية، و اختلفت في طرق تناولها، فهناك من تناولها ضمن اتجاهين : اتجاه يضيق من مفهومها و اتجاه يوسع من مفهومها، وهناك من الدراسات من تناولت هذه التعريفات ضمن طائفتين، طائفة التعريفات التي تقوم على معيار واحد، وتشمل تعريفات قائمة على معيار قانوني، كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة، وتشمل أيضا تعريفات قائمة على معيار شخصي تتطلب توفر المعرفة والدراية التقنية لدى مرتكبيها، وطائفة التعريفات القائمة على معايير متعددة وتشمل التعريفات التي تبرز موضوع الجريمة و أنماطها و بعض العناصر المتصلة بوسائل ارتكابها أو بيئة ارتكابها أو سمات مرتكبيها، وهي الطريقة التي ارتأينا اعتمادها في تناولنا لمختلف ما جاء من تعريفات بشأن الجرائم المعلوماتية، باعتبارها الأكثر دقة في تقصي هذه التعريفات، وعليه نتناول فيما يلي التعريفات القائمة على معيار واحد والتعريفات القائمة على معايير متعددة.

1.2.1.1.1. التعريفات القائمة على معيار واحد

تشتمل التعريفات القائمة على معيار واحد، على تعريفات قائمة على وسيلة ارتكاب الجريمة، وتعريفات قائمة على محل الجريمة، و أخرى قائمة على شخص مرتكبها.

1.1.2.1.1.1. التعريفات القائمة على وسيلة ارتكاب الجريمة

اعتمد أصحاب هذه التعريفات في تعريفهم للجريمة المعلوماتية على وسيلة ارتكابها، فيعرفها الفقيه الألماني (Tiedemann) على أنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"[8] ص02، و يعرفها الفقيه (Leslie D.Ball) على أنها " فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية" [9] ص 85، كما يعرفها الفقيه (Merowe) بأنها " الفعل غير المشروع الذي يتورط في ارتكابه الحاسوب الآلي " [10] ص09، و يعتبر الفقيه (Massé) أن الجرائم المعلوماتية هي" عبارة عن اعتداءات قانونية ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[11] ص19، و تذهب الدكتورة نائلة محمد فريد قورة إلى تعريف الجريمة المعلوماتية على أنها " كل نشاط يؤدي فيه نظام الحاسوب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية ".[5] ص 32

النقد

إن الاستناد في التعريف إلى وسيلة ارتكاب الجريمة يعد منتقدا من جانب الفقه بشكل عام، و ذلك لأن القانون الجنائي لا يهتم بوسيلة ارتكاب الجريمة، بل ينصب اهتمامه على الفعل أو النشاط غير المشروع الذي يقترفه الجاني [6]ص 85 هذا من جهة، و من جهة أخرى فإن القول بأن مجرد استعمال الحاسوب الآلي في ارتكاب الجريمة يضفي عليها وصف الجريمة المعلوماتية، قول غير وجيه، ذلك أن الحاسوب الآلي قد يكون وسيلة في ارتكاب العديد من الجرائم التقليدية، فمن يحمل جهاز الحاسوب الآلي أو أحد مكوناته المادية فيصيب به أحدهم فيرديه قتيلا، ففي مثل هذه الحالة نكون أمام جريمة قتل وليس أمام جريمة معلوماتية رغم أن الوسيلة المستخدمة في ارتكاب الجريمة هي الحاسوب الآلي.

2.1.2.1.1.1 التعريفات القائمة على محل الجريمة

ذهب البعض إلى تعريف الجريمة المعلوماتية تبعا للمحل الذي ترد عليه، حيث يعرفها الفقيه (Rosblat) على أنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول

إلى المعلومات المخزنة داخل الحاسوب الآلي، أو التي تحول عن طريقه" [9] ص82، و يعرفها الفقيه (Parker) بأنها " كل فعل إجرامي متعدد أيا كانت صلته بالمعلومات، تنشأ عنه خسارة تلحق المجني عليه أو كسب يحققه الفاعل" [12] ص74 . كما حاول كلا من الأستاذين (Vivant) و (Le Stains) وضع تعريف يراعى فيه موضوع الجريمة و ذلك بوصفها بأنها " مجموعة الأفعال غير المشروعة و المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب "[4] ص44، و ذهب مجموعة من خبراء منظمة التعاون الاقتصادي و التنمية عام 1983 إلى تعريف الجريمة المعلوماتية على أنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات"[5] ص30 ، كما أشارت الدكتورة هدى حامد قشقوش بأن الجرائم المعلوماتية هي " مجموع الجرائم التي تتصل بالمعلوماتية" .[13] ص 559

النقد

إن هذه التعريفات، و رغم أنها أعطت للجريمة المعلوماتية سمتها الخاصة و هي تعلقها بالبيانات و المعلومات، غير أنها جاءت قاصرة عن تعريف الجريمة المعلوماتية التعريف الصحيح، حيث أنها جاءت عامة و مطلقة تحتمل العديد من التفسيرات كونها لم تحدد على وجه الدقة الأفعال غير المشروعة التي يمكن إدخاله في إطار الجرائم المعلوماتية، فضلا عن أن هناك من التعريفات من وسعت من نطاق الأفعال التي يمكن اعتبارها جرائم معلوماتية لتشمل فضلا عن السلوك غير المشروع، السلوك غير الأخلاقي و الذي يخرج أصلا عن نطاق التجريم.

3.1.2.1.1.1. التعريفات القائمة على مرتكب الجريمة

استندت هذه التعريفات على مدى إلمام الجاني مرتكب الجريمة المعلوماتية بالتقنية المعلوماتية، ومن بين هذه التعريفات، التعريف الذي جاء به الفقيه (David Thompson) الذي عرف الجريمة المعلوماتية على أنها " أية جريمة يكون متطلبا لاقترافها، أن يتوفر لدى فاعلها معرفة بتقنية الحاسوب " [9] ص 86 ، كما عرفها الفقيه (Stein Schjolberg)على أنها " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه ، و التحقيق فيه و ملاحقته قضائيا" [14] ص 16. و في ذات السياق فقد تبنت وزارة العدل الأمريكية في دليلها لعام 1989 الدراسة التي قام بها معهد ستانفورد للأبحاث، فعرفت الجريمة المعلوماتية على أنها " أية جريمة لفاعلها معرفة فنية بالحواسب تمكنه من ارتكابها"[6] ص 90، كما عرفها الدكتور

اليوسف عبد العزيز على أنها " جرائم يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب في عمل غير قانوني".[15] ص218

النقد

إن تعريف الجريمة المعلوماتية وفق سمات خاصة بمرتكب الجريمة يعد أمرا قاصرا لا يحيط بحقيقة الأفعال غير المشروعة و لا يساهم في توضيح مفهوم تلك الجرائم، كما أنه يتطلب البحث في ظروف خاصة بالجاني، و هذا ما لا يعول عليه في القانون الجنائي، لأنه قانون موضوعي لا يعتد بالظروف الشخصية إلا على سبيل الاستثناء[6] ص 91، كما أن هذه التعريفات تضيق على نحو كبير من الجريمة المعلوماتية ، حتى أن البعض يرى أن الجريمة المعلوماتية في ظل هذه التعريفات سوف تصبح أشبه بالخرافة[5] ص 29، فهذه الأخيرة تشترط لقيام الجريمة المعلوماتية أن يكون مرتكبها على قدر من المعرفة بتقنيات الحاسوب الآلي، غير أن هذا الأمر لا يمكن الأخذ به على إطلاقه، ذلك أنه في الكثير من الأحيان نجد أن مرتكب الجريمة المعلوماتية مجرد هاو لا يملك من المعرفة التقنية إلا القليل، فإن كان هناك من الجرائم المعلوماتية من تتطلب قدرا كبيرا من هذه المعرفة كجريمة اختراق موقع مثلا، فإن جريمة مثل جريمة الإتلاف المعلوماتي لا تتطلب مثل هذه المعرفة.

2.2.1.1.1 . التعريفات القائمة على معايير متعددة

إن القصور الذي اعترى التعريفات القائمة على معيار واحد في تعريف الجريمة المعلوماتية، أدى بالبعض و محاولة للوصول إلى تعريف يعرف هذه الجريمة بشكل أكثر دقة، إلى الاستناد في تعريفاتهم للجريمة المعلوماتية على أكثر من معيار، فيعرفها خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي و التنمية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية و المعنوية يكون ناتجا بطريق مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "[16] ص21، و ليس بعيدا عن هذا التعريف يعرفها الدكتور محمد سامي الشوا بأنها " كل فعل أو امتناع عمدي يهدف إلى الاعتداء على الأموال المادية و المعنوية الذي ينشأ حتما نتيجة الاستخدام غير المشروع لتقنية المعلومات[2] ص 516 ، كما عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين المنعقد في فينا في الفترة ما بين 10 و 17 أفريل 2000 الجريمة المعلوماتية على أنها " أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، و تشمل تلك الجريمة من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[17] ص110

النقد

إن هذه التعريفات استطاعت أن تغطي نوعا ما القصور الذي اعترى التعريفات التي استندت على معيار واحد، بحيث ركزت على الوسيلة المستخدمة في ارتكاب الجريمة المعلوماتية وكذا على محلها ،فأحاطت بمختلف الأفعال التي قد تشكل جريمة من الجرائم المعلوماتية، غير انه ما يؤخذ على هذه التعريفات أنها أغفلت عنصرا هاما من عناصر الجريمة، فالتعريف الكامل للجريمة هو ما حدد عناصر الجريمة إلى جانب بيانه لأثرها أي الجزاء المترتب عنها،فبيان جميع عناصر الجريمة من شأنه أن يعطي تعريفا دقيقا لوصف الجريمة عموما و يميز بينها و بين غيرها من الأفعال التي تخرج عن دائرة التجريم.

وعليه، ما يلاحظ من خلال ما تم استعراضه من تعريفات للجريمة المعلوماتية، وجود اختلاف جوهري فيما بينها، ويمكن القول أن هذا الاختلاف من شأنه أن يؤدي إلى الاختلاف في الأركان التي تقوم عليها الجريمة المعلوماتية، و هذا ما قد يثير العديد من المشكلات العملية، لعل من أهمها صعوبة مواجهتها و تعذر إيجاد الحلول المناسبة لمكافحتها، ولهذا وجب أن يكون هناك تنسيق بين الدول المختلفة من أجل وضع تعريف جامع مانع للجريمة المعلوماتية ،على أن يراعى في هذا التعريف عدة اعتبارات مهمة ، من أهمها: [5] ص 32

- يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات و الاتصالات ، بمعنى أن يكون التعريف مقبولا و مفهوما على المستوى العالمي.

- يجب أن يراعى في هذا التعريف التطور المتلاحق لتكنولوجيا الحواسب الآلية بصفة خاصة، بحيث لا يقتصر على التكنولوجيا الراهنة، بل يسمح باستيعاب ما قد يجد من صور للجريمة المعلوماتية نتيجة لهذا التطور.

- أن يوضح التعريف خصوصية الجريمة المعلوماتية بحيث يبدو واضحا الدور الذي يقوم به الحاسوب الآلي في ارتكاب الجريمة.

2.1.1 . موضـــوع الجـــرائم المعلوماتية

إن تحديد موضوع أو محل الجريمة المعلوماتية، يعتبر من أكثر المسائل إثارة للجدل، فإذا كان هناك اتفاق حول كون النظام المعلوماتي شرط لقيام الجريمة المعلوماتية، و هو ذلك النظام الذي يستخدم لإنشاء رسائل بيانات أو إرسالها أو استلامها أو تخزينها أو تجهيزها على

أي وجه آخر " [18] ص 18،و الذي يطلق عليه المشرع الجزائري مصطلح "منظومة معلوماتية " و يعرفه على أنه "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين" ، إلا أن هذه الجريمة قد ترتكب على النظام المعلوماتي نفسه، و قد يكون النظام ذاته وسيلة لارتكابها، فمتى يكون هذا النظام محلا أو موضوعا للجريمة المعلوماتية ؟

للإجابة عن هذا السؤال لابد أن نميز بين حالتين : يكون النظام في الأولى محل اعتداء، و يكون في الثانية وسيلة اعتداء، و عليه سنقسم هذا المطلب إلى فرعين، نتعرض في الفرع الأول لحالة وقوع الاعتداء على النظام المعلوماتي، و نتطرق في الفرع الثاني إلى حالة وقوع الاعتداء بواسطة النظام المعلوماتي.

1.2.1.1. وقوع الاعتداء على النظام المعلوماتي

قد يقع الاعتداء في الجريمة المعلوماتية على النظام المعلوماتي نفسه، و هنا لابد من التمييز بين ما إذا انصب الاعتداء على إحدى مكوناته المادية، أو ما إذا انصب الاعتداء على إحدى مكوناته المعنوية، ذلك أن النظام المعلوماتي يشتمل على مكونات ذات طبيعة مادية و أخرى ذات طبيعة معنوية.

1.1.2.1.1. وقوع الاعتداء على المكونات المادية للنظام المعلوماتي

قد يقع الاعتداء على المكونات المادية للنظام المعلوماتي وهي مجموعة العناصر الفيزيائية المستعملة لمعالجة المعلومات[19] ص1001 و المتمثلة فيما يلي:

1.1.1.2.1.1. وحدات الإدخال

هي الوسائل التي يتم عن طريقها إدخال البيانات إلى جهاز الحاسوب الآلي . تبعا لذلك فإن وظيفة وحدات الإدخال هي إيصال البيانات إلى داخل النظام ليتم معالجتها و تخزينها [20] ص23 و من بين وحدات الإدخال، لوحة المفاتيح، الفأرة، الشاشة التي تعمل باللمس، الكاميرا، القلم الضوئي و غيرها.

2.1.1.2.1.1. وحدات التشغيل المركزية

تقوم هذه الوحدات بوظيفتين أساسيتين هما التحكم و التجهيز الحسابي، و تعطي أوامر دقيقة لإدخال البيانات و البرامج و إخراج النتائج و هي تتكون من خلال ثلاث وحدات فرعية ، وحدة التحكم ، وحدة الذاكرة، و وحدة الحساب و المنطق.[21] ص444

3.1.1.2.1.1. وحدات الإخراج

هي الوحدات التي يمكن من خلالها تحويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة أو مرئية أو الاثنين معا [22] ص42، وهي عبارة عن وسائط تستخدم من أجل إظهار نتائج ما تمت معالجته من بيانات بالنظام المعلوماتي، و من أشهر الوسائل المستخدمة في إظهار هذه النتائج الطابعة.

إن هذه الوحدات تعتبر من المكونات الرئيسية للنظام المعلوماتي، بالإضافة إلى جميع الكابلات و شبكات الربط و الشرائط التي تسجل عليها البرامج و المعطيات، و قد تكون هذه المكونات محلا للسرقة أو محلا للإتلاف العمدي كالضرب بآلات حادة أو إشعال الحرائق بها ...الخ، و هذا النوع من الاعتداء لا يثير ثمة مشكلة، باعتبار أن هذه المكونات محل الاعتداء تتمتع بالحماية الجنائية للنصوص التقليدية باعتبارها من الأموال المنقولة التي تخضع سرقتها أو إتلافها للنصوص الجنائية التقليدية[7] ص 22.فالموقف الغالب يتجه إلى اعتبار الاعتداء على المكونات المادية للنظام المعلوماتي مما يندرج في نطاق الجرائم التقليدية، وعليه فإنه لا يشكل موضوعا للجرائم المعلوماتية، إلا أنه و رغم ذلك هناك من الدراسات من أدخلت هذا النوع من الاعتداء ضمن ظاهرة الجرائم المعلوماتية، و هو في رأينا مسلك غير صائب.

2.1.2.1.1. وقوع الاعتداء على المكونات غير المادية للنظام المعلوماتي

يشتمل النظام المعلوماتي على مكونات ذات طبيعة معنوية تتمثل بشكل أساسي في البرامج و المعلومات و البيانات، و التي تعرف بمعطيات الحاسوب أو الكيانات المنطقية.

1.2.1.2.1.1. البرامج

البرامج هي مجموعة من التعليمات يمكن للنظام استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة [18] ص 22، و تنقسم هذه البرامج إلى نوعين:

1.1.2.1.2.1.1. برامج التشغيل

يطلق عليها أيضا برامج الاستغلال أو التنفيذ، و هي تلك البرامج التي تمكن الحاسوب من أداء الوظيفة المحددة له، و هي لهذا السبب تعد جزءا من الحاسوب نفسه و يتولى الإشراف عليها برنامج مشرف أو مراقب لتنظيم أداء هذه البرامج لدورها . [23] ص05

2.1.2.1.2.1.1 برامج التطبيق

هي البرامج التي تصمم للقيام بمهام محددة، من بين هذه البرامج ما يستخدمه الفرد لمعالجة النصوص و الكلمات، كما أن هناك من البرامج ما تستعمله الشركات في تنظيم عملها و في إعداد جداول أجور المرتبات الخاصة بالعاملين فيها، و تعرف هذه البرامج في الآونة الأخيرة استخداما واسعا على مستوى المحاكم و المجالس القضائية حيث تستعمل في تنظيم الملفات و القضايا.

2.2.1.2.1.1 . البيانات

هي عبارة عن كلمات وأرقام و رموز و حقائق و إحصائيات خام، لا يوجد صلات بينها، و هي صالحة لتكوين فكرة أو معرفة بمعرفة الإنسان أو الأدوات أو الأجهزة التي يسخرها الإنسان لذلك وهي ما تسمى " بعملية المعالجة الآلية". [7] ص 29

3.2.1.2.1.1. المعلومات

هي ترجمة للبيانات الموجودة في الحاسوب الآلي عند تشغيله و تسمح بتكوين محتوى معرفي، يمكن لذوي الشأن معالجته و نقله بطريقة تسمح باستخلاص نتائج معينة. [4] ص37

و على ذلك ، فالاعتداء يكون منصبا على المكونات غير المادية للحاسوب الآلي، إن وقع على البرامج المستخدمة أو البيانات المعالجة آليا أو المعلومات المخزنة في الحاسوب الآلي، فقد تكون هذه الأخيرة عرضة للتعديل أو التلاعب أو الإتلاف . إن هذا النوع من الاعتداء هو الذي يشكل بحق موضوعا للجرائم المعلوماتية، فهذه المكونات نظرا للطابع الخاص الذي تتميز به، لم تشملها النصوص التشريعية التقليدية بالحماية و تقع عاجزة عن مواجهة ما قد يقع عليها من جرائم نظرا لحداثتها النسبية.

2.2.1.1 .وقوع الاعتداء بواسطة النظام المعلوماتي

قد يستعان بالنظام المعلوماتي من أجل ارتكاب جريمة، و في هذه الحالة لا تقع الجريمة على النظام المعلوماتي نفسه أو أحد مكوناته، و إنما يكون هذا النظام أداة الجريمة، كأن يستخدم الحاسوب الآلي لارتكاب السرقة أو النصب أو الاحتيال أو خيانة الأمانة.

يرى البعض[4] ص 46 انه في هذه الحالة نكون بصدد جرائم تقليدية بحتة ، يكون فيها النظام المعلوماتي أو جهاز الحاسوب الآلي هو أداة ارتكاب الجريمة و وسيلة تنفيذها. إلا أن هناك[22] ص80،81 من ذهب إلى ضرورة التمييز بين الاعتداءات التي يكون فيها الحاسوب الآلي كأي وسيلة من الممكن أن يستخدمها الجاني لتنفيذ جريمته، كالقتل عن طريق برمجة جهاز تفجير يتم التحكم فيه عن بعد، و بين الاعتداءات التي لا يتصور ارتكابها إلا بحاسوب آلي و ضد حاسوب آلي، كالسرقة من الأرصدة، أو التحويل من حساب إلى آخر أو تغطية اختلاس أو الدخول إلى موقع خاص بفك رموزه و نسخ محتوياته أو تخريبها...الخ، حيث اعتبر أن مثل هذه الاعتداءات، صحيح أنها ترتكب بواسطة حاسوب آلي، إلا أنها تنال بذات الوقت من حاسوب آلي آخر و بالذات من كيانه المعنوي، أي أن محل الاعتداء سيكون برنامج أو معلومات، فنكون في هذه الحالة أمام جرائم معلوماتية بأتم معنى الكلمة.

وفي نفس السياق ذهب البعض [24] ص97 إلى القول، أن ما يراه البعض جريمة بذاتها فإنه في الحقيقة نتيجة للفعل وأثر للاعتداء المباشر على المعطيات ولو كانت في الحقيقة هدف الفاعل الرئيسي، ووصفه مجازا بمحل الاعتداء غير المباشر أو الثانوي أو اللاحق، واعتبر أن محل الاعتداء المباشر الذي انصب عليه سلوك الفاعل من تغيير أو تلاعب أو نقل أو إتلاف أو استيلاء هو المعطيات و المعطيات فقط ، بذاتها وبما تمثله. ولعل هذا المثال يوضح الأمر أكثر:

فلو قلنا أن احد الأشخاص قام باختراق شبكة المعلومات، بتجاوز إجراءات الأمن مستخدما كلمة سر مثلا، واستخدم النظام الذي اخترقه دون تصريح أو إذن مسبق ودون مقابل، ولم يحدث ضررا للنظام ذاته ولم يستدل على المعلومات السرية المخزنة داخله أو غير ذلك، بمعنى انه استخدم النظام فقط (والمراد هنا في الحقيقة استخدام برنامج معين أو معلومات داخل النظام لأداء احتياجات خاصة به).فغرض الفاعل هنا واضح، لقد دخل النظام خلسة بغية الحصول على منفعة خاصة أتاحها له الاستخدام غير المشروع لمعطيات مخزنة في النظام، ولو أن شخصا آخر قام بذات الفعل و استولى على المعطيات المخزنة داخل النظام وكانت تمثل سرا

متصلا مثلا بالحياة الخاصة (بيانات شخصية) فأفشاها أو اتجر بها أو ابتز بواسطتها، هل يغير هدف الفاعل، محل الجريمة؟ما من شك أن محل الجريمة و موضوعها في الحالتين هو المعطيات، في الأولى قصد الفاعل استخدامها فقط، وفي الثانية استولى عليها للقيام بفعل أخر. [24] ص 98

و عليه يمكن القول أن النظام المعلوماتي قد يلعب دورين في الجريمة ، فقد يكون هدفها في حالة ما إذا استهدف الاعتداء نظام معلوماتي أخر، و قد يكون وسيلتها إذا استهدف الاعتداء أموال أو أصول. و على ذلك فإن النظام المعلوماتي يستهدف معطيات سواء بذاتها ، أو بما تمثله من أموال أو أصول .

خلاصة ما تقدم أن موضوع الجريمة المعلوماتية هو معطيات الحاسوب أي المعلومات والبيانات المعالجة آليا والبرامج بكل أنواعها سواء المدخلة أو المعالجة أو المخزنة داخل الجهاز، فهذه الجرائم تستهدف الحق في المعلومات ويمتد تعبير الحق في المعلومات ليشمل الحق في انسيابها وتدفقها والحق في المعلومات بذاتها أو بما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية ، ويكون النظام المعلوماتي دور الأداة فيها.

3.1.1 . أنـــــواع الجرائم المعلوماتية

لم يتوقف الاختلاف بين الفقهاء والدارسين لظاهرة الجرائم المعلوماتية عند تعريفها فحسب، وإنما امتد هذا الاختلاف ليشمل أيضا تصنيفها، فوجدت العديد من التصنيفات، فيصنفها الأستاذ (Martin Vasik) إلى جرائم الدخول و الاستعمال غير المصرح بهما إلى نظام الحاسوب الآلي، و جرائم الاحتيال المعلوماتي و سرقة المعلومات، و كذا الجرائم التي يساعد الحاسوب الآلي على ارتكابها و الأفعال التي تساعد على ارتكاب جرائم الحواسب الآلية [25]ص114،115، و ذهب الفقيه (Ulrich Sieber) إلى تقسيم الجرائم المعلوماتية إلى ثلاثة أقسام، يتعلق القسم الأول بجرائم الحاسوب الآلي الاقتصادية والثاني بجرائم الحاسوب الآلي التي تعتدي على الحياة الخاصة، و القسم الثالث يتعلق بتلك الجرائم التي تهدد المصالح القومية والسلامة الشخصية للأفراد [6] ص 121.و قد حاول بعض الفقهاء العرب وضع تصنيف للجرائم المعلوماتية، من بينهم الدكتور أحمد حسام طه حيث صنفها إلى فئتين رئيسيتين، الجرائم الموجهة ضد النظم المعلوماتية، و الجرائم المرتكبة عن طريق الاستعانة بنظم المعلوماتية[26]ص41. كما صنفها الدكتور عبد الفتاح بيومي حجازي إلى جرائم العبث

بالحاسوب الآلي، جرائم الإخلال بأمن الحاسوب الآلي، و جرائم غش الحاسوب الآلي[27]ص02.

بالإضافة إلى التصنيفات التي جاء بها الفقهاء للجرائم المعلوماتية، لم تتوان بعض الهيئات الدولية في وضع تصنيف لها من بينها المجلس الأوروبي ، الذي صنف أنواع الاعتداءات التي يتعرض لها الحاسوب الآلي إلى طائفتين، الطائفة الأولى تضم قائمة إلزامية كجرائم التزوير و الاحتيال المعلوماتي و تخريب الحاسوب الآلي....الخ، و هي طائفة الجرائم التي ألزم المجلس على الدول الأعضاء فيه النص عليها في تشريعاتها الجنائية، أما الطائفة الثانية فتضم قائمة اختيارية كالتجسس المعلوماتي، الاستعمال غير المصرح به لنظام الحاسوب الآلي....الخ.

و بعيدا عن الاختلافات الفقهية التي جاءت بشأن تصنيف الجرائم المعلوماتية و التي يمكن إرجاعها بشكل أساسي إلى الاختلافات الجوهرية في تعريفها، آثرنا التطرق إلى أهم أنواع الجرائم المعلوماتية و ذلك من خلال تصنيفها إلى طائفتين أساسيتين تناسقا مع موضوعها:طائفة الجرائم التي يكون فيها النظام المعلوماتي هدفا للاعتداء و طائفة الجرائم التي يكون فيها النظام المعلوماتي وسيلة للاعتداء.و لاستيعاب أفضل لهذه الجرائم، ارتأينا الحديث عن كل نوع من أنواع هذه الجرائم مع بيان أركانه.

و عليه سنقسم هذا المطلب إلى فرعين، نتناول في الفرع الأول الجرائم المعلوماتية الواقعة على النظام المعلوماتي، و نتناول في الفرع الثاني الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي.

1.3.1.1. الجرائم المعلوماتية الواقعة على النظام المعلوماتي

أشرنا فيما سبق إلى أن الاعتداء على المكونات المادية للنظام المعلوماتي يخرج عن إطار دراستنا، ذلك أن الاعتداء على هذه المكونات يشكل جرائم تقليدية بحتة، و على ذلك فالجرائم المقصودة هنا هي تلك الجرائم الواقعة على المكونات المعنوية للحاسوب الآلي، أي مجموع الاعتداءات التي تنصب على معطيات الحاسوب من معلومات و برامج. و هذه الجرائم متعددة و متنوعة لا يسعنا ذكرها جميعها، و لهذا سنقتصر على ذكر أهمها وفقا لما يلي:

1.1.3.1.1. جريمة سرقة البرامج و المعلومات

يطلق على هذه الجريمة جريمة قرصنة البرامج و المعلومات أو القرصنة المعلوماتية و يقصد بها " نسخ البرامج على نحو غير مشروع أو الحصول دون وجه حق على معلومات مخزنة في ذاكرة الحاسوب بطريقة مباشرة أو غير مباشرة".[28] ص99

1.1.1.3.1.1. الركن الشرعي في جريمة سرقة البرامج و المعلومات

تعرف جريمة سرقة البرامج و المعلومات انتشارا واسعا، فرغم ما سنته التشريعات من نصوص من أجل الحد من هذه الجريمة، إلا أنها بقيت عاجزة عن مجابهتها، خاصة و أن ما تتسبب فيه هذه الجريمة من خسائر يستدعي المسارعة لوضع الحلول الكفيلة بالحد منها. وقد سعى المشرع الجزائري على غرار باقي التشريعات إلى محاولة وضع حد لمثل هذه الاعتداءات الخطيرة، فقضى بحماية بيانات و برامج الحاسوب الآلي و ذلك من خلال الأمر 10/97 المؤرخ في 1997/03/06 المعدل و المتمم بالأمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف و الحقوق المجاورة، حيث أنه و بمقتضى المادتين 04 و 05 من الأمر رقم 10/97،أصبحت الحماية التي قررها المشرع للمصنفات الأدبية تشتمل على مصنفات و قواعد البيانات و جميع الوثائق المتعلقة بسير و معالجة المعطيات.

2.1.1.3.1.1. الركن المادي في جريمة سرقة البرامج و المعلومات

قد يتخذ الركن المادي في جريمة سرقة البرامج و المعلومات إما صورة الاعتداء على البرامج و إما صورة الاعتداء على المعلومات.

1.2.1.1.3.1.1. سرقة البرامج

تتعدد صور و أساليب سرقة البرامج ، و لعل من أبرزها ما يلي:

1.1.2.1.3.1.1. تقليد البرامج

يقصد به محاكاة برنامج بصنع أو إنتاج نسخ على مثاله، بحيث تبدو عند تسويقها كالأصل، و النسخ الجزئي للبرنامج كافيا للقول بتقليده ما دامت المحاكاة تتعلق بأجزائه الرئيسية [7] ص95.و حتى يكون هذا النوع من التقليد غير مشروع لا بد أن يكون قد تم دون وجه حق، أي تم تعديا على حق من الحقوق المحمية قانونا، و كثيرا ما نلحظ هذا النوع من

التقليد على مستوى برامج الألعاب الالكترونية حيث يتم تسويق العديد من هذه الألعاب بعد تقليدها .

2.1.2.1.3.1.1. سرقة البرنامج المصدر

حيث يتم في هذه الحالة سرقة البرنامج الأصلي، و إزالة هويته بإدخال تغييرات على شكله و هيئته، و إعادة تجهيزه ليبدو كما لو كان منتجا جديدا لصانع أخر، و أكثر المهددين بخطر هذا النمط من القرصنة هم منتجي حزم البرامج الجاهزة التي جرى تسويقها على نطاق واسع، ومن المتوقع تفاقم حدة هذا الخطر كلما تزايدت بين هؤلاء حدة المنافسة. [25] ص132

3.1.2.1.3.1.1. النسخ المباشر للبرامج

يتم ذلك من خلال طرق من بينها، الحصول على البرامج من الشبكة العالمية للمعلومات، حيث يتم تحميلها و من ثم نسخها ليتم بيعها في الأسواق دون ترخيص بذلك، وهو حال معظم البرامج المتواجدة بأسواقنا اليوم سواء كانت من برامج التشغيل أو كانت من البرامج التطبيقية و كذا برامج الترجمة.

هذا، و تتنوع أساليب قرصنة البرامج، فمنها التقليدية و منها الفنية. و من صور الأساليب التقليدية، رشوة أو ابتزاز الموظفين العاملين في شركات إنتاج برمجيات الحواسب الآلية، أو تسلل الموظفين إلى الشركات المراد التجسس على برامجها للعمل فيها لفترة وجيزة تسمح لهم بالاطلاع على أسرار و دقائق برامجها، أو الإعلان عن وظائف و إجراء مقابلات مع المتقدمين لشغلها للحصول منهم على وصف لأعمالهم أو عمليات الشركات التي ينتمون إليها. و يقدر البعض أن 63% من عمليات سرقة البرامج ترتكب عن طريق الموظفين العاملين في شركات إنتاج البرامج الذين ينقلون البرامج الجديدة في حقائب أوراقهم و يغادرون مكاتبهم رأسا إلى القراصنة [25] ص133 . أما من الأساليب الفنية المستخدمة في قرصنة البرامج هي استخدام شاشات التسجيل عن بعد و أدوات المراقبة السمعية، ففي إحدى حالات القرصنة كانت الوسيلة المستخدمة هي التقاط و تسجيل موجات البرامج المعلوماتية التي يجري بثها عبر الأثير.[25] ص 134

2.2.1.1.3.1.1. سرقة المعلومات

قد تتم عملية سرقة المعلومات بإحدى الطرق التالية: [20] ص 115

1.2.2.1.1.3.1.1. الالتقاط الذهني للمعلومات

يتم ذلك عن طريق النظر أو الاستماع، و يتم هذا الالتقاط بالاختزان أو الحفظ الواعي أو العرض للمعلومات اثر مطالعتها بالبصر، إن كانت قد ظهرت على شاشة الحاسوب في شكل مرئي، أو بعد وصولها إلى الأذن بعد أن تمثلت في صورة صوتية صادرة عن جهاز الحاسوب.

2.2.2.1.1.3.1.1. النسخ غير المشروع للمعلومات

يتم ذلك إما عن طريق التعامل المباشر مع النظام المعلوماتي المخزنة فيه البيانات على هيئة نبضات كهربائية أو على وسائط التخزين الرئيسية أو الثانوية، و إما عن طريق التوصل غير المرخص به مع النظام عبر الاتصال عن بعد.

3.2.2.1.1.3.1.1. الاعتراض المتعمد

يقصد به رصد إشارات إلكترومغناطيسية في الأنظمة المعلوماتية ، بغية استخراج المعلومات المفهومة أو المقروءة منها.

3.1.1.3.1.1. الركن المعنوي في جريمة سرقة البرامج و المعلومات

جريمة القرصنة سواء انصبت على البرامج أو على المعلومات هي جريمة عمدية يتطلب لقيامها توافر القصد الجنائي بعنصريه العلم و الإرادة جنبا إلى جنب مع الركن المادي، أي العلم بعناصر الجريمة و اتجاه الإرادة إلى ارتكاب السلوك الإجرامي.

2.1.3.1.1. جريمة التلاعب بالبرامج و المعلومات

إن التلاعب بالبرامج و المعلومات يعتبر من الجرائم الشائعة التي استفحلت في الآونة الأخيرة خاصة في بلداننا العربية .

1.2.1.3.1.1.الركن الشرعي في جريمة التلاعب بالبرامج و المعلومات

نظرا للانتشار الرهيب الذي عرفه هذا النوع من الجرائم، سارعت مختلف التشريعات إلى تجريمه، و من بين هذه التشريعات المشرع الجزائري، حيث نص على هذه الجريمة في المادة 394 مكرر1 من قانون العقوبات " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث

(3)سنوات و بغرامة من 500.000 دج إلى 2.000.000 دج،كل من أدخل بطريق الغش معطيات في نظام أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها".

2.2.1.3.1.1 .الركن المادي في جريمة التلاعب بالبرامج و المعلومات

يتمثل السلوك الإجرامي في هذه الجريمة في أفعال الإدخال أو المحو أو التعديل، و يكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها، و من ثم قيام الركن المادي في الجريمة، لأن القاسم المشترك في هذه الأفعال جميعها هو انطوائها على تلاعب في المعلومات أو البرامج التي يتضمنها نظام معالجة البيانات، بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[29] ص37

1.2.2.1.3.1.1. التلاعب في المعلومات

إن التلاعب في المعلومات إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا، و التي أصبحت مجرد إشارات أو رموز تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة. كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه . فلا تقع الجريمة على المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي أدخلت، ولم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة، حتى و لو لم تكن المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال[30]ص30.و عموما فإن التلاعب في المعطيات الموجودة داخل النظام المعلوماتي يتخذ إحدى الأشكال التالية:

1.1.2.2.1.3.1.1. إدخال معلومات وهمية

يقصد بفعل الإدخال إضافة معطيات جديدة، فقد يقوم الجاني بارتكاب جريمته من خلال إدخال بيانات لم تكن موجودة من قبل، و يتم عادة إدخال هذه البيانات بقصد التشويش على صحة المعلومات القائمة[10] ص232. و في غالب الأحيان تتم هذه الأفعال في المؤسسات المالية أو البنوك أو الشركات الكبرى و المنشآت التي يكثر بها عدد المستخدمين. و صورة ذلك أن يقوم المسؤول عن القسم المعلوماتي (الذي يعتبر في أفضل الأوضاع لارتكاب هذا النمط غير المشروع من التعدي على المعلومات) بضم مستخدمين غير موجودين بالفعل أو الإبقاء على مستخدمين تركوا الوظيفة من اجل أن يقوم بتحصيل مرتباتهم.[6]ص 178،179

2.1.2.2.1.3.1.1. تعديل معلومات موجودة

يقصد بالتعديل تغيير المعطيات الموجودة داخل النظام و استبدالها بمعطيات أخرى[29] ص42، و هي بمثابة تزوير باعتبار أن الجاني في هذه الحالة يقوم بتغيير الحقيقة، ويكون تغيير الحقيقة في نطاق المعالجة الآلية للمعطيات عن طريق الحذف، بإزالة كلمة أو رمز معين، أو عن طريق الإضافة بزيادة عبارات أو بيانات غير صحيحة، أو بتغيير فحوى الرسالة المنقولة . فمثلا قد يحتجز الفاعل أمر دفع موجه من بنك لآخر ويزيف الرسالة بحيث يتم الدفع لحسابه، أو قد يقوم باصطناع بيانات ليس لها وجود من قبل ونسبتها كذبا إلى غير مصدرها[10] ص234. إن تعديل المعلومات عادة ما يكون في المستحقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات أو أوامر الدفع وقوائم المبيعات وأنظمة التحويل الالكترونية للأموال والودائع المصرفية.

3.1.2.2.1.3.1.1. محو المعلومات

يقصد به تدمير المعلومات والبيانات التي تمت معالجتها سواء كليا أو جزئيا قصد محو آثارها، ويتم ذلك عادة عن طريق برامج معلوماتية كبرامج الفيروسات والتي تعتبر من اخطر ما قد يقوم به الجاني، خاصة إن كانت هذه المعلومات تخص عملاء في شركة أو مؤسسة مالية، فقد تؤدي إلى فقدان الشركة لثقة عملائها.

2.2.2.1.3.1.1. التلاعب في البرامج

سبق و أشرنا إلى أن البرامج نوعان ، برامح التشغيل و برامج التطبيق ، و التلاعب في البرامج ، قد ينصب على برامج التشغيل كما قد ينصب على برامج التطبيق.

1.2.2.2.1.3.1.1. الاعتداء على برامج التشغيل

يتم التلاعب في برامج التشغيل إما من خلال إعداد برنامج ناقص، و إما من خلال اصطناع برنامج. أما الطريقة الأولى فمقتضاها أن أي برنامج عند إعداده من المبرمجين يتضمن أخطاء وعيوب قد لا يكتشف البعض منها إلا عند استخدامه، فهم يتركون ممرات خالية وفواصل وشفرات في البرامج حتى يستطيعوا بعد ذلك تنفيذ التعديلات الضرورية [9] ص 172تعرف هذه الممرات بالمداخل المميزة أو المصيدة، وعن طريقها يمكن اللجوء إلى كل التعليمات التي تحتويها ذاكرات الحاسوب الآلي ومن ثم التوصل إلى الشفرات، إلا انه يصل

الأمر أحيانا ببعض المبرمجين من ذوي النوايا السيئة والذين لهم دراية بأهمية السلاح التقني الموجود بين أيديهم، بأن يتغاضوا عن استبعاد هذه المداخل المميزة، وهذا ما يمكنهم من استخدامها وفقا لأهوائهم [2] ص 554. و تجدر الإشارة هنا إلى أن هذا النوع من الاعتداء لا يقوم به إلا الجاني الذي له معرفة فنية كبيرة في مجال البرمجة.

أما الطريقة الثانية فتتمثل في إمكانية قيام بعض الأشخاص المحترفين في المجال المعلوماتي بتصنيع وتشكيل برامج معينة من اجل استخدام الحاسوب الآلي في التخطيط للجريمة ومراقبتها وتنفيذها والانتهاء منها[4] ص 79، فيكون بذلك البرنامج المصطنع مخصص فقط لارتكاب الجريمة. مثال ذلك ما قامت به إحدى الشركات الأمريكية بلوس انجلوس ، والتي اختلقت بفضل حاسوبها الآلي ومعاونة مبرمجيها، عددا وهميا من المؤمن عليهم بواسطة وثائق تأمين عددها 000 46 وثيقة اقتصر دورها على إدارة الحسابات. وإمعانا في التضليل قام الجناة بوضع شفرة خاصة ببرنامج تمت برمجته بدقة تامة، بحيث لا يظهر في الطباعة إلا الوثائق السليمة تماما.[10] ص237

2.2.2.2.1.3.1.1. التلاعب في برامج التطبيق

تعتبر حالات التلاعب في البرامج التطبيقية الأكثر انتشارا، حيث تمثل 15 % من الحالات التي تم حصرها[9] ص172، ويقوم الجاني بالاعتداء على برامج التطبيق إما بتعديلها وإما بزرع برنامج فرعي غير مسموح به.

فالبرامج التطبيقية - كما سبق الإشارة إليها- هي البرامج التي يتم بالفعل تطبيقها داخل المؤسسات أو الشركات أو المنشآت، و هي تتعلق بالنواحي المالية أو الإدارية أو التنفيذية في هذه الجهات العاملة في مجال المعلوماتية[4] ص 80، و الجاني يقوم بتعديل هذه البرامج من اجل القيام بعمليات اختلاس النقود، حيث تكثر هذه الجرائم في مجال الحسابات . وقد يتم التلاعب في هذه البرامج عن طريق زرع برنامج فرعي غير مسموح به في البرنامج الأصلي، ومن خلاله يصبح بالإمكان الدخول إلى النظام المعلوماتي، حيث تكمن خطوة هذا البرنامج في حجمه الصغير وسريته وإمكانية دفنه بين تعليمات البرنامج المتعددة، الأمر الذي يؤدي إلى سلب بعض التعليمات دون إمكانية اكتشاف عملية السلب هذه، حتى بواسطة أكثر وحدات الضبط دقة[7] ص42. مثال ذلك قيام مبرمج بأحد البنوك بزرع برنامج فرعي بمنشأة للكيانات المنطقية بإدارة الحسابات، يتجاهل كل عمليات السحب التي تتم بمعرفة المبرمج سواء عن

طريق بطاقات أو شيكات حسابية، فيتحمل البنك هذه المسحوبات في باب ميزانية الإدارة.[9] ص175

2.2.1.3.1.1. الركن المعنوي في جريمة التلاعب بالبرامج و المعلومات

جريمة التلاعب في المعلومات و البرامج جريمة عمدية، يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم و الإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، و يعلم أيضا أن ليس له الحق في القيام بذلك و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.[31] ص145

3.1.3.1.1. جريمة إتلاف البرامج والمعلومات

إن جوهر الإتلاف يتمثل في تخريب الشيء محل الإتلاف أو الانتقاص من منفعته بجعله غير صالح للاستعمال أو تعطيله[13] ص 564 ، و الإتلاف المقصود هنا هو ذلك الإتلاف الذي ينصب على المكونات المعنوية للحاسوب الآلي دون مكوناته المادية، ذلك أن إتلاف هذه الأخيرة يبقى يخضع للنصوص التقليدية في قانون العقوبات . ويطلق على إتلاف المكونات المعنوية للحاسوب الآلي بالإتلاف المعلوماتي أو التخريب المنطقي أو تدمير نظم المعلومات، وهو يتخذ إحدى صورتين، إما أن يتم محو المعلومات كلية و تدميرها الكترونيا، و إما أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف لها بجعلها غير صالحة للاستعمال.[13] ص 567

1.3.1.3.1.1. الركن الشرعي في جريمة إتلاف البرامج و المعلومات

تجدر الإشارة إلى أن هناك تداخل بين جريمة التلاعب بالبيانات و البرامج و جريمة الإتلاف المعلوماتي، حتى أن هناك من الدراسات من ذهبت إلى اعتبار الجريمة جريمة واحدة، فكلاهما ينصب على المحو و التعديل و الإدخال، غير أننا نرى التفريق بين الجريمتين على أساس الهدف الذي يرمي إليه الجاني من جريمته، فإذا كان هدف الجاني في جريمة التلاعب بالبرامج و المعلومات هو الحصول على فائدة شخصية لنفسه، فإن الهدف وراء إتلافه للمعلومات و البرامج غالبا ما يكون لمجرد الإضرار بالغير. و على ذلك فنص المادة 394 مكرر1 من قانون العقوبات الجزائري قد يحمل معنى التلاعب في البرامج و المعلومات، كما قد

تحمل معنى إتلاف المعلومات، طالما لم يحدد المشرع الجزائري الهدف من المحو و الإدخال و التعديل في البرامج و المعلومات.

2.3.1.3.1.1. الركن المادي في جريمة إتلاف البرامج و المعلومات

ينصب فعل الإتلاف المعلوماتي على مجموعة الأوامر و التعليمات اللازمة لتشغيل أجهزة الحاسوب الآلي و إنجاز مهامه، و أكثر ما يتم التوسل به لتنفيذ التخريب المنطقي هو البرامج ذات الأثر التدميري التي تستهدف محو جزء أو كل برامج أو ملفات الحاسوب أو البيانات و المعلومات المخزنة به، و كذلك سائر البرامج الخبيثة التي تصيب نظام الحاسوب بالشلل و العطب [25] ص 153، و هذه البرامج متعددة و لعل من أهمها:

1.2.3.1.3.1.1. الفيروسات

الفيروس ببساطة شديدة هو برنامج حاسوب مثل أي برنامج تطبيقي أخر، ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد، وهو إحداث أكبر ضرر ممكن بنظام الحاسوب الآلي، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه ببرامج أخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر وينمو ذاتيا، وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسوب المختلفة وكذلك بين مواقع مختلفة من الذاكرة، حتى يحقق أهدافه التدميرية. [32] ص26

2.2.3.1.1.1.1. برامج الديدان (الدودة المعلوماتية)

هي عبارة عن برامج قائمة بذاتها وتتواجد بشكل مستقل عن أي برنامج آخر، تكون مصممة للانتقال عبر شبكات الاتصال من جهاز إلى آخر دون حاجة إلى وسيط، وهذا ما يميزها عن الفيروس الذي يحتاج إلى وسيط لكي ينتقل إلى جهاز آخر.هذه البرامج لها القدرة على تعطيل أو إيقاف نظام الحاسوب الآلي بصورة كاملة، وهي تستنسخ نفسها عدة مرات، وتنتشر من خلال الوصلات الالكترونية، وتدفع معلومات غير صحيحة، تؤدي في النهاية إلى إغلاق النظام ومن ثم إتلافه، فهي تعمل على الجزء المتعلق بنظام التشغيل.[29] ص 108

3.2.3.1.3.1.1. برنامج حصان طراودة

برنامج حصان طراودة هو برنامج ضار يختفي داخل برنامج آخر ، ظاهره مفيد ولكن محتوياته مدمرة وعندما يتم تشغيل البرنامج ينشط البرنامج الخفي ويبدأ في النشاط و إحداث آثاره المدمرة، ولهذا سمي "حصان طراودة" للتشابه في أسلوب الهجوم بينها

[33]ص81 ، وتكمن خطورة هذا البرنامج في كونه يدخل إلى النظام المعلوماتي بصمت و هدوء، فيكون من الصعب جدا اكتشافه. وعادة ما يتم استخدام هذا النوع من البرامج لارتكاب عمليات النصب والاحتيال والاختلاس وسرقة الخدمات والتجسس والتخريب.

4.2.3.1.3.1.1. القنابل المعلوماتية

هي عبارة عن برامج يكون هدفها تدمير البرامج ومن ثم إتلافها، و تبدأ آثارها المدمرة عند حصول واقعة محددة أو حلول تاريخ معين و هي نوعان :[20] ص127

1.4.2.3.1.3.1.1. القنبلة المنطقية

هي تلك التي تؤدي إلى تدمير المعلومات عند حدوث ظرف معين أو لدى تغيير أمر ما، و يتحقق ذلك مثلا عند شطب اسم أحد الموظفين في شركة من القائمة الموجودة في الحاسوب.

2.4.2.3.1.3.1.1 القنبلة الزمنية

هي على نقيض القنبلة المنطقية، ذلك أنها تعمل في ساعة محددة من يوم معين، أي في لحظة زمنية محددة بالساعة و اليوم و السنة، ففي فرنسا مثلا قام محاسب خبير في نظم المعلومات و بدافع الانتقام على إثر فصله من المنشأة التي يعمل بها بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة بحيث تنفجر بعد 06 أشهر من رحيله و قد أدى ذلك إلى إتلاف كل البيانات المتعلقة بها.[20] ص127

3.3.1.3.1.1. الركن المعنوي في جريمة إتلاف البرامج و المعلومات

جريمة الإتلاف المعلوماتي جريمة عمدية، يشترط لقيامها توافر القصد الجنائي العام بعنصريه العلم و الإرادة .أي أن يعلم الجاني بأن البرامج و المعلومات التي يقع عليها فعله المادي غير مملوكة له،و أنها مملوكة لجهة أو لشخص آخر.وأن يريد الجاني بفعله إحداث إتلاف أو تخريب أو تعييب في البرامج أو المعلومات الموجودة داخل الجهاز، و ينتفي القصد الجنائي إذا قام شخص بإدخال أحد الاسطوانات داخل الجهاز لنسخ أحد البرامج، و تصادف أن الاسطوانة المدخلة كانت محملة بالفيروسات و انتقلت هذه الفيروسات للبرنامج المراد نسخه فنتج عن ذلك أن تلف البرنامج و قلت كفاءته في العمل.[32] ص 108،109

2.3.1.1 .الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي

إن الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي هي تلك الجرائم التي يكون فيها النظام المعلوماتي أداة لارتكاب الجريمة، و الجرائم التي تقع تحت هذه الطائفة عديدة و متنوعة ، و لعل من أهمها:

1.2.3.1.1. جريمة الدخول و البقاء غير المشروع في النظام المعلوماتي

تعد هذه الجريمة من الأنشطة الجرمية الأكثر انتشارا، و هي تتطلب عادة تجاوز إجراءات الحماية التقنية للنظام كتجاوز كلمة السر و الجدران النارية و غيرها، ويستخدم النظام المعلوماتي في هذه الحالة كوسيلة لتحقيق الولوج أو البقاء.

1.1.2.3.1.1. الركن الشرعي في جريمة الدخول أو البقاء في النظام المعلوماتي

نص المشرع الجزائري على جريمة الدخول أو البقاء في النظام المعلوماتي في الفقرة الأولى من المادة 394 مكرر من قانون العقوبات " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) و بغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

2.1.2.3.1.1. الركن المادي في جريمة الدخول أو البقاء في النظام المعلوماتي

يتخذ السلوك الإجرامي في هذه الجريمة صورة الدخول أو البقاء غير المشروع في النظام المعلوماتي.

1.2.1.2.3.1.1. فعل الدخول

يقصد به الدخول إلى محتويات جهاز الحاسوب الآلي ذاته، أي إجراء اتصال بالنظام محل الحماية بالطرق الفنية اللازمة لذلك[32]ص 108.و فعل الدخول يقع من أي إنسان أيا كانت صفته، يشترط فقط أن يكون ممن ليس لهم الحق في الدخول إلى النظام، حيث تقوم الجريمة في كل حالة يكون فيها الدخول مخالفا للشروط التي نص عليها القانون أو الاتفاق أو مخالف لإرادة من له حق السيطرة على النظام[20] ص 49، و لا يشترط لقيام الجريمة في هذه الحالة أن يترتب عليها ضرر، فهي تقوم لمجرد الدخول غير المشروع.

2.2.1.2.3.1.1. فعل البقاء

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية ضد إرادة من له الحق في السيطرة على هذا النظام . و البقاء المعاقب عليه داخل النظام قد يتحقق مستقلا عن الدخول إلى النظام، و قد يجتمعا. فيكون البقاء معاقب عليه استقلالا حين يكون الدخول إلى النظام في الأصل مشروع، كأن يكون الدخول إلى النظام قد تم عن طريق الصدفة أو الخطأ أو السهو، إذ يتوجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورا، فإذا بقي رغم ذلك، فإنه يعد مرتكبا لجريمة البقاء غير المشروع[20] ص52، وقد يجتمع الدخول غير المشروع و البقاء معا، و ذلك في الفرض الذي لا يكون فيه للجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة، ثم يبقى داخل النظام بعد ذلك. ففي هذا الفرض يكون الاجتماع المادي بين الجريمتين.[31] ص133

وتجدر الإشارة أنه و رغم أن جريمة الدخول أو البقاء في النظام المعلوماتي من الجرائم الشكلية التي لا تتطلب لقيامها تحقق نتيجة ، غير أنه في الكثير من الأحيان فإن هذا الدخول أو البقاء يكون من أجل ارتكاب جرائم أخرى، بحيث يمكن اعتبار هذه المرحلة مقدمة لارتكاب العديد من الجرائم. و لهذا نجد المشرع الجزائري شدد من العقوبة إذا ترتب عن هذا الدخول أو البقاء محو أو تعديل للمعطيات التي يحتويها النظام أو تخريب للنظام ذاته، حيث تنص الفقرة الثانية من المادة 394 مكرر" تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة .وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من ستة(6)أشهر على سنتين (2) و الغرامة من 50.000دج الى 150.000دج"

3.1.2.3.1.1. الركن المعنوي في جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

جريمة الدخول و البقاء غير المشروع جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم و الإرادة، أي أن تتجه إرادة الجاني إلى الدخول أو البقاء في النظام المعلوماتي مع علمه أن دخوله أو بقاؤه غير مسموح به، و على ذلك ينتفي القصد الجنائي إذا كان الجاني قد دخل النظام أو بقي فيه ظنا منه أنه لا يزال يملك الحق في الدخول إليه، أو كان يجهل أنه تم منع الدخول إلى ذلك النظام.

2.2.3.1.1. جريمة التجسس المعلوماتي

تعتبر جريمة التجسس المعلوماتي من الجرائم التي أصبحت تشكل خطرا كبيرا على الأفراد و كذا المؤسسات و حتى الدول، حيث أصبح التجسس يشمل مختلف الجوانب ، بدءا بالأفراد، و ذلك من خلال التعدي على خصوصياتهم و أسرارهم و بياناتهم الشخصية، انتقالا إلى المؤسسات التجارية و الصناعية و ذلك من خلال كشف الأسرار التسويقية و التجارية و كذا كشف نتائج الأبحاث الصناعية و التجارية، وصولا إلى المؤسسات الأمنية و العسكرية للدول من خلال الحصول على الخطط العسكرية و أسرار الدولة الحربية و حجم العتاد الحربي و غير ذلك من المعلومات التي قد يشكل الحصول عليها تهديدا حقيقيا للدول .

1.2.2.3.1.1. الركن الشرعي في جريمة التجسس المعلوماتي

نص المشرع الجزائري على جريمة التجسس في المادة 64 من قانون العقوبات، و اشتمل هذا النص بصفة أساسية على التجسس الذي يستهدف أمن الدولة، والملاحظ أن المشرع قد راعى أخطار التجسس المعلوماتي الذي يتم بوسائل التقنية المعلوماتية، و هذا ما يستشف من الفقرة الثانية من المادة 63 من قانون العقوبات التي تقضي".. الاستحواذ بأية وسيلة كانت على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو أحد عملائها" .

2.2.2.3.1.1. الركن المادي في جريمة التجسس المعلوماتي

يتخذ الركن المادي في جريمة التجسس المعلوماتي عدة أشكال، ذلك أن أساليب التجسس المعلوماتي متنوعة و متعددة و هي في تطور مستمر، و لعل من أبرزها :

1.2.2.2.3.1.1. التقاط المعلومات المتواجدة ما بين الحاسوب الآلي و النهاية الطرفية

يحدث هذا الالتقاط بواسطة توصيل خط تحويلة يعمل على تكبير الذبذبات الالكترونية وإرسالها إلى النهاية الطرفية التي تقوم بعملية التجسس، وقد يحدث ذلك أيضا باستخدام جهاز مرسل صغير يمكنه نقل البيانات عن بعد، ويمكن الالتقاط كذلك عن طريق وضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية حيث يحدث التقاط الإشعاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر الصناعي واحتجاز مضمونها.[7] ص39

2.2.2.2.3.1.1. التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي

يقوم الجاني في هذه الحالة بالتقاط الإشعاعات الصادرة عن الجهاز المعلوماتي، ثم تسجيلها وحل شفرتها بواسطة أجهزة الكترونية متطورة.ومن الوجهة العملية فإن الطابعات المستخدمة مع الحاسوب الآلي هي بطبيعتها طابعات سريعة، ومن ثم يصدر عنها إشعاعات إلكترومغناطسية أثناء تأدية وظيفتها، وفي هذه الحالة أيضا يمكن ربط الطابعة المستخدمة في ارتكاب الجريمة مع الطابعة الموجودة داخل المركز المعلوماتي المستهدف ثم يطلب منها نسخ المعلومات المتداولة حرفيا. [4] ص 39

3.2.2.2.3.1.1. التقاط المعلومات عن بعد

تقوم هذه التقنية على معرفة محتوى اتصال قد يتم داخل نظام حاسوب واحد، أو نظامين مختلفين أو بين أنظمة ترتبط فيما بينها من خلال شبكة اتصالات، و ذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال [28] ص217 .فمن خلال هذه الوسيلة يمكن جمع المعلومات عن بعد، حيث من الممكن - على سبيل المثال - جمع معلومات يتم إرسالها من خلال نظام حاسوب داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، و تقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسوب والتي تتحول إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى.[5] ص363،364

3.2.2.3.1.1. الركن المعنوي في جريمة التجسس المعلوماتي

يتحقق الركن المعنوي في جريمة التجسس المعلوماتي بتوافر القصد الجنائي بعنصريه العلم و الإرادة ،ذلك أن جريمة التجسس هي جريمة عمدية، فيجب أن يكون الجاني عالما بأن السلوك الذي يقترفه يمثل اختراقا و انتهاكا لحرمة و سرية مواد مرسلة عن طريق الشبكة المعلوماتية و أجهزة الحواسب الآلية، فإن كان يعتقد أن هذه المادة منشورة بصورة علنية و من حق الجميع الإطلاع عليها و سماعها تنتفي الجريمة ، كما يجب أن يكون عالما أنه ليس بيده مسوغا قانونيا يبيح له هذا التجسس، فإن كان يعتقد أنه يمتلك هذا المسوغ إنتفت الجريمة.[34] ص341

3.2.3.1.1. جريمة الاعتداء على الحياة الخاصة للأفراد

إن الانتشار الواسع للحاسوب الآلي على مستوى الأفراد أصبح يمثل تهديدا كبيرا لخصوصياتهم و أسرارهم، ذلك أن الحواسب تتميز بسرعة فائقة في العمل و سعة غير محدودة في استيعاب البيانات، التي لا تنحصر فحسب في حالة تخزين هذه البيانات، بل تتعداها لاستخراج هذه البيانات من ذاكرة الحاسوب الآلي، الأمر الذي يمكن القول معه بإمكانية الإطلاع على قدر لا يستهان به من هذه البيانات التي قد تكون متكاملة إلى حد بعيد و متصلة بجوانب الحياة الخاصة للفرد، وذلك بمجرد جولة سريعة قد لا تستغرق أكثر من ثوان معدودة . [7] ص286

1.3.2.3.1.1. الركن الشرعي في جريمة الاعتداء على الحياة الخاصة

مراعاة للخطورة التي قد تمثلها التقنية المعلوماتية من خطر على خصوصيات الأفراد و أسرارهم، قضى المشرع الجزائري في المادة 303 مكرر من قانون العقوبات " يعاقب بالحبس من ستة (6)أشهر إلى ثلاث (3)سنوات و بغرامة من 50.000دج إلى 300.000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت و ذلك:

- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه .
- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه....".

كما يعاقب المشرع الجزائري في المادة 394مكرر2 كل من يقوم بحيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات التي تم الحصول عليها نتيجة الدخول أو البقاء في النظام المعلوماتي و كذا نتيجة التلاعب في معطياته و من بينها المعطيات المتعلقة بالحياة الخاصة للأفراد.

2.3.2.3.1.1. الركن المادي في جريمة الاعتداء على الحياة الخاصة

يتخذ السلوك الإجرامي في جريمة الاعتداء على الحياة الخاصة للأفراد عدة صور، و لعل من أهمها:

1.2.3.2.3.1.1. الإطلاع غير المشروع على البيانات الشخصية

إن الإطلاع على البيانات الموجودة على الحاسوب الآلي والخاصة بالأفراد يعد انتهاكا جسيما لخصوصياتهم ، وذلك في الأحوال التي يستدعي الاطلاع على مثل هذه البيانات الحصول على إذن مسبق من صاحبها ، فلا يشكل هذا الفعل انتهاكا في الحالة التي تكون هذه المعلومات مباحة للكافة، أو في الحالة التي يكون مسموح فيها للشخص الإطلاع عليها . و الإطلاع على المعلومات السرية يمكن أن تتم بطريقتين، طريقة مباشرة و أخرى غير مباشرة. أما الطريقة المباشرة فتتمثل بالولوج إلى المعلومات السرية بواسطة الحاسوب الآلي حاوي المعلومات ذاته، و ذلك باقتحام الفاعل لمكان تواجد الحاسوب الآلي و استغلاله لذلك، أما غير المباشرة فتتمثل في الاختراقات عن بعد لأنظمة الاتصال المعلوماتية بمعونة أجهزة تحليل الشفرات. [12] ص219

2.2.3.2.3.1.1. الإفشاء غير المشروع للبيانات و إساءة استخدامها

في غالب الأحيان يكون الحصول على المعلومات الخاصة بحياة الأفراد و أسرارهم ليس مجردا، و إنما بهدف استغلالها في تحقيق أغراض غير مشروعة، كإفشائها أو التهديد بإفشائها.و هذا الإفشاء و التهديد قد يتم بأي وسيلة كانت، فقد يتم الإفشاء أو التهديد عن طريق وسائل تقليدية كالكتابة مثلا، و قد يتم عن طريق وسائل حديثة، كاستخدام قنوات الاتصال المتعددة كالبريد الإلكتروني، أو المواقع الخاصة و التي تشكل مجالا خصبا لارتكاب هذه الأفعال، نظرا لسرعتها الفائقة في نقل المعلومات عبر مختلف أرجاء العالم.

3.2.3.2.3.1.1. الاعتداء على سرية الاتصالات و المراسلات

إن الاعتداء على سرية الاتصالات و المراسلات الذي يتم عن طريق وسائل الاتصال الحديثة تشكل خرقا لخصوصيات الأفراد و أسرارهم، ويمكن اعتبار هذا النوع من الاعتداء من قبيل التجسس المعلوماتي، الذي يستهدف أسرار الأفراد و خصوصياتهم من خلال التصنت على محادثاتهم الخاصة و الإطلاع على مضمون رسائلهم الالكترونية التي تتم عبر الشبكة.

3.3.2.3.1.1. الركن المعنوي في جريمة الاعتداء على الحياة الخاصة

جريمة الاعتداء على الحياة الخاصة جريمة عمدية تستوجب لقيامها، توافر القصد الجنائي بعنصريه العلم و الإرادة، أي أن تتجه إرادة الفاعل إلى الاعتداء على خصوصيات الأفراد وأسرارهم مع علمه أنه لا يملك الحق في ذلك، حيث تنتفي الجريمة إذا كان الإطلاع قد

وقع من شخص مكلف بالإطلاع على هذه البيانات من أجل تخزينها مثلا، أو كانت الأسرار المراد إفشاؤها أو المهدد بإفشائها غير سرية و مباحة للجميع بحيث لا يحرص صاحبها على إبقائها سرا، كما تنتفي الجريمة إذا كان الاعتداء على سرية الاتصالات و المراسلات قد تم بموجب مسوغ قانوني.

و في الأخير تجدر الإشارة إلى أن أنواع الجرائم المعلوماتية بالتعدد و التنوع بحيث لا يمكن حصرها، فنبقى دائما نترقب ظهور الجديد منها، فكما يقول البعض [17] ص139فإن الحديث عن الأنواع المختلفة للجرائم المعلوماتية و ذكرها، و ربما ذكر عددها لن يتوقف عند هذا الحد،بل يتجاوزه مستقبلا إلى أكثر من ذلك، و ذلك مرده إلى كون تكنولوجيا المعلومات لم تصل بعد إلى مرحلة النضج النهائي، فهي مازالت تكتب تاريخها الذهبي، و طالما الأمر كذلك فإن الجرائم المعلوماتية لم تصل بعد إلى صيغها و أنواعها النهائية.

2.1. الطبيعة الخاصة بالجرائم المعلوماتية

إن الثورة الرقمية التي فجرتها تكنولوجيا المعلومات و الاتصالات، وما صاحبها من مستجدات في مجال التقنية المعلوماتية، قد غيرت من شكل ونوعية و أسلوب الجرائم المعاصرة . فارتباط الجرائم المعلوماتية بالحاسوب الآلي، وما يتمتع به هذا الأخير من تقنية عالية، جعل منها جرائم ذات طبيعة خاصة، تميزت عن غيرها من الجرائم التقليدية سواء من حيث صفاتها أو من حيث مرتكبيها وكذا من حيث ضحاياها، فهي نوع متميز من الإجرام المعاصر، تتم في بيئة غير تقليدية كونها تقع خارج إطار الواقع المادي الملموس، وهذا ما يجعل منها جرائم ذات طبيعة هادئة لا عنف فيها و لا سفك دماء، وبهذا الشكل فهي تشكل مصدر إغراء كبير لمرتكبيها، كما أن الكثير منها يثير شكلا جديدا من الجرائم العابرة للحدود الوطنية أو القارية أو الدولية التي لا تعترف بالحدود بين الدول و القارات. ليس هذا فحسب، فمرتكبي هذا النوع من الجرائم، هم فئة من المجرمين لهم صفات خاصة تميزهم عن غيرهم من المجرمين، وهم يستخدمون في ارتكاب جرائمهم أساليب خاصة و تقنيات عالية الكفاءة يغلب عليها الطابع الفني و التقني، فضلا عن أن ارتباط هذه الجرائم بمختلف مناحي الحياة أدى إلى تعدد فئات ضحاياها من مجرد كونهم أشخاص عاديين إلى المؤسسات المالية و الاقتصادية و كذا القطاعات الحكومية . و عليه سنحاول من خلال هذا المبحث، التطرق إلى مجموعة السمات و الخصائص المميزة للجرائم المعلوماتية، و ذلك من خلال ثلاثة مطالب، نتناول في المطلب الأول الصفات الخاصة بالجرائم المعلوماتية، ثم نتطرق في المطلب الثاني إلى الصفات

الخاصة بمرتكبي هذه الجرائم، و نخصص المطلب الأخير للحديث عن الصفات الخاصة بضحايا الجرائم المعلوماتية.

1.2.1.الصفات الخاصة بالجرائم المعلوماتية

تتميز الجريمة المعلوماتية بصفات خاصة تميزها عن غيرها من الجرائم، حيث توصف بأنها جريمة هادئة لا عنف فيها و لا سفك دماء، و هي من الجرائم التي تشكل إغراء كبيرا أمام مرتكبيها، كما أنها جريمة لا حدود لها، فهي لا تعترف لا بالحدود و لا بالمسافات، و هذا ما سنحاول التعرض له تباعا في ثلاثة فروع، نتناول في الفرع الأول الطبيعة الهادئة للجرائم المعلوماتية، ثم نتطرق في الفرع الثاني إلى طبيعتها المغرية، و من ثم نتعرض في الفرع الثالث لطبيعتها المتعدية الحدود.

1.1.2.1.الجرائم المعلوماتية جرائم هادئة

إن استخدام الحاسوب الآلي في ارتكاب الجريمة، غير من المفهوم التقليدي لها، فإذا كانت الجريمة بصورتها التقليدية تتسم في غالب الأحيان بالعنف و القوة، بحيث أن ارتكاب جرائم كالقتل أو الاغتصاب أو الاختطاف يتطلب عادة أن يقوم الجاني بمجهود عضلي، فإن الجريمة في ظل المعلوماتية لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية و التفكير العلمي المدروس القائم على معرفة تقنيات الحاسوب الآلي و القدرة على التعامل معه و كذا الذكاء في استخدامه، فهي ترتكب عن طريق نبضات الكترونية غير مرئية، لا تتطلب أكثر من عدد من اللمسات على أزرار يقوم بها الجاني ليكون قد ارتكب اخطر جرائمه، و هذا ما جعل البعض يصفها بأنها جرائم هادئة.

و رغم أن الكثير من يعترف بالطبيعة الهادئة للجرائم المعلوماتية، إلا أن هناك من ذهب إلى القول أن هذه الجرائم لا تختلف عن بقية الجرائم الأخرى من حيث العنف، فمكتب التحقيقات الفيدرالي التابع للولايات المتحدة الأمريكية و المعروف بـ (FBI) ذهب إلى وصف الجرائم المعلوماتية بأنها جرائم عنف، على أساس أن الدافع الذي يدفع مرتكبي هذه الجرائم، سواء من متلصصين أو دخلاء، و معتمدين على نظم الحاسوب الآلي هي دوافع متماثلة مع دوافع مرتكبي العنف من مفجري القنابل أو مشعلي الحرائق . [22] ص145

و قد انتقد البعض هذا التشبيه، فذهبوا إلى القول: «الحق أنه تشبيه لا يعتمد في حقيقته على الآثار التي تتولد عن هذه الجرائم أو ما يصاحب النشاط الذي ترتكب به من آثار، إنما في

الحقيقة تشبيه يعتمد على الدوافع، و هو في اعتقادنا إن صح في نطاق بعض الجرائم، فهو لا يصح في جميع الجرائم التي تقع على الكيان المعنوي للحاسوب الآلي، و توضيح ذلك أن مثل هذا الوصف إن كان ينطبق على الجرائم التي يسعى فيها الجناة إلى تدمير المعلومات و البرامج و إتلافها، فهي تقترب من جرائم الحريق المتعمد التي تقع و التي يكون القصد من ارتكابها تسبيب الأضرار للمجني عليه، و لكنها لا تنطبق على الجرائم التي يكون القصد منها الحصول على نفع مادي ، و الفئة الأخيرة هي الغالبة في جرائم الحاسوب الآلي».[22] ص145

وعليه يمكن القول أنه من غير المعقول وصف الجرائم المعلوماتية بأنها جرائم عنف على أساس التشابه في الدوافع فقط، ذلك أن جل الجرائم المعلوماتية لا تحتاج سوى لمجرم له قدرة على توظيف خبراته في مجال التقنية المعلوماتية لارتكابها دون حاجة لسفك دماء.

و تجدر الإشارة إلى أن الطبيعة الهادئة للجرائم المعلوماتية، أصبحت تشكل عائقا كبيرا أمام سلطات البحث و التحري، فبطبيعتها هذه، أصبح من السهل ارتكابها و طمس معالمها ومحو آثارها حتى قبل اكتشافها، وسنترك تفصيل ذلك لاحقا.

2.1.2.1. الجرائم المعلوماتية جرائم مغرية

لما كانت الجريمة المعلوماتية تتميز بالدقة و السرعة في تنفيذها، كنتيجة حتمية للتقنيات الرقمية المستخدمة في تنفيذها، و التي تعتبر ذات طبيعة سريعة في أدائها و دقيقة في إصابة الهدف، فتبدأ الجريمة و تنتهي بسرعة بالغة[35] ص05، و أمام ضخامة الفوائد و المكاسب التي يملك الجاني تحقيقها باقتراف مثل هذه الجرائم دون جهد يذكر، و دون أن يخاف أن يكتشف أمره ، أمام ذلك كله شكلت الجرائم المعلوماتية إغراء كبيرا للمجرمين، لاستغلال التكنولوجيا الحديثة بغية اقتراف الجرائم بصورها المتعددة، خصوصا عندما يكون الجاني موظفا في شركة تعتمد الحاسوب الآلي في عملها، إذ يكون لديه كافة المعلومات اللازمة لتحقيق اختراقات متعددة و متتالية لأنظمة الحاسوب الآلي في الشركة و تحقيق أرباح طائلة. [12] ص 108

و لم يعد الأمر مقتصرا على إغراء العمال في الشركات التي تستخدم الحاسوب الآلي في عملها فحسب، و إنما انتقل الأمر إلى إغراء العديد من أفراد المجتمع، خاصة و أن الحاسوب الآلي أصبح في متناول الجميع، مما أدى إلى ازدياد ارتكاب الجرائم المعلوماتية والتي أصبحت

تشكل خطرا كبيرا على خصوصيات الأفراد و على اقتصاد المؤسسات والشركات، و حتى على الأمن القومي للبلاد.

وبالإضافة إلى ذلك، يمكن القول أن غياب الأنظمة و القوانين الرادعة لمواجهة هذا النوع المستحدث من الجرائم، بحيث هناك عدد من التشريعات لم تنتبه بعد لمثل هذه الجرائم ولم تصل لصياغة النصوص التي تجب كافة الأفعال التي تقوم بها الجريمة، و كذا عجز السلطات المعنية عن التصدي لهذه الجرائم و الكشف عنها و تعقب الجناة فيها و محاكمتهم، يشكل و بلا شك مصدر إغراء كبير لمرتكبي هذا النوع من الجرائم، حيث أصبح هؤلاء يرتكبون جرائمهم و هم مطمئنين، و ذلك لثقتهم الكاملة أن هذه الجرائم لا تزال خافية المعالم على السلطات، و بالتالي فإن أمر اكتشافهم و ملاحقتهم و إثبات الجريمة بحقهم، أمر لا يزال صعب المنال.

3.1.2.1.الجرائم المعلوماتية جرائم متعدية الحدود

الجريمة المعلوماتية تعتبر شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية[36] ص360، فلم تعد تقتصر الجريمة المعلوماتية على النطاق الوطني فحسب، بل بدأت تأخذ بعدا دوليا امتدت فيه الجريمة إلى خارج الحدود الوطنية إلى دول و قارات أخرى.

فبعد ظهور شبكات المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسب الآلية في نقل و تبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة، قد تتأثر بالجريمة المعلوماتية في آن واحد[5] ص52. فأصبحت هذه الجرائم تتميز بالتباعد الجغرافي بين الفاعل و المجني عليه، و من الوجهة التقنية بين الحاسوب أداة الجريمة و المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدف بالاعتداء [37] ص57، فغالبا ما يكون الجاني في بلد و المجني عليه في بلد آخر، و هذه أكثر المسائل التي تثير إشكالات في مجال الجرائم المعلوماتية من حيث الإجراءات الجنائية الواجب إتباعها و كذا القانون الواجب التطبيق.

و من القضايا التي لفتت النظر إلى البعد الدولي للجريمة المعلوماتية، قضية عرفت باسم مرض نقص المناعة المكتسبة (الإيدز). و تتخلص وقائعها عام 1989، في قيام احد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته

كان يحتوي على فيروس، و كان يترتب على مجرد تشغيله تعطيل جهاز الحاسوب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي، حتى يتمكن المجني عليه من الحصول على مضاد للفيروس. و في الثالث من شهر فيفري من عام 1990 تم إلقاء القبض على المتهم " جوزيف بوب " في أوهايو بالولايات المتحدة الأمريكية، و تقدمت المملكة المتحدة بطلب تسليمه لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، و بالفعل وافق القضاء الأمريكي على تسليم المتهم، و تم توجيه إحدى عشر تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. و أيا كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث(فيروس).[5] ص 53

إن الطبيعة المتعدية الحدود للجرائم المعلوماتية، و ما ينجم عنها من أخطار على المستوى الدولي، كانت سببا في تنامي الدعوات الرامية إلى ضرورة تضافر الجهود الدولية من أجل مكافحة الجرائم المعلوماتية، و ذلك من خلال الاتجاه إلى عقد معاهدات و اتفاقيات دولية تكفل التعاون من أجل ملاحقة المجرمين و معاقبتهم.

هذا و يمكن القول أنه سيأتي اليوم الذي يضم العالم الجرائم المعلوماتية إلى الجرائم الدولية، مثل تلويث البيئة، و جرائم الإرهاب.و تصبح من الجرائم التي لا تخضع للتقادم، و تخضع إلى قضاء جنائي دولي ،ذلك لأن أضرارها عامة و تهدد جميع مستخدمي الأجهزة الإلكترونية، و أصحاب المواقع على الشبكة العنكبوتية و في مختلف أرجاء العالم.

2.2.1. الصفات الخاصة بمرتكبي الجرائم المعلوماتية

إن التغير الذي طرأ على أنماط الجريمة، بحيث لم تعد تستهدف النفس والمال فقط، بل تجاوزتهما إلى الاعتداء على المعلومات و البيانات المعالجة آليا، أدى إلى التغيير في أنماط مرتكبيها وصفاتهم أيضا.فقد أدى ظهور الجرائم المعلوماتية إلى ولادة طائفة جديدة من المجرمين لهم من الصفات ما يميزهم عن غيرهم من المجرمين التقليديين، أطلق عليهم الفقه تسمية " مجرمي المعلوماتية "، و هم الذين لديهم مهارات تقنية أو دراية بالتكتيك المستخدم في

نظام الحاسوب الالكتروني والقادرين على استخدام هذا التكتيك لاختراق الرمز السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه"[38] ص15. وعليه سنحاول من خلال هذا المطلب تحديد أهم الصفات التي تميز مجرمي المعلوماتية عن غيرهم من المجرمين، وذلك من خلال تقسيمه إلى ثلاثة فروع، نتناول في الفرع الأول سمات مرتكبي الجرائم المعلوماتية، ثم نتعرض بعد ذلك لأهم فئاتهم، ونخصص الفرع الثالث للحديث عن أهم الدوافع التي قد تحملهم على ارتكاب جرائمهم.

1.2.2.1. سمات شخصية مرتكبي الجرائم المعلوماتية

اختلفت الآراء حول سمات شخصية مجرمي المعلوماتية، حيث تجد دراسات علم الإجرام الحديثة صعوبة في إيجاد ضابط لهم، وذلك بسبب التغيير الحاصل في محيط هذه الظاهرة الإجرامية المستحدثة، و الناجم عن التطور المستمر لتكنولوجيا المعلومات، ولكن و رغم ذلك فإن هذه الصعوبات لم تحل دون اقتراب الباحثين في هذا المجال من ملامح وسمات مرتكبي الجرائم المعلوماتية، و لعل من أهم السمات التي توصلوا إليها، و التي تميز مجرمي المعلوماتية عن غيرهم من المجرمين ما يلي :

1.1.2.2.1. الذكاء

يعرف الإجرام المعلوماتي بأنه إجرام الأذكياء[39] ص77، فهذا النوع من الإجرام يتطلب مقدرة عقلية و ذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسائر مادية كبيرة تلحق بالمجني عليه، فالمجرم المعلوماتي يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف أو الإتلاف المادي، بل يحاول أن يحقق أهدافه بهدوء [5] ص77 . فنحن لسنا بصدد سارق عادي أو محتال أو خائن أمانة بمفهومه التقليدي، بل أمام شخص يتمتع بمستوى عال من الذكاء، الذي يسخره في السيطرة على الحاسوب الآلي وجعله وسيلة سهلة في يده، إما لتعديل البيانات أو لاصطناع البرامج والنظم التي تستخدم في الاعتداء أو السحب من أجهزة التوزيع الآلي للنقود أو السلب بالقوة الالكترونية أو الإتلاف للبرامج والمعدات أو تخريبها أو لجعل الحاسوب يدلي بما في جعبته من أسرار معلوماتية لاستغلالها في أهداف إجرامية.[40] ص40

2.1.2.2.1. المهارة

تعد المهارة من أهم سمات المجرم المعلوماتي، ذلك أن ارتكاب جريمة من الجرائم المعلوماتية يقتضي أن يكون الفاعل على درجة عالية من المهارة في استخدام التقنية المعلوماتية،

والقدرة على اختراق نظم الحماية وكلمات السر الموضوعة للبرامج والمعلومات والبيانات، وهذا لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال أو تكون لديه خبرة كبيرة فيه، بل إن الواقع قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة، عن طريق التعليم أو الخبرة المكتسبة في العمل[5] ص57، فقد يكون تعاملهم مع الحاسوب الآلي مجرد هواية يمارسونها، و من خلال ممارستهم الدائمة لهذه الهواية اكتسبوا مهارة خاصة في التعامل مع الحاسوب الآلي، فاقت في بعض الأحيان مهارة ذوي الخبرة في مجال تكنولوجيا المعلومات.

3.1.2.2.1. المعرفة

يتميز المجرم المعلوماتي بإلمام جدي بالتقنية العالية، ومعرفته لكافة الظروف المحيطة بالجريمة المراد تنفيذها، وإمكانيات نجاحها أو فشلها . فكون الحاسوب الآلي هو أداة ارتكاب الجريمة، وكذا المحل الذي يرد عليه السلوك الإجرامي، فإن المجرم المعلوماتي يستطيع تجربة جريمته على أنظمة مماثلة لتلك التي يريد استهدافها وذلك قبل تنفيذ جريمته، فيمكنه بذلك تحديد احتمالات فشل جريمته أو نجاحها و سد الثغرات التي قد تؤدي إلى اكتشافها.

4.1.2.2.1. التمتع بالسلطة اتجاه النظام المعلوماتي

يقصد بالسلطة هنا الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي و التي تمكنه من ارتكاب جريمته. فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، و قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، و التي تعطي الفاعل مزايا متعددة كفتح الملفات و قراءتها و كتابتها و محو و تعديل المعلومات التي تحتوي عليها، كما قد تتمثل هذه السلطة في الحق في استعمال الحاسوب الآلي أو إجراء بعض التعاملات أو مجرد الدخول إلى الأماكن التي تحتوي على أنظمة الحواسب الآلية . وقد تكون السلطة التي يتمتع بها الجاني غير حقيقية، كما في حالة استخدام شفرة الدخول الخاصة بشخص أخر[5] ص58. و لهذا نجد أن الغالبية العظمى من مرتكبي الجرائم المعلوماتية هم من الموظفين في المؤسسات و التي تكون لهم بحكم وظيفتهم، السيطرة الكاملة على الأنظمة المعلوماتية مما يجعل ارتكابهم للجرائم المعلوماتية سهل المنال.

5.1.2.2.1 . الخوف من كشف جريمته

يتصف مجرمو المعلوماتية بالخوف من كشف جرائمهم و افتضاح أمرهم.صحيح أن هذه الخشية تصاحب المجرمين على اختلاف أفعالهم الإجرامية، إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب على افتضاح أمرهم من ارتباك مالي و فقد للمركز الوظيفي في كثير من الأحيان و كذا المكانة . و يساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الحواسب الآلية نفسها، فإن أكثر ما يعرض المجرم إلى اكتشاف أمره أن يطرأ أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها .فإن من أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسب الآلية سواء كانت المحل التي يرد عليه السلوك الإجرامي أو الوسيلة المستخدمة لتنفيذه، إنما تؤدي عملها بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي تمر بها أي من العمليات التي يقوم بها من مرة إلى أخرى، و هو ما يساعد على عدم كشف الجريمة طالما أن جميع خطوات التنفيذ معروفة مسبقا، بحيث لا يحتمل أن تتدخل عوامل غير متوقعة يكون من شأنها الكشف عن الجريمة . [5] ص 60

و على ذلك يمكن القول أن خوف مجرمي المعلوماتية من اكتشاف أمرهم يفسره انتماؤهم في الغالب الأعم إلى طبقة اجتماعية متعلمة و مثقفة، توليهم ثقة كبيرة خاصة في مجال عملهم، حيث نجد العديد من مجرمي المعلوماتية هم من الموظفين الأكفاء الذين هم محل ثقة من مدراءهم.

2.2.2.2.1. فئات مرتكبي الجرائم المعلوماتية

لم تتوصل دراسات علم الإجرام حتى الآن إلى وضع تصنيف ثابت لفئات مجرمي المعلوماتية ، و ذلك راجع دون شك للتطور و التغير السريع في أنماط الجريمة المعلوماتية، و ما جاء من تصنيفات، ما هي إلا نتيجة للدراسات و الأبحاث التي تناولت مرتكبي هذا النوع من الجرائم ،و من أهم فئات هؤلاء ما يلي :

1.2.2.2.2.1. فئة الهواة

يطلق البعض[2] ص522 على هذه الفئة تسمية " صغار نوابغ المعلوماتية" و تتكون هذه الأخيرة من صغار السن المولعين بالحاسوب الآلي، و الذين يقترفون أفعالهم الإجرامية عن طريق استخدام الأجهزة الخاصة بهم أو بمدارسهم. و غالبا ما تنحصر أفعالهم الإجرامية في ممارسة الاعتداءات على أنظمة الحاسوب الآلي رغبة في التحدي و الاكتشاف

و إثبات المقدرة و الميل للمغامرة ، فليس لاعتداءاتهم حدود، و هم يتبادلون المعلومات فيما بينهم عن وسائل الاختراق و آليات نجاحها و اطلاع بعضهم البعض عن أماكن الضعف في نظم الحاسوب الآلي [26] ص 36 . و لعل من بين هؤلاء ما اصطلح على تسميتهم بالقراصنة العابثين أو (الهاكرز) وهم أولئك الذين يقومون بعمليات اختراق للأنظمة المعلوماتية دون أن تتوافر لديهم دوافع حاقدة أو تخريبية و إنما ينطلقون من دوافع التحدي و إثبات المقدرة .

إن مجرمي هذه الفئة يثيرون جدلا واسعا، ففي الوقت الذي كثر فيه الحديث عن مخاطر هذه الفئة- على الأقل مواصلتها العبث بالحواسب - ظهرت دراسات و مؤلفات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام إلى دائرة العبث، و أحيانا البطولة[17] ص42. فقد ذهب البعض إلى اعتبار هؤلاء كأبطال يقدمون خدمة للتقنية من خلال إظهارهم لنقاط الضعف و عيوب أمن المعلومات ، دون أخذهم بعين الاعتبار أن هذا العبث قد يتحول إلى خطر حقيقي إذا أصبح هذا الهاوي الصغير للأفعال غير المشروعة، محترفا لأعمال السلب و غيرها من الجرائم مما يصعب الاستدلال عليه لما يملكه من مهارة و دراية بتقنية المعلومات. و لهذا نجد الرأي الغالب، يذهب إلى تصنيف هذه الفئة ضمن مجرمي المعلوماتية ، وذلك لما تمثله أفعالهم من خطورة على الأنظمة المعلوماتية سواء على المستوى المحلي أو على المستوى الدولي .

و من جانبنا نرى أنه لا يمكن التساهل مع هذه الفئة من الأحداث نظرا لما تتسبب فيه أفعالهم من أضرار قد تكلف خسائر جسيمة ، بل من الواجب اعتبار هؤلاء العابثين جانحين، يستلزم جنوحهم التقويم و الإصلاح. و لا يمكن أن نصل إلى تقويمهم و إصلاحهم إذا كنا نبتسم لعبثهم و نمجد انحرافهم.

و من الأمثلة الشهيرة لهذه الفئة من الهواة، أفراد العصابة (414) الأمريكية و التي نسب إليها أكثر من 60 فعلا و تعديا و اختراقا لذاكرات الحاسوب الآلي، كذلك قيام أولاد المدرسة الثانوية في مانهاتن عام 1980 باختراق شبكة اتصالات البيانات الكندية و تدمير ملفات زبائن الشركة.[14] ص41

2.2.2.2.1. المحترفون

تعتبر هذه الفئة من اخطر الفئات التي ترتكب الجرائم المعلوماتية، لأن الهدف الذي تقوم عليه هذه الأخيرة ينحصر في نية ارتكاب الفعل الإجرامي ، على عكس مجرمي الفئة الأولى، الذين قد يرتكبون جرائمهم دون أن تكون لهم نوايا آثمة. و من بين مجرمي هذه الفئة ،

القراصنة المحترفون أو (الكراكرز) و هم أولئك المتخصصون بفك شفرات البرامج[38] ص15 فهم نوع من الهاكرز المتخصصين، إلا أن اعتداءاتهم تعكس ميولا إجراميا خطيرا .

يتميز أصحاب هذه الفئة بأنهم أشخاص يتمتعون بقدرات عالية، باعتبارهم من المتخصصين في المعلوماتية، حيث تشير الإحصائيات التي أجريت في هذا الشأن إلى ما يلي:[22] ص137

- أن 25% من الجرائم المعلوماتية قام بها محللون للنظم.
- أن 18% من هذه الجرائم قام بها مصممون للنظم أو المبرمجون.
- أن 18%منها قام بها مستخدمو النظم.
- أن 16% من هذه الجرائم قام بها الصرافون.
- أن 11% قام بها شاغلو النظم .
- أن 12% قام بها الأجانب الخارجون عن المنشأة .

و عليه فإن أغلب أفراد هذه الفئة ممن يعملون في منشأة تستخدم الحاسوب الآلي في أعمالها، و هم بحكم وظيفتهم يتصلون بالحاسوب الآلي اتصالا وثيقا، الأمر الذي يجعلهم مطلعين باستمرار على محتويات الحاسوب وأسرار العمل[14] ص43. وما يساعد على نجاح عملياتهم غير المشروعة أنهم كثيرا ما ينظر إليهم بوصفهم مستخدمين مثاليين، والغالبية العظمى فيهم تشغل مراكز قيادية هامة، ويتمتعون لذلك بثقة كبيرة في مجال عملهم، أي أن الجرائم المرتكبة بواسطتهم تشبه إلى حد كبير الجرائم المرتكبة بواسطة ذوي الياقات البيضاء من حيث كونهم من أصحاب التخصصات العالية ولهم الهيمنة على التقنيات الحديثة وعلى قدر من الذكاء الاجتماعي. [4] ص64

إن جرائم هذه الفئة تنصب في الغالب على الأموال والتلاعب في حسابات البنوك والمؤسسات المالية . كما قد يقوم مجرمو هذه الفئة بمهمات إستخباراتية تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها سواء كانوا يعملون لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها.[22] ص137

ومن الأمثلة العديدة على هذه الفئة المحترفة ،قيام موظف في قسم معالجة البيانات في أحد مصانع اسطوانات بجنوب ألمانيا، بإعداد و وضع برامج تصحيحية في حاسوب المصنع تلغي بصفة دائمة مديونية شركة تابعة لشريكه في معاملاتها المالية في المصنع، وذلك بجعل ما

تدين به هذه الشركة "صفرا" دائما، كما استخدم برنامج آخر للحيلولة عند غيابه أو قيامه بإجازة، دون إخراج حاسوب المصنع مخرجات تتعلق بحسابات هذه الشركة والمشتريات التي لم تسدد ثمنها للمصنع، إضافة إلى تفريغ قاعدة البيانات المخزنة بحاسوب المصنع من أي بيانات تتعلق بمديونيتها .وخلال الفترة الواقعة بين عام 1975 و 1982 تمكن الجاني وشريكه من الحصول على مواد ومعدات من المصنع بلغ ثمنها 000 153 4 مارك إلى أن صدر حكم من القضاء الألماني بحبسهما سنة 1985 لمدة خمس سنوات ونصف.[12]، ص85

3.2.2.1. دوافع ارتكاب الجرائم المعلوماتية

إن الدافع هو قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، و هو بذلك يختلف من جريمة إلى أخرى، تبعا لاختلاف الناس من حيث السن و الجنس و درجة التعليم و غير ذلك من المؤثرات، كما يختلف بالنسبة للجريمة الواحدة[41] ص427. و رغم أن الدافع لا يعتبر من عناصر الجريمة إلا أنه يلعب دورا كبيرا في الكشف عن مجرميها.ولعل من أهم الدوافع التي تدفع المجرم المعلوماتي لارتكاب جريمته ما يلي :

1.3.2.2.1. البحث عن الربح المادي

البحث عن الربح المادي يعتبر من أهم دوافع المجرمين المعلوماتيين[42]ص66، حيث يقوم هؤلاء بتوجيه إمكانياتهم ومهاراتهم وخبراتهم في مجال المعلوماتية من أجل الحصول على الأموال سواء بطريقة مباشرة، كالدخول إلى أنظمة المؤسسات المالية وتحويل الأموال إلى حسابات خاصة بهم، وإما بطريقة غير مباشرة بإتاحة الاطلاع على معلومات معينة مقابل مبالغ مالية ضخمة، خاصة إذا كانت هذه المعلومات ذات أهمية كبيرة لطالبيها.

فقد أشارت مجلة (Sècuritè Informatique) على لسان الأستاذ (Parker) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد بوشرت من اجل اختلاس أموال ،و 23 % من أجل سرقة معلومات، 19 % أفعال إتلاف و 15% سرقة وقت الآلة أي الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية . [44] ص24

و في الواقع فإن المحرك لاقتراف الجرائم المعلوماتية، يمكن أن ينطلق من مجرد النجاة من غرق الديون المستحقة، أو من المشاكل العائلية الراجعة إلى النقود أو من الخسائر الضخمة لألعاب القمار أو من إدمان المخدرات.[2]ص 530

2.3.2.2.1. إثبات التفوق العلمي

قد يكون الدافع إلى ارتكاب الجريمة المعلوماتية بعيدا عن النية الإجرامية، و إنما يكون مجرد رغبة في إثبات الذات من خلال تحدي تقنية الأنظمة المعلوماتية و إثبات تفوقهم عليها و قدرتهم على اختراقها و الدخول إليها، لدرجة أنهم و إزاء ظهور أي تقنية مستحدثة يسعون بكل الطرق إلى إيجاد وسائل التفوق عليها. و قد يتولد لدى البعض منهم صفة الغرور و المتعة بحيث يقدم المجرم على ارتكاب الجريمة تعاليا و تفاخرا بقدرته على إحداث الآثار المترتبة عنها.

3.3.2.2.1. الانتقام

يعد دافع الانتقام من اخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة، لأن هذا الدافع غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، لأنه غالبا ما يكون احد موظفيها، و يكون له هذا الدافع – الانتقام – نتيجة إما لفصله من العمل أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[33]ص19. فعلى سبيل المثال، دفع الانتقام بمسؤول عن النظام، تم طرده من المؤسسة التي يعمل بها في سنة 1999، إلى زرع قنبلة منطقية في برنامج موجود في آلات العمل لمستخدمه السابق، مما أدى إلى تعطيل المؤسسة عن العمل لمدة شهر كامل.[43] ص19

4.3.2.2.1 . التجسس

قد يكون الدافع إلى ارتكاب الجريمة المعلوماتية هو جمع معلومات لمصلحة جهات معينة قد تكون أشخاص أو مؤسسات أو دول، حيث أصبحت المعلومات في الوقت الحاضر تشكل سلاحا فتاكا في يد من يمتلكه .ولهذا تسعى العديد من الجهات إلى تجنيد أفراد تكون مهمتهم الأساسية هي القيام بعمليات التجسس لصالحها، فالتنافس الاقتصادي أدى بالمؤسسات إلى السعي جاهدة للحصول على الأسرار التسويقية و خطوات الإنتاج و كذا عناوين العملاء، و غير ذلك من المعلومات التي تخص نظيراتها من المؤسسات .كما أن التسابق الفضائي و العسكري و النووي أدى بالدول إلى تكثيف عمليات التجسس من خلال اختراق النظم الأمنية و العسكرية و النووية من أجل الحصول على المعلومات التي تجعلها قادرة على مواجهة أي خطر يهددها .

3.2.1. الصفات الخاصة بضحايا الجرائم المعلوماتية

لقد نوقش موضوع ضحايا الجرائم المعلوماتية بصفة خاصة خلال الأعمال التحضيرية للمؤتمر السابع للأمم المتحدة لمنع الجريمة و معاقبة المجرمين في عام 1985[11]ص29، و الضحية في الجريمة المعلوماتية هو ذلك الشخص الطبيعي أو المعنوي صاحب الحق أو المصلحة المشمولان بالحماية الجنائية، و اللذان أضرت بهما الجريمة أو عرضتهما للخطر[33]ص37. و يتنوع ضحايا الجرائم المعلوماتية، من مجرد أشخاص عاديين إلى مؤسسات مالية و قطاعات حكومية و دولية، حيث أن انتشار الحاسوب الآلي على مستوى هذه المؤسسات و القطاعات أدى إلى سهولة استهدافها.فبعد أن كان من الصعب على أي فرد أن يطالها بجرائمه، أصبح اليوم بإمكانه و بمجرد ضغطه على مفتاح من مفاتيح الحاسوب أن يتسبب لها في أضرار قد تكلفها غاليا.

وما يميز ضحايا هذا النوع من الجرائم هي ردود أفعالهم اتجاه ما يطالهم من جرائم معلوماتية و التي اختلفت عن ردود أفعال غيرهم من الضحايا . وعلى ذلك سنحاول من خلال هذا المطلب تحديد أهم صفات ضحايا الجرائم المعلوماتية، و ذلك من خلال تقسيمه إلى فرعين، نتطرق في الفرع الأول إلى فئات ضحايا الجرائم المعلوماتية، ثم نتطرق في الفرع الثاني إلى ردود أفعال هؤلاء الضحايا.

1.3.2.1. فئات ضحايا الجرائم المعلوماتية

إن وقوع الجريمة المعلوماتية في بيئة الحاسوب الآلي، جعل من الفئات المستهدفة هي تلك المعتمدة أكثر من غيرها على أجهزة الحاسوب الآلي، و هذه الفئات قد تكون أشخاصا طبيعية كما قد تكون أشخاصا معنوية، و من أهمها:

1.1.3.2.1 المؤسسات المالية و الاقتصادية

تعتبر المؤسسات بمختلف أشكالها سواء الاقتصادية منها أو المالية هدفا رئيسيا للعديد من مرتكبي الجرائم المعلوماتية، حيث تشير الإحصائيات إلى أن 19% من الجرائم المعلوماتية تستهدف البنوك، و 16% منها تستهدف الإدارات و 10% تستهدف البنوك، و تستهدف 10% منها المعلومات[2]ص 536. و على ذلك فإن المؤسسات المالية تعتبر الأكثر استهدافا من قبل مجرمي المعلوماتية، و ذلك لما تحتويه من أموال .فعادة ما تكون هذه المؤسسات ضحية

جرائم استيلاء على حسابات العملاء و كذا جرائم تحويل الأموال و التحايل باستخدام بطاقات الائتمان المزيفة و غيرها من الجرائم التي تنصب على أموالها.

ومن الأمثلة العديدة على ما قد يصيب مثل هذه المؤسسات المالية، ما حدث في أكتوبر عام 2000، حيث ابتكرت مجموعة من حوالي 20 شخصا بعضهم يرتبط بعائلات المافيا و بمساعدة شخص يعمل في بنك صقلية، نسخة رقمية طبق الأصل لنظام اتصال البنك بشبكة الانترنت . بعد ذلك قررت المجموعة استعمال هذه النسخة الرقمية المطابقة للأصل لتحويل مبلغ (400) مليار دولار من البنك، كان الإتحاد الأوروبي قد خصصها لتمويل مشاريع إقليمية في صقلية، و كان من المقرر غسل الأموال عبر مؤسسات مالية مختلفة مثل بنوك سويسرا، إلا أن الخطة باءت بالفشل عندما باح بالسر شخص من المجموعة إلى السلطات الرسمية [28]ص 71،70 .و تجدر الإشارة هنا إلى أن مثل هذه العملية لو تمت لكانت ألحقت خسائر مالية كبيرة.

و بالإضافة إلى قطاعات المال، تزداد رقعة الجريمة لتشمل شركات التأمين، فقد شهدت (لوس أنجلوس) أشهر الجرائم من هذا النوع ، عندما تمكن أحد موظفي شركة تأمين كبرى باستخدام نظامها الحاسوبي من خلق عملاء وهميين مؤمن عليهم، و تمكن من بيع 46.000 بوليصة تأمين إلى شركة مناظرة.[12] ص 89

كما تعتبر المؤسسات الصناعية و التجارية المجال الخصب الذي ترتكب فيه العديد من الجرائم المعلوماتية، خاصة التجسسية منها، حيث يعمد العديد من أصحاب هذه المؤسسات لمعرفة حجم المبيعات و عناوين العملاء و غيرها من المعلومات التي تخص نظيراتها من المؤسسات المنافسة لها. فقد أشار تقرير صادر عن وزارة التجارة و الصناعة البريطانية إلى زيادة نسبة التجسس على الشركات من 32% عام 1994 إلى 54% عام 1999[34] ص 343، كما أظهر استفتاء أجري عام 1996 لمسؤولي الأمن الصناعي في الشركات الأمريكية، حصول الكثير من الدول و بشكل غير مشروع على معلومات سرية لأنشطة تجارية و صناعية في الولايات المتحدة الأمريكية. [44] ص65

و على ذلك يمكن القول، أن استخدام هذه المؤسسات للأنظمة المعلوماتية، سيجعلها في عرضة دائمة للعديد من الجرائم المعلوماتية، ولهذا فلا بد عليها أن تسعى جاهدة لتفعيل نظم حماية أنظمتها بالشكل الذي يجعلها في منأى عن مثل هذه الاعتداءات التي قد تكلفها خسائر جسيمة.

2.1.3.2.1. المؤسسات العسكرية

المؤسسات العسكرية هي من أهم مؤسسات الدولة و أكثرها استخداما للمعلوماتية، و بالتالي فهي كانت و ما زالت تعد منشطا مهما و مجالا خصبا لمحاولات التجسس و الاختراق، نظرا لما يتوفر لدى العاملين فيها من معلومات تهم أمن الدولة[34] ص342، حيث أصبحت الدولة التي تمتلك المعلومات هي الدولة الأقوى، فلم تعد الحرب حرب أسلحة و متفجرات، و إنما أصبحت الحرب في الوقت الحاضر حرب معلومات، فقد أضحت المعلومات السلاح الرئيسي التي تعتمد عليه الدول في قهر أعدائها. ولهذا انتشرت عمليات التجسس الالكتروني قصد رصد مختلف البيانات المتعلقة بأسرار الدولة و مشروعاتها النووية، و كذا حجم عتادها العسكري و إمكانياتها و عدد قواتها و غير ذلك.

و لعل من أهم الحالات التي استهدفت هذا النوع من المؤسسات، تلك الحالة التي تتلخص وقائعها في قيام ثلاثة طلبة ألمان بالعمل لحساب المخابرات السوفيتية، حيث قاموا بمدها بالشفرات الخاصة بأنظمة حواسب آلية غاية في الأهمية، و منها نظام الحاسوب الخاص بوزارة الدفاع الأمريكية و معمل للأبحاث في (لولا موس)و إحدى الشركات الفرنسية و معاهد علمية متفرقة في أوربا و أمريكا الشمالية و اليابان.و تمكن الجناة في هذه الواقعة من الدخول إلى أنظمة الحواسب سالفة الذكر عبر شبكات المعلومات، حيث تمكنوا من استغلال بعض الثغرات التي تعترض الإجراءات الأمنية لهذه الأنظمة للحصول على الشفرات الخاصة بها . وقد تم اكتشاف الجناة بالصدفة حيث استغرقت عملية تتبعهم عاما كاملا، قدموا بعدها للمحاكمة أمام القضاء الألماني، ووجهت إليهم تهمة التجسس لصالح دولة أجنبية، و كان ذلك في عام 1989.[5] ص280

3.1.3.2.1. الأشخاص

إن الانتشار المطرد لأجهزة الحواسب الآلية على مستوى الأفراد، و اتصال هذه الأجهزة في معظم الأحيان بشبكة الاتصالات الدولية، جعل هؤلاء عرضة للعديد من الجرائم المعلوماتية، كجرائم التجسس، و التي باتت من أخطر الجرائم التي يتعرض لها الأشخاص لما تشكله من انتهاك صارخ لخصوصياتهم و أسرارهم، بالإضافة إلى جرائم السب و القذف عبر الانترنت ،حيث أصبحت هذه الشبكة وسيلة تستخدم للنيل من شرف الأفراد و اعتبارهم و كرامتهم من خلال ما يتم إرساله من رسائل الكترونية محملة بعبارات مسيئة و مشينة.

وبعد أن أصبح بإمكان إبرام العديد من العمليات المالية عبر شبكة الانترنت كشراء المنتجات المعروضة عبر المواقع مثلا ،اتسعت دائرة جرائم النصب و الاحتيال المعلوماتي ضد الأفراد.و لعل خير مثال لما يتعرض له الأفراد من جرائم نصب و احتيال، وقوع الشعب الأمريكي ضحية لجريمة النصب من قبل بعض الأشخاص مستغلين الحادث الإرهابي الذي حدث في الولايات المتحدة الأمريكية في الحادي عشر من سبتمبر سنة 2001، حيث قامت العديد من الجهات بإنشاء عدة مواقع على شبكة الانترنت بغرض جمع تبرعات للضحايا. و على هذا الأساس قامت حكومة الولايات المتحدة بتحذير رعاياها من الوقوع ضحايا لتلك العمليات الإجرامية.[33] ص 44

و تعتبر جرائم الإتلاف المعلوماتي عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الالكتروني، لأن هذا البريد الالكتروني من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الأشخاص، بالإضافة إلى سرقة أرقام بطاقات الائتمان.[33] ص43

2.3.2.1. ردود أفعال ضحايا الجرائم المعلوماتية

تختلف ردود أفعال ضحايا الجرائم المعلوماتية عن ردود غيرهم من الضحايا،فإن كان أي ضحية مهما كانت الجريمة المرتكبة ضده، يسارع إلى الإبلاغ عنها للسلطات المختصة، فإنه على العكس من ذلك فإن الضحية في الجرائم المعلوماتية يفضل إبقاء ما يلحقه من اعتداء جراء هذا النوع من الجرائم طي الكتمان، و هذا ما تؤكده العديد من الدراسات التي أجريت في هذا الشأن.

ففي دراسة أجراها المعهد الوطني للعدالة التابع لوزارة العدل الأمريكية و التي شملت 127 من العاملين في مجال التحقيق في الجرائم المعلوماتية، يمثلون 114 وكالة رسمية و غير رسمية، كان غالبية المشاركين يرون أن معظم الجرائم المعلوماتية لا يبلغ عنها للشرطة ، كما توصلت دراسة أخرى أجراها معهد أمن الحاسوب بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية، إلى أن 70% من الجرائم التي يتم اكتشافها لا يتم الإبلاغ عنها لسلطات إنفاذ العدالة [45] ص10، و في دراسة أجريت عام 1980 في فرنسا أشارت النتائج إلى أن الجرائم المعلوماتية التي تم التبليغ عنها للسلطات المختصة بلغت 15% فقط من مجموع الجرائم المرتكبة[46] ص358. و لهذا فإن الغالبية العظمى من الجرائم المعلوماتية التي يتم اكتشافها لا تكون إلا بمحض الصدفة.

إن تكتم الضحية عن الإبلاغ عما يلحقه من جرائم معلوماتية أدى إلى استحالة تحديد حجم الجرائم المعلوماتية المرتكبة، و بالتالي إلى ارتفاع الرقم الأسود، حيث تؤكد دراسة أجريت في الولايات المتحدة الأمريكية أن الرقم الأسود لجرائم المعلوماتية يميل إلى الارتفاع ، فاستنادا إلى تحليل الباحثين و في ضوء تقارير جمعيات صانعي الحواسب يظهر أن الرقم الأسود ما يقارب نسبة 60% من الجرائم المعلوماتية.[46] ص 358

و لا يقف الأمر عند استحالة تحديد حجم الجرائم المعلوماتية فحسب ، و إنما ردود الأفعال السلبية لضحايا هذه الجرائم، قد تكون خير معين لمرتكبيها، حيث أن اطمئنانهم لعدم التبليغ عنهم قد يساهم في ازدياد نشاطهم و خلق مجالات إجرامية جديدة و انتشار و اتساع رقعة إجرامهم.

و يمكن القول أن تكتم ضحايا الجرائم المعلوماتية وإحجامهم عن الإبلاغ عما يصيبهم من اعتداءات راجع بشكل أساسي إلى طبيعة هؤلاء الضحايا، فكما سبق و أسلفنا فإن معظم ضحايا الجرائم المعلوماتية هم مؤسسات مالية و اقتصادية لها سمعتها و تخشى من التشهير بها، ليس هذا فحسب فهناك العديد من الأسباب التي تجعل هؤلاء الضحايا يفضلون التكتم عما يصيبهم من جرائم معلوماتية، و سنترك الحديث عن هذه الأسباب عند تطرقنا لإحجام المجني عليهم عن الإبلاغ كصعوبة من الصعوبات التي تعترض سبيل إثبات الجرائم المعلوماتية .

3.1. أثر الطبيعة الخاصة بالجرائم المعلوماتية في الإثبات الجنائي

إن الطبيعة الخاصة بالجرائم المعلوماتية سواء من حيث صفاتها، أو من حيث صفات مرتكبيها و كذا من حيث صفات ضحاياها - والتي نوهنا عنها فيما سبق- تركت آثارا واضحة في إثبات هذا النوع من الجرائم، فقد أفرزت جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول، في العديد من الصعوبات التي أصبحت تشكل عائقا كبيرا أمام السلطات التي تعنى بإثبات هذه الجرائم، الأمر الذي أدى في الكثير من الأحيان إلى عدم اكتشاف العديد منها في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبونها أو تعذر إقامة الدليل اللازم لإثباتها . فمن بين الصعوبات التي تكتنف إثبات الجرائم المعلوماتية، ما تعلق منها بالجرائم ذاتها، سواء من حيث غياب الآثار التقليدية عنها أو من حيث المكان الذي ترتكب فيها أو من حيث قصور القوانين الإجرائية التي تنظمها، كما أن هناك من الصعوبات ما تعلق منها بأدلة إثبات هذا النوع من الجرائم، فهي أدلة غير مرئية، يسهل إخفاؤها و تدميرها، بالإضافة إلى أنها أدلة يمكن القول عنها أنها أدلة محمية. ليس هذا فحسب، و إنما

يشكل العامل البشري فيها أحد أهم هذه الصعوبات. وعليه سنحاول من خلال هذا المبحث ، بحث جملة الصعوبات التي تكتنف إثبات الجرائم المعلوماتية كأثر للطبيعة الخاصة بها. وارتأينا تقسيمه إلى ثلاث مطالب، نتناول في المطلب الأول الصعوبات المتعلقة بالجرائم المعلوماتية ذاتها، و نتطرق في المطلب الثاني للصعوبات المتعلقة بأدلة إثباتها، و نخصص المطلب الأخير للحديث عما يثيره العامل البشري من صعوبات في هذا المجال.

1.3.1 الصعوبات المتعلقة بالجرائم المعلوماتية ذاتها

سبق و أن تحدثنا عن الصفات الخاصة بالجريمة المعلوماتية، وقلنا أن من أهم صفاتها أنها جريمة هادئة أو ناعمة لا عنف فيها ولا سفك دماء، فهي لا تتطلب سوى بضع لمسات ليرتكب الجاني جريمته. وإن كان يرى الجاني في هذا امتياز له، فعلى العكس من ذلك ، فإن سلطات البحث والتحري تجده عائقا من عوائق إثبات هذا النوع من الجرائم، وذلك كون ارتكابها بهذه الطريقة يجعلها خافية المعالم و الآثار .و باعتبارها جريمة من الجرائم العابرة للحدود يجعل أيضا من أمر تحديد مكان ارتكابها وملاحقة مرتكبيها أمرا في غاية الصعوبة، فضلا عما يثيره القصور في القوانين الإجرائية الخاصة بهذه الجرائم من صعوبات في مجال إثباتها . كل هذا سنحاول التطرق إليه تباعا في هذا المطلب، و ذلك من خلال ثلاثة فروع، نتحدث في الفرع الأول عن غياب الآثار التقليدية في الجرائم المعلوماتية ثم نخصص الفرع الثاني للحديث عن صعوبة تحديد مكان ارتكاب هذه الجرائم، وسنتناول في الفرع الأخير القصور الذي يعتري القوانين الإجرائية في مواجهة الجرائم المعلوماتية.

1.1.3.1. غياب الآثار التقليدية في الجرائم المعلوماتية

على عكس الجرائم التقليدية التي تظهر آثارها بمجرد ارتكابها كالسرقة أو القتل أو الاغتصاب وغيرها من الجرائم، فإن الجرائم المعلوماتية جرائم لا تترك آثارا بعد ارتكابها، فليس هناك آثار مادية يمكن فحصها أو شهود يمكن استجوابهم أو حالات تلبس يمكن إدراكها بالحواس.

إن الجرائم المعلوماتية ما هي في حقيقتها سوى نبضات الكترونية تملأ الكون من حولنا، وتنساب كما تنساب الأشعة التي باستطاعتها أن تخترق كل ما في الكون من حواجز فتنفذ منها، وكما يمكن إرسالها، يمكن استقبالها من قبل الجاني، عن طريق محطات طرفية أو

محطات تستقبل النبضات والإشاعات المنبعثة من كابلات الربط [22] ص226، وعلى ذلك فهي تفتقد للآثار التقليدية للجريمة.

وقد يرجع السبب في عدم تخلف آثار عن الجرائم المعلوماتية، إلى ما لاحظه جانب من الفقه، من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسوب الآلي، دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على جهاز الحاسوب ويتوافر أمام المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد، فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى، حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطريقة آلية، وحسب الأوامر المعطاة لجهاز الحاسوب الآلي. ويمكن في الفروض السابقة اقتراف بعض أنواع الجرائم كالاختلاس والتزوير، وذلك بإدخال بيانات غير مطلوبة و غير معتمدة في نظام الحاسوب الآلي أو تعديل البرنامج المخزن في الجهاز، وتكون النتيجة مخرجات على هوى مستعمل الجهاز الذي أدخل البيانات أو عدل البرنامج دون استخدام وثائق أو مستندات، وبالتالي تفتقد الجريمة لآثارها التقليدية.فمثلا جريمة التزوير في محرر رسمي أو عرفي بقصد استعماله، تفترض وجود محرر مزور تم تزويره بغرض الاستعمال .هذا المحرر في ذاته من الآثار التقليدية لجريمة التزوير، كذلك في جريمة الاختلاس في صورتها العادية نجد مستندات تشير إلى أرقام وحقائق قد تكون مبالغ مالية في الحسابات أو بضاعة في المخزن اختلسها صاحب العهدة لنفسه، لكن عند ارتكاب هذه الجريمة بطريقة الحاسوب الآلي، لا يظهر للمشاهد سوى أرقام وبيانات لا يعلمها سوى صاحب الشأن نفسه. [47] ص124

إلا انه و رغم ذلك، لا يمكن القول بأن الجريمة المعلوماتية لا تتخلف عنها آثار مادية مطلقا، وإنما لابد من التمييز بين حالتين:

♦الحالة الأولى

هي حالة ارتكاب الجريمة المعلوماتية من خارج مسرح الجريمة، فسبق أن قلنا أن ما يميز الجريمة المعلوماتية هي إمكانية ارتكابها من مسافات قد تصل إلى دول وقارات ، فالمجرم المعلوماتي يمكنه أن يرتكب جريمته من أي مكان كان، دون أن يضطر إلى التواجد بمسرح الجريمة، كأن يقوم مثلا بالتعدي على مواقع الكترونية على الشبكة، ففي مثل هذه الحالة لا يمكن لنا أن نتصور تخلف أي آثار مادية قد تدل عليه.

◆الحالة الثانية

هي حالة ارتكاب الجريمة المعلوماتية من داخل مسرح الجريمة، فقد يرتكب المجرم المعلوماتي جريمته مثلا من داخل المؤسسة التي يعمل بها، كأن يقوم بعمليات تزوير للبيانات الموجودة على أجهزة الحاسوب الآلي لهذه المؤسسة مثلا، فمثل هذه الجريمة تتطلب التواجد الفعلي للفاعل بمسرح الجريمة، وفي هذه الحالة يمكن القول أنه مهما بلغت درجة ذكاء المجرم وحرصه، إلا وترك سهوا ما يدل عليه، كأن يغفل عن الأقراص المضغوطة التي سجل عليها نتائج ما قام به من تعديلات على البيانات أو البرامج، أو قد يغفل عن الأوراق التي كانت بها المعلومات أو البيانات المزورة التي أراد إدخالها. كل هذا قد يشكل آثرا من آثار جريمته.

ليس هذا فحسب، فقد يخلف الجاني في الجريمة المعلوماتية بعض الآثار التقليدية، كأن يترك بصمات أصابعه على المكتب الذي يوجد عليه الحاسوب الآلي، نتيجة عدم لبسه للقفازات، أو يترك آثار أقدامه أثناء دخوله إلى الغرفة التي يوجد بها النظام الذي تم العبث به وغيرها .إلا انه ورغم ما تكتسيه هذه الآثار من أهمية في الجرائم التقليدية، كونها تساعد في كشف الحقيقة من حيث إثبات وقوع الجريمة وتحديد مرتكبيها ، فإن هذه الآثار قد لا يكون لها أي نفع في إطار الجرائم المعلوماتية، فبصمات الأصابع المتواجدة بمسرح الجريمة لا تدل دلالة قاطعة على أن صاحبها هو من قام بالعبث بالنظام المعلوماتي، خاصة وأن هذا النظام قد يستخدمه العديد من الأشخاص.[22] ص226،227

وعليه يمكن القول أن عدم تخلف آثار للجريمة المعلوماتية، راجع بشكل أساسي إلى كونها تتم في بيئة غير مرئية، بعيدة كل البعد عن البيئة التي ترتكب فيها الجرائم التقليدية، ولذلك فإن من النادر تخلف آثار مادية عنها، و حتى و إن تخلفت مثل هذه الآثار ، فإن إثبات صلتها بالجاني أمر في غاية الصعوبة.

2.1.3.1. مكان ارتكاب الجرائم المعلوماتية

إذا كان الأصل أن عناصر الركن المادي لأي جريمة تكتمل في مكان واحد، أو بالأحرى في إقليم دولة واحدة، كأن يقدم أحدهم على طعن المجني عليه أو إطلاق الرصاص عليه، مما يفضي إلى وفاته في الحال أو بعد لحظة وجيزة . فإن الجرائم المعلوماتية، وفي غالب الأحيان يتجزأ ركنها المادي ويتوزع على أكثر من مكان واحد، مثال ذلك ما حدث في الكويت، حيث قام مبرمج انجليزي يعمل بأحد البنوك في دولة الكويت بالتلاعب في نظام الحاسوب الآلي

الخاص بالبنك، ليقوم بإجراء خصومات من أرصدة العملاء، ثم يقوم بإيداعها في الحساب الخاص به. وبعد عودة المتهم إلى انجلترا قام بالكتابة إلى البنك سائلا إياه أن يقوم بتحويل الحساب الخاص به إلى عدة حسابات بنكية في انجلترا، وهو ما قام به البنك بالفعل، وقدم المتهم للمحاكمة بتهمة الحصول على أموال الغير بطرق الاحتيال وحكم عليه بعقوبة السجن، إلا أن المتهم طعن في الحكم استنادا إلى عدم اختصاص القضاء الانجليزي، بما أن فعلي السحب والإيداع قد تما في الكويت وليس في انجلترا، إلا أن محكمة الاستئناف رفضت الطعن المتقدم، وردت على دفع المتهم، بأن النشاط الإجرامي لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الانجليزية. [5] ص54

فالجريمة المعلوماتية - كما سبق ذكره- جريمة ترتكب عبر المسافات حيث لا يتواجد الفاعل بمسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تبعد المسافات بين الفعل الذي يتم من خلال جهاز الحاسوب الآلي وبين النتيجة أي المعطيات محل الاعتداء، وما يزيد الأمر تعقيدا هو أن هذه المسافات لا تقف عند الحدود الإقليمية لدولة معينة، بل قد تمتد إلى النطاق الإقليمي لدول أخرى . فبعد دخول شبكة الاتصالات الدولية معظم دول العالم أصبحت الجريمة لا تعترف لا بالمكان ولا بالزمان، فأصبح اليوم من المحتمل باستخدام التكنولوجيا أن يقوم المستخدم بالضغط على لوحة المفاتيح في الدولة (س) لكي يقوم بتعديل بيانات مخزنة في الدولة (ص) حتى ولو لم يكن يعلم أن البيانات قد تم تخزينها هناك. [48] ص127

إن مسألة التباعد الجغرافي بين الفعل والنتيجة، أدى إلى العديد من المشكلات خاصة فيما يتعلق بإجراءات الملاحقة القضائية، سواء من حيث إمكانية امتداد أنشطة التحري والتحقيق إلى خارج الدولة ومن ثم البحث عن الأدلة وفحصها وجمعها، وكذا من حيث إمكانية تحويل الأدلة التي تم جمعها إلى الدولة التي يجري فيها التحقيق، فالبحث عن بيانات مخزنة في أنظمة أو شبكات الكترونية خارج إقليم الدولة، وكذا امتداد إجراءات التفتيش والضبط إليها يعد من أهم الصعوبات التي تواجهها أجهزة العدالة الجنائية، لما في ذلك من مساس بسيادة الدولة .

فإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس المعيار المعتمد في جل التشريعات، وهو مكان القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة، حيث ينعقد الاختصاص القضائي لسلطات التحقيق بأي من الأماكن المذكورة، فإن حل

هذه المشكلة على المستوى الدولي يحتاج إلى اتفاقيات ثنائية أو جماعية بين الدول يتم من خلالها تنظيم إجراءات التحري والتحقيق في مجال الجرائم المعلوماتية والتي تمتد إلى خارج الإقليم الوطني. [47] ص192

والملاحظ أن التشريعات الجنائية السارية اليوم في معظم دول العالم تميل إلى الطابع الإقليمي الذي يقيد حركة الإجراءات الجنائية بواسطة السلطات غير الوطنية، فهذه التشريعات لا تواكب حركة الاتصالات والمعلوماتية التي عمت أرجاء العالم. ولهذا شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في الجرائم المعلوماتية ، إلا أن ذلك لم يحقق تقدما في معالجة مشكلات الاختصاص وتبادل الأدلة الجنائية وتسليم المجرمين، لذلك فإن الأمر في حاجة إلى قوانين جنائية أكثر مرونة للتعامل مع سرعة تقدم الحاسوب الآلي في كل مناحي الحياة. [49] ص373

3.1.3.1. قصور القوانين الإجرائية في مواجهة الجرائم المعلوماتية

إن القصور الذي اعترى لفترة طويلة القوانين الجنائية الموضوعية فيما يتعلق بالجرائم المعلوماتية، انتقل إلى القوانين الجنائية الإجرائية، فنظرا للطبيعة الخاصة للجرائم المعلوماتية ، أصبحت هذه القوانين عاجزة عن ملاحقة مرتكبيها و إثبات ما يرتكبون من جرائم بحقهم و من ثم محاكمتهم.

و على الرغم من هذه الطبيعة الخاصة التي تميز الجرائم المعلوماتية، فإن إجراءات البحث عنها لا تزال تتم في إطار القوانين الإجرائية التقليدية التي وضعت لتطبق على جرائم تقليدية، لا صعوبة كبيرة في إثباتها. فلا يكفي القول بوجود نصوص تجريمية تتصدى للسلوكيات المستحدثة في بيئة الحاسوب الآلي بنظرية متطورة تواكب التطور التكنولوجي - سواء من حيث دقة تحديد السلوك المجرم وفق نموذج قانوني واضح أو سواء من حيث تقدير العقوبة المقررة له- وإنما لابد من استكمال هذه الحلقة من الشرعية الجنائية في الجرائم المعلوماتية، بحلقة ثانية تنظم الإجراءات الواجب اتخاذها من قبل جهات التحري والتحقيق لإثبات هذا النوع من الجرائم في حق مرتكبيها، وذلك على نحو يضمن شرعية الإجراءات من جهة، وعدم المساس بالحريات الشخصية من جهة ثانية.

فالتفتيش في هذا النمط من الجرائم يتم عادة على شبكات المعلومات، وقد يتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة، و هذا هو الوضع الغالب في ظل شيوع الشبكات الداخلية على مستوى الشركات أو المؤسسات، والشبكات المحلية و الإقليمية و الدولية على

مستوى الدول . وامتداد التفتيش إلى نظم غير النظام محل الاشتباه، محل تحديات كبيرة، أولها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش. [50] ص46

كما أن الضبط في الجرائم المعلوماتية لا يتوقف على تحريز جهاز الحاسوب الآلي فحسب، بل قد يمتد من ناحية ضبط المكونات المادية، إلى مختلف أجزاء النظام التي تزداد يوما بعد يوم، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الاشتباه، أي على أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف، وهذه الحقائق بدورها تثير مشكلات متعددة منها المعايير المقبولة للضبط المعلوماتي ومعايير التحريز، إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صاحبه - وإن كان المشتبه به - عندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عدة معلومات و بيانات قد يحرص على سريتها أو قد تكون محل حماية بحكم القانون أو لطبيعتها أو لتعلقها بجهات أخرى. [51] ص03

بالإضافة إلى ذلك فإن أدلة الإدانة ذات نوعية مختلفة فهي معنوية الطبيعة، كسجلات الكمبيوتر و معلومات الدخول و الاشتراك و النفاذ و البرمجيات، و هي تثير بدورها مشكلات جمة أمام القضاء، من حيث مدى قبولها و حجيتها و المعايير المتطلبة لتكون كذلك، خاصة في ظل قواعد الإثبات التقليدية. [8] ص08

إن كل هذا يدعونا للقول بأن اعتماد إجراءات تقليدية لإثبات جرائم متطورة بهذا الشكل، لا يفي بالغرض، و لذلك لابد من تحديث القوانين الجنائية الإجرائية بما يتناسب و طبيعة الجرائم المعلوماتية، و ذلك من خلال إعادة تقييم و مراجعة إجراءات البحث و التحري من تفتيش و ضبط و غيرها من الإجراءات، لتشمل المعلومات الرقمية والأنظمة المعلوماتية و أنظمة الاتصالات الحديثة .

و في هذا الإطار بدأت بعض التشريعات تعمل من أجل سد ما يشوب قوانينها الجنائية الإجرائية من فراغ في مجال الجرائم المعلوماتية، و من بينها المشرع الجزائري، فقد خطى هذا الأخير خطوة كبيرة في هذا المجال من خلال إصداره للقانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، و التي تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية

أو نظام للاتصالات، حيث تضمن القانون مجموعة من القواعد الإجرائية التي تنظم تفتيش المنظومات المعلوماتية و كذا حجزها بالإضافة إلى تنظيم إجراءات مراقبة الاتصالات الالكترونية.

2.3.1. الصعوبات المتعلقة بأدلة الجرائم المعلوماتية

تعتبر الأدلة الجنائية السبيل الوحيد الذي تعتمد عليه أجهزة العدالة الجنائية في إثبات الوقائع و تقصي الحقائق من أجل تحقيق العدل الذي ينشده كل فرد في المجتمع، و إن كانت الأدلة التي ألفتها أجهزة العدالة الجنائية في السابق ملموسة أو مرئية أو مسموعة، تتحدث عن نفسها كالأسلحة و العيارات النارية و غيرها، فإن الأدلة في ظل الثورة المعلوماتية أخذت شكلا جديدا، حيث أفرزت الجرائم المعلوماتية اليوم، أدلة جنائية ذات طبيعة مختلفة يصعب التعامل معها ، فهي أدلة معنوية الطبيعة، غير مرئية أو ملموسة ، سهلة الإخفاء، ويمكن حتى القول أنها أدلة محمية، و بطبيعتها هذه أصبحت تشكل عائقا كبيرا أمام أجهزة العدالة الجنائية التي تسعى إلى البحث عن الأدلة التي تفيد في إثبات ما يرتكب من جرائم معلوماتية في حق مرتكبيها، وذلك بسب عدم قدرتها على رؤية الدليل ، و كذا سهولة إخفائه و تدميره قبل اكتشافها له، بالإضافة إلى إمكانية وضع الجناة تدابيرتعيق وصولها إليه . و هذا ما سنتعرض له تباعا في هذا المطلب، حيث نخصص الفرع الأول للحديث عن غياب الدليل المرئي في الجرائم المعلوماتية، ثم نتطرق في الفرع الثاني إلى سهولة إخفاء الدليل في هذا النوع من الجرائم ، و نتعرض في الفرع الثالث إلى إعاقة الوصول إلى الدليل فيها.

1.2.3.1. غياب الدليل المرئي في الجرائم المعلوماتية

إن الجرائم التقليدية، غالبا ما ينجم عنها أدلة مادية ملموسة و مرئية يسهل على أجهزة العدالة الجنائية – بتجاربها الناجحة في هذا المجال – التعامل معها، كبصمات الأصابع و آثار الأقدام و غير ذلك، إلا أن الأمر يختلف في الجرائم المعلوماتية، فما ينجم عن هذه الأخيرة من أدلة، ما هي إلا أدلة غير مرئية لا يمكن إدراكها بالحواس الطبيعية للإنسان، و لا يستطيع التعامل معها إلا من كان بارعا في استيعاب التقنية المعلوماتية.

فالجرائم المعلوماتية ترتكب عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسوب الآلي و شبكة الاتصالات العالمية بصورة آلية ، كما تنساب الكهرباء عبر الأسلاك، و قد يتم نقلها بالإشعاعات، و غالبا ما يتم هذا عن طريق وحدات

طرفية بعيدة ، بل ربما تكون هذه الوحدات لاسلكية الاتصال مما يصعب ضبطها، بل إن هذه الجرائم يمكن ارتكابها عن طريق الهاتف، حيث يمكن من خلاله إصدار تعليمات للحاسوب الآلي و من مسافات بعيدة قد تتعدى إقليم الدولة[22] ص214، ومن ثم فإن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التي تقع عليها أو بواسطتها، ما هي إلا بيانات غير مرئية لا تفصح عن شخصية معينة ، و هذه البيانات مسجلة إلكترونيا بكثافة بالغة و بصورة مرمزة غالبا، على دعائم أو وسائط للتخزين، ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها و إن كانت قابلة للقراءة من قبل الآلة نفسها ، و لا يترك التعديل أو التلاعب فيها أي اثر مما يقطع أي صلة بين المجرم و جريمته. [46] ص344

إن الطبيعة غير المرئية للأدلة المتحصلة من الجرائم المعلوماتية، جعل البعض[52] ص111 يذهب إلى اعتبار هذه الأدلة نوع متميز من وسائل الإثبات لها من الخصائص و المواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأخرى(الأدلة القانونية، الأدلة الفنية، الأدلة القولية و الأدلة المادية)، و قد اصطلح على هذا النوع من الأدلة، بالأدلة الرقمية و التي تعرف بأنها "الأدلة المأخوذة من أجهزة الكمبيوتر، و تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة، و هي مكونات رقمية لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم ، و ذلك من أجل الربط بين الجريمة و المجرم و المجني عليه و بشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ و تطبيق القانون " [53] ص88

إن غياب الأدلة المرئية في الجرائم المعلوماتية و ظهور أدلة غير مرئية أصبحت تعرف بالأدلة الرقمية ، ألقت بظلالها على جهات البحث و التحري في هذا النوع من الجرائم، حيث أصبح من الصعب على هذه الجهات التعامل مع هذا النوع الجديد من الأدلة و الكشف عنها، و من ثم إثبات الجريمة في حق مرتكبيها، خاصة و أن المجرم المعلوماتي مجرم لديه من الذكاء و الخبرة الفنية و المعرفة العالية، ما يمكنه من اقتراف جريمته دون أن يترك سبيلا للاهتداء إليه، فهو يخطط جيدا بحيث لا يترك وراءه أي دليل، و إن ترك وراءه دليل فهو دليل خفي غير مرئي يصعب على جهات البحث و التحري، وبمعرفتها المتواضعة في مجال التقنية المعلوماتية اكتشافه.

و من بين الأمثلة الدالة على خفاء الدليل في الجرائم المعلوماتية، ما قام به محاسب في شركة لشحن الفاكهة والخضروات، فإثر قيامه بعملية التدقيق و المراجعة لهذه الشركة ، لاحظ أن عمليات التدقيق و المراجعة في هذه الشركة غير دقيقة . فقام بالتلاعب في بيانات الحاسوب و أدخل 18 شركة وهمية، جعل لها في حسابات شركة الشحن التي يعمل بها ، مستحقات مالية عن خدمات تؤديها لها، على أن يقوم هو بالاستيلاء على هذه المستحقات، وقد حرص على ألا يجاوز اختلاسه لهذه المستحقات النسب المعقولة التي يمكن أن تثير الشكوك. وبهذه الطريقة تمكن في أول سنة من اختلاس ربع مليون دولار دون الإخلال بنتائج حسابات الشركة التي يعمل بها، و على مدى خمس سنوات وبهذه الطريقة بلغت قيمة ما اختلسه أكثر من مليون دولار، ولم يكتشف تلاعبه سوى احد البنوك الذيشك في الحسابات الخاصة بإحدى الشركات الوهمية التي أسسها، و ذلك لضخامة الشيكات التي تسدد عن عمال هذه الشركات الوهمية، لمنظمات العمل. [47] ص109،110

2.2.3.1. سهولة محو الدليل في الجرائم المعلوماتية

إن من الأسباب الأساسية التي تقف عائقا وراء صعوبة إثبات الجريمة ، هي قدرة الجاني على تدمير الأدلة التي من الممكن أن تتخلف عن مثل هذه الجرائم. و القدرة على تدمير الأدلة و إن كان يملكها الجاني في أغلب الجرائم متى سمحت له الفرصة، و كان له الوقت الكافي لذلك ، إلا أن ما يميز الجرائم المعلوماتية هي قدرة الجاني على تدمير الأدلة بوقت قياسي قد لا يستغرق أكثر من دقائق وربما بعض من أجزاء الدقيقة، بحيث لا تتجاوز تلك الفترة عدد من الثواني [22] ص212 . فالجرائم المعلوماتية لا تحتاج لارتكابها سوى لبعض من اللمسات على لوحة مفاتيح الحاسوب الآلي، وبلمسات مماثلة يستطيع الجاني محو آثار جريمته، فبمجرد أن يشعر الجاني أن أمره سينكشف حتى يبادر إلى إلغاء كل ما قام به، مما يجعل من أمر طمس الدليل ومحوه كليا ، قبل اكتشافه أمر في غاية السهولة .

وتجدر الإشارة إلى أنه ومع مرور الوقت اكتسب الجناة خبرة واسعة في التلاعب بالبيانات وإتلافها في غضون ثوان محدودة قبل أن تتمكن الأجهزة المختصة من كشفهم أو التعرف عليهم، ويتأتى ذلك عادة بالاستعانة ببرامج معينة لها خاصية إتلاف أو تدمير البيانات بصورة تلقائية بعد مضي فترة من الزمن بحسب رغبة مصمم البرنامج وفي الوقت الذي يشاء[54] ص02، و من بين هذه البرامج برامج القنابل المنطقية أو الزمنية والتي سبق و أن أشرنا إليها. هذا و يسعى العديد من الجناة من ذوي الخبرة في مجال التقنية المعلوماتية إلى

ابتكار برامج أكثر تطورا بحيث يكمن عملها، بأنه بمجرد محاولة شخص غير مصرح به الولوج إلى النظام المعلوماتي أو استخدام الحاسوب المزود بهذا البرنامج، فإن هذا الأخير يصدر أمرا بإتلاف جميع البيانات المخزنة به و تدميرها بصورة تلقائية.

كما يلجأ الجناة إلى وسيلة أخرى من أجل محو آثار جرائمهم، وهي ليست بتقنية جديدة، وإنما وسيلة يمكن اعتبارها بالتقليدية مقارنة بما وصلت إليه تقنيات تدمير البيانات، تتمثل هذه الأخيرة في الإغلاق الفجائي لجهاز الحاسوب الآلي بصورة غير آمنة مما يؤدي إلى تدمير البيانات والبرامج و المعلومات التي لم يتم تخزينها بالذاكرة ، و لهذا ينصح البعض [53] ص115 بعدم غلق جهاز الحاسوب الآلي فورا، و ذلك لمنع مسح الأدلة، و يرون أن قطع التيار الكهربائي المفاجئ عن جهاز الحاسوب يسبب العديد من المخاطر تتمثل في محو المعلومات التي لم يتم تخزينها من جراء غلقه، بمعنى فقدان كافة العمليات التي كان يتم تشغيلها.

ومن الأمثلة العديدة التي تؤكد سهولة محو الدليل، ما شهدته ألمانيا، حيث أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليه، و ذلك من خلال محو هذه البيانات بالكامل بواسطة مجال كهربائي في حالة اختراقه من قبل الغير[28] ص56. كما حدث في النمسا أن قام أحد مهربي الأسلحة بعمل تعديلات على أوامر تشغيل حاسوبه الصغير الذي يدون فيه عناوين العملاء والمتعاملين معه، بحيث يمكن من خلال لوحة المفاتيح عند القيام بعملية النسخ أو الطبع تدمير كافة البيانات ومحوها و ذلك حتى لا تلاحقه الأجهزة الأمنية المتخصصة، ولكن حدس هذه الأجهزة كان أقوى من تصوره، حيث شعرت أن شيئا ما في جهاز الحاسوب الشخصي المملوك للمهرب الذي تم ضبطه، غير طبيعي، فقامت بنسخ الأقراص الممغنطة عن طريق أنظمة حواسبها وليس بحاسوبه الشخصي، وبالتالي لم تدمر البيانات والمعلومات المخزونة كما كان يهدف الجاني. [55] ص345، 346

وعليه يمكن القول، أن سهولة محو الدليل في الجرائم المعلوماتية يؤدي في الكثير من الأحيان إلى عرقلة أجهزة الضبط والتحقيق، وعدم تمكينها من الوصول إلى الأدلة وضبطها، وما يزيد الأمر تعقيدا، أنه في العديد من الحالات يكون مرتكب الجريمة المعلوماتية موظفا في الشركة أو المؤسسة التي تعرضت للاعتداء، فيسهل عليه في هذه الحالة محو آثار جريمته حتى

قبل الوصول إليه، وحتى أن هناك البعض منهم من يتملص من جريمته بإرجاع ذلك إلى خطأ في البرامج أو الأجهزة أو في أنظمة تشغيل أو تصميم نظام المعالجة الآلية للمعطيات.

3.2.3.1. إعاقة الوصول إلى الدليل في الجرائم المعلوماتية

عادة ما تلجأ الجهات ذات الأنظمة المعلوماتية إلى إحاطة البيانات المخزنة الإلكترونية والمنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للإطلاع عليها أو نسخها من خلال تشفيرها أو ترميزها، وهي ذات التقنيات التي قد يلجأ إليها الجناة من أجل إعاقة الوصول إلى البيانات التي تثبت إدانتهم، فهي حرب بين المجني عليهم الذين يحاولون بكل ما لديهم من وسائل، حماية أنظمتهم المعلوماتية من أي تعدي أو خرق، و بين الجناة الذين يجتهدون لشل فعالية هذه الوسائل دون إمكانية الوصول إليهم.

فالجناة في الجرائم المعلوماتية، غالبا ما يحيطون أعمالهم الإجرامية بجدران من الحماية، تجعل من الصعب على أجهزة العدالة الجنائية اكتشافهم و الوصول إلى أي أدلة تدينهم، فيستخدمون في سبيل ذلك كلمات مرور قوية تكون في غالب الأحيان طويلة تجمع بين الأحرف الأبجدية و الأرقام و الرموز ، مما يجعل من الصعب جدا تجاوزها.

و قد يلجأ البعض منهم إلى طمس هوية البيانات التي يستخدمونها في ارتكاب جرائمهم من خلال أساليب أخرى كالتشفير و الترميز . و تجدر الإشارة هنا، إلى أن التشفير يختلف عن الترميز، حيث يقصد بالتشفير تحويل بيانات أو إرسالها إلى جهة محددة عبر وسط ناقل، بحيث لا يمكن لأي جهة غير المرسل إليها تفسير هذه البيانات المبهمة واستخلاص البيانات أو المعلومات المفهومة منها. أما الترميز فيعني عملية تحويل المعلومات من هيئة معينة إلى هيئة أخرى وفق نظام محدد لا يمكن فهمها إلا من خلال نظام يفك هذا الترميز، وتحويله إلى أشكال وبيانات ومعلومات تظهر على الشاشة و يفهمها القارئ ، فبرنامج (Word) هو برنامج مرمز رقميا، لذلك فهو يحتاج إلى برنامج على نفس النظام يقوم بفك ترميزه و يحوله إلى رموز مفهومة تظهر على الشاشة . [27] ص43

يرى البعض[46] ص347 أن استخدام هذه الأساليب يعد إحدى العقبات الكبرى التي تعيق رقابة البيانات المخزنة أو المنقولة عبر الحدود الدولية، والتي تقلل من قدرة جهات التحري والتحقيق والملاحقة على الإطلاع عليها، الأمر الذي يجعل حماية حرمة البيانات الشخصية

المخزنة في مراكز الحواسب والشبكات و المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة.

إن ازدياد انتشار هذه الأساليب في الدول المتقدمة وما ينجم عنها من مخاطر، أدى بالبعض منها إلى استحداث تشريعات، تم بموجبها تجريم اللجوء إلى هذه التقنيات بدون ترخيص من الأجهزة المتخصصة . ومن بين هذه الدول هولندا، حيث سنت تشريعا يقضي بوضع ضوابط لعمليات التشفير، كضرورة الحصول على ترخيص من الجهات المعنية، إلى جانب إيداع مفاتيح التشفير لدى هذه الجهات . و كذلك فعلت فرنسا الشيء ذاته، و أصبح من شأن الإقدام على هذا التشفير بدون ترخيص أن يصبح الفعل جريمة يعاقب عليها القانون، ويعاقب أيضا الشخص الذي أعد برنامج التشفير بدون ترخيص[54]ص 31، كما لجأت الحكومة الأمريكية إلى التحكم في عمليات تصدير أجهزة التشفير و أنظمتها، باعتبارها تعد من أسرار و متطلبات الأمن القومي، ولا تسمح القوانين الأمريكية باستخدام التشفير، إلا إذا كانت المعلومات المراد تشفيرها مالية و بين بنوك معروفة، أو كانت المعلومات معروفة المحتوى أو إذا توافرت أدلة تفيد في أن التشفير لا يمكن استخدامه لأغراض أخرى.

فضلا عن استخدام الجناة لكلمات السر وأساليب التشفير والترميز من أجل إعاقة الوصول إلى دليل إدانتهم، فإنهم يلجؤون أيضا إلى إخفاء هوياتهم، و ذلك من خلال استخدام حواسب آلية، غير حواسبهم الشخصية كاستخدام حواسب زملائهم أو استخدام الحواسب الموجودة بالأماكن العامة، فعادة ما يلجأ هؤلاء إلى مقاهي الانترنت باعتبار أن هذه الأخيرة لا تقوم بالتحقق من هويات مرتاديها ولا تسجل أسماءهم، الأمر الذي يحول دون تعقبهم أو كشف أمرهم ،فتظل أنشطتهم مجهولة وبمنأى عن علم السلطات المعنية بمكافحة الجرائم المعلوماتية.

3.3.1. الصعوبات المتعلقة بالعامل البشري في الجرائم المعلوماتية

من صعوبات إثبات الجرائم المعلوماتية ما تعلق منها بالعامل البشري ،فبعد أن تعودت البشرية على نوع معين من الجرائم كالقتل والسرقة وغيرها من الجرائم التقليدية، ظهرت الجرائم المعلوماتية وغيرت الأوضاع .فالطبيعة الخاصة لهذه الجرائم المستحدثة، أدت إلى وجود صعوبة في التعامل معها ،سواء من قبل جهات التحري والتحقيق، التي بنقص خبرتها وافتقارها للتأهيل الكافي في الميدان التقني، أصبحت غير قادرة على إثبات هذا النوع من الجرائم، الذي يتطلب معرفة ومهارة تقنية كبيرة في مجال المعلوماتية، وسواء من قبل ضحايا هذه الجرائم والتي اختلفت مواقفهم، فبعد أن كان الضحية ايجابيا يبادر بإبلاغ السلطات بأي جريمة وقعت

ضده، أصبح هو من يتستر على ما يصيبه من اعتداء يشكل جريمة من الجرائم المعلوماتية مما يزيد من صعوبة اكتشافها، بالإضافة إلى كل هذا فإن غياب التنسيق والتعاون بين الدول في مجال مكافحة الجرائم المعلوماتية يزيد من صعوبة إثباتها و ملاحقة مرتكبيها . وهذا ما سنتعرض له تباعا في هذا المطلب حيث سنقسمه إلى ثلاث فروع، نتحدث في الفرع الأول عن نقص خبرة جهات التحري والتحقيق في الجرائم المعلوماتية ، و نتطرق في الفرع الثاني لإحجام المجني عليهم عن الإبلاغ و المساعدة في الجرائم المعلوماتية ونتناول في الفرع الأخير غياب التنسيق الدولي في مجال الجرائم المعلوماتية.

1.3.3.1. نقص خبرة جهات التحري والتحقيق في الجرائم المعلوماتية

إذا كانت الجريمة بشكل عام يمكن وصفها بأنها حرب بين الجاني الذي يحاول طمس معالمها ومنع ما يتخلف عنها من آثار قد تكشف عنه، فيأخذ من الاحتياطات ما يلزم حتى لا يترك أي دليل يوصل إليه، وبين جهات التحري والتحقيق التي تسعى بكل ما هو متاح لها قانونا الكشف عن الجرائم وضبط مرتكبيها وتقديم الأدلة عنها. فإن هذه الحرب في ظل الجرائم المعلوماتية هي حرب أشد استعارا بين الجاني وجهات التحري والتحقيق ،خاصة أن ما يملكه مرتكبي الجرائم المعلوماتية من الخبرة والمعرفة في مجال التقنية المعلوماتية يفوق بكثير ما تملكه جهات التحري والتحقيق في هذا المجال، فالجرائم المعلوماتية يرتكبها المتخصصون في الميدان مستغلين جهل محيطهم بما وصلوا إليه من تحكم في الموضوع.

إن هذا الأمر يضعنا أمام معادلة غير متكافئة، يمثل الطرف الأول فيها جهات تحر وتحقيق ناقصة خبرة في مجال التقنية المعلوماتية، و يمثل الطرف الثاني فيها مجرمون غير عاديون لهم من المهارات والقدرات في هذا المجال ما يجعل من الصعب الاستدلال عليهم، لدرجة أنهم يطلقون على أنفسهم اسم "النخبة" بدعوى أنهم الأكثر معرفة بأسرار الحاسوب الآلي ولغاته المتميزة، و هم يطلقون على رجال الشرطة والنيابة والقضاء صفة الضعفاء أو القاصرين. [47] ص168

إن نقص خبرة سلطات البحث و التحري في الجرائم المعلوماتية يؤدي في الكثير من الأحيان إلى إفلات مرتكبي هذه الجرائم من العقاب لعدم قدرة هذه الأخيرة على إثبات إدانتهم، كما يرى البعض [49] ص351 أن المستوى الثقافي المتدني لرجال الأمن و المحققين العاملين الآن في مجال مكافحة الجرائم المعلوماتية، هو خير معين لمرتكبي هذه الجرائم، فقد أثبتت الوقائع أن هناك جرائم متعلقة بالحاسوب الآلي ارتكبت على مرأى و مسمع من رجال

الأمن، بل قام بعض رجال الأمن بتقديم المساعدة لمرتكبي هذه الجرائم دون قصد وعن جهل أو على سبيل واجبات المهنة التي يلزمهم بها القانون .

ليس هذا فحسب، فهناك معلومات تكاد تكون من الثوابت في عقول العديد من الناس الذين لديهم معرفة ودراية عالية بماهية عمل الحاسوب والانترنت، تتمثل هذه المعلومات في أنه مازال القانون ورجاله غير قادرين بعد على معرفة الجرائم المعلوماتية معرفة تامة، وإن تمت معرفتهم لها، فإنهم غير قادرين بعد على متابعة وملاحقة المجرم ومن ثم معاقبته وفق ما ارتكب من جريمة.[17] ص262

إن الطبيعة الخاصة للجرائم المعلوماتية من حيث اعتمادها بشكل أساسي على تقنية المعلومات و وسائل التكنولوجيا، ومن حيث الأساليب المتطورة التي ترتكب بها، جعلت من الصعب على جهات التحري والتحقيق - خاصة الذين انحصرت معلوماتهم في جرائم قانون العقوبات التقليدية - التعامل مع هذه الجرائم بمهارة و احترافية كتعاملها مع غيرها من الجرائم التقليدية، و يمكن إرجاع ذلك لسببين:

◆عدم القدرة على التعامل مع الأدلة المعلوماتية

إن ضخامة كم البيانات والمعلومات المخزنة على الحاسوب الآلي، والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل الجريمة، قد تشكل عقبة من العقبات التي تعيق عمل جهات التحري والتحقيق، فما يتميز به الحاسوب الآلي من قدرة هائلة في تخزين البيانات بما يوازي الآلاف من الصفحات الورقية، يجعل من مهمة فرز البيانات التي يحتاجها التحقيق من تلك التي لا يحتاجها مهمة في غاية الصعوبة. وقد تستغرق من الوقت ما قد يؤدي إلى ضياع الدليل، هذا من جهة، ومن جهة أخرى فإن الأمر قد يكون جد مرهق لهذه الجهات، خاصة وأنها لم تتعود على التعامل مع الأشياء ذات الطبيعة المعنوية، مما يؤدي بها في الكثير من الأحيان إلى الضجر والملل، وبالتالي قد تصرف النظر عن مواصلة البحث لاقتناعها بأنه لا جدوى من ذلك.

◆ عدم القدرة على فهم الأدلة المعلوماتية

فقد يحدث أن تجد هذه الجهات نفسها أمام لغة لا تفهمها، لاسيما وأن للعاملين في مجال الحاسوب مصطلحات علمية خاصة، أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات

بالحروف اللاتينية الأولى لتكون لغة غريبة تعرف بلغة المختصرات وهي لغة جديدة ومتطورة. [34] ص69

كما لا يقف الأمر عند عدم قدرة سلطات البحث و التحري على فهم اللغة المستخدمة فحسب، وإنما يمتد أيضا إلى صعوبة فهمها للدليل ذاته . مثال ذلك أن إثبات التدليس والذي يقع على نظام المعالجة الآلية للمعطيات، يتطلب تمكين مأمور الضبط القضائي أو سلطات 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 يستعصي الأمر فهما على مأمور الضبط القضائي لعدم قدرته على فك رموز الكثير من المسائل الفنية الدقيقة التي من خلال ثناياها قد يتولد الدليل، أيضا فإن فهم الدليل الموصل إلى إثبات الجرائم المعلوماتية قد يزداد صعوبة في تلك الحالات التي يتصل فيها الحاسوب الآلي بشبكة الاتصالات العالمية، ففي مثل هذه الحالات فإن فهم الدليل قد يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجوده واختيار أفضل السبل لضبطه[56]ص08، وهذا ما لا يتوافر لدى جهات التحري والتحقيق التي مازالت تفتقر إلى التأهيل العلمي الكافي في الميدان التقني. ليس هذا فحسب بل إن افتقارهم لهذا التأهيل قد يؤدي في بعض الحالات إلى تدمير الأدلة، فقد يتسبب المحقق دون قصد أو بطريق الخطأ في إتلاف الدليل الالكتروني أو تدميره، كما في حالة محو البيانات الموجودة على الاسطوانة الصلبة، كما قد يتجاهل الدليل الالكتروني تماما ظنا منه انه غير مهم، أو لا يقوم بمصادرة جهاز الحاسوب المستخدم في ارتكاب الجريمة أو ملحقاته مثل الطابعة أو الماسح الضوئي.[18] ص46

ولعل خير دليل على ما تعانيه جهات التحري والتحقيق من صعوبات في مجال إثبات الجرائم المعلوماتية نتيجة نقص خبراتهم في مجال المعلوماتية ، ما حدث في ألمانيا عام 1971 حين اكتشفت شركة طلبيات بريدية سرقة أشرطة ممغنطة تحتوي على (300.000) عنوان لعملائها، فاستصدرت من المحكمة أمرا بوقف الأعمال، وذلك لاستعادة كل هذه العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من الذين ارتكبوا السرقة . وتنفيذا لذلك سمحت الشركة المنافسة لمساعد مأمور التنفيذ أن يدخل مقر الحاسوب الآلي الخاص بها وذلك للحصول على هذه العناوين، فوجد نفسه وسط كم هائل من الأشرطة والأقراص الممغنطة التي لا يدري عنها شيئا وليست لديه القدرة لفحص محتوياتها، فغادر مقر الشركة دون أية معلومات.[55] ص81

وعليه يمكن القول أن ما تملكه جهات التحري والتحقيق من علم ومعرفة بأصول البحث والتحقيق في الجرائم ، لا يكفي لوحده في كشف خبايا الجرائم المعلوماتية ، وإنما لابد من اكتسابها مهارات التعامل مع الحاسوب الآلي، وكذا التقنيات المرتبطة به، نظرا لارتباط هذه الجرائم بشكل أساسي بالتقنية العالية، فالتعامل باحترافية مع هذا النوع من الجرائم يقتضي من جهات التحري و التحقيق أن تكون ملمة بالجوانب التقنية للحاسوب الآلي بقدر إلمامها بالجوانب القانونية للإجراءات الواجب عليها إتباعها، و سنرى هذا في الفصل الثاني من هذه المذكرة.

2.3.3.1. إحجام المجني عليهم عن الإبلاغ و المساعدة في الجرائم المعلوماتية

إن أية جريمة تقع، من المفروض أن تكون للسلطات المعنية علم بها حتى يتسنى لها القيام بالتحقيقات اللازمة بشأنها، وذلك من خلال ما يصلها من شكاوى وبلاغات من الجهات المتضررة، وهذا هو الغالب في الجرائم التقليدية، إلا أن الملاحظ في مجال الجرائم المعلوماتية أنه نادرا ما يصل إلى علم السلطات ارتكاب جريمة من هذه الجرائم ، و هذا راجع بشكل أساسي لإحجام المجني عليهم عن الإبلاغ عنها . وفضلا عن هذا فإن المجني عليهم في الجرائم المعلوماتية لا يمتنعون عن الإبلاغ عنها فحسب،و إنما يمتد امتناعهم إلى تقديم المساعدة للسلطات المختصة في حالة اكتشافها لهذه الجرائم.

1.2.3.3.1 إحجام المجني عليهم عن إبلاغ السلطات المختصة

إن دور المجني عليهم في الجرائم المعلوماتية غالبا ما يكون سلبيا إلى حد كبير، إذ يفضل العديد منهم إبقاء ما لحقهم من ضرر سرا، و يمكن إرجاع ذلك للأسباب التالية :

- أن المجني عليه، و في الكثير من الأحيان لا يكتشف وقوعه ضحية جريمة من الجرائم المعلوماتية إلا بعد فترة طويلة نسبيا من ارتكابها، وقد تكون هذه الجريمة محدودة الأثر فيتغاضى عنها . ليس هذا فحسب بل هناك من المجني عليهم من لا يعلم أصلا أن ما يقع على نظامه المعلوماتي من اعتداءات و هجمات يشكل جريمة معلوماتية معاقب عليها قانونا ، وهذا الفرض نجده خاصة في بلداننا العربية التي لازالت فيها هذه الجرائم في بداياتها الأولى.

- أن المجني عليه قد يتردد عن الإبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكابها قد يؤدي إلى تكرار وقوعها بناء على تقليدها من قبل الآخرين . كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه الذي

تعمل به أنظمته المعلوماتية مما يسهل عملية اختراقه مرة أخرى[57]ص166، فضلا عن كشفه لهشاشة البرنامج المستخدم من المجني عليه، إذا كان شركة أو مؤسسة و بالتالي فقدان سمعتها و انصراف العملاء عنها.

◆أن الجهات المتضررة أو المستهدفة بالجرائم المعلوماتية غالبا ما تكون مؤسسات مالية أو شركات تجارية، تخشى من التشهير و الدعاية المضرة و فقدان ثقة العملاء، فقد يؤدي فقدان ثقة عملائها إلى خسائر اقتصادية أكثر من التي تسببت فيها الجريمة ذاتها[11] ص235 ، كما قد تخشى في حالة الإبلاغ عن هذه الجرائم أن تؤدي أعمال التحقيق التي تقوم بها الشرطة إلى احتجاز حواسبها أو تعطيل شبكاتها لفترة طويلة عن العمل، مما قد يتسبب في زيادة خسائرها المالية .

و لهذا نجد هذه الشركات و المؤسسات المالية تحرص على عدم اكتشاف ما تعرضت له أنظمتها من اعتداءات حتى من قبل موظفيها، بل قد يصل بها الأمر إلى الترضية الودية للجناة، كما حدث في احد البنوك الانجليزية، حيث قام احد الأشخاص بنقل 8 مليون جنيه إسترليني من إحدى أرصدة البنك إلى رقم حساب في سويسرا، و تم القبض عليه أثناء محاولته سحب المبلغ المذكور ، فبدل أن يقوم البنك بتحريك دعوى جنائية ضده، قام بدفع مبلغ 1 مليون جنيه إسترليني له ، بشرط عدم إعلام الآخرين بجريمته و إخطار البنك بالآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحساب البنك الرئيسي.[46] ص357

إن هذه الحادثة تشكل جريمة خطيرة يكون قد ارتكبها البنك، ففي النظام البريطاني يعاقب المجني عليهم الذين ينشرون إعلانا لمن يرد المسروقات بإعطائه مكافأة مالية، لأن هذا يعد تعاونا مع المجني عليه، ليس هذا فحسب، فإن ردود أفعال مثل هذه ستساعد بشكل كبير على انتشار مثل هذه الجرائم، و ستشكل مصدر إغراء كبير لمرتكبيها، مستغلين في ذلك تخوف مثل هذه المؤسسات و الشركات من التشهير.

1.2.3.3.1. إحجام المجني عليهم عن مساعدة السلطات المختصة

إن المجني عليه في الجريمة المعلوماتية لا يمتنع عن الإبلاغ فحسب ، و إنما يمتنع حتى عن تقديم الأدلة أو تقديم أي مساعدة لسلطات التحقيق، إن وقعت الجريمة و علمت بها هذه السلطات . الأمر الذي يشكل صعوبة أمامها، ليس في اكتشافها فحسب بل و في إثباتها أيضا، و الواقع العملي يكشف عن الكثير من حالات عدم تعاون المجني عليه في مثل هذه

الجرائم[22] ص218، فقد يخشى اكتشاف السلطات مثلا لمعلومات اسمية لم يقم بالإخطار عنها قبل جمعها ،أو أي بيانات قد تنقله من مركز الضحية إلى مركز المتهم .

وفضلا عن هذا، هناك من يرى [42]ص 56،57انه في بعض الحالات يكون للضحية دورا غير مباشر في مساعدة الجناة ، وذلك بسبب وجوده في ظروف تجعل من قابليته للتعرض للجريمة مرتفع و بشكل كبير، و يرجع ذلك بشكل أساسي للقصور الذي يعتري أنظمته المعلوماتية مما يسهل للجناة ارتكاب جرائمهم ، فالملاحظ أن معظم المؤسسات لا تعتمد مسؤولا أمنيا للحواسب الشخصية خاصة ، مما يوقع هذه المؤسسات في مشاكل أمنية معقدة، بالإضافة إلى عدم إدراكها لأهمية منظومة المعلومات و طريقة حماية أجهزة التخزين المتداولة بين جميع أفراد المؤسسة.[58] ص67

و عليه يمكن القول ، أنه و بعدم تعاون ضحايا الجرائم المعلوماتية مع السلطات المعنية ، فإن المجهودات المبذولة من قبل هذه الأخيرة لن تكون فعالة بالقدر اللازم . و من اجل تفعيل عملية الإبلاغ عن الجرائم المعلوماتية، و من ثم المساهمة بطريقة ايجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها ، طالب البعض في الولايات المتحدة الأمريكية أن تفرض النصوص المتعلقة بجرائم الحاسوب الآلي إلتزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال، مع تقرير جزاء على الإخلال بهذا الالتزام ، و عرض هذا الاقتراح على لجنة خبراء مجلس أوروبا، إلا انه تم رفضه باعتبار انه من غير المقبول تحويل المجني عليه إلى جاني.[28] ص55

أما على المستوى العربي فهناك من التشريعات من تضمنت قوانينها نصوص تعاقب على الامتناع عن الإبلاغ عن بعض الجرائم ، إلا انه لا يوجد نص يجعل من الإبلاغ عن الجرائم المعلوماتية التزاما يرتب الإخلال به جزاء لصاحبه .

و من جانبنا نرى انه من غير المعقول معاقبة شخص لمجرد التزامه الصمت ، لأن ذلك يشكل تعديا على الحريات الشخصية للفرد، فإذا كان التزام الصمت حق من حقوق الفرد و هو متهم، فكيف لا يكون له هذا الحق و هو ضحية، فبدل اللجوء إلى معاقبة الضحية لامتناعه عن الإبلاغ عما يتعرض له من اعتداءات تشكل جريمة من الجرائم المعلوماتية ، لا بد من اعتماد تدابير و إيجاد حلول أكثر فعالية لتشجيع الأفراد على التبليغ على هذا النوع من الجرائم، مثلما ذهبت إليه بعض الدول كهولندا و الولايات المتحدة الأمريكية.

و مهما يكن، ومن أجل مكافحة الإجرام المعلوماتي و من أجل اطمئنان البشر إلى التعامل بالتقنيات المعلوماتية باعتبارها وسيلة العصر، يحتم الأمر أن يتعاون الجميع على ملاحقة كل من تسول له نفسه السطو على البرامج و استغلال معارفه للكسب غير المشروع و لتعطيل التعامل.

3.3.3.1 .غياب التنسيق الدولي في مجال الجرائم المعلوماتية

لما كانت الجرائم المعلوماتية في غالب الأحيان، جرائم عابرة للحدود، فإن التعاون الدولي هو من أهم سبل مكافحة هذه الجرائم و ملاحقة مرتكبيها، فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم و يطمئن مرتكبوها من عدم إمكانية ملاحقتهم، إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها، ما ارتكبوه من جرائم.[59] ص 194

فلا شك أن اختلاف التشريعات فيما بينها فيما يتعلق بشروط قبول الأدلة و تنفيذ بعض الإجراءات كالتفتيش و الضبط عبر الحدود يشكل عائقا أمام جهات التحري و التحقيق التي تسعى إلى إثبات ما يرتكب من جرائم معلوماتية، و لذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة المعلوماتية بواسطة الحاسوب الآلي و الانترنت، أسوة بجهات البحث الجنائي الوطنية و الدولية- الانتربول- لإثبات الجريمة عند وقوعها و تحديد أدلتها و فاعليها ، و هو ما يعني كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات، وتبادل الخبرات و المعلومات حول هذا النوع من الجرائم و مرتكبيها و سبل مكافحتها.[47] ص187

و رغم الإقرار بضرورة التعاون الدولي في مجال مكافحة الجرائم المعلوماتية ، إلا أن وجود بعض العقبات تقف بمثابة حجر عثرة في وجه هذا التعاون ، ومن بينها :

- عدم وجود مفهوم مشترك للجريمة المعلوماتية [18] ص48 و قد لاحظنا ذلك من خلال تطرقنا لتعريف الجريمة المعلوماتية - فيظهر من خلال ما جاء من تعريفات للجرائم المعلوماتية وجود اختلاف بين في تناول هذا النوع من الإجرام ، و لهذا لا نجد نموذج واحد متفق عليه يمثل النشاط الإجرامي لمثل هذه الجرائم ، فما قد تعتبره دولة ما جريمة من جرائم المعلوماتية، تعتبره دولة أخرى فعلا مباحا، فالتجريم أمر نسبي يختلف من دولة إلى أخرى، و هذا الأمر يدعو إلى ضرورة المسارعة من أجل خلق انسجام بين قوانين الدول المختلفة،

و ذلك من خلال الاتفاق على ما يمكن اعتباره جريمة من جرائم المعلوماتية، حتى لا يترك للجناة منفذ للإفلات من العقاب.

◆ عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة المعلوماتية بين الدول المختلفة، خاصة ما تعلق منها بأعمال الاستدلال و التحقيق، لاسيما و أن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين، هو أمر غاية في الصعوبة.

◆ عدم وجود معاهدات للتسليم أو للتعاون الثنائي أو الجماعي بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة بالجرائم المعلوماتية و سرعة التحريات فيها.[46] ص361

إن هذه العقبات تدعو إلى ضرورة تفعيل التعاون الدولي، وذلك لا يتأتى إلا من خلال التركيز على الموضوعات التالية، والعمل على تعظيم وجودها والأخذ بها وهي كالأتي : [59] ص197

◆ الانضمام إلى المعاهدات الدولية التي تعمل على زيادة التعاون والتنسيق بين الجهود التي تبذلها الدول في مكافحة الجرائم المعلوماتية. وفي هذا الإطار تجدر الإشارة إلى أن هناك العديد من الدول من بدأت تعمل على هذا الأمر،من بينها الجزائر و الولايات المتحدة الأمريكية، حيث تم عقد اتفاقية للتعاون في المجال القضائي بين البلدين و ذلك بتاريخ 07 أفريل 2010 من اجل إرساء شراكة أكثر فعالية في مجال مكافحة الجريمة المعلوماتية، ومن نتائج هذه الشراكة انه تم حل قضيتين في مجال الجريمة المعلوماتية من بينها قضية المجرم المعلوماتي الذي قام بتحويل كم هائل من البيانات والتي تتعلق بعدة شركات عالمية ومن خلالها استطاع ابتزاز هذه الشركات للحصول على أموال ، هذا المجرم ظن انه في مأمن في الجزائر، إلا انه ونتيجة التنسيق بين البلدان وتبادل المعلومات تم تحديده وجمع الأدلة ضده وملاحقته قضائيا.

◆ إدخال تلك المعاهدات الدولية حيز التنفيذ الفعلي أي تنفيذ ما تنص عليه تلك الاتفاقية من إجراءات دون أي إبطاء.

◆ العمل على وجود اكبر قدر ممكن من التناسق والتطابق فيما بين قوانين الدول المختلفة و المتعلقة بمكافحة الجرائم المعلوماتية، فلا يكون الفعل الذي تم ارتكابه جريمة في بلد

ما و غير معاقب عليه في قانون بلد أخر، فمن هنا يجد المجرمون الملاذ الآمن الذي يلجؤون إليه دون أي اعتبار لما ارتكبوه من جرائم.

- تعاون جميع الدول في تسليم المطلوبين أمنيا إلى الدول التي تطالب بهم لارتكابهم جرائم معلوماتية.

و عليه يمكن القول أنه لابد من المسارعة إلى إيجاد تنسيق دولي بين مختلف الدول في مجال الجرائم المعلوماتية و الذي سيحل الكثير من المشاكل، خاصة ما تعلق منه بإجراءات البحث و التحري عن الجرائم المعلوماتية التي ترتكب خارج الحدود الإقليمية للدولة.

الفصل 2
مراحل إثبات الجرائم المعلوماتية

إن الجريمة كفعل ضار في المجتمع، يمر إثباتها بمراحل تهدف إلى التحقق من وقوع الفعل و إسناده إلى فاعله، و قد درجت مختلف التشريعات على تقسيم مراحل إثبات الجريمة إلى ثلاث مراحل، مرحلة تمهيدية تهدف إلى البحث و التحري عن الجرائم و هي ما تعرف بمرحلة البحث و التحري، مرحلة تحضيرية يتم خلالها جمع الأدلة و تمحيصها للقول بكفايتها للاتهام أو عدم كفايتها لذلك، وتسمى بمرحلة التحقيق، وتنتهي مراحل الإثبات بمرحلة نهائية وهي مرحلة الجزم بالأدلة القائمة للقول بثبوت الجرم من عدمه ومن ثم القضاء بالبراءة أو بالإدانة ، وتتمثل هذه المرحلة في مرحلة المحاكمة. وكل مرحلة من هذه المراحل تتميز عن سابقتها سواء من حيث الجهة القائمة عليها أو من حيث الإجراءات المتبعة خلالها.

والجريمة المعلوماتية كغيرها من الجرائم تمر في إثباتها بذات المراحل، غير أن الوصول بهذه المراحل إلى أهدافها أصبح في ظل الجرائم المعلوماتية يعتمد على مدى المزاوجة بين التقنية والقانون . ذلك أن الصعوبة التي تكتنف إثبات هذا النوع من الجرائم نظرا لحداثة أساليب ارتكابها وكذا سرعة تنفيذها وسهولة إخفاء ومحو آثارها و عدم إمكانية الوصول إليها وغير ذلك من الأمور التي سبق ونوهنا عنها ، أصبحت تقتضي لتجاوزها أن تجمع جهات التحري والتحقيق والمحاكمة القائمة على مراحل إثبات هذه الجرائم بين المعرفة التقنية والمعرفة القانونية، فتكون على إلمام بأنظمة الحواسب الآلية وكيفية عملها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموضها و سرعة التصرف بشأنها من حيث كشفها واتخاذ الاحتياطات اللازمة للمحافظة على البيانات والأجهزة المستخدمة في ارتكابها بشكل لا يؤدي إلى إتلافها، وصولا إلى المناقشة العلمية للأدلة الناجمة عنها.

إن هذا الأمر أصبح يتطلب برامج متخصصة في التدريب لاستيعاب هذه المهارات في أعمال الاستدلال والتحقيق والمحاكمة، وكذا الاستعانة بالوسائل الفنية اللازمة لإثبات الجرائم المعلوماتية، فضلا عن ضرورة تطوير أساليب البحث والتحقيق والمحاكمة التقليدية بما يتلاءم والطبيعة التقنية لهذه الجرائم وتعقيدها. و هذا ما سنحاول تفصيله في هذا الفصل ،وحتى نعطي كل مرحلة من مراحل الإثبات حقها، ارتأينا تقسيم هذا الفصل إلى ثلاثة مباحث نتناول في المبحث الأول مرحلة البحث و التحري عن الجرائم المعلوماتية، ثم نتناول في المبحث الثاني

مرحلة التحقيق في الجرائم المعلوماتية، لنصل في المبحث الأخير للحديث عن مرحلة المحاكمة في هذا النوع من الجرائم.

1.2.مرحلة البحث و التحري عن الجرائم المعلوماتية

تعتبر مرحلة لبحث و التحري بمثابة مرحلة تمهيدية تهدف إلى البحث والتحري عن الجرائم والكشف عن مرتكبيها، وتحتل هذه المرحلة أهمية خاصة من حيث أنها الأساس الذي تقوم عليه جميع الدعاوى العمومية، فهي مرحلة سابقة للإجراءات القضائية لا يمكن الاستغناء عنها، بالرغم من أنها مرحلة تبدو ثانوية خاصة بالنظر لطبيعتها شبه القضائية وسلطة التصرف في نتائجها – مقارنة بوظيفتي الاتهام والتحقيق- فهي ضرورية للمتابعة من حيث تهيئة القضية بالبحث والتحري فيها، ثم تقديمها للنيابة العامة للتصرف في القضية على ضوء نتائجها بإعمال سلطتها في الملاءمة بين تحريك الدعوى العمومية وبين الأمر بحفظها[60] ص186. يسهر على هذه المرحلة مجموعة من الأشخاص أضفى عليهم القانون صفة الضبطية القضائية، إلا أنه واعتبارا لما تتسم به الجرائم المعلوماتية من تعقيد، أصبحوا غير قادرين لوحدهم على مواجهة ما قد يرتكب منها، الأمر الذي استدعى استحداث أجهزة خاصة إلى جانبهم، و كذا إعداد برامج تدريبية، و ذلك لتطوير مهاراتهم و تزويدهم بالقدرات اللازمة للتصدي لهذا النوع من الجرائم التي أصبحت تقتضي تعديل العديد من المفاهيم التقليدية في جمع الاستدلالات و البحث عن الجرائم و مرتكبيها. و هذا ما سنحاول التطرق إليه من خلال هذا المبحث، والذي سنقسمه إلى ثلاثة مطالب ، نتناول في المطلب الأول الجهة المختصة بالبحث و التحري في الجرائم المعلوماتية ، ثم نتناول في المطلب الثاني المتطلبات الضرورية للبحث و التحري عن هذا النوع من الجرائم،و نتطرق في المطلب الثالث إلى إجراءات البحث و التحري عن الجرائم المعلوماتية.

1.1.2. الجهة المختصة بالبحث و التحري عن الجرائم المعلوماتية

تناط مهمة البحث و التحري عن الجرائم المقررة في قانون العقوبات و القوانين المكملة له و كذا الكشف عن مرتكبيها لجهاز الضبطية القضائية، حيث يلعب هذا الجهاز دورا كبيرا في البحث و التحري عن الجرائم و مرتكبيها، إلا أن هذا الدور اضمحل نوعا ما مع ظهور الجرائم المعلوماتية، حيث أصبحت هذه الجرائم تشكل عبئا كبيرا على هذا الجهاز، وذلك بالنظر إلى قلة خبرته في مجال المعلوماتية و تقنياتها، الأمر الذي أدى بالعديد من الدول إلى استحداث أجهزة خاصة تتولى مهمة البحث و التحري عن هذا النوع المستحدث من الجرائم. و هذا ما سنحاول التطرق إليه تباعا في هذا المطلب حيث نخصص الفرع الأول منه

للحديث عن الضبطية القضائية في الجرائم المعلوماتية، و نخصص الفرع الثاني للحديث عن الأجهزة الخاصة بمكافحة الجرائم المعلوماتية.

1.1.1.2. الضبطية القضائية في الجرائم المعلوماتية

يطلق على جهاز الضبط القضائي تعبير الضبطية القضائية و يطلق على من يباشرون اختصاصها تعبير ضباط الشرطة القضائية،و تعريف الضبطية القضائية مستمد من اختصاصها، فهي تشمل جميع الموظفين الذين خولهم القانون مباشرة إجراءات الاستدلال[61] ص381. تختلف وظيفة الضبط القضائي عن وظيفة الضبط الإداري، فوظيفة الضبط القضائي تكمن في التحري عن الجريمة والبحث عن مرتكبيها و جمع كافة العناصر أو الدلائل اللازمة للتحقيق في الدعوى الجنائية، في حين أن وظيفة الضبط الإداري تنصب على الوقاية من الجرائم و مكافحة وقوعها، و ذلك من خلال اتخاذ الاحتياطات اللازمة التي تحول دون وقوعها، و على ذلك فإن مهمة الضبط القضائي تبدأ أين تنتهي مهمة الضبط الإداري . و قد اهتمت جل التشريعات الوضعية بتحديد الأشخاص الذين تثبت لهم صفة الضبطية القضائية، فأوردتهم على سبيل الحصر في قوانينها الإجرائية، و يمكن إجمالهم في فئتين:

الفئة الأولى**:** هي الفئة التي تملك صلاحية مباشرة إجراءات التحري و البحث عن جميع أنواع الجرائم، و قد حدد المشرع الجزائري هذه الفئة في المادتين 15 و 19 من قانون الإجراءات الجزائية و تشمل ضباط الشرطة القضائية من رؤساء المجالس الشعبية البلدية، ضباط الدرك الوطني، ضباط الشرطة، محافظو الشرطة ذوو الرتب في الدرك الوطني و رجال الدرك الذين أمضوا في سلك الدرك ثلاث سنوات على الأقل و الذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة، و مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل، كما تشمل هذه الفئة أيضا على أعوان الضبط القضائي من موظفي مصالح الشرطة و ذوي الرتب في الدرك الوطني و رجال الدرك و مستخدمو مصالح الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية.

الفئة الثانية: هي الفئة التي لا يضفى عليها صفة الضبطية القضائية إلا بالنسبة للجرائم المتعلقة بوظائفهم، فتقتصر مهمتهم على البحث و التحري عما يرتكب من جرائم تدخل في إطار وظائفهم، و هذه الفئة حددها المشرع الجزائري في المادة 21 من قانون الإجراءات الجزائية، و هم رؤساء الأقسام و المهندسون و الأعوان الفنيون المختصون في الغابات و حماية الأراضي

و استصلاحها والتي تختص بالبحث و التحري و معاينة جنح و مخالفات قانون الغابات و تشريع الصيد و نظام السير و جميع الأنظمة التي عينوا فيها بصفة خاصة و إثباتها في محاضر ضمن الشروط المحددة في النصوص الخاصة، كما تقوم بتتبع الأشياء المنزوعة و ضبطها في الأماكن التي تنقل إليها ووضعها تحت الحراسة.

إن عمل ضابط الشرطة القضائية – باعتباره إجراء قانونيا يراد له أن ينتج أثارا قانونية- لا يكون صحيحا إلا إذا باشره ضابط شرطة مختص، و من ثمة كان الاختصاص شرطا لصحة الإجراء، و يعد ذلك تطبيقا للمبادئ القانونية العامة، بالإضافة إلى أنه تطبيق لمبدأ عام في الإجراءات الجنائية . و يطبق شرط الاختصاص في مجاليه النوعي و الإقليمي . فإذا كان ضابط الشرطة القضائية ذا اختصاص نوعي محدد تعين عليه أن يلتزم حدود اختصاصه النوعي، فلا يجوز له أن يتخذ إجراء في شأن جريمة لا يختص بها. أما إذا كان ضابط الشرطة القضائية ذا اختصاص نوعي عام، فإنه يتعين عليه أن يلتزم حدود اختصاصه الإقليمي[61] ص385. و يتحدد الاختصاص الإقليمي لضابط الشرطة القضائية وفقا للتشريع الجزائري بالدائرة الإقليمية التي يمارس فيها وظائفه العادية، و يجوز له في حالة الاستعجال تمديد اختصاصه إلى كامل دائرة اختصاص المجلس القضائي الملحق به ، كما يمكن أن يمتد اختصاصه في هذه الحالة إلى كافة الإقليم الوطني إذا طلب منهم ذوو الاختصاص من الجهات القضائية ذلك، و في غير هذه الأحوال أعطى القانون لضابط الشرطة القضائية الحق في تمديد اختصاصه المحلي إلى كامل التراب الوطني، وذلك إذا تعلق الأمر بجرائم حددها حصرا و هي جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف [62] ، و على ذلك يمكن القول أن المشرع الجزائري قد أخذ بعين الاعتبار طبيعة الجرائم المعلوماتية و ما تتطلبه من سرعة في التحرك، فوسع مجال الاختصاص الإقليمي لضباط الشرطة القضائية ليشمل كافة التراب الوطني.

إن الضبطية القضائية تلعب دورا فعالا في البحث عن الجرائم و مرتكبيها ، فهي بمثابة اليد اليمنى لجهات التحقيق، إلا أن فعالية هذا الدور لم تعد ذاتها مع ظهور الجرائم المعلوماتية، فلم تعد قادرة لوحدها و بمعرفتها المتواضعة في ميدان التقنية المعلوماتية بمجابهة هذا النوع من الجرائم، الأمر الذي دعى إلى استحداث أجهزة متخصصة تكون مهمتها الأساسية البحث و التحري عن هذا النوع المستحدث من الجرائم ، و هذا ما سنراه تباعا في الفرع الثاني.

2.1.1.2 .الأجهزة الخاصة بمكافحة الجرائم المعلوماتية

إن عدم قدرة جهات الضبط القضائي على مجابهة ما أفرزه التطور التكنولوجي في مجال التقنية المعلوماتية من جرائم، أدى إلى ظهور الحاجة إلى أجهزة متخصصة لها القدرة بمعرفتها و مهاراتها في المجال التقني على مجابهة هذا النوع المستحدث من الجرائم، لذا دعى المجلس الأوربي في توصيته رقم 95 (13) المؤرخة في 11 ديسمبر 1995 في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، إلى ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسوب الآلي و إعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات [46] ص354، و هذا ما ذهبت إليه العديد من الدول، فإلى جانب ما تقوم به الضبطية القضائية من بحث و تحري عن الجرائم المعلوماتية، قامت بإنشاء أجهزة خاصة تكون عونا لها، تضم العناصر المؤهلة و القادرة على استيعاب التقنية المعلوماتية .

1.2.1.1.2.الأجهزة الخاصة بمكافحة الجرائم المعلوماتية في الدول الأجنبية

إن التزايد المستمر للجرائم المعلوماتية في الدول الأجنبية، و ما ينجم عنها من خسائر جسيمة أصبحت تهدد هذه الدول في اقتصادها و أمنها وسلامتها ، أدى بها إلى التحرك من أجل وضع حد للعجز الذي يعتري أجهزة الشرطة لديها، فأنشأت أجهزة شرطة متخصصة لمكافحة هذه الجرائم، و من بين هذه الدول أمريكا وفرنسا.

1.1.2.1.1.2.الأجهزة الخاصة بمكافحة الجرائم المعلوماتية في الولايات المتحدة الأمريكية

تعتبر الولايات المتحدة الأمريكية من أكثر الدول عرضة للجرائم المعلوماتية ، حيث تعرف فيها هذه الجرائم انتشارا واسعا، و لذلك كانت السباقة إلى وضع أقسام و وحدات شرطة متخصصة لمواجهة هذا النوع من الإجرام و الحد من خسائره، ومن بينها: [63] ص108،109

- قسم جرائم الحاسوب و جرائم حقوق الملكية الفكرية الذي تم إنشاؤه سنة 1991 والذي يختص بالكشف عن جرائم الحاسوب الآلي وعن ملاحقة مرتكبيها.

- وحدة جرائم الانترنت وهي وحدة تختص بالتحقيق في جرائم حقوق الملكية الفكرية وفي الجرائم المرتبطة بالتقنية العالية ويترأسها مدير مساعد لمكتب التحقيقات الفيدرالي، ولها مرتبة وحدة التفتيش الجنائي.

◆ مكتب رئيس التكنولوجيا وهو مكتب مفوض مباشرة من مكتب مدير التحقيقات الفيدرالية الأمريكي، لتسيير مختلف المشروعات التكنولوجية وملاحقة مرتكبي الجرائم الواقعة في ذلك المجال.

◆وحدة مكافحة الإجرام المعلوماتي وهي وحدة متخصصة تابعة لقسم العدالة الأمريكي مكلفة بمكافحة الإجرام المعلوماتي، تتكون من خبراء في تقنيات الحوسبة والانترنت ومن مستشارين قانونيين.

2.1.2.1.1.2.الأجهزة الخاصة بمكافحة الجرائم المعلوماتية في فرنسا

إن فرنسا كغيرها من الدول المهددة من هذا النوع من الجرائم، قامت بإنشاء بعض أجهزة شرطة ودرك متخصصة في مكافحة الجرائم المعلوماتية ، من بينها:

◆فرقة التحري في جرائم تكنولوجيا المعلومات و التي تم إنشاء هذه الفرقة في 11 فيفري 1994، و التي عرفت قبل إعادة تنظيم أجهزة الشرطة القضائية في فرنسا بتسمية جهاز التحري في جرائم تكنولوجيا المعلومات ، تقوم هذه الأخيرة بالتحري حول الجرائم المرتكبة بواسطة أنظمة معلوماتية، وهي تقوم بذات المهام التي يتولاها أجهزة الشرطة القضائية العادية . [11] ص 202

◆الفرقة المركزية لقمع الجريمة المعلوماتية وهي فرقة تابعة للمديرية المركزية للشرطة القضائية، تم إنشاؤها عام 1994 ، وهي تقوم بتحرياتها حول الجرائم المعلوماتية المرتكبة على المستوى الوطني و كذا الدولي، حيث تربطها علاقات بأجهزة الشرطة الدولية كالأنتربول و كذا فريق العمل الأوروبي حول الجرائم المعلوماتية.[64] ص60

◆المكتب المركزي لمكافحة الجرائم المرتبطة بتكنولوجيا المعلومات و الاتصالات و الذي تم إنشاؤه بموجب المرسوم رقم 2000 – 405 المؤرخ في 2000/05/15 على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الاقتصاد و المالية و الصناعة (المديرية العامة للجمارك و الحقوق غير المباشرة و المديرية العامة للمنافسة و الاستهلاك و قمع الاحتيال)، و هو يتمتع كغيره من المكاتب المتخصصة، باختصاص وطني يتحدد نطاقه في الجرائم الخاصة و المرتبطة بتكنولوجيا المعلومات و الاتصالات (سواء أكانت تلك التكنولوجيا محلا للاعتداء أو وسيلة لارتكاب و تسهيل ارتكاب ذلك الاعتداء) . [63] ص 123،124

2.2.1.1.2 الأجهزة الخاصة بمكافحة الجرائم المعلوماتية في الدول العربية

إن إنشاء أجهزة خاصة بمكافحة الجرائم المعلوماتية لم يقتصر على الدول الأجنبية فحسب، بل امتد حتى إلى الدول العربية رغم أنها لم تعرف خطر هذه الجرائم إلا حديثا، فقد بدأت العديد من الدول العربية في إعادة تكييف جهازها الأمني وفقا لما يتضمن مكافحة فعالة لهذا النوع من الجرائم، و من بين هذه الدول مصر و الجزائر .

1.2.2.1.1.2.الأجهزة الخاصة بمكافحة الجرائم المعلوماتية في مصر

بدأت أجهزة الشرطة المصرية في انتهاج سياسة التقدم العلمي و التكنولوجي و مواكبة التطور للحاق بالمسيرة العلمية من خلال الاعتماد على التقنيات الحديثة لمواجهة الصور المستحدثة من الإجرام المعلوماتي، و كان ثمرة هذا التطور إنشاء إدارة جديدة تختص بمكافحة جرائم الحواسب و شبكات المعلومات. تم إنشاء هذه الإدارة بالقرار رقم (13507) سنة 2002 ، وهي تابعة للإدارة العامة للمعلومات و التوثيق و تخضع للإشراف المباشر لمدير الإدارة العامة و تشرف عليها فنيا مصلحة الأمن العام[33] ص220، تعد هذه الإدارة إدارة جديدة في تكوينها و نوعيتها تختص بمكافحة مثل تلك الجرائم، و تتكون من اجل ذلك من ضباط على أعلى درجة من التخصص و الحرفية في تكنولوجيا الحواسب و شبكة الانترنت ، مقسمين على أجهزتها المتخصصة و المتمثلة في قسم العمليات، قسم التأمين، قسم البحوث و المساعدات الفنية.[33] ص143

2.2.2.1.1.2.الأجهزة المتخصصة بمكافحة الجرائم المعلوماتية في الجزائر

نتيجة الارتفاع المستمر للجرائم المعلوماتية في الجزائر،رأى المشرع الجزائري ضرورة التحرك من أجل مواجهة فعالة لهذا النوع الجديد من الجرائم، حيث قام بإنشاء فرق متخصصة من الشرطة القضائية على مستوى أمن كل الدوائر عبر الوطن، مهمتها البحث و التحري عن الجرائم المعلوماتية، و هو الآن في طور إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و التي نص على إنشائها القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها[65]، و التي من مهامها تنشيط عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و هي جميع الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية فضلا عن جرائم المساس بأنظمة

المعالجة الآلية للمعطيات المنصوص عنها في قانون العقوبات الجزائري، كما تقوم هذه الهيئة بمساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم ، بالإضافة إلى قيامها بالتنسيق مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي هذه الجرائم [66] ، ويرتقب أن يتم قريبا تنصيب هيئة مختصة بمكافحة الجرائم المعلوماتية، و ذلك مباشرة بعد صدور النص التنظيمي الخاص بمكافحة هذه الظاهرة الذي هو قيد التحضير.

2.1.2 .المتطلبات الضرورية للبحث و التحري في الجرائم المعلوماتية

وجدت أجهزة الضبط القضائي صعوبات جمة منذ ظهور ما يعرف بالجرائم المعلوماتية سواء في كشف غموضها أو القبض على مرتكبيها، و ذلك نظرا للطبيعة الخاصة التي تتميز بها هذه الجرائم، بل وصل بها الأمر في الكثير من الأحيان إلى ارتكاب أخطاء جسيمة أدت إلى الإضرار بالأجهزة و الملفات و الأدلة الخاصة بإثبات هذه الجرائم نتيجة نقص خبرتها في ميدان التقنية المعلوماتية . الأمر الذي أصبح يدعو و بشدة إلى ضرورة تطوير كفاءات هذه الأجهزة و تدعيمها بالقدرات و المهارات العلمية و الفنية و وسائل التقنية اللازمة لمواجهة تحديات القرن[67] ص61، و ذلك لا يكون إلا من خلال إعداد برامج تدريبية يكون من شأنها تأهيل أجهزة الضبط القضائي من الناحية الفنية و القانونية. فالبحث و التحري عن الجرائم المعلوماتية يتطلب توافر مهارات فنية لازمة، تمكن هذه الأجهزة من تحقيق المهمة المطلوبة منها وبالكفاءة اللازمة. و على ذلك سنتطرق في هذا المطلب إلى تدريب سلطات البحث و التحري عن الجرائم المعلوماتية كفرع أول، و نتطرق في الفرع الثاني من هذا المطلب إلى المهارات الفنية الواجب توافرها لدى سلطات البحث و التحري عن هذه الجرائم.

1.2.1.2.تدريب سلطات البحث و التحري عن الجرائم المعلوماتية

إن التدريب السليم لأجهزة الضبط القضائي على تقنيات البحث و التحري عن الجرائم المعلوماتية أصبح مطلوب و بشدة، و ذلك ضمانا لمواجهة فعالة لهذه الجرائم من جهة، وتفاديا لما قد يرتكب من أخطاء تؤدي إلى ضياع أدلة إثباتها، من جهة أخرى. و لهذا اتجهت العديد من الدول مثل كندا(سنة1980) و فرنسا (سنة 1983) و انجلترا (سنة 1987) و فلندا(سنة 1990) إلى إعطاء دورات تدريبية لضباط الشرطة القضائية عن كيفية التحقيق في جرائم الحاسوب الآلي[68] ص118، و في الولايات المتحدة الأمريكية فإن التدريب على التحقيق في الجرائم المعلوماتية يتم من خلال دورات متخصصة مدة كل منها أربعة أسابيع تتم بمعرفة مكتب

التحقيقات الفيدرالي، و ذلك لتزويد محقق الشرطة و العاملين في أجهزة العدالة الجنائية بمعارف و مهارات حول برمجة الحاسوب و تشغيله[55] ص131. و على المستوى العربي، فإن الجمعية المصرية للقانون الجنائي و من خلال مؤتمرها السادس المنعقد في القاهرة سنة 1993 حول جرائم الحاسوب و الجرائم الأخرى في مجال تكنولوجيا المعلومات، أوصت بوجوب تدريب رجال الضبطية القضائية و النيابة العامة و القضاة على طرق و كيفية استخدام أجهزة المعلومات و طرق الاستدلال و التحقيق و جمع الأدلة في الجرائم المتعلقة بها، أما على المستوى الدولي فإن الشرطة الدولية تنظم دورات تدريبية في مجال شبكات الحواسب الآلية و ذلك من اجل تحسين أداء الأعضاء من رجال الشرطة في مجال الكشف عن الجريمة و جمع المعلومات و متابعة الجناة و إقامة الدليل في الجرائم التي ترتكب في هذا المجال . [68] ص118

و على ذلك يمكن القول أن جمع الاستدلالات في الجرائم المعلوماتية يتطلب مهارات و قدرات على التعامل مع أجهزة الحواسب الآلية و شبكاتها، و هذا لا يتأتى إلا بالتدريب السليم الذي يراعى فيه حسن اختيار الجهة القائمة على التدريب، المنهج التدريبي، الأسلوب المتبع في التدريب و غير ذلك من العناصر التي يقتضيها التدريب السليم.

1.1.2.1.2.المدرب

لابد أن يعهد بتدريب أجهزة الضبط القضائي إلى جهات متخصصة في مجالات الحواسب الآلية و برامجها، لها من القدرات الفنية و العلمية ما يمكنها من تطوير مهارات أجهزة الضبط القضائي في مجال التحري عن الجرائم المعلوماتية، فضلا عن إلمامها ببعض الجوانب القانونية و ذلك لضمان تأهيل فعال من الناحية القانونية و التقنية.

2.1.2.1.2 .المتدرب

لابد أن يكون المتدرب مؤهلا للتدريب، وهذا يتطلب قدرات ذهنية و نفسية خاصة لتلقي هذا التدريب، و الملاحظ أن تدريب المتخصصين في معالجة البيانات و نظم التشغيل يؤتي ثماره وبسرعة عن أولئك المنضمين لأجهزة العدالة كما في الشرطة و التحقيق الجنائي، فيتعين توافر الخبرة لدى متلقي برنامج التدريب.[55] ص129

3.1.2.1.2.منهج التدريب

يتعين أن يكون منهج التدريب علميا من الناحية النظرية و العلمية، و أن يتناول الأتي: [17] ص263

- أنواع المخاطر و التهديدات التي يمكن أن تتعرض لها شبكة الحاسوب الآلي.
- مفاهيم الحاسوب الآلي و الانترنت من برامج و تطبيقات و أسماء الأجهزة.
- أنواع الجرائم الناشئة عن الحاسوب الآلي و الانترنت.
- منهج البحث و التحري أي الإجراءات المتبعة للتحري في هذه الجرائم و يشمل ذلك :
  - إجراءات التحري .
  - تخطيط التحري.
  - تجميع المعلومات و تحليلها.
  - مراجعة النظم الفنية للبيانات.
  - أساليب العمل الجنائي.
  - أساليب عرض و دراسة الحالات.
- أمن الحاسوب و شبكاته.
- القانون و نظرية الإثبات.
- استخدام الحاسوب كوسيلة للحصول على أدلة الاتهام.
- الملاحقة الدولية و التعاون المشترك في مجال الجرائم المعلوماتية.

4.1.2.1.2.أسلوب التدريب

التدريب قد يكون بصفة رسمية و قد يكون بصفة غير رسمية . فيكون التدريب غير رسمي بتكليف المتدرب بالعمل مع شخص لديه خبرة في التحقيق في الجرائم المعلوماتية، أما التدريب الرسمي فيكون من خلال حلقات دراسية ونقاش و هو ما يسمى بـ" ورش العمل" ، و ذلك حول جرائم الحاسوب الآلي و شبكات المعلومات و إساءة

استخدامها[55] ص130. و في هذا الشأن يرى البعض[55] ص131 أنه من الأمثل انتهاج ما يسمى بـ " أسلوب الفرق"، و يعني تدريب فريق أو مجموعة متخصصة في جرائم الحاسوب الآلي مرة واحدة، بحيث يكون لكل عضو من الفريق مهمة محددة فضلا عن إلمامه بمهام زملائه الآخرين، كما يرى أنه من الأفضل تقسيم هذا الفريق إلى ثلاث مجموعات رئيسية هي:

- مجموعة مهمتها تنفيذ القانون (رجال الضبط و التحقيق الجنائي) .
- متخصصون في التدقيق و المراجعة الحسابية.
- متخصصون في معالجة البيانات إلكترونيا.

إن من شأن هذا التدريب أن يكسب أجهزة الضبط القضائي مهارات أساسية لا غنى عنها لجمع الاستدلالات في الجرائم المعلوماتية و هذا ما سنراه في الفرع التالي.

2.2.1.2.المهارات الفنية الواجب توافرها لدى سلطات البحث و التحري

إن التحري و البحث عن الجرائم المعلوماتية يتطلب أن يتوافر لدى أجهزة الضبط القضائي مهارات فنية تمكنها من التعامل مع هذا النمط الجديد من الجرائم، فلا يكفي أن تكون هذه الأجهزة على دراية بأصول البحث و التحري في الجرائم و التي يفترض بداهة وجودها لديها، و إنما لابد أن يكون لدى هذه الأخيرة مهارات خاصة نابعة من التطور التكنولوجي الحاصل في مجال التقنية المعلوماتية و تأثيره على أساليب البحث و التحري التقليدية، و لعل من أهم هذه المهارات ما يلي:

1.2.2.1.2.الإطلاع على الجوانب المتعلقة بالجرائم المعلوماتية

إذا كان الإطلاع على الجوانب المتعلقة بأي جريمة واجب على كل ضابط شرطة قضائية، فلا يعقل أن يقوم بالتحري و البحث عن الجريمة و هو لا يعلم شيئا عنها، فإن هذا الواجب يبرز أكثر في مجال الجرائم المعلوماتية و ذلك نظرا لحداثتها، فحسن تعامل هذا الأخير مع هذا النوع المستحدث من الجرائم يقتضي منه أولا و قبل كل شيء معرفة ماهيتها و كذا خصائصها و أنواعها و صفات مرتكبيها، و هذا الأمر لا يحتاج إلى تدريب مكثف و إنما يحتاج فقط إلى الإطلاع على ما تم من دراسات بشأن الجرائم المعلوماتية.

2.2.2.1.2.معرفة الأساليب و الأدوات المستخدمة في ارتكاب الجرائم المعلوماتية

الجرائم المعلوماتية كثيرة ومتعددة يستخدم مرتكبوها أساليب متجددة و أدوات برامجية متطورة تساعدهم على ارتكاب هذه الجرائم، و هذه الأدوات من التجدد و السرعة في التطور، بحيث لا يمكن أن يحيط بها أي برنامج تدريبي يستهدف رجل الضبط القضائي، و لا حل لذلك إلا بالمتابعة المستمرة و الإطلاع على النشرات الأمنية التي تصدرها منظمات رسمية و غير رسمية ذات مصداقية من خلال الانترنت[45] ص38. كما أنه من الأهمية بمكان معرفة الأساليب المستخدمة في ارتكاب الجرائم المعلوماتية و ذلك لتحديد أساليب المواجهة .

3.2.2.1.2.التعرف على المكونات المادية للحاسوب و كيفية التعامل المبدئي معها

إن سلامة التعامل مع المكونات المادية للحاسوب يقتضي أن يكون ضابط الشرطة القضائية على معرفة تامة بها ، بحيث يتمكن من التمييز بين مختلف الحواسب و ملحقاتها و مسمى كل منها و الهدف من استخدامها و ما هي احتمالات توظيفها لارتكاب أي من الجرائم المعلوماتية، حيث أن عدم تعرفه عليها قد يؤدي إلى إهمالها أو حتى إتلافها دون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها. [45] ص33

و لا يكفي أن يتعرف ضابط الشرطة القضائية على المكونات المادية للحاسوب فحسب، و إنما لابد أن يلم أيضا بكيفية التعامل معها، فقد يقوم هذا الأخير مثلا بقطع التيار الكهربائي عن الحواسب جهلا منه أن مثل هذا الفعل قد يؤدي إلى فقد البيانات الموجودة بالذاكرة، كما قد يعرض الأقراص المرنة و غيرها من وسائط التخزين لمصدر حراري قوي فيؤدي إلى إتلافها . و لذلك فمن الضروري أن يكون ضابط الشرطة القضائية على معرفة بأصول التعامل مع مثل هذه المكونات فيأخذ من الاحتياطات ما يلزم ليحول دون تلفها.

4.2.2.1.2.معرفة أساسيات عمل شبكات الحاسوب الآلي و أهم مصطلحاتها

لأن الكثير من الجرائم المعلوماتية يتم ارتكابها من خلال الشبكات و خصوصا شبكة الانترنت، فإن ضابط الشرطة القضائية بحاجة إلى معرفة مبادئ الاتصال الشبكي و أنواعه المختلفة و كيفية انتقال البيانات من جهاز إلى أخر على شكل حزم و مبادئ البرتوكولات الرئيسية الخاصة بالاتصال بالشبكة[69] ص131. و تبرز أهمية فهم ضابط الشرطة القضائية لمبادئ عمل شبكات الحاسوب في أنها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في الفضاء السيبراني، من اختراق الشبكات و الحواسب و اعتراض حزم البيانات أثناء انتقالها عبر

الشبكة و التجسس عليها و تحويل مسارها، كما أنها تعطي تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة و المعوقات الفنية التي قد تحول دون ذلك [25] ص59، بالإضافة إلى هذا فإن ضابط الشرطة القضائية لابد أن يكون على علم بالمصطلحات المستخدمة في مجال الحواسب و شبكاتها كأن يعلم مثلا أن (L.A.N) هو اختصار لكلمة (Local Area Network) و التي تعني شبكة محلية، أما (W.A.N) فهي اختصار لكلمة (Wide Area Network) و التي تعني شبكة واسعة النطاق[45] ص34، و غير ذلك من المصطلحات . ذلك أن للمجرمين المعلومتيين لغة خاصة بهم، اعتادوا على استخدامها فيما بينهم، حتى لا يتم اكتشاف أمرهم.

5.2.2.1.2.تمييز أنظمة تشغيل الحاسوب المختلفة و كيفية التعامل معها

تختلف أنظمة التشغيل المعتمدة في الحاسوب تبعا لرغبة كل مستخدم، ولهذا لابد على ضابط الشرطة القضائية أن يكون لديه فهم مبدئي لهذه الأنظمة و مميزاتها و خصائصها، فقد يوجد مثلا بمسرح الجريمة حواسب و هي في وضع التشغيل، فلا يعرف ضابط الشرطة القضائية، و الذي ليست لديه أي فكرة عن الحواسب و أنظمة تشغيلها كيفية التصرف حيال هذا الوضع، فقد يقوم بإيقافها مما يؤدي إلى محو الأدلة الموجودة في ذاكرتها و قد يقرر الإبقاء عليها مشتغلة وفي هذه الحالة قد يتضمن برامج تعمل على محو الأدلة تلقائيا، و لهذا فإن توفر معرفة مبدئية بهذه الأنظمة لدى الضابط قد يغني عن الوقوع في مثل هذه الأخطاء.[69] ص131

و من أجل ذلك، على الدول أن تشترط على شركات الحواسب الآلية و البرمجة اطلاع السلطات بكل المستجدات في مجال الحواسب الآلية و أخر التقنيات المعتمدة من قبلها، وذلك حتى تكون السلطات المعنية في الدولة على بينة بكل ما هو جديد، و بالتالي تتهيأ لضبط التعامل و التحكم في المراقبة.

3.1.2.إجراءات البحث و التحري عن الجرائم المعلوماتية

إجراءات البحث و التحري هي جمع المعلومات حول الجريمة و مرتكبيها بهدف تحضير الدعوى الجنائية و مباشرتها [70] ص337 . و لا تختلف إجراءات البحث و التحري عن الجرائم المعلوماتية عن غيرها من الجرائم، فجميع الجرائم تحتاج إلى إجراءات تتشابه في عمومها، و قد درج الفقه على تقسيم هذه الإجراءات إلى قسمين يضم الأول إجراءات البحث و التحري في الأحوال العادية و يضم القسم الثاني إجراءات البحث و التحري في حالة التلبس، إلا أن اعتماد هذا التقسيم في إطار الجرائم المعلوماتية لن يكون سليما، ذلك أن القانون وسع من اختصاص ضباط الشرطة القضائية في حالة ما إذا تعلق الأمر بجرائم معلوماتية نظرا

لخطورتها و الطبيعة الخاصة التي تتميز بها، فأصبح بإمكان ضابط الشرطة القضائية و في الأحوال العادية لهذه الجرائم، القيام ببعض الإجراءات المخولة له استثناء في حالة التلبس كالتفتيش مثلا، و لهذا ارتأينا تناول أهم ما يعني موضوع دراستنا من إجراءات دون وضع تقسيم معين لها. و عليه نتطرق إلى المعاينة في الجرائم المعلوماتية كفرع أول، ثم نتناول التفتيش و الضبط فيها كفرع ثان و نخصص الفرع الثالث للحديث عن سماع الأقوال في هذا النوع من الجرائم ، و من ثم ننتهي في الفرع الرابع إلى الحديث عن التسرب و المراقبة الالكترونية فيها.

1.3.1.2. اجراءات المعاينة في الجرائم المعلوماتية

المعاينة هي رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة [71] ص233. و إن كانت المعاينة تلعب دورا كبيرا في كشف غموض العديد من الجرائم التقليدية، فإنها لا تؤدي ذات الدور في الجرائم المعلوماتية، و هذا راجع إلى قلة الآثار المادية المتخلفة عنها و كذا سهولة العبث بهذه الآثار إن وجدت.

و حتى يكون لهذه المعاينة فائدة في كشف الحقيقة في مجال الجرائم المعلوماتية، لا بد أن يكون ضباط الشرطة القضائية القائمون بها ممن تتوفر فيهم الكفاءة العلمية و الخبرة الفنية في مجال الحواسب ، كما يتوجب على هؤلاء مراعاة بعض الخطوات الضرورية في المعاينة ، سواء قبل انتقالهم لمسرح الجريمة أو عند وصولهم إليه.

1.1.3.1.2.الخطوات الواجب على ضباط الشرطة القضائية إتباعها قبل الانتقال لمسرح الجريمة

يجب على ضباط الشرطة القضائية قبل التحرك لمعاينة مسرح الجريمة إتباع الخطوات التالية : [49] ص356،357

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة المتوقع مداهمتها و شبكاتها، لتحديد إمكانية التعامل معها فنيا من حيث الضبط و التأمين و الحفظ.

- إعداد خريطة الموقع الذي سيتم معاينته و تفاصيل المبنى أو الطابق من المبنى موضوع البلاغ و تحديد مواقع الأجهزة و الخزائن و الملفات، ويتم ذلك عبر مصادر المعلومات السرية .

◆الحصول على الاحتياجات الضرورية من أجهزة و برامج للاستعانة بها في الفحص و التشغيل .

◆تأمين التيار الكهربائي بحيث لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

2.1.3.1.2.الخطوات الواجب على ضباط الشرطة القضائية إتباعها عند الوصول إلى مسرح الجريمة

فور وصول ضباط الشرطة القضائية إلى مسرح الجريمة، ينبغي عليهم مراعاة الخطوات التالية : [34] ص172

◆تصوير الحاسوب الآلي و ما يتصل به من أجهزة بدقة تامة وسائر ملحقاته و الأجهزة الطرفية المتصلة به و المحتويات و الأوضاع العامة بمكانه، مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسوب، و يراعى تسجيل وقت وتاريخ ومكان التقاط كل صورة.

◆تحديد نوع نظام المعالجة الآلية للمعطيات، جهاز حاسوب آلي متصل أو محمول[72] ص34، وينبغي عدم العبث به و تدوين الحالة التي هو عليها في حالة تشغيل أو إطفاء.

◆إن تعلق الأمر بشبكة، فيجب إحصاء الطرفيات و تحديد طبيعة الروابط الموجودة بينها لمعرفة الطريقة التي تتم بها نقل المعلومات من موقع لأخر (الاسطوانات ، الأشرطة الممغنطة، خطوط الاتصالات)، و من المهم أيضا معرفة ما إذا كانت هناك أجهزة حواسب خارج نظام معالجة المعلومات و لكن بها إمكانية الاتصال بالشبكة . [68] ص120

◆عدم نقل أي معلومة من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجالات لقوى مغناطيسية، يمكن أن تتسبب في محو أو إتلاف البيانات المسجلة. [73] ص22

◆التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة و أوراق الكربون المستعملة و الشرائط الممغنطة و غير السليمة أو المحطمة و فحصها و رفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة .

◆التحفظ على مستندات الإدخال و المخرجات الورقية للحواسب ذات الصلة بالجريمة لرفع و مضاهاة ما قد يوجد عليها من بصمات .

◆إبعاد جميع الموظفين عن أجهزة الحواسب الآلية، و كذلك عن الأماكن الأخرى التي بها أجهزة الحواسب الآلية.

2.3.1.2. اجراءات التفتيش و الضبط في الجرائم المعلوماتية

سبق و أشرنا إلى أن العديد من التشريعات منحت ضباط الشرطة القضائية صلاحيات واسعة في حالة ما إذا تعلق الأمر بجريمة من الجرائم المعلوماتية، و من بين هذه التشريعات المشرع الجزائري، حيث أصبح بإمكان ضباط الشرطة القضائية القيام بعمليات التفتيش و كذا الضبط في حالة ما إذا تعلق الأمر بجريمة من الجرائم المعلوماتية[74] و ذلك في غير أحوال التلبس.

1.2.3.1.2. إجراءات التفتيش في الجرائم المعلوماتية

يثير التفتيش في الجرائم المعلوماتية العديد من المشكلات،غير انه و باعتبار أن التفتيش من الصلاحيات المخولة أصلا لسلطات التحقيق، و استثناء لسلطات الضبط القضائي، ارتأينا التطرق لهذه المشكلات عند حديثنا عن التفتيش كإجراء من إجراءات التحقيق.وسنقتصر هنا فقط عن الحديث عن الصلاحيات التي منحها القانون لضباط الشرطة القضائية في حالة قيامهم بعمليات التفتيش في الجرائم المعلوماتية.

إن الطبيعة الخاصة بالجرائم المعلوماتية من سرعة في التنفيذ و سهولة في محو الآثار المتخلفة عنها، جعلت العديد من التشريعات تحيد عن بعض الضوابط المقررة في البحث و التحري عن الجرائم، حيث وسعت من الصلاحيات الممنوحة لضباط الشرطة القضائية في حالة ما إذا تعلق الأمر بهذا النوع من الجرائم، ومن بين هذه التشريعات المشرع الجزائري، حيث أصبح بإمكان ضباط الشرطة القضائية القيام بعمليات التفتيش في الجرائم المعلوماتية حتى و لو كانت في غير أحوال التلبس، كما لم يعودوا مقيدين عند إجراء التفتيش في مسكن المتهم بجريمة معلوماتية بضرورة حضور المتهم أو ممثل له أو شاهدين ، و كذا هو الحال في حالة ما إذا تم التفتيش في مسكن الغير.

ليس هذا فحسب و إنما منح المشرع الجزائري ضباط الشرطة القضائية الحق في الخروج عن الميعاد القانوني للتفتيش (5 صباحا- 8 ليلا) ، و أصبح بإمكانهم إجراء عمليات التفتيش في مثل هذه الجرائم في أي وقت من ساعات الليل و النهار بشرط الحصول على إذن من وكيل الجمهورية.

2.2.3.1.2. إجراءات الضبط في الجرائم المعلوماتية

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبيها[75] ص11، و الضبط في الجريمة المعلوماتية قد يرد على أشياء ذات طبيعة مادية ، كما قد يرد على أشياء ذات طبيعة معنوية .

1.2.2.3.1.2. إجراءات ضبط الأدلة المادية في الجرائم المعلوماتية

الأدلة المادية هي التي تنبعث من عناصر مادية ناطقة بنفسها و تؤثر في اقتناع القاضي بطريقة مباشرة [76] ص07، و لعل من ابرز الأدلة المادية التي لها قيمتها الخاصة في إثبات الجرائم المعلوماتية و التي على ضابط الشرطة القضائية التركيز عليها في بحثه ما يلي:[34] ص275

◆الأوراق: كالأوراق التحضيرية التي يتم استعمالها كمسودة للجريمة، و الأوراق الأصلية التي يتم طباعتها و حفظها، و الأوراق التي يتم رميها في سلة المهملات و أي أوراق ذات صلة بالجريمة.

◆جهاز الحاسوب الآلي : فهو مصدر الجريمة المعلوماتية و يلعب دورا كبيرا في إثباتها و التعرف على مرتكبيها.

◆ملحقات الحاسوب الآلي : كجهاز معدل الموجات الذي قد يحتوي على أدلة هامة، خاصة إذا كان يحمل تقنية الرد الآلي على المكالمات، بالإضافة إلى الطابعات فمنها ما تحتوي على ذاكرة تحتفظ ببعض الصفحات التي سبق طباعتها، و كذا الماسحات الضوئية، و غيرها من الملحقات التي تفيد في إثبات الجريمة.

◆الأقراص المرنة و الصلبة : حيث تعتبر من أهم الأدلة لما قد تحتويه من معلومات تفيد في إثبات الجريمة المعلوماتية .

إن هذا النوع من الأدلة لا يثير أي إشكال، حيث يتم ضبطها و فق قواعد الضبط و التحريز التقليدية.

2.2.2.3.1.2. إجراءات ضبط الأدلة المعنوية في الجرائم المعلوماتية

الأدلة المعنوية أو ما اصطلح على تسميتها بالأدلة الرقمية، هي كما سبق وذكرنا الأدلة المأخوذة من أجهزة الحاسوب، و التي تكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج و تطبيقات و تكنولوجيا خاصة، و بعكس الأدلة المادية، فإن هذه الأخيرة أثارت العديد من التساؤلات حول مدى صلاحياتها لتكون محلا للضبط ، حيث اختلفت التشريعات بشأن ضبطها فظهر اتجاهان:

◆الاتجاه الأول: يرى أصحاب هذا الاتجاه انه من غير المتصور أن يرد الضبط على البيانات لانتفاء الكيان المادي عنها، وأن ذلك الإجراء يمكن أن يتم فقط في حالة ما إذا جسدت هذه البيانات الالكترونية في دعامة مادية[77] ص265. و من بين التشريعات التي ذهبت مع هذا الاتجاه التشريع الألماني، و التشريع الروماني، و كذا التشريع الجزائري، و هذا ما يستشف من نص المادة 06 من القانون رقم 04-09 السابق الذكر حيث جاء فيها "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و انه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها، على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في أحراز وفق للقواعد المقررة في قانون الإجراءات الجزائية .."

◆الاتجاه الثاني : يرى أصحاب هذا الاتجاه انه لا يوجد مانع من أن يرد الضبط على البيانات الالكترونية، فما هي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية تقبل التسجيل و الحفظ و التخزين على وسائط مادية، و بالإمكان نقلها و بثها و استقبالها وإعادة إنتاجها فوجودها المادي لا يمكن إنكاره [63] ص265، و من التشريعات التي أيدت هذا الاتجاه، التشريع الكندي حيث تمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت او يشتبه في ارتكابها أو أن هناك نية في أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوعها.

و على ذلك يمكن القول أن الضبط في الجريمة المعلوماتية، قد يرد على أدلة ذات طبيعة مادية كما قد يرد على أدلة ذات طبيعة معنوية . و نظرا لحساسية الأدلة المضبوطة في

هذا النوع من الجرائم يرى المتخصصون ضرورة إتباع مجموعة من القواعد عند ضبطها ولعل من أهمها ما يلي:

◆تحريز الأقراص والاسطوانات داخل أكياس خاصة (ورقية أو بلاستيكية)، وذلك بعد ترقيمها وتدوين الحالة والمكان الذي وجدت فيه (داخل الجهاز ، قرب الجهاز) مع مراعاة حمايتها من الكسر والعوامل الجوية، وإبعادها عن أي مجال مغناطيسي تلافيا لشطب المعلومات والتسبب في ضياعها.[78] ص07

◆ضرورة ضبط الدعامة المادية الأصلية التي تحويها البيانات دون أن يقتصر هذا الضبط على نسخ هذه الدعامة، مع ضرورة تمكين الجهة مالكة هذه الدعامة من نسخها حتى لا يتعطل العمل العادي لهذه الجهة.[55] ص224

◆ضرورة تدوين بعض البيانات الضرورية على الأقراص والشرائط التي تم حفظ البيانات عليها، كالتاريخ والوقت و توقيع الشخص الذي قام بإعداد النسخة، اسم أو نوع نظام التشغيل، اسم البرنامج أو الأوامر المستعملة لإعداد النسخ وكذا المعلومات المضمنة في الملف المحفوظ.[52] ص121

◆ضرورة مراعاة بعض القواعد الفنية الخاصة بنقل وحماية الأحراز المعلوماتية حتى لا تتعرض كلها أو بعضها لتلف جزئي أو كلي، حيث تتطلب هذه الأحراز معاملة خاصة نظرا لكونها تتأثر بأقل صدمة أو تأثير مغناطيسي. [55] ص225

3.3.1.2. سماع الأقوال في الجرائم المعلوماتية

يعد سماع أقوال من لديهم معلومات عن الجريمة من صميم أعمال الاستدلال التي يقوم بها ضابط الشرطة القضائية، فهذه الأقوال مصدر هام للمعلومات التي يسعى هذا الأخير إلى تجميعها، ولهذا منحت التشريعات ضباط الشرطة القضائية صلاحية سماع أي شخص لديه معلومات تفيد في كشف الحقيقة.

وفي إطار الجرائم المعلوماتية حيث التكنولوجيا المتطورة والمعقدة، نجد أن الغالبية العظمى التي تملك معلومات عن هذه الجرائم هم من ذوي الاختصاص في تقنيات الحواسب الآلية وعملها، كمشغلي الحاسوب ومزودي الخدمة وخبراء البرمجة والمحللين، فبحكم عملهم وخبرتهم، غالبا ما تكون لديهم المعلومات اللازمة للدخول إلى الأنظمة المعلوماتية، وغيرها من المعلومات التي قد تفيد في جمع الأدلة اللازمة للتحقيق وتوجيه الاتهام، فكلما كثر كم المعلومات

التي يحصل عليها ضابط الشرطة القضائية من هؤلاء، وكلما كانت هذه المعلومات دقيقة، كلما مكنه ذلك من إثبات كيفية وقوع الجريمة والعلاقة بين الآثار المتخلفة عنها والوصول إلى مرتكبيها بأسرع وقت ممكن .

ولهذا أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل في الفترة من 4 الى6 سبتمبر 1994، بضرورة وجود تعاون فعال من جانب الشهود أو غيرهم من مستخدمي تكنولوجيا المعلومات حتى تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية، كما ذهبت العديد من التشريعات إلى سن قوانين خاصة من أجل تفعيل مساعدة الشهود وغيرهم للسلطات المختصة، كالتشريع الأمريكي الذي وضع قانونا خاصا يتعلق بتعاون متعهدي خدمات الرسائل في مجال الاتصالات الالكترونية المسجلة[68]ص107، وهناك من التشريعات من ذهبت إلى فرض التزامات على مقدمي الخدمات كالتشريع الجزائري، فبعد صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أصبح يتعين على مقدمي الخدمات القيام بما يلي: [79]

◆تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.

◆تزويد السلطات بالمعطيات التي تسمح لهم بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

◆تعريف السلطات بالخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

◆إمداد السلطات بالمعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، و كذا المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

وتجدر الإشارة أنه على ضابط الشرطة القضائية الذي يتولى سماع أقوال من لديهم معلومات عن الجرائم المعلوماتية المرتكبة ، أن يعرف كيفية استيفاء المعلومات الضرورية التي تفيد في اكتشاف الحقيقة، فيولي أهمية كبيرة للأسئلة التي يطرحها، فمن خلالها يمكنه التعرف على نوع الجريمة المرتكبة و الأسلوب الإجرامي المتبع في ذلك، بالإضافة إلى تحديد دوافع

ارتكابها، و الذي يؤدي إلى تفسير منطقي للوقائع و الآثار المعثور عليها و يساهم في الإيقاع بمرتكبيها.

4.3.1.2. التسرب و المراقبة الالكترونية في الجرائم المعلوماتية

أدى التطور في أساليب ارتكاب الجرائم إلى ضرورة استحداث إجراءات تتناسب و هذه الأساليب و تساهم في كشفها ، و هو ما ذهبت إليه العديد من التشريعات، فأصبح لضباط الشرطة القضائية الحق في القيام بعمليات التسرب و كذا التقاط الصور و تسجيل الأصوات و اعتراض المراسلات، و القيام بعمليات مراقبة الكترونية، رغم ما تمثله هذه الإجراءات من مساس بحرية الأشخاص، و لعل أهم ما يخص موضوع دراستنا هو التسرب و المراقبة الالكترونية.

1.4.3.1.2.التسرب في الجرائم المعلوماتية

هو عبارة عن عملية مراقبة للمشتبه في ارتكابهم جرائم، يقوم بها ضابط الشرطة القضائية تحت هوية مستعارة أو وهمية و ذلك لإيهام المشتبه به بأنه فاعل معه أو شريك . و إن كانت عملية التسرب في الجرائم التقليدية تقتضي التنقل و التواجد الفعلي مع المشتبه فيه، مما يجعل منها عملية صعبة و مرهقة لرجل الضبط القضائي، فإن التسرب في الجرائم المعلوماتية قد لا يحتاج إلى مثل هذا التنقل، فبإمكان ضابط الشرطة القضائية القيام به و هو في مكتبه و ذلك من خلال الدخول باسم وهمي عبر منتديات الحوار و غرف الدردشة النصية أو الصوتية للبحث عن الجرائم و مرتكبيها.

فنظرا لأهمية هذا الإجراء في الكشف عن الجرائم و مرتكبيها نجد العديد من المؤسسات الضبطية حول العالم تقوم باستخدامه، و ذلك عن طريق تجنيد عناصرها أو الغير للدخول إلى العالم الافتراضي، و بالأخص عبر حلقات النقاش و قاعات الدردشة و الاتصال المباشر مستخدمين في ذلك أسماء و صفات و هيئات مستعارة ووهمية بقصد البحث عن الجرائم و مرتكبيها و تقديمهم إلى المحاكمة [63] ص196،195، كما نظمته العديد من التشريعات في قوانينها الداخلية كالمشرع الجزائري، حيث أنه و بموجب المادة 65 مكرر 11 من القانون رقم 06 -22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم لقانون الإجراءات الجزائية، منح ضابط الشرطة القضائية سلطة القيام بعمليات التسرب، و ذلك في جرائم حددها حصرا و من بينها الجرائم المعلوماتية، فيجوز لضابط الشرطة القضائية متى تعلق الأمر بجريمة من الجرائم

المعلوماتية و اقتضت ضرورة التحقيق و التحري ذلك أن يقوم بعملية تسرب، و ذلك بشرط الحصول على إذن مسبق من وكيل الجمهورية أو قاضي التحقيق يكون مكتوب ومسبب تحدد فيه نوع الجريمة، هوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته أو المدة القصوى لعملية التسرب.

2.4.3.1.2.المراقبة الالكترونية في الجرائم المعلوماتية

تعرف المراقبة الالكترونية بأنها العمل الذي يقوم به المراقب (بكسر القاف) باستخدام التقنية الالكترونية لجمع البيانات من المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن (التاريخ والوقت) لتحقيق غرض أمني أو لأي غرض آخر[80]ص03. ومن ثم فإن المراقبة الالكترونية هي وسيلة من الوسائل التي يستعملها ضابط الشرطة القضائية لجمع البيانات والمعلومات عن المشتبه فيه، وذلك من خلال إخضاع اتصالاته الالكترونية للمراقبة .وبهذا الشكل فهي تلعب دورا كبيرا في مساعدة سلطات البحث والتحري، إذ أنها تؤدي في نهاية الأمر إلى تمهيد السبيل و الإسراع بإيقاع المجرمين والقبض عليهم . إلا أنه ورغم ما لهذا الإجراء من أهمية، فإنه يشكل في نفس الوقت مساسا خطيرا بحريات الأفراد التي كفلتها جل الدساتير، ولهذا سعت العديد من التشريعات إلى تنظيم هذا الإجراء بما يكفل الموازنة بين خصوصيات الأفراد ومقتضيات العدالة. ومن بين هذه التشريعات التشريع الفرنسي، والتشريع الأمريكي، وبالمثل فعل المشرع الجزائري، فبعد أن أباح في المادة 65 مكرر من القانون رقم 06-22 المؤرخ في2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية، اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية متى اقتضت ضرورات التحري ذلك، جاء في القانون رقم 04-09 السالف الذكر وأجاز وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها[81]، بشرط الحصول على إذن مكتوب من السلطة القضائية المختصة، ومن ثم حدد الحالات التي تسمح باللجوء إلى مثل هذه المراقبة والتي تتمثل فيما يلي : [82]

◆للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .

◆في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

◆لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

◆في إطار تنفيذ طلبات المساعدة القضائية المتبادلة .

إن عمليات المراقبة الالكترونية تتم من خلال استخدام برمجيات متطورة وأجهزة سريعة وقوية كبرامج تتبع مصدر الاتصال الشبكي. وهذه العملية تشبه تتبع آثار أقدام المشتبه فيه في الجرائم التقليدية، غير أنها تتم في درب الفضاء السبيراني، حيث يتم تتبع الطريق الذي سلكه المشتبه فيه، للوصول إلى الحاسوب أو الشبكة المتضررة[45]ص32 .ولعل أقوى أنظمة المراقبة الالكترونية المعروفة وأكثرها شهرة وإثارة للجدل النظام الذي يطلق عليه carnivore ويعني أكلات اللحم.

هذا و يجب أن يراعي ضابط الشرطة القضائية على إثر قيامه بعمليات المراقبة تحري السرعة في تحرياته وذلك نظرا للطبيعة التي تختص بها الانترنت من سرعة تغيير المعلومات وزوالها، حيث أن كل ما يكتب في منتديات الانترنت لا يتم الاحتفاظ به لفترات طويلة، وحتى ولو تم أرشفة المعلومات القديمة وحفظها فأحيانا لا تتوافر الأدوات اللازمة للبحث والتنقيب في هذا الأرشيف بحثا عن المعلومات التي قد تفيد التحقيق. [45] ص33

2.2.مرحلة التحقيق في الجرائم المعلوماتية

تعتبر مرحلة التحقيق مرحلة هامة من مراحل الدعوى الجزائية، إذ تهدف إلى إثبات وقوع الجريمة و الوصول إلى الحقائق كما حدثت، و استجلاء الحقيقة و كشف أسرار الجريمة و معرفة الأطراف المشاركة و المساعدة في التنفيذ و زمن وقوع الجريمة و الأسلوب المستخدم، و ذلك من خلال إجراءات مشروعة قانونا[83] ص20.فهي بمثابة مرحلة تحضيرية للمحاكمة تكفل أن تعرض الدعوى الجنائية على القضاء و هي معدة لأن يفصل فيها[61] ص501. و ما يميز هذه المرحلة في الجرائم المعلوماتية أنها تجري في بيئة رقمية، أين يتوجب التعامل مع شكل جديد من الأدلة التي يصعب اكتشافها و التي أصبحت تشكل عبئا كبيرا على جهات التحقيق، خاصة و أن هذه الأخيرة لا تملك من الخبرة و المعرفة في مجال التقنية المعلوماتية إلا القليل جدا، الأمر الذي أصبح يدعو إلى ضرورة تشكيل فريق متكامل من خبراء وفنيين في مجال الحواسب الآلية إلى جانب جهات التحقيق، و تزويد هذه الأخيرة بالمهارات و الوسائل اللازمة للتحقيق في هذا النوع من الجرائم ، فضلا على ضرورة تطوير الإجراءات التقليدية للتحقيق في الجرائم بما يتلاءم وطبيعة الجرائم المعلوماتية و تعقيدها. و هذا ما سنحاول التطرق

إليه من خلال هذا المبحث، الذي سنقسمه إلى ثلاث مطالب، نتطرق في المطلب الأول لجهات التحقيق في الجرائم المعلوماتية، ثم نتناول في المطلب الثاني البرمجيات المساعدة في التحقيق في الجرائم المعلوماتية، لننتهي في المطلب الثالث للحديث عن إجراءات التحقيق في هذا النوع من الجرائم.

1.2.2.جهات التحقيق في الجرائم المعلوماتية

جرت العادة في مختلف التشريعات على إسناد مهمة التحقيق في الجرائم إلى فرد واحد، غير أن التحقيق في الجرائم المعلوماتية أصبح أكبر من أن يدركه شخص واحد بمفرده، نظرا لكون التحقيق في مثل هذه الجرائم أصبح يتطلب مهارات وقدرات فنية عالية، لا يمكن أن تجتمع في فرد واحد، لذلك فإن تشكيل فريق يجمع بين الجانب التقني والجانب القانوني أصبح أمرا متطلبا وبشدة، وهذا ما سنحاول تبيانه من خلال تقسيم هذا المطلب إلى فرعين، نتناول في الفرع الأول المحقق في الجرائم المعلوماتية ثم نتناول في الفرع الثاني فريق التحقيق في هذا النوع من الجرائم.

1.1.2.2.المحقق في الجرائم المعلوماتية

المحقق هو ذلك الشخص المكلف بالتحقيق في الجريمة واكتشاف جميع جوانبها الغامضة والقيام بما يلزم من إجراءات قانونية لجمع الأدلة وإلقاء القبض على فاعلها أو فاعليها وتقديمهم للعدالة[84] ص34، وهو بذلك يلعب دورا هاما في إثبات الجريمة، حيث تناط به مهمة فحص الأدلة وتمحيصها للقول بكفايتها أو عدم كفايتها للاتهام .وقد اختلفت التشريعات في تحديد شخص المحقق، فمنها من جمعت سلطتي الاتهام والتحقيق في شخص واحد، فأسندت مهمة التحقيق في الجرائم إلى النيابة العامة كالمشرع المصري مثلا، حيث تنص المادة 199 من قانون الإجراءات الجنائية المصري "النيابة العامة تباشر التحقيق في مواد الجنح والجنايات طبقا للأحكام المقررة لقاضي التحقيق..." ، ومنها من أخذت بمبدأ الفصل بين سلطتي الاتهام والتحقيق، فأسندت هذه المهمة لقاضي فرد سمي بقاضي التحقيق كالمشرع الجزائري، حيث تنص المادة 68 فقرة 1 من قانون الإجراءات الجزائية الجزائري "يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي...".

إن المشكلة الأساسية التي تواجه المحقق في الجرائم المعلوماتية هي خلفية المحقق نفسه. فمتخصصي الحاسوب قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على

تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم إلى المحاكمة، ففي كثير من الأحيان نجد متخصص الحاسوب يظن أن لديه الدليل الحاسم، ولكن من الناحية القانونية يتبين أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحقق ذو الخلفية القانونية قد تكون لديه خبرة واسعة في التحقيق، ولكن يفتقد المعرفة الكافية بتقنيات الحاسوب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[44]ص222،221.ولهذا أصبح من اللازم أن يجمع المحقق في الجرائم المعلوماتية بين المعرفة القانونية وكذا المعرفة التقنية، حتى يتسنى له أداء مهمته بأكمل وجه، وعليه يمكن القول أن المحقق الكفء في الجرائم المعلوماتية هو المحقق الذي تجتمع فيه مجموعة من الصفات منها ما هي عامة يشترك فيها مع غيره من المحققين، ومنها ما هي خاصة ومن متطلبات التحقيق في الجرائم المعلوماتية .

1.1.1.2.2.الصفات العامة للمحقق في الجرائم المعلوماتية

هي الصفات الأساسية التي يتوجب توافرها لدى أي محقق، ومن أهمها:

1.1.1.1.2.2. الإيمان بضرورة التحقيق

إن الشرط الرئيسي لنجاح المحقق في أداء مهامه اقتناعه بضرورة التحقيق واعتقاده الراسخ بأن الغرض من الإجراءات التي يتخذها ضد المتهمين أو في صالحهم بالنسبة للقضايا التي تعرض عليه، هو الكشف عن الحقيقة وإقرار العدالة، لذلك يجب أن يكون مؤمنا برسالته في استظهار الحقيقة، وأن يعتقد أن الوصول إلى معرفتها هو هدفه وغايته المنشودة[85] ص 72، كما يجب أن يدرك دائما انه في حالة صراع دائم ومستمر بينه وبين المجرم المعلوماتي، فالأول ينشد الحقيقة والثاني يجتهد في تضليل العدالة و طمس الحقائق والأدلة [34] ص95 . كما على المحقق أن لا يكون من الذين يأخذون بالظاهر و يبنون اقتناعهم على الأقاويل العامة أو الخاصة، بل يجب أن يؤمن بضرورة الوقوف على الحقيقة بكشفها من خلال السبل العلمية و التقنية التي مارسها و تدرب عليها.

2.1.1.1.2.2.قوة الملاحظة والذاكرة القوية

قوة الملاحظة هي المعرفة الدقيقة والسريعة لتفاصيل الأشياء التي تقع تحت إحدى الحواس[86] ص307، فينبغي أن يكون المحقق قوي الملاحظة سريع الإدراك والفهم وأن تتصف ملاحظته بالدقة والموضوعية والشمول بكافة العناصر المكونة للموقف، و يساعده على ذلك النظر إلى الأحداث نظرة كلية إجمالية واعية[87] ص307. كما يجب أن ترافق قوة

الملاحظة الذاكرة القوية حتى يستطيع المحقق أن يتذكر جميع الأحداث و الخطوات التي عاشها لقضية معينة قد يطول أمر التحقيق فيها، دون حاجة للرجوع لمحضر التحقيق، وبالتالي يستطيع ربط الأحداث مع بعضها البعض [84] ص38 ،وهو الحال في الجرائم المعلوماتية التي غالبا ما يتطلب التحقيق فيها وقتا طويلا بسبب التعقيد الذي يكتنفها.

3.1.1.1.2.2.الدقة والترتيب

يجب أن تسيطر الدقة والترتيب على أفكار المحقق وأعماله، فيقوم بفحص كافة الجزئيات التي لها علاقة بالجريمة، ولا يترك أي صغيرة لها علاقة، إلا وألقى عليها نظرة فاحصة، ويكون عمله بالترتيب والتسلسل وفقا لإجراءات التحقيق حتى يكون العمل متماسكا ومترابطا لا خلل فيه[83] ص24، ولعل أكثر مرحلة تقتضي إعمال المحقق لهذا الترتيب هي مرحلة المعاينة، حيث يتم الانتقال في معاينة الأماكن من الأكبر إلى الأصغر، أي من الشارع محل الجريمة إلى المبنى محل الجريمة إلى الشقة محل الجريمة، وهكذا حتى الوصول إلى الهدف .

4.1.1.1.2.2.السرعة في القيام بالأعمال

يقتضي أن يكون المحقق سريعا في اتخاذ الإجراءات، لأن التأخر في ذلك من شأنه أن يؤدي في الكثير من الأحيان إلى ضياع الدليل، خاصة وأن الدليل في الجرائم المعلوماتية - كما سبق الإشارة إليه - دليل سهل المحو و التدمير، ولذلك فعلى المحقق و فور علمه بوقوع الجريمة، التحرك فورا و انجاز الأعمال، فلا يترك أي إجراء يستوجبه التحقيق إلا وقام به. ولعل من ابرز الأمور التي تتطلب السرعة في الانجاز وعدم التأخير ما يلي: [83] ص 25

- الانتقال إلى مكان الجريمة.
- سرعة اخذ أقوال الشهود والمجني عليه أو عليهم.
- القبض على المتهم واخذ أقواله.
- انجاز أعمال التحقيق الأخرى.

5.1.1.1.2.2.الثقافة القانونية

لابد أن يكون المحقق ملما بالقواعد النظرية والتطبيقية للإجراءات الجزائية خاصة منها ما يتعلق بالتحقيق الابتدائي، من مراعاة حقوق الدفاع ومباشرة الإجراءات اللازمة بصفة

صحيحة، واتخاذ التدابير الاحتياطية المناسبة وتجنب حالات البطلان وكيفية إصدار الأوامر القضائية وتحريرها وسلوك الطعن فيها ومدى خضوعها للرقابة، كما يجب أن تكون له المؤهلات الكافية في القانون الجنائي العام والخاص حتى يتمكن من تحديد مسؤولية الجاني وتكييف الوقائع المنسوبة إليه والتصرف فيها وفقا للقانون[85]ص73، خاصة وأن الجرائم المعلوماتية تعتبر نوع مستحدث من الجرائم التي تتطلب من المحقق أن يكون على اطلاع دائم بما يستجد في هذا المجال.

2.1.1.2.2.الصفات الخاصة بالمحقق في الجرائم المعلوماتية

إن الطبيعة المعقدة للجرائم المعلوماتية، أصبحت تقتضي من المحقق أن يتوافر على صفات خاصة للتحقيق في هذا النوع من الجرائم، ولعل من أهم هذه الصفات ما يلي

1.2.1.1.2.2.الإلمام بقوانين المعاملات الالكترونية وتكنولوجيا المعلومات

لا يكفي أن يكون المحقق ملما بالقوانين الجنائية التي يتشكل منها التحقيق الجنائي، بل عليه أن يستزيد من المعلومات العامة وسائر العلوم الأخرى التي تتصل بمهنته، سواء اتصالا مباشرا أو غير مباشر، لا سيما القوانين المتعلقة بتكنولوجيا المعلومات والاتصالات وشبكة الانترنت[34] ص118 لأن ذلك يساعده في التعرف على ما يعتبر من الأعمال مجرما في مجال التقنية المعلوماتية، وما يعتبر مباحا منها .

2.2.1.1.2.2.الإلمام ببعض العلوم الحديثة في مجال الحاسوب والأدلة الرقمية

يقتضى من المحقق في الجرائم المعلوماتية إلى جانب ما يكتسبه من معرفة بمختلف العلوم كعلم الإجرام وعلم العقاب وغيرها من العلوم التي تكون له سندا في إجراءاته ،أن يلم ببعض العلوم الحديثة المتصلة بتكنولوجيا المعلومات كعلوم الحاسوب وعلوم الأدلة الجنائية وعلوم التحليل السلوكي للأدلة الرقمية، حيث أن علوم الحاسوب تقدم المعلومات التكنولوجية الدقيقة، وهي مطلوبة لفهم المظهر أو الهيئة أو الكينونة الفريدة للدليل الرقمي، بينما علوم الأدلة الجنائية من شأنها أن تقدم مظهرا علميا لتحليل أي شكل من أشكال الأدلة الرقمية، وتساهم علوم التحليل السلوكي للأدلة الرقمية في الربط المحدد بين المعارف التكنولوجية وبين الطرق العلمية لاستخلاص الدليل الرقمي، لفهم أفضل للسلوك الإجرامي التقني.[53] ص90

3.2.1.1.2.2.معرفة أساسيات التعامل مع التقنية المعلوماتية

لا بد أن يكون المحقق في الجرائم المعلوماتية على معرفة بكيفية التعامل مع الحاسوب وشبكاته، وعلى دراية بأهم تقنيات أمن المعلومات وطريقة عملها، لأن هذه المعرفة والدراية تساعد المحقق على استيعاب أفضل للجريمة المرتكبة و الوسائل المستخدمة في ارتكابها، كما قد تجنبه الوقوع في أخطاء قد تكلفه فقدان أدلة الجريمة وضياعها.

4.2.1.1.2.2.القدرة على التخطيط

التخطيط هو النشاط الذي يقرر من خلاله المحقق ما يريد أن يعلمه وماذا يجب عمله وأين ومتى وكيف وبوساطة من وما هي الإمكانيات المطلوبة لأداء البحث والتحري عن هذه الجرائم[84] . وعلى ذلك فإن المحقق في الجرائم المعلوماتية لابد أن يكون قادرا على تحديد الأسلوب الأمثل للتعامل مع هذا النوع من الجرائم، ومن أهم المرتكزات التي عليه أخذها بعين الاعتبار والتي تساعده في تحديد الخطة المناسبة للتحقيق في الجرائم المعلوماتية ما يلي:[45] ص13

- حجم ونوع الحادث الذي يكون المحقق بصدد التحقيق فيه.
- بعض الظروف المحيطة بالحادث:
  - مدى أهمية الأجهزة والشبكات المتضررة.
  - مدى حساسية البيانات التي يحتمل أنها سرقت أو أتلفت.
  - من هم المتهمون المحتملون.
  - اطلاع الرأي العام عن الجريمة أم لا .
  - مستوى الاختراق الأمني الذي تسبب فيه الجاني.
  - مستوى المهارة الفنية التي يبدو أن الجاني يتمتع بها .
- تحديد طبيعة مسرح الجريمة وذلك لتحديد الأسلوب الأمثل للتفتيش بحثا عن الأدلة التي تكون موجودة فيه، والذي يعد من أهم خطوات عملية التحقيق، وعدم نجاح المحقق في تحديد هذا الأسلوب قد يؤدي إلى عدم الحصول على أية نتائج أو إلى الحصول على كم كبير من النتائج التي لا فائدة منها.

إن توفر الصفات السابقة الذكر في المحقق، لا يكون إلا بالتكوين الخاص له، حتى يكون أهلا للتحقيق في هذا النوع المستحدث من الجرائم و بالكفاءة اللازمة.

2.1.2.2.فريق التحقيق في الجرائم المعلوماتية

لا يمكن للمحقق مهما بلغت خبرته ومهما بلغت كفاءته المعرفية، أن يعمل بمفرده بل إنه دائما في حاجة إلى أشخاص يعاونونه في أدائه لعمله [86] ص310، وهذه الحاجة تظهر أكثر أثناء التحقيق في جريمة من الجرائم المعلوماتية، فالمحقق لازال غير قادر بعد على التعامل بالشكل الجيد وبالمهارة اللازمة مع هذا النوع من الجرائم، ذلك أنه إذا كان ملما بأصول التحقيق في مختلف الجرائم والقواعد الإجرائية المعتمدة في ذلك، فإنه قد لا يكون ملما بأصول التعامل مع الحواسب الآلية وشبكاتها، وبالتالي قد لا يدرك تماما ماهية الأدلة التي يسعى إليها، بينما هناك أخصائيون في الحاسوب الآلي ذوو معرفة واسعة بتقنية المعلومات وشبكات الاتصال، يعرفون أصول التعامل مع الحواسب وكيفية عملها، إلا أنهم يفتقدون المعرفة القانونية التي تكفل المحافظة على شرعية الأدلة وقيمتها أمام القضاء.

وعلى ذلك وأمام غياب المعرفة التقنية لدى المحقق وغياب المعرفة القانونية لدى أخصائيي الحواسب الآلية، أصبح من الضروري تشكيل فريق عمل يجمع بين المعرفة التقنية والمعرفة القانونية، تكون مهمته الأساسية البحث عن الأدلة التي تثبت الجريمة المعلوماتية بحق مرتكبيها، وذلك وفق سياسة عمل واضحة يكتنفها التنظيم والتنسيق بين أفراد الفريق.

إن فريق العمل في الجرائم المعلوماتية يتكون من أشخاص يتصل علمهم مباشرة بالجريمة المعلوماتية، ولا يمكن التحقيق في أي جريمة تنتمي لهذه الفئة من الجرائم إلا بهم، فوجودهم ضروري في مسرح الجريمة، وتتوافق خبرتهم مع الطبيعة المميزة لهذا النوع من الجرائم [45]ص17، فضلا عن بعض الأشخاص الذين يقتضي أي مسرح جريمة تواجدهم. وعلى ذلك يمكن تحديد أعضاء فريق التحقيق في الجرائم المعلوماتية، كما يلي:

1.2.1.2.2.قائد الفريق

إن من أهم الأمور في توجيه عمل مجموعة من الناس أن تتوافر لهم وحدة القيادة وهي القيادة على التوجيه و السير بالفريق في اتجاهات واضحة و محددة المعالم[84] ص99، وقائد فريق التحقيق في الجرائم المعلوماتية هو المحقق الجنائي الذي له خبرة طويلة في مجال التحقيق الجنائي، و لديه معرفة جيدة بالطبيعة الخاصة للجرائم المعلوماتية، و تلقى دورات تدريبية كافية عن الحاسوب و الشبكات، حيث يتولى السيطرة بشكل كامل على مسرح الجريمة و توزيع المهام على الفريق ورسم خطة و إستراتيجية العمل و الإشراف على قيامهم بأعمالهم و توزيع الأدوار

بينهم، و التنسيق مع الجهات ذات العلاقة و اتخاذ كافة القرارات المتصلة بالتحقيق [78] ص04 ، و كل ذلك في إطار من النزاهة و التجرد.

2.2.1.2.2.خبير حاسوب وشبكات

إن الأقراص الصلبة ، الطابعات و باقي مكونات الحاسوب الآلي قد تتلف بسرعة إذا لم يتم معالجتها بالشكل الصحيح [85] ص25 ، الأمر الذي يقتضي وجود شخص لديه خبرة و معرفة في علوم الحاسوب و الشبكات مع الإلمام بإجراءات التحقيق الجنائي و أساليبه و كيفية التعامل مع مسرح الجريمة، و يكون مسؤولا عن رفع و تحريز الأدلة الجنائية الرقمية بالطريقة المناسبة فنيا التي لا تؤثر على سلامة الدليل و صلاحيته لإقامة الدعوى و العرض في المحكمة . [45] ص18

3.2.1.2.2.خبير تدقيق حسابات

إن العديد من الجرائم المعلوماتية التي ترتكب كجرائم التحويل الالكتروني غير المشروع للأموال مثلا ، و التي يستخدم فيها المجرمون وسائل تقنية عالية الكفاءة يصعب من خلالها اكتشاف ما يشوب حسابات العملاء من خلل، تقتضي وجود خبير تدقيق حسابات. وخبير تدقيق الحسابات هو شخص متخصص في المراجعة المحاسباتية ،وعلى درجة من الخبرة في التعامل مع الأنظمة البرمجية المستخدمة، التي يتم بواسطتها تبادل النقد الالكتروني .وهو يعمل مع خبير الحاسوب والشبكات على تحديد أسلوب الجريمة وما إذا كان هناك تلاعب في الأنظمة المتضررة، بالإضافة إلى تحديد الحجم التقريبي للخسائر المادية الناجمة عن الحادث.[78] ص04

4.2.1.2.2.خبير تصوير

في الكثير من الأحيان يكون التصوير مفيدا للتحقيق فهو ليس مجرد وسيلة لتوثيق مسرح الجريمة فحسب، وإنما من خلاله قد يجد المحقق العديد من الأجوبة لتساؤلاته[85] ص23، فالتصوير يعتبر من الأركان الهامة في المعاينة الفنية الحديثة، لأن أجهزة التصوير تكون أوضح في نقل جزئيات مسرح الجريمة من الكتابة التي تعتمد اعتمادا كليا على العنصر البشري، ولهذا فهي تقدم للمحقق صورة واضحة وحقيقية لمكان الحادث بعد ارتكاب الجريمة[86] ص116، وبالتالي فإن وجود خبير تصوير مهم جدا في مسرح الجريمة، حيث يتولى مهمة تصوير كل المواقع داخل مسرح الجريمة وخارجه وتصوير أدلة الجريمة مع

الاهتمام بشكل خاص بتصوير الأجزاء الخلفية للحاسوب الآلي وشاشاته وكذا جميع ملحقاته وذلك بالوضع الذي تم العثور عليها فيه.

5.2.1.2.2.خبير رسم هندسي

إن الرسم الهندسي يكمل الوصف بالكتابة والصورة الفوتوغرافية ويظهر ما تعجز عن إيضاحه، كبيان العلاقة بين شيئين عن طريق بيان حجمهما وتحديد أبعادهما و المسافة بينهما، كما أنه يجمع مكان الجريمة جمعا شاملا في مساحة صغيرة [87] ص67، وهذا ما يساعد على إعطاء نظرة كاشفة لموقع الجريمة، ولهذا أصبح من الضروري الاستعانة بخبير رسم هندسي. وهو ذلك الذي يقوم بعمل رسم تخطيطي لمسرح الجريمة بطريقة فنية دقيقة مستخدما مقياسا مناسبا للرسم، بما يوضح تقسيماته و أماكن تواجد الأدلة والأشخاص فيه.[69] ص78

6.2.1.2.2.خبير بصمات

إن تواجد خبير في رفع البصمات بأنواعها المختلفة، حسب ما وصل إليه علم التحقيق الجنائي كبصمات العين، و نفس الإنسان، و صوته و رائحته إلى جانب بصمات أنامله بمسرح الجريمة، يكتسي أهمية في معظم الجرائم وليس فقط في الجرائم المعلوماتية، فمن خلال ما يقوم برفعه من بصمات يتم تحديد الفاعل مرتكب الجريمة، على أن يركز الخبير اثر التحقيق في جريمة من الجرائم المعلوماتية على رفع جميع البصمات من على مختلف مكونات الحاسوب المادية وكذا جميع ملحقاته.

2.2.2.البرمجيات المساعدة في التحقيق في الجرائم المعلوماتية

إن التحقيق في مختلف الجرائم ، غالبا ما يحتاج إلى مجموعة من الأدوات والوسائل التي تساعد في جمع الأدلة وتحريزها كأدوات رفع البصمات، وأدوات رفع آثار الأقدام وغيرها من الوسائل التي تستعين بها جهات التحقيق وهي بصدد التحقيق في جريمة من الجرائم .وبظهور الجرائم المعلوماتية ظهرت إلى الوجود أدوات ووسائل جديدة تتناسب وطبيعة هذه الجرائم، ذلك أن التحقيق فيها يتم في بيئة رقمية، حيث تجد جهات التحقيق نفسها وسط كم هائل من البيانات التي يحتاج استخراج الأدلة منها إلى وسائل خاصة ذات طابع فني محض، تتمثل في مجموعة من البرمجيات التي غالبا ما تستخدم في بنية نظم المعلومات. حيث تلعب هذه الأخيرة دورا كبيرا في مساعدة جهات التحقيق على جمع الأدلة في البيئة الرقمية بشكل سريع ودقيق، وهي على نوعين منها ما هو خاص بأمن المعلومات ومنها ما هو خاص بالتحقيق في الجرائم

المعلوماتية .وعليه سنقسم هذا المطلب إلى فرعين نتطرق في الفرع الأول إلى البرمجيات الخاصة بأمن المعلومات، ونتعرض في الفرع الثاني إلى البرمجيات الخاصة بالتحقيق في الجرائم المعلوماتية.

1.2.2.2.البرمجيات الخاصة بأمن المعلومات

هي مجموعة من البرمجيات التي تهدف إلى حماية الشبكات من الاعتداء عليها ، و في سبيل ذلك تقوم بمراقبة العديد من الأنشطة و العمليات الحاسوبية التي تجري فيها و تحتفظ بها في سجلات خاصة، بحيث يجد فيها فريق التحقيق الكثير من المعلومات التي قد تساعد في جلاء غموض الجريمة [45] ص23. و لعل من أهم هذه البرمجيات ما يلي :

1.1.2.2.2.الجدار الناري

هو نوع من البرامج التي تعمل على حماية الحواسب و الشبكات من خلال تقنين و ضبط الاتصالات الحاسوبية الصادرة عنها و الواردة إليها، و قد يكون الجدار الناري على شكل برنامج يركب على نفس الحاسوب المطلوب حمايته أو يركب على صناديق الكترونية مستقلة يتم ربطها بالشبكة، و جعل جميع الاتصالات الحاسوبية تمر من خلالها، حيث يتم تطبيق شروط معينة على جميع حزم البيانات، بحيث يتم تحديد الحزم التي يمكن أن تنتقل من إحدى جهات الجدار الناري إلى الجهة الأخرى[69] ص86. فانتقال الحزم يترك آثارا يمكن أن نتعرف من خلالها على الجهاز الذي اتصل أو اخترق الموقع.

و على ذلك فإن هذا البرنامج يقوم بعملية مسح للمعلومات التي تصل من شبكة الأنترنت و يقوم بتحليلها، و عندما يجد أي شك في المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة، فإنه يقوم بمنع هذه المحاولة وطرحها خارج الشبكة، أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول على أجهزة الحواسب الآلية[33] ص158.وأثناء تولي هذا البرنامج لهذه المهمة يقوم بتوثيق عمليات الاتصال الخارجة والداخلة، وإنشاء سجلات توضح مصدر وجهة كل اتصال منها، بحيث تحفظ هذه السجلات على شكل ملفات حاسوبية يمكن الرجوع إليها وقراءتها في أي وقت[45] ص24. ولذلك فإن هذا البرنامج يساعد بشكل كبير فريق التحقيق، فمن خلال ما يقوم بتوثيقه من معلومات يمكن التعرف على مصدر الاتصال الذي يقف وراء الجريمة وبالتالي معرفة مرتكبيها.

2.1.2.2.2.الخادم الوكيل

هو نوع من البرامج يعمل على التحكم في سير الاتصالات بين شبكة الانترنت وبين الشبكة الداخلية المحلية، ويمكنه القيام بمهام أخرى كإخفاء البيانات ومراقبة عمليات اختراق المواقع[88] ص441، وتعتبر من المهام الرئيسية التي يمكن إعداد هذا البرنامج للقيام بها، القيام بدور المخزن الوسيط للبيانات الواردة من الانترنت أو ما يعرف ب " Cache" وهذا المخزن يحوي نسخة من كل ملف أو صورة، قام مستخدمو الشبكة التي يقدمها هذا النوع من الخوادم بتحميلها من الانترنت، وذلك بهدف تخفيف الضغط على وصلة الانترنت، وتحسين الأداء العام للشبكة بالإضافة إلى تلبية بعض طلبات المستخدمين لصفحات متوفرة لدى الخادم ،وذلك في حالة انقطاع اتصال الشبكة كليا بالانترنت. وفي هذا المخزن الوسيط قد يجد المحقق الكثير من الأدلة التي ربما تم حذفها عمدا من الحواسب الأخرى.[45] ص25،24

3.1.2.2.2 نظام كشف الاختراق

هذه الفئة من البرمجيات تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة. ويتم ذلك من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات التشغيل الخاصة بتسجيل الأحداث فور وقوعها في جهاز الحاسوب الآلي أو الشبكة، ومقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، والتي يطلق عليها أهل الاختصاص مصطلح التوقيع. وفي حالة اكتشاف النظام وجود أحد التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة[34] ص307،306. ويمكن أن تقدم هذه السجلات معلومات قيمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها.[69] ص88

4.1.2.2.2.نظام جرة العسل

هو نظام حاسوبي يتم تصميمه خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة، دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الاعتداء على هذا النظام ،و ذلك بهدف إغرائه بمهاجمته، ليتم منعه من الاعتداء على أي حاسوب أخر في الشبكة ،في الوقت الذي يتم فيه جمع أكبر قدر ممكن من

المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء وتحليلها ومن ثم اتخاذ إجراء وقائي فعال[89] ص40، وهذه المعلومات التي يتم جمعها تفيد في تحليل أبعاد الجريمة في حالة وقوعها وتمد فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.[69] ص88

5.1.2.2.2.أداوت تدقيق ومراجعة العمليات الحاسوبية

هي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجلها في ملفات خاصة يطلق عليها (logs)، والكثير من هذه الأدوات مضمنة في أنظمة التشغيل المختلفة، وبعضها يأتي كبرامج مستقلة يتم تركيبها على أنظمة التشغيل بعد إعدادها للعمل، وكل ما يحتاج إليه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها وإعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة، حتى يتمكن من تسجيل المعلومات التي قد يكون لها علاقة بالحادثة، وربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبها. [45] ص26

2.2.2.2.2.البرمجيات الخاصة بالتحقيق في الجرائم المعلوماتية

هي مجموعة من البرمجيات التي يستعين بها فريق التحقيق من اجل البحث عن الأدلة الرقمية الموجودة على الحواسب الآلية وكذا شبكات الاتصال، وكذا في جمع المعلومات التي تفيد في إثبات الجريمة واسترجاع أدلتها في حالة تلفها. وهذه البرمجيات متعددة ومتنوعة ولعل من أهمها:

1.2.2.2.2.برمجيات التتبع

تقوم هذه البرمجيات بالتعرف على محاولات الاختراق التي تتم، وتقديم بيان شامل لها إلى المستخدم الذي تم اختراق جهازه، ويحتوي هذا البيان على اسم الحدث وتاريخ حدوثه وعنوان IP الذي تمت من خلاله عملية الاختراق واسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الانترنت ومعلومات أخرى[34] ص306، ومن الأمثلة على هذا النوع من البرامج برنامج « HACK TRACER » وهو مصمم للعمل في الأجهزة المكتبية وساكنا في خلفية سطح المكتب، وعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسوب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق، ثم يبدأ في عملية مطاردة تستهدف اقتفاء أثر مرتكب عملية الاختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله[90] ص100.فهذه البرمجيات تساعد فريق التحقيق في معرفة المخترق للموقع أو المحاول اختراقه، و بالتالي اكتشاف المجرم.

2.2.2.2.2.برمجيات البحث عن البيانات و استرجاعها

إن برمجيات البحث عن البيانات هي برمجيات تساعد على البحث على الملفات التي تتواجد بها بيانات معينة، بحيث تعمل على إيجاد البيانات المراد البحث عنها من قبل فريق البحث، و هي بذلك توفر الكثير من الوقت و الجهد، مثال ذلك برنامج(Xtree Pro Gold) و هو برنامج معالجة ملفات يمكن من خلاله العثور على الملفات من أي مكان على الشبكة أو على القرص الصلب، كما يستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة، و كذا لقراءة البرامج في صورتها الأصلية، كما يمكن استخدامه للبحث عن كلمات معينة أو عن أسماء ملفات أو غير ذلك . [44] ص228

بالإضافة إلى هذه البرمجيات يوجد برمجيات استعادة البيانات المحذوفة، إذ يعتقد الكثير من مرتكبي الجرائم المعلوماتية أن حذف ملف يعني انه تم محوه تماما من القرص الصلب ، و هذا الاعتقاد خاطئ، إذ أن البيانات المخزنة في هذه الملفات تبقى على القرص الصلب حتى و لو تم إعادة تهيئته، و من الممكن استعادتها مرة أخرى[69] ص86. فهذا النوع من البرمجيات هي وسيلة للتعرف على المعتدي على نظام جهاز الحاسوب الآلي ،و بالتالي تعد دليلا كاشفا على المجرم.

3.2.2.2.2.برمجيات عرض الصور و محتوى الملفات المختلفة

هي عبارة عن برمجيات تسمح باستعراض مختلف الصور و الملفات الموجودة على أجهزة الحاسوب ، فبرنامج عرض الصور يمكن أن يقدم خدمة جيدة للمحققين من خلال تمكينهم من مشاهدة و استعراض الصور الرقمية المخزنة داخل الحواسب أو وسائط التخزين الخارجية، و تبرز الحاجة لهذه البرمجيات في جرائم حيازة و نشر مواد و صور ذات طابع إباحي. كما أن برمجيات عرض الملفات بدورها قد تكون عونا كبيرا لهم ، من خلال قدرتها على تمييز محتوى مئات الصيغ المختلفة للملفات و من أشهرها برنامج (Quick View Plus) الذي يستطيع تمييز و عرض محتوى 225 مستند مختلف ، ثم إنشاؤها باستخدام برامج إنشاء المستندات المختلفة. [45] ص28

4.2.2.2.2.برمجيات ضغط و فك ضغط الملفات

توفر تقنيات الحاسوب إمكانية أرشفة الملفات المختلفة من خلال تجميع عدة ملفات في ملف واحد و ضغط هذا الملف و تحويله إلى صيغة أخرى خاصة بنظام الأرشفة، مع محاولة

تصغير حجم هذا الملف من خلال استخدام تقنيات الضغط الرقمية ، و حتى يتمكن فريق التحقيق من معرفة محتوى هذه الملفات المضغوطة، يجب أن يتمكن من فك الضغط و تحرير الملفات الموجودة داخل الأرشيف الكبير، ثم محاولة معاينة محتوى كل ملف منها لاستخراج أي أدلة جنائية رقمية قد تكون موجودة فيها[69] ص91. من أشهر هذه البرمجيات ما يعرف ببرنامج (Winrar) .

5.2.2.2.2.برمجيات كسر كلمات المرور والمستندات

يلجأ العديد من المجرمين إلى إحاطة ملفاتهم و مستنداتهم بنوع من الحماية، و ذلك من خلال وضع كلمات مرور تمنع أي كان من الاطلاع على محتوياتها ما لم يحصل على كلمة المرور التي تسمح بفتح هذه المستندات أو الملفات ، و لهذا قد يجد فريق التحقيق نفسه أمام مستندات محمية لا يمكن فحصها إلا بعد نزع الحماية عنها، فيمكنهم من خلال استخدام برامج كسر كلمات المرور إزالة هذه الحماية، و من ثم اختراق ملف المعتدي و الاطلاع على المستندات التي قد تشكل دليلا هاما في الدعوى. و من بين هذه البرمجيات يوجد برنامج (Password Recovery Suit).

3.2.2.إجراءات التحقيق في الجرائم المعلوماتية

إجراءات التحقيق هي مجموعة الإجراءات التي تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت و تجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة[61] ص501، و إجراءات التحقيق التي أوردها القانون هي المعاينة، التفتيش، الضبط، سماع الشهود، الاستجواب و الخبرة، و لم يلزم القانون في مباشرتها ترتيبا معينا، فجهات التحقيق لها أن ترتب هذه الإجراءات بما يتلاءم و طبيعة الجريمة المرتكبة، فهي غير ملزمة أساسا بمباشرتها جميعها، بل لها أن تباشر منها فقط ما تراه ضروريا لمصلحة التحقيق . و على الرغم من العقبات التي تعترض اتخاذ هذه الإجراءات في مجال الجرائم المعلوماتية- و التي سبق و ذكرناها- إلا أنها تبقى تلعب دورا هاما في إثبات هذا النوع من الجرائم، مع الأخذ بعين الاعتبار ضرورة تطويرها بما يتلاءم و طبيعة هذه الجرائم المستحدثة التي تتطلب من جهات التحقيق معاملة خاصة . و عليه سنحاول التطرق في هذا المطلب إلى هذه الإجراءات و ذلك في أربع فروع ، نتناول في الفرع الأول إجراءات المعاينة في الجرائم المعلوماتية ، ثم نتناول في الفرع الثاني إجراءات التفتيش و الضبط فيها، و من ثم نتطرق في الفرع الثالث إلى سماع

الشهادات والقيام بالاستجوابات في هذا النوع من الجرائم، لنصل في الفرع الأخير للحديث عن الخبرة في هذه الجرائم.

1.3.2.2.إجراءات المعاينة في الجرائم المعلوماتية

إن مسرح الجريمة هو الساحة التي ينشدها الباحث و المحقق الجنائي ليصل إلى ضالته في الكشف عن غموض الحادث الإجرامي و معرفة كيفية وقوعه ليصل إلى الأدلة المادية التي تؤدي إلى الإيقاع بالجاني[53] ص127، و إذا كان للجرائم التقليدية دائما مسرحا تجري عليه الأحداث و تترك عليه آثارها المادية، مما يتيح الفرصة عن طريق المعاينة، للكشف عن الآثار المادية التي خلفها ارتكاب الجريمة و التحفظ على الأشياء التي تفيد في كشف الحقيقة بصدد الجريمة المرتكبة، فالأمر على غير ذلك في الجرائم المعلوماتية حيث لا يوجد لها مسرحا بهذا المعنى، إلا إذا اعتبرنا المكتب الذي توجد فيه الأجهزة و الأنظمة المعلوماتية التي كانت محلا للجريمة وأدواتها مسرحا لها[91] ص03، ولهذا فكما سبق وذكرنا، فإن المعاينة لا تكتسي ذات الأهمية التي تكتسيها في الجرائم التقليدية، ولكن ورغم ذلك فإنها قد لا تخلو من فائدة في الكشف عن بعض الأدلة، إذا تمت وفق ما تقتضيه طبيعة الجرائم المعلوماتية. و على ذلك نجد القانون أعطى جهات التحقيق صلاحية الانتقال والقيام بالمعاينات اللازمة التي قد تفيد في إظهار الحقيقة، فتنص المادة 79 من قانون الإجراءات الجزائية الجزائري "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات " .

وحتى تكون للمعاينة في الجرائم المعلوماتية، الفائدة المتوخاة منها في الجرائم التقليدية لابد على جهات التحقيق مراعاة مجموعة من الضوابط، وهي ذات الضوابط التي تلتزم بها جهات الضبط القضائي على اثر قيامهم بمعاينة في مثل هذه الجرائم والتي سبق وذكرناها.وعليه سنجملها فيما يلي: [55] ص317

◆تحديد أجهزة الحاسوب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع فرصة ممكنة، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف وذلك لأجل تعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها، ويراعى تصوير الأجهزة الموجودة، خاصة الأجزاء الخلفية منها، كما يجب وضع عوازل و أختام تمنع استعمال الأجهزة، لئلا يقع أي تلاعب من طمس للمعلومات أو تخريب في الجهاز.

◆ضرورة وضع حراسة كافية على مكان المعاينة ومراقبة التحركات داخل مسرح الجريمة، بل ورصد الاتصالات الهاتفية من و إلى مسرح الجريمة، مع إبطال مفعول أجهزة الهاتف المتحرك التي قد تساعد في تدمير أدلة الجريمة المعلوماتية متى تم توصيلها بالأجهزة محل المعاينة.

◆ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها ومعرفة السجلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل، وذلك عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار وبروتوكولات الاتصال عبر الانترنت إن تعلقت الجريمة بهذه الشبكة.

◆التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ومن ثم ترفع عليها البصمات ذات الصلة بالجريمة، بالإضافة إلى التحفظ على مستندات الإدخال والمخرجات الورقية للحاسوب ذات الصلة بالجريمة أيضا.[92] ص17

2.3.2.2.إجراءات التفتيش والضبط في الجرائم المعلوماتية

التفتيش إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة[93] ص544.والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة من خلالها يتم الكشف عن أدلة الجريمة، فالضبط هو غاية التفتيش القريبة أي الأثر المباشر الذي يسفر عنه هذا الإجراء[94]ص135. و على ذلك نتطرق فيما يلي إلى إجراءات التفتيش في الجرائم المعلوماتية و من ثم نتطرق لما ينجم عن هذا التفتيش من أثر، ألا و هو الضبط .

1.2.3.2.2.إجراءات التفتيش في الجرائم المعلوماتية

إن التفتيش في الجرائم المعلوماتية كما قد يقع على المكونات المادية للحاسوب، قد يقع أيضا على المكونات المعنوية له، وكذا على شبكاته.

1.1.2.3.2.2.تفتيش المكونات المادية للحاسوب الآلي

يخضع الولوج إلى المكونات المادية للحاسوب للإجراءات القانونية الخاصة بالتفتيش، أي يجب مراعاة مكان وجود ذلك الحاسوب أثناء مباشرة ذلك الإجراء، فيما إذا كان مكانا عاما أو خاصا، ذلك لأن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كان موجودا في مكان خاص كمسكن المتهم أو احد ملحقاته، كان له حكمه، فلا يجوز تفتيشه إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة[63] ص237 .و على ذلك يمكن أن نفرق بين حالتين:

◆الحالة الأولى: حيث نكون بصدد جريمة عادية، ففي هذه الحالة فإن تفتيش مكونات الحاسوب الآلي المادية يخضع للقواعد العامة في التفتيش، حيث تقضي المادة 82 من قانون الإجراءات الجزائية الجزائري، بعدم جواز تفتيش مسكن المتهم إلا بحضوره، وإن تعذر ذلك وجب على قاضي التحقيق أن يطلب منه تعيين ممثل له، وإذا امتنع عن ذلك يعين قاضي التحقيق شاهدين من غير الخاضعين لسلطته.

◆الحالة الثانية: حيث نكون بصدد جريمة معلوماتية، فإن المشرع الجزائري وسع من صلاحيات قاضي التحقيق، و أصبح له الحق في إجراء التفتيش بغير حضور المتهم وفي أي ساعة من ساعات الليل والنهار إذا تعلق الأمر بجريمة من الجرائم المعلوماتية، وبذلك يجوز لقاضي التحقيق و في حالة وجود الحاسوب الآلي في مسكن المتهم الخروج عن القواعد العامة المقررة لتفتيش مسكن المتهم . كذلك الحال في حالة ما إذا كانت الحواسب متصلة بحاسوب أو نهاية طرفية في مكان أخر كمسكن الغير مثلا، فإن قاضي التحقيق لم يعد ملزما بحضور صاحب المسكن، أو أقاربه أو أصهاره في حالة غيابه أو حضور شاهدين من غير الخاضعين لسلطة قاضي التحقيق، إذا تعلق الأمر بهذا النوع من الجرائم، و هذا ما قضت به المادة 45 من قانون الإجراءات الجزائية السالفة الذكر.

2.1.2.3.2.2.تفتيش المكونات غير المادية للحاسوب الآلي

أثار تفتيش المكونات المعنوية للحاسوب الآلي جدلا كبيرا في الفقه، فذهب رأي في الفقه إلى القول أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها، و في هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي

شيء يكون ضروريا لجمع و حماية الدليل، و يفسر الفقه اليوناني عبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة الكترونيا[46] ص372، بينما يذهب رأي أخر إلى عدم إنطباق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير الملموسة ، و لذلك يقترح مواجهة هذا القصور التشريعي بالنص صراحة على تفتيش الحاسوب، بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد، تتركز في البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسوب[34]ص198،197، و هذا ما ذهبت إليه العديد من التشريعات، حيث أجازت صراحة تفتيش نظم الحاسوب الآلي. و من بين هذه التشريعات، التشريع الجزائري حيث نظم من خلال القانون رقم 09-04 السالف الذكر، قواعد تفتيش المنظومات المعلوماتية ، فأجاز الدخول بغرض التفتيش و لو عن بعد إلى أي منظومة معلوماتية أو جزء منها، و كذا تفتيش المعطيات المخزنة بها ، و تفتيش أي منظومة تخزين معلوماتية.

3.1.2.3.2.2.تفتيش شبكات الحاسوب الآلي

إن الحديث عن تفتيش شبكات الحاسوب الآلي يقتضي التمييز بين 3 احتمالات:

◆الاحتمال الأول: اتصال حاسوب المتهم بحاسوب أو نهاية طرفية موجودة في مكان أخر داخل الدولة.

هناك من التشريعات من أجازت امتداد التفتيش إذا تبين أن الحاسوب الآلي للمتهم متصل بحاسوب آلي في مكان آخر داخل الدولة، كالتشريع البلجيكي، حيث تقضي المادة 88 من قانون تحقيق الجنايات البلجيكي بجواز امتداد التفتيش إلى نظام معلوماتي أخر غير مكان البحث الأصلي، و ذلك في حالة ما إذا كان ذلك ضروريا لكشف الحقيقة بشأن الجريمة محل البحث أو في حالة وجود مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث ، كما أجاز المشرع الجزائري ذلك في الفقرة الثانية من المادة الخامسة من القانون رقم 09-04 المشار إليه سابقا ، و ذلك في حالة وجود أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و كان بالإمكان الدخول إليها انطلاقا من المنظومة الأولى.

◆الاحتمال الثاني : اتصال حاسوب المتهم بحاسوب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة.

سبق وأشرنا إلى أن امتداد التفتيش خارج إقليم الدولة قد يثير الكثير من المشاكل ، و ذلك لما يمثله من مساس بسيادة دولة أخرى، و لهذا و تفاديا لذلك، وجب أن يتم التفتيش في حالة اتصال حاسوب المتهم بحاسوب آلي أو نهاية طرفية موجودة في مكان آخر خارج الدولة، وفقا لاتفاقيات تعاون خاصة ثنائية أو دولية. و هو ما ذهب إليه المشرع الجزائري، حيث تنص الفقرة الثالثة من المادة الخامسة السالفة الذكر على ما يلي: «إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى ، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل»

و على ذلك فإن التفتيش في الجرائم المعلوماتية يمتد ليشمل مكونات الحاسوب المادية و كذا المعنوية، بالإضافة إلى شبكاته، و هذا التفتيش يمكن أن يتم بعدة طرق، فمثلا المرشد الفيدرالي الأمريكي جاء بأربع طرق أساسية للتفتيش و هي كالأتي : [34] ص226،227

- تفتيش الحاسوب الآلي و طبع نسخة ورقية من ملفات معينة في ذات الوقت.
- تفتيش الحاسوب الآلي و عمل نسخة الكترونية من ملفات معينة في ذات الوقت.
- عمل نسخة الكترونية طبق الأصل من جهاز التخزين بالكامل في الموقع ، و بعد ذلك يتم إعادة عمل النسخة لتعمل من جهاز التخزين خارج الموقع.
- ضبط الجهاز و إزالة ملحقاته و مراجعة محتوياته خارج الموقع.

2.2.3.2.2.إجراءات الضبط في الجرائم المعلوماتية

إن الضبط و باعتباره الأثر المباشر للتفتيش، ثار بشأنه الجدل ذاته المثار بشأن التفتيش الواقع على المكونات المعنوية ، و قد سبق و أن تطرقنا إلى هذا في حديثنا عن الضبط كإجراء من إجراءات الاستدلال، و بينا ما هي الضوابط الواجب مراعاتها أثناء القيام بعملية ضبط مكونات الحاسوب الآلي سواء المادية منها أو المعنوية ، و باعتبار أن الضبط في الجرائم المعلوماتية يحتاج إلى ذات الضوابط سواء تمّ من قبل سلطات جمع الاستدلالات أو من قبل سلطات التحقيق ، فسنحيل إلى ما سبق قوله في هذا الشأن و ذلك منعا من التكرار.غير أننا ومع ذلك أثرنا إلا أن نؤكد على احتياطيين رئيسيين ، على جهات التحقيق مراعاتهما و هي بصدد تحريز المعطيات الالكترونية ،وهما: [95] ص05

◆الاحتياط الأول

هو جعل الرجوع ممكنا للمعطيات الأصلية التي أخذت عنها النسخة كلما دعت الضرورة إلى ذلك، و تظهر ضرورة هذا الاحتياط من خلال إتاحته إمكانية إثبات مطابقة النسخ المضبوطة عليها المعطيات الالكترونية للأصل.

◆الاحتياط الثاني

يتعلق بمعالجة المعطيات الالكترونية المضبوطة ، ففي الأغلب يتعين على المحقق و الخبير البحث عن المعلومات المطلوبة ضمن المعطيات المضبوطة، و يتم ذلك من خلال العديد من الإجراءات التي تحتاج إلى تحليل و معالجة للمعطيات، الأمر الذي يترتب عنه التغيير في المعطيات. لذا كان لا بد من العناية بتدوين و تصنيف هذه الإجراءات بصورة دقيقة، فمن خلال ذلك يمكن التأكد من مصداقية الدليل. و لتحقيق ذلك يتعين على المحقق المكلف بالتحقيق أن يحرص على الحصول على نسخة أخرى إضافية من المعطيات وذلك للعمل بها كدليل على إجراءات المعالجة التي وقعت على المعطيات الالكترونية.

3.3.2.2.سماع الشهادات و القيام بالاستجوابات في الجرائم المعلوماتية

استكمالا للتحقيقات التي يقوم بها المحقق في الجرائم المعلوماتية، فإن له الحق في سماع أي شخص له علاقة بالجريمة المرتكبة سواء كان شاهدا أو متهما، باعتبار أن ذلك يساهم بشكل كبير في تنوير طريقه ويساعده في تحديد ملامح القضية بشكل أكثر دقة، وذلك من خلال ما قد يتم تقديمه من معلومات تفيد في كشف غموض الجريمة.

1.3.3.2.2.سماع الشهادات في الجرائم المعلوماتية

الشهادة هي تقرير شخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه [76] ص10، وسماع الشهود كسائر إجراءات التحقيق متروك للسلطة التقديرية للمحقق، فله أن يسمع الشهود أو يستغني عنهم وفقا لمقتضيات التحقيق. ونظرا لأهمية هذا الإجراء فقد نظمته مختلف التشريعات، من ضمنها المشرع الجزائري حيث خص القسم الرابع من الفصل الأول من الباب الثالث المتضمن جهات التحقيق لإجراءات سماع الشهود وذلك في المواد من 88 إلى 99 من قانون الإجراءات الجزائية.

إن ما يميز سماع الشهود في الجرائم المعلوماتية أن الشاهد في هذا النوع من الجرائم غالبا ما يكون من ذوي الاختصاص والخبرة في مجال التقنية المعلوماتية، حتى أصبح يطلق عليه بالشاهد المعلوماتي تمييزا له عن الشاهد التقليدي، ويعرفه البعض[96] ص23 على انه "الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسوب الآلي، والذي لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب عن معلومات داخله" .وبهذا المفهوم فإن الشاهد المعلوماتي يشمل عدة طوائف لعل من أهمها:

◆مشغلو الحاسوب الآلي: وهم الخبراء الذين تكون لديهم الدراية التامة بتشغيل جهاز الحاسوب الآلي والمعدات المتصلة به واستخدام لوحة المفاتيح في إدخال البيانات، كما تكون لديهم معلومات عن قواعد كتابة البرامج.[92] ص21

◆المبرمجون: وهم أشخاص متخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين ،كاتبو برامج التطبيقات وكاتبو برامج النظم.[34] ص264

◆المحللون: المحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراستها وتحليلها، وذلك بتقسيم النظام إلى وحدات واستنتاج العلاقات الوظيفية من تلك الوحدات، كما يقوم بتتبع البيانات داخل النظم عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب.[96] ص24

◆مهندسو الصيانة والاتصالات: وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكاته.

◆مديرو النظم: وهم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية.

إن هؤلاء وبحكم خبرتهم في مجال التقنية المعلوماتية و اطلاعهم على ما تم من أفعال، فلا بد من سماعهم كشهود على ما وقع، حيث يتوجب عليهم تقديم ما بحوزتهم من معلومات قد تفيد في إظهار الحقيقة، إلا أن السؤال المطروح هو هل يلتزم هؤلاء بطبع الملفات والإفصاح عن كلمات المرور و الشفرات التي يعرفونها ؟ هناك اتجاهان في هذا الصدد :

◆**الاتجاه الأول :** يرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع الملفات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة،

و يميل إلى هذا الاتجاه الفقه الألماني، حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسوب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.[46] ص390

◆الاتجاه الثاني: يرى هذا الاتجاه أن من بين الالتزامات التي يتحملها الشاهد، القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات، فبعض الدول مثل السويد و فنلندا و النرويج تنص تشريعاتها على انه يقع على عاتق الشهود واجب بأن ينعشوا الذاكرة بفحص الأماكن و المستندات التي توجد تحت سيطرتهم إذا لم يترتب على ذلك أضرار خطيرة. [68] ص106

و من جانبنا نرى انه إذا كان الالتزام بالشهادة بمفهومه التقليدي لا يتضمن إلتزام الشاهد المعلوماتي بالبوح بأسرار الدخول إلى أنظمة المعالجة الآلية للمعطيات و كذا طبع الملفات، فإنه لابد من تفعيل التشريعات ليشتمل الالتزام بالشهادة في الجريمة المعلوماتية، الالتزام بالإعلام، و التعاون مع سلطات التحقيق، فما يملكه الشاهد المعلوماتي من معلومات قد يختصر الكثير من الوقت و الجهد على هذه الجهات، و يمكن القول أن المشرع الجزائري قد أصاب إلى حد بعيد عندما وضع التزامات على عاتق مقدمي الخدمات بمساعدة السلطات المعنية بالتحقيق في الجرائم المعلوماتية كما سبق و اشرنا.

هذا و تجدر الإشارة إلى أنه على الشاهد المعلوماتي عندما يقدم المعلومات التي لديه لابد أن يقدمها بأسلوب سهل و مفهوم، حتى يكون بمقدور سلطات التحقيق فهم و إدراك تلك المعلومات، كما يتعين عليه أن يتوخى التحديد و الدقة في المعلومات التي يقدمها أو التي يبلغها لسلطات التحقيق و التحري .[34] ص266

2.3.3.2.2.القيام بالاستجوابات في الجرائم المعلوماتية

الاستجواب من إجراءات التحقيق التي يتولاها المحقق، يتضمن مناقشة المتهم تفصيلا في التهمة المنسوبة إليه، و مواجهته بأدلة الاتهام القائمة ضده، و محاصرته بالأسئلة الدقيقة المتعلقة بالاتهام، و ليس أمام المتهم إلا تفنيد التهمة أو التسليم بها والاعتراف بالجريمة [70]ص449 . و يتم الاستجواب على مرحلتين، المرحلة الأولى عند حضور المتهم لأول مرة أمام المحقق حيث يكاد يكون دور المحقق فيها سلبيا ، فتقتصر مهمته على التعرف على هوية المتهم و إحاطته علما بالوقائع المنسوبة إليه دون مناقشتها و تنبيهه بحقوقه ، و المرحلة الثانية هي المرحلة التي يصبح فيها دور المحقق أكثر إيجابا حيث يستجوب المتهم في

الموضوع، فيستفسره المحقق عن الوقائع المنسوبة إليه من خلال توجيه الأسئلة له و تلقي الأجوبة عنها .

و لا يختلف الاستجواب في الجرائم المعلوماتية عن الاستجواب في غيرها من الجرائم ، إلا أنه قد أثير التساؤل حول مدى إمكانية إجبار المتهم على الكشف عن شفرة الدخول إلى المعلومات المجرمة ؟ .و في هذا الصدد يرى البعض انه لا يجوز قانونا إجبار المتهم على طباعة ملفات البيانات المخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية [68] ص105 ذلك أن القاعدة العامة في المسائل الجنائية تقضي بأنه لا يجوز إجبار الشخص على تقديم دليل ضد نفسه،و إنما على سلطات التحقيق أن تكون في المستوى المطلوب و تصل إلى الحقيقة من خلال خبرتها و دقتها و ذكائها دون حاجة لإكراه الشخص و إجباره على البوح بما لديه من معلومات.

من كل ما سبق يمكن القول انه لا يوجد اختلاف كبير بين الشهادة والاستجواب في الجريمة المعلوماتية عن غيرها من الجرائم، و لكن يرى البعض[49] ص369،368 أن الأسلوب الأمثل للتحقيق مع الأشخاص ذوي العلاقة بالجرائم المعلوماتية يقتضي تتبع الخطوات التالية:

◆قبل البدء في اخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين يقوم المحقق وخبير الحاسوب الآلي بتبادل المعلومات فيما بينهم، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم، كما يقوم الخبير بشرح الأبعاد التقنية والنقاط التي ينبغي استجلائها بواسطة كل من الأشخاص موضع التحقيق .

◆يتم حصر النقاط المطلوب استيضاحها من قبل الخبير و المحقق ومن ثم يتولى المحقق ترتيب تلك النقاط.

◆يقوم المحقق بالحصول على كافة المصطلحات التي يمكن استخدامها مع بيان معاني تلك المصطلحات للاستفادة منها عند الضرورة .

◆يضع المحقق خطة التحقيق على ضوء المعطيات الأخرى التي يراها.

◆يبدأ اخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير والذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب، وذلك وفق كيفية يتم الاتفاق عليها.

◆مراعاة القوانين الوطنية فيما يتصل بسلطة التحقيق والمدى المسموح به للخبير في مشاركة المحقق وحضور الاستجواب.

4.3.2.2.الخبرة في الجرائم المعلوماتية

الخبرة من وسائل جمع الأدلة في التحقيق الجنائي، وهي إعطاء أو إدلاء أهل فن أو علم معين برأيهم في مسائل فنية تتعلق بتلك الفتوى أو العلوم[60] ص341. وتلعب الخبرة دورا كبيرا في إثبات الجرائم، فهي تساعد في تقديم الدليل العلمي الفني الذي يعجز المحقق بحكم ثقافته وعلمه عن استخلاصها ، ولهذا نجد العديد من التشريعات تنظمها في قوانينها ، من بينها المشرع الجزائري، والذي نظم أحكامها في المواد من 143 – 154 من قانون الإجراءات الجزائية. وإذا كانت للخبرة هذه الأهمية في الجرائم التقليدية، فإن أهميتها تزداد و بشكل كبير في الجرائم المعلوماتية، ذلك أن الحواسب وشبكات الاتصال بينها على أنواع، ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة، والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها.[78] ص08

1.4.3.2.2.المسائل التي يستعان فيها بالخبرة في الجرائم المعلوماتية

إن المحقق دائما في حاجة إلى خبير يرافقه للاستعانة به في استجلاء أي مسألة معلوماتية قد تستعصي عليه. ولعل من أهم المسائل التي يستعان بها بالخبرة في مجال الجرائم المعلوماتية ما يلي:[46] ص394،395

◆وصف تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور، وكذا وصف طبيعة بيئة الحاسوب أو الشبكة، من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية للبيانات ونمط وسائل الاتصالات وتردد موجات البث وأمكنة اختراقها.

◆وصف الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي يكون عليها .

◆بيان كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

◆بيان كيف يمكن عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يلحقها تلف.

◆بيان كيفية تجسيد الأدلة في صورة مادية بنقلها إن أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسوب أو النظام أو الشبكة أو الدعامة الممغنطة.

2.4.3.2.2.دور الخبير في إثبات الجرائم المعلوماتية

يلعب الخبير دورا هاما في إثبات الجريمة المعلوماتية، فوجوده حتمي وضروري ولا يمكن الاستغناء عنه، وذلك أن هذا الأخير هو من يقوم باستخلاص الدليل.ويمكن إيجاز الخطوات التي يقوم بها الخبير لاستخلاص الدليل فيما يلي:[92] ص36

◆خطوات ما قبل التشغيل والفحص

- التأكد من مطابقة محتويات أحراز المطبوعات لما هو مدون عليها.
- التأكد من صلاحية وحدات نظام التشغيل.
- تسجيل بيانات وحدات المكونات المضغوطة، كالنوع ، الطراز، الرقم ....الخ

◆خطوات التشغيل والفحص

- استكمال تسجيل بيانات الوحدات من خلال قراءات الجهاز.
- عمل نسخة أو نسخ- مطابقة للأصل – من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب.
- تحديد أنواع وأسماء المجموعات البرامجية، برامج النظام ، برامج التطبيقات، وما إن كانت هناك برامج معينة ذات علاقة بموضوع الجريمة.
- تحديد ما إذا كانت هناك برامج أو ملفات أو بيانات أو معلومات ذات دلالة ترابطية بموضوع الجريمة.
- إظهار الملفات المخبأة، والنصوص المخفية داخل الصور.
- تحويل الدليل الرقمي إلى هيئة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها إذا كانت صور أو نصوص أو وضعها في أي وعاء أخر حسب نوع البيانات والمعلومات المكونة للدليل.[92] ص36

◆تحديد مدى الترابط بين الدليل المادي والدليل الرقمي

في هذه المرحلة يتم فحص كل من الدليل المادي المضبوط والدليل المادي المستخرج من جهاز الحاسوب الآلي (والذي أصله هو الدليل الرقمي) الموجود بملفات النظام المضبوط، صور، نصوص، أصوات..الخ ، وبذلك يكون تم الربط بين الدليل الرقمي، والدليل المادي، مما يكسب الدليل الموثوقية واليقينية اللتان تؤديان إلى قبوله لدى جهة التحري وجهة الحكم .[92]ص36

◆ تدوين النتائج وإعداد التقرير

حيث يتم إعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإضافية المصورة أو المسجلة وغيرها، لاعتمادها ثم تصديرها إلى جهة التحقيق أو جهة الحكم .[32]ص36

3.2 مرحلة المحاكمة في الجرائم المعلوماتية

إن مرحلة المحاكمة هي المرحلة الأخيرة من مراحل إثبات الجريمة وفيها يتحقق مصير المتهم إما بالإدانة إذا توافرت الأدلة الجازمة بذلك، وإما بالبراءة إذا لم تتوفر الأدلة الجازمة بذلك. ولا تختلف مرحلة المحاكمة في الجرائم المعلوماتية عن غيرها من الجرائم، ذلك أن القانون وضمانا منه لتحقيق العدالة التي ينشدها كل فرد في المجتمع، قرر أن تجري المحاكمة وفي جميع الجرائم وفق قواعد تتشابه في عمومها سواء من حيث الجهة المختصة بها و سواء من حيث المبادئ المقررة لها و كذا من حيث إجراءات سير المحاكمة فيها. غير أن فعالية هذه المرحلة في ظل الجرائم المعلوماتية أصبح يتطلب من جهات الحكم المنوط بها الفصل في الدعاوى المتعلقة بهذا النوع من الجرائم، أن تكون على معرفة ببعض الفنيات المتعلقة بالحواسب الآلية وأنظمتها وغير ذلك من التقنيات التي تعتبر بيئة هذه الجرائم، فضلا عن معرفة كيفية التعامل مع الأدلة التي تفرزها وشروط قبولها وكذا القدرة على تقييمها وتقدير حجيتها في الإثبات .ليس هذا فحسب وإنما فعالية هذه المرحلة في ظل الجرائم المعلوماتية أصبح يستدعي إضفاء نوع من الخصوصية على إجراءات المحاكمة فيها وفق ما يتلاءم وطبيعة هذه الجرائم ومرتكبيها. كل هذا سنحاول التطرق إليه من خلال تقسيم هذا المبحث إلى ثلاثة مطالب، نتناول في المطلب الأول جهة الحكم في الجرائم المعلوماتية حيث سنركز بشكل أساسي على القاضي الناظر في الدعاوى المتعلقة بهذه الجرائم، ثم نتناول في المطلب الثاني إجراءات

المحاكمة في الجرائم المعلوماتية، و نتطرق في المطلب الأخير إلى شروط قبول الأدلة المعلوماتية و حجيتها في الإثبات.

1.3.2.جهة الحكم في الجرائم المعلوماتية

تتم محاكمة المتهمين في الجرائم المعلوماتية أمام المحاكم الجنائية العادية وفقا لقانون الإجراءات الجزائية، ذلك أن هذه المحاكم هي صاحبة الولاية العامة لمحاكمة جميع الأفراد وفي جميع الجرائم، ولا يجوز انتزاع أي شخص من أمام هذه المحاكم ليحاكم أمام محاكم خاصة أو استثنائية[97] ص96، غير أنه و إن كان هذا هو الأصل، إلا أن الجرائم المعلوماتية و بطبيعتها الخاصة أصبحت تفرض واقعا أخر، إذ أصبح و لا بد أن يكون لهذا النوع المستحدث من الجرائم محاكم خاصة به ، يكون قوامها المعرفة التقنية المتخصصة لدى القضاة المعينين فيها.و في انتظار أن يبادر المشرع الجزائري لاتخاذ مثل هذه الخطوة ، فإن المحاكم العادية تبقى صاحبة الولاية و الاختصاص للنظر في هذا النوع من الجرائم.

جعل المشرع المحاكم على أنواع و غاير في تشكيلتها، فتنقسم تبعا لنوع الجريمة إلى محاكم جنح ومخالفات ومحاكم جنايات، وتنقسم تبعا لشخص المتهم إلى محاكم خاصة بالبالغين ومحاكم خاصة بالأحداث، وتشمل في تشكيلتها على قاض وممثلا للنيابة العامة وكاتبا للجلسة (محاكم الجنح والمخالفات ومحاكم الأحداث)، و قد تستزيد التشكيلة بمستشارين ومحلفين (محكمة الجنايات). والجريمة المعلوماتية كغيرها من الجرائم قد تنظر الدعوى بشأنها بإحدى هذه المحاكم تبعا لتكييفها (جناية ،جنحة، مخالفة)، وتبعا لشخص مرتكبها (بالغ، حدث)، وذلك بالتشكيلة التي قررها القانون لها .إلا أن أكثر ما يهمنا في هذا الشأن هو القاضي الناظر في هذه الدعوى، فإذا كانت الجرائم المعلوماتية وبطبيعتها الخاصة أصبحت تتطلب توافر مهارات فنية خاصة لدى سلطات جمع الاستدلالات وكذا سلطات التحقيق الموكل إليها مهمة البحث والتحقيق فيها، فما هو الحال بالنسبة للقاضي الموكل له مهمة الفصل فيها؟وهذا ما سنحاول الإجابة عليه في هذا المطلب من خلال تقسيمه إلى فرعين، نتطرق في الفرع الأول للقاضي الناظر في الجرائم المعلوماتية ثم نتطرق في الفرع الثاني لأهمية تدريب القضاة في هذا النوع من الجرائم .

1.1.3.2.القاضي الناظر في الجرائم المعلوماتية

القاضي هو عماد المحكمة وذروة سنامها باعتباره القوام على كفالة تحقيق سائر عناصرها ومقتضياتها ومراقبة توجيه دقة الإجراءات فيها، فضلا عن دوره الأصيل في فهم الوقائع وسبر أغوار النصوص وتحري مراداتها ابتغاء الوصول إلى صحيح الحكم والنطق بكلمة الحق و العدل[98] ص179. وقد اختلفت التشريعات في تحديدها لطريقة اختيار القاضي فمنها من جعل عملية اختيار القاضي تتم من خلال انتخابه، كما هو الحال في بعض الولايات المتحدة الأمريكية، التي ترى أن اختيار القاضي بهذا الشكل هو احد مظاهر سيادة الأمة، ومنها من أسند هذه العملية للسلطة التشريعية كما هو الحال في سوريا حيث تسند مهمة اختيار قضاة المحكمة العليا لمجلس النواب، و هناك من التشريعات من جعل هذه العملية بيد السلطة التنفيذية كما هو الحال في الجزائر، حيث يتم تعيين القضاة بموجب مرسوم رئاسي بناء على اقتراح من وزير العدل وبعد مداولة المجلس الأعلى للقضاء.

إن هذه التشريعات، وإن اختلفت في طرق اختيارها للقاضي إلا أنها تسعى كلها لأن يكون القاضي المختار ممن تتوفر فيهم الصفات اللازمة التي تكفل للقضاء عدالته وتصونها من حياد واستقلال ونزاهة وكفاءة علمية وغيرها، إلا انه وبظهور الجرائم المعلوماتية أصبح من اللازم أن يتوفر في القاضي إلى جانب ما استلزمته جل التشريعات من صفات، صفات أخرى فرضتها الطبيعة الخاصة بهذه الجرائم، فأصبح الوصول إلى الحكم السديد والعادل في مثل هذا النوع من الجرائم يتوقف على مدى تفهم القاضي لفحوى التقدم العلمي ومعرفته بالأساليب الإجرامية التي استحدثتها هذه الجرائم، والتي يغلب عليها الطابع الفني المحض. وعليه نتعرض فيما يلي لأهم الصفات الواجب توافرها في القاضي الناظر في الدعاوى المتعلقة بجرائم معلوماتية سواء العامة منها أو الخاصة .

1.1.1.3.2.الصفات العامة الواجب توافرها في القاضي الناظر في الدعاوى المتعلقة بجرائم معلوماتية

لا يتاح للقاضي أداء رسالته المتوخاة منه وهي تحقيق العدالة من خلال إثبات ما يقع من جرائم بحق مرتكبيها، إلا إذا توفرت فيه الصفات التالية:

1.1.1.1.3.2.الاستقلال

إن ما يتمتع به القاضي من استقلالية هو من الدعائم الأساسية التي تقوم عليها المحاكمة العادلة، و القاضي المستقل هو القاضي الذي لا رقيب عليه، إلا ضميره و القانون، فهذا الأخير لا يمكنه أداء رسالته إلا إذا كان حرا في قراراته مستقلا عن أي تأثير كان سواء من السلطتين التشريعية أو التنفيذية، و سواء من الهيئات القضائية الأخرى، أو من المتقاضين أو حتى من المجتمع كله. لذلك فقد عمدت معظم الدساتير على النص على استقلالية القاضي، فتنص المادة 138 من الدستور الجزائري لسنة 1996 «السلطة القضائية مستقلة و تمارس في إطار القانون »، فالقاضي لابد أن يتسم دائما بالاستقلالية و أن يكون في منأى عن كل أشكال التبعية لدى ممارسته لمهامه.

2.1.1.1.3.2.التجرد و الحياد

إن التجرد والحياد يعتبران من أهم الصفات الواجب على القاضي التحلي بهما، ذلك أنهما تمثلان ضمانة أساسية للخصوم من أي نوع من أنواع التحيز، فحياد القاضي و تجرده يعني أن ينظر في الدعوى دون أن يتحيز لمصلحة احد أطرافها، أي أن ينظر فيها متجردا عن الميل و الهوى، و إنما مستهدفا إنزال حكم القانون على وقائعها [61] ص702،701، و لذلك فإن القاضي ملزم بأن يتصف بالحيادية المطلقة، فقد دعت المبادئ الأساسية بشأن استقلال السلطة القضائية التي أقرتها الأمم المتحدة في ديسمبر 1985 إلى ضرورة أن تفصل السلطة القضائية في المسائل المعروضة عليها دون تحيز[99] ص294، و في هذا الصدد نصت المادة 148 من الدستور الجزائري «القاضي محمي من كل أشكال الضغوط و التدخلات و المناورات التي قد تضر بأداء مهمته أو تمس نزاهة حكمه» .

3.1.1.1.3.2. المساواة

تمثل المساواة السمة الأساسية التي تجسد حياد القاضي، فعلى القاضي أن يتبع سلوكا يضمن للجميع معاملة سوية و مطابقة للقانون، و أن يسير الدعاوى المعروضة عليه بالمساواة و دون تمييز وأن يتجرد من المؤثرات الذاتية و الخارجية [100]ص05، ليس هذا فحسب و إنما على القاضي أن يضمن عدم المساس بهذه المساواة من قبل الخاضعين لسلطته، فلا يسمح لهم بالتمييز بين الأشخاص المعنيين بقضايا منظورة أمامه. و في هذا الشأن تنص المادة 140 من الدستور الجزائري «أساس القضاء مبادئ الشرعية و المساواة ، الكل سواسية أمام القضاء و هو في متناول الجميع و يجسد احترام القانون»

4.1.1.1.3.2.الانضباط

إن صفة الانضباط لابد أن تكون من الصفات الملازمة للقاضي، نظرا لما تكتسيه من أهمية في حسن سير العدالة، فعلى القاضي أن يقوم بواجباته القضائية بكل نجاعة و إتقان و في الآجال المعقولة، و أن يكون منضبطا في مواعيد عمله و متمكنا من ملفاته.

5.1.1.1.3.2.الشجاعة الأدبية

الشجاعة الأدبية هي الجرأة التي تساعد القاضي على حسم الموقف واتخاذ القرار المناسب المستمد من القانون و العدل، فهي الثقة بالنفس و الإيمان بالحق و الإحساس بجسامة المسؤولية، و هي التي تسهل مواجهة الصعاب، و تجاوز الحرج و التردد و الانصياع [101] ص05، فيمارس القاضي مهامه على أساس التقدير الجيد للوقائع و تفهمه الواعي للقانون بحسب ما يمليه عليه ضميره ، و دون أن يخاف في الحق لومه لائم.

6.1.1.1.3.2.الكفاءة العلمية

فلا بد أن يكون القاضي ملما بأكبر قدر ممكن من المعرفة القانونية و ما يتصل بها من علوم كعلم الإجرام و علم العقاب و غيرها من العلوم التي تساعد القاضي في أدائه لمهامه، و عليه أن لا يقتصر في معرفته على ما هو محلي فحسب، و إنما لا بد أن يكون على اطلاع بالتطورات الحاصلة في المجال القانوني في مختلف التشريعات و كذا الاتفاقيات الدولية المنعقدة في المجال القضائي.

2.1.1.3.2.الصفات الخاصة بالقاضي الناظر في الدعاوى المتعلقة بجرائم معلوماتية

إن الصفات الخاصة الواجب توافرها في القاضي الناظر في الدعاوى المتعلقة بجرائم معلوماتية ، لا تختلف كثيرا كما سبق و تطرقنا إليه عند حديثنا عن الصفات الخاصة بالمحقق في هذه الجرائم ، ذلك أن ظهور هذه الجرائم أصبح يقتضي المعرفة التقنية إلى جانب المعرفة القانونية لدى رجال العدالة الجنائية ، و على ذلك يمكن اختصار أهم ما يجب أن يتصف به القاضي في الجرائم المعلوماتية فيما يلي :

1.2.1.1.3.2.الإلمام بالجوانب المتعلقة بالجرائم المعلوماتية

فعلى القاضي أن يكون على معرفة جيدة بهذا النوع المستحدث من الجرائم و من مختلف جوانبها، من حيث خصائصها و أنواعها و كذا الفئات التي ينقسم إليها مرتكبوها،

و مميزات كل فئة من هذه الفئات، و كذا الواقع الحالي و الاتجاهات المستقبلية لها و معرفة وفهم التشريعات المحلية المتعلقة بهذه الجرائم، و الإلمام باتجاهات القوانين و التشريعات في البلدان الأخرى، و الوقوف على الأبعاد الدولية لهذه الجرائم و آليات التعاون المشترك بين الدول و التعرف على الاتفاقيات و المعاهدات الموجودة بهذا الخصوص.و على القاضي فضلا عن هذا، دراسة و تحليل القضايا المشهورة للاستفادة من التجارب السابقة لرجال العدالة في مواجهة هذا النوع من الجرائم.[45] ص40

2.2.1.1.3.2.الإلمام بمختلف القوانين و العلوم المتصلة بالجرائم المعلوماتية

على القاضي أن يكون ملما بمختلف النصوص القانونية المجرمة للأفعال المعتبرة جرائم معلوماتية ، و أن يدرك فحوى هذه النصوص و كيفية تطبيقها، بالإضافة إلى هذا فلا بد أن يكون القاضي على قدر من المعرفة بمختلف العلوم المرتبطة بتكنولوجيا المعلومات (علوم الحاسوب ، علوم الأدلة الجنائية ، علوم التحليل السلوكي للأدلة)، حيث أن هذه العلوم مجتمعة تساعد القاضي على معرفة ماهية الدليل المعلوماتي، فيسهل عليه تقديره.

3.2.1.1.3.2.معرفة التقنيات المستخدمة في ارتكاب الجرائم المعلوماتية و أهم مفرداتها

إن القاضي الناظر في الدعاوى المتعلقة بجرائم معلوماتية يقتضي أن يكون على قدر من المعرفة بأساسيات التقنية المعلوماتية من حواسب آلية و شبكات اتصال و غير ذلك، ففهم القاضي لوظائفها و أسلوب عملها و طرق استخدامها يساعده في استيعاب أفضل للجريمة المرتكبة، كما يساعده أيضا في فهم التقارير المعدة من قبل الخبراء بشأن هذه الجرائم، و التي تعد من أهم الوثائق التي يرجع إليها القاضي في حكمه.

و لا يكفي أن يكون القاضي على معرفة بالتقنيات المعلوماتية فحسب، و إنما لابد أن يكون ملما بالمصطلحات المستخدمة في مجال المعلوماتية، فكما سبق و ذكرنا، فإن من أهم الصعاب التي قد تواجه أجهزة العدالة الجنائية هي اللغة المستخدمة في مجال الجرائم المعلوماتية و التي تعرف "بلغة المختصرات"، و لهذا فبدون معرفة القاضي لهذه المصطلحات و معانيها و دلالتها سيكون من الصعب عليه استيعاب ما قد يدلي به الشهود أو المتهمين من أقوال في هذه الجرائم.

2.1.3.2.أهمية تدريب القضاة في الجرائم المعلوماتية

إذا كان تدريب سلطات الاستدلال و التحقيق في الجرائم المعلوماتية أصبح أمرا ملحا و بشدة نظرا لتعقيد هذه الجرائم و ما تتميز به من خصوصية في إثباتها، فإن تدريب جهات الحكم على معالجة القضايا المتعلقة بها و كيفية قبول أدلتها في الإثبات و تقديرها ، أصبح أمرا أكثر إلحاحا، خاصة و أن ما يملكه القضاة من معرفة بقواعد الإثبات التقليدية لم يعد كافيا لوحده لإثبات هذا النوع من الجرائم، و إنما أصبح الأمر – كما سبق ووضحنا – يتطلب قضاة ذوي صفات وسمات خاصة من حيث الإلمام بتقنيات الحاسوب الآلي و برامجه و أنظمته و مفرداته و طبيعة الجرائم الواقعة عليه .

إن هذا الأمر دفع بالعديد من الدول إلى تنظيم دورات تدريبية يكون من شأنها إمداد القضاة بالمهارات الفنية اللازمة للفصل في القضايا المتعلقة بهذا النوع من الجرائم ، حيث أصبح التدريب يكتسي أهمية خاصة بظهورها ، فمن ناحية يعد الوسيلة الفعلية و التطبيقية الناجحة والمؤثرة التي تكفل الاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل ميسرة، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف على الأخطاء والسلبيات التي يمكن أن يكشف عنها التطبيق العملي للقوانين والأنظمة واللوائح ووضع الحلول الكفيلة بتجنبها.[102] ص602

على أنه، و على الرغم من الأهمية التي أصبح يكتسبها التدريب خاصة مع التقدم في أساليب ارتكاب الجرائم، والتي أصبح يستعصى على القضاة وبمعرفتهم المتواضعة بالتقنية المعلوماتية استيعابها ، إلا أن هناك[102]ص605،604 من ذهب إلى القول انه من الصعب تطبيق مثل هذا التدريب على القضاة و ارجع ذلك لأمرين:

◆الأمر الأول يتعلق بعدم تقبل القضاة أن يقوم بتدريبهم مدربون قد يكونوا في نفس مستواهم الوظيفي أو اقل درجة في السلم الإداري هذا من جهة، ومن جهة أخرى قد لا تتوافر لديهم الخبرات المتخصصة في المجال القضائي.

◆الأمر الثاني يتعلق بالوقت الذي يتم فيه تنفيذ البرامج التدريبية، هل يتم تنظيم هذه البرامج قبل الالتحاق بالعمل الوظيفي أم انه يمكن أن يصبح هذا التدريب عملية مستمرة في أثناء مباشرتهم أعمالهم مع الأخذ بعين الاعتبار كثرة القضايا التي تعرض على المحاكم وقلة القضاة

مقارنة بأعداد القضايا، مما يجعل تفرغ القاضي لحضور هذه الدورات التدريبية أمرا يكتنفه العديد من الصعوبات .

من جانبنا نرى أن مثل هذه الصعوبات يمكن التغلب عليها، إذا كان هناك تنظيم جيد لمثل هذه الدورات وجعل الإشراف عليها يتم من قبل أشخاص أكفاء، لهم القدرة على نقل معارفهم بالشكل اللازم الذي يضمن إكساب القضاة المهارات اللازمة في مجال التقنية المعلوماتية، فضلا عن هذا ،لابد أن تسعى الدول إلى جعل هذه الدورات مستمرة ودورية خاصة في ظل التطورات المتلاحقة في مجال الجرائم المعلوماتية، و التي تقتضي التأهيل المستمر و المتواصل للقضاة بالشكل الذي يكفل الوصول إلى إصدار الحكم القضائي السديد و القادر على تحقيق العدالة بمختلف مقتضياتها.

2.3.2.إجراءات المحاكمة في الجرائم المعلوماتية

إن إجراءات المحاكمة هي مجموعة الإجراءات التي تستهدف تمحيص أدلة الدعوى، ما كان منها ضد مصلحة المتهم و ما كان في مصلحته، و تهدف بذلك إلى تقصي كل الحقيقة الواقعية و القانونية في شأنها، ثم الفصل في موضوعها، إما بالإدانة إن كانت الأدلة جازمة بذلك، و إما بالبراءة إذا لم تتوفر الأدلة الجازمة بالإدانة[61] ص651. و لا تختلف إجراءات المحاكمة في الجرائم المعلوماتية عن غيرها من الجرائم، فجميع الجرائم تخضع لإجراءات محاكمة واحدة في عمومها، و تقرر لها ذات المبادئ التي تضفي عليها صفة الشرعية الإجرائية و تضمن حسن سير العدالة و حماية حقوق المعنيين بالدعوى، و مع ذلك و نظرا للطبيعة التقنية للجرائم المعلوماتية و التي تستدعي تقديم معلومات و مصطلحات تقنية قد يستعصى فهمها على القضاة، وجب إضفاء نوع من الخصوصية على هذه المرحلة المهمة من مراحل إثبات الجريمة . وهذا ما سنحاول التطرق إليه ، وذلك من خلال تقسيم هذا المطلب إلى فرعين، نتناول في الفرع الأول المبادئ العامة لإجراءات المحاكمة في الجرائم المعلوماتية، ثم نتناول في الفرع الثاني إجراءات سير المحاكمة في الجرائم المعلوماتية .

1.2.3.2.المبادئ العامة لإجراءات المحاكمة في الجرائم المعلوماتية

يقرر القانون مجموعة من المبادئ التي يستوجب مراعاتها في المحاكمة، و هي تعد ضمانة من ضمانات المحاكمة العادلة ، و تتمثل هذه المبادئ فيما يلي:

1.1.2.3.2.علانية الجلسة

يقصد بالعلانية تمكين جمهور الناس – بغير تمييز- من مشاهدة جلسات المحاكمة و متابعة ما يدور فيها من مناقشات و مرافعات و ما يتخذ فيها من إجراءات و ما يصدر فيها من قرارات و أحكام [103] ص105 . و تكتسي العلانية أهمية كبيرة، ذلك أن محاكمة المتهم بجلسة علنية يحضرها من يشاء من الأفراد، يبعث الطمأنينة في قلوبهم. فلا يخشون الانحراف في الإجراءات أو التأثير في مجريات الدعوى، ويدعم الثقة في أحكام القضاء فيعرف الجمهور مدى تجرد المحاكم و حيادها و مدى إيمانها بالعدل و التزامها بحكم القانون [97] ص164 . ونظرا لهذه الأهمية فقد حرصت جل التشريعات الحديثة على النص على هذا المبدأ في قوانينها، فنص المشرع المصري عليه في المادة 268 من قانون الإجراءات الجزائية "يجب أن تكون الجلسة علنية و يجوز للمحكمة مع ذلك مراعاة للنظام العام أو محافظة على الآداب، أن تأمر بسماع الدعوى كلها أو بعضها في جلسة سرية، أو تمنع فئات معنية من الحضور فيها" ، كما نص المشرع الجزائري على هذا المبدأ في المادة 285 من قانون الإجراءات الجزائية بقوله "المرافعات علانية ما لم يكن في علانيتها خطر على النظام العام أو الآداب، و في هذه الحالة تصدر المحكمة حكمها القاضي بعقد الجلسة سرية في جلسة علنية غير أن للرئيس أن يحظر على القصر دخول الجلسة، و إذا تقررت سرية الجلسة تعين صدور الحكم في الموضوع في جلسة علنية..." .

ورغم أن الأصل في المحاكمة هي العلنية إلا أن القانون و حماية لمقتضيات النظام العام و الآداب العامة أجاز جعلها كلها أو بعضها سرية ، فقد تقرر المحكمة نظر الدعوى في جلسة سرية إذا تعلق الأمر بجريمة معلوماتية استهدفت الدفاع الوطني وذلك حماية للنظام العام، كما قد تنظر الدعوى في جلسة سرية إذا كان المجرم المعلوماتي مرتكب الجريمة حدثا. وإذا ما قررت السرية فإن إجراءات المحاكمة تدور على ذات النهج و وفق ذات القواعد التي تجري فيها لو كانت الجلسة علنية، على انه يجب العودة إلى حالة العلنية في جلسات المحاكمة إذا مازال السبب الذي دعا لرؤية الدعوى بصورة سرية[97] ص169. و باعتبار العلنية أحد المبادئ الأساسية للمحاكمة، فإن إغفالها يؤدي إلى بطلان إجراءات المحاكمة و كذا الحكم الصادر عنها.

2.1.2.3.2 .شفوية إجراءات المحاكمة

يقصد بمبدأ الشفوية وجوب أن تجري شفويا- أي بصوت مسموع – جميع الإجراءات، فالشهود و الخبراء يدلون بأقوالهم شفويا أمام القاضي، و يناقشون فيها شفويا و الطلبات

و الدفوع تقدم شفويا، و في النهاية فإن المرافعات سواء مرافعات الادعاء و الدفاع تتلى شفويا، فهذا المبدأ يقرر عدم جواز اكتفاء القاضي بمحاضر التحقيق الابتدائي المكتوبة، و إنما عليه أن يسمع بنفسه الشهود و اعتراف المتهم و يطرح كل ذلك للمناقشة الشفوية . و في تعبير عام فإن كل دليل يعتمد عليه القاضي في حكمه يجب أن يكون قد طرح شفويا في الجلسة، و جرت في شأنه المناقشة الشفوية ،و يستمد القاضي اقتناعه من حصيلة هذه المناقشات الشفوية ولا يستمده من المحاضر المكتوبة[61] ص878. وعلى ذلك فإن الشفوية تشمل كل إجراءات المحاكمة بلا استثناء، بدءا من جلسة الافتتاح التي ينادى فيها على الخصوم و الشهود إيذانا بنظر الدعوى، و انتهاء بجلسة الختام التي تنطق فيها المحكمة بالحكم علنا، و لا يفلت من الشفوية أي إجراء [103] ص113 ، و ذلك نظرا لأهميتها ، فهي الطريقة المثلى التي يتمكن بها القاضي من تكوين عقيدته، فمن خلال سماعه لتحاور الخصوم و مناقشته للشهود و الخبراء يمكن أن يستخلص ما اكتنف التحقيق الابتدائي من غموض.

و قد أخذت العديد من التشريعات بهذا المبدأ فالمواد من 268 إلى 294 من قانون الإجراءات الجزائية تدل دلالة قاطعة على أخذ المشرع المصري بهذا المبدأ ،و نص المشرع الجزائري على هذا المبدأ من خلال المادة 353 من قانون الإجراءات الجزائية "إذا ما انتهى التحقيق بالجلسة سمعت أقوال المدعي المدني في مطالبته و طلبات النيابة العامة و دفاع المتهم و أقوال المسؤول بالحقوق المدنية عند الاقتضاء ..."، وكذا المادة 233 "يؤدي الشهود شهادتهم شفويا..." . إن جزاء الإخلال بمبدأ الشفوية هو البطلان حيث يبطل الحكم الذي اعتمد على دليل لم يتم مناقشته شفويا في الجلسة .

3.1.2.3.2.حضور الخصوم

يعني تمكين جميع الخصوم في الدعوى من الحضور في جلسات المحاكمة و عرض ما لديهم من أدلة و الرد عليها و مناقشتها و دحضها إن أمكن، فالأصل أن يواجه كل خصم خصمه بما لديه من أدلة و أسانيد، و أن تتاح لكل منهما فرصة الرد على الآخر إما بتفنيد أدلته و نقض أسانيده، أو بتقديم أدلة و أسانيد مضادة، و هكذا تدور الدعوى بين الخصوم سجالا حتى يستنفد كل خصم ما في جعبته، و عندئذ يكون القاضي قد أحاط بجوانب الدعوى و فهم مسائلها و أصبح في وسعه أن يكون عقيدته و أن يحكم فيها و هو على بينة من أمره . [103] ص118

إن أول ما يقتضيه هذا المبدأ هو حق جميع الخصوم في حضور جميع إجراءات المحاكمة، سواء ما دار منها في الجلسة أو ما جرى خارج الجلسة، كما لو انتقلت المحكمة – أو

ندبت أحد أعضائها – لإجراء معاينة، إذ يتعين أن يدعى جميع الخصوم للحضور فيها، و يقتضي هذا المبدأ كذلك أن يكون لكل خصم الحق في أن يطرح ما لديه من أدلة، و في أن يدحض الأدلة التي يقدمها خصمه، و يتفرع عن هذا المبدأ عدم جواز أن يبني القاضي حكمه على دليل لم يطرح في الجلسة، ولم يتح للخصوم مناقشته [61] ص886 . و في هذا الصدد يقرر المشرع الجزائري في المادة 2/212 من قانون الإجراءات الجزائية "لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه".

و رغم أن الأصل هو حضور الخصوم جلسات المحاكمة، إلا أن القانون أعطى الحق للقاضي أن يحرم احد هؤلاء من الحضور، و ذلك في حالة ما إذا اخل بالنظام العام للجلسة أو أحدث شغبا فيها، حيث تنص المادة 295 من قانون الإجراءات الجزائية الجزائري "إذا حدث بالجلسة أن أخل احد الحاضرين بالنظام بأية طريقة كانت فللرئيس أن يأمر بإبعاده من قاعة الجلسة . و إذا حدث في خلال تنفيذ هذا الأمر أن لم يمتثل له أو أحدث شغبا صدر في الحال أمر بإيداعه السجن..." ، و تنص المادة 270 من قانون الإجراءات الجزائية المصري "...و لا يجوز إبعاده عن الجلسة إلا إذا وقع منه تشويش يستدعي ذلك، و في هذه الحالة تستمر الإجراءات إلى أن يمكن السير فيها بحضوره و على المحكمة أن توقفه على ما تم في غيبته من الإجراءات " ، كما قد تجري المحاكمة في غير حضور المتهم ، إذا كان المجرم المعلوماتي المتهم حدثا ، حيث تقرر المادة 467 من قانون الإجراءات الجزائية الجزائري في فقرتها الثانية "...و يجوز لها إذا دعت مصلحة الحدث إعفاءه من حضور الجلسة، و في هذه الحالة يمثله محام أو مدافع أو نائبه القانوني و يعتبر القرار حضوريا..." .

4.1.2.3.2.تدوين الإجراءات

و يقصد بالتدوين أن تكون جميع الإجراءات التي تمت بالجلسة مكتوبة، ذلك أن الإثبات بالكتابة يعتبر ضمانة لا غنى عنها في السير في إجراءات الدعوى و الفصل فيها على نحو لا يثير الجدل و التأويل أو التحوير في الوقائع المطروحة، إضافة إلى أن إمكانية الطعن في الحكم واردة و ترتبط صحته بصحة الإجراءات الثابتة بالكتابة[104] ص422. و لا تعارض بين شفوية الإجراءات و تدوينها، فالشفوية تعني مباشرة الإجراء بالكلمة المنطوقة، سواء كان القائم به طرفا في الدعوى أو لم يكن طرفا فيها، أما التدوين فيعني تسجيل الإجراء من قبل كاتب الجلسة – تحت إشراف ورقابة رئيس المحكمة- و إثباته على نحو ما تم بالكلمة المكتوبة، ليكون هذا دليلا من بعد على حصول الإجراء من جهة، و على الكيفية التي حصل بها من جهة أخرى،

فالشفوية كما يصفها بعض الفقهاء بحق هي الأصل، و التدوين هو صورة هذا الأصل.[103] ص135

وقد حرصت التشريعات على النص على هذا المبدأ، من بينها المشرع الجزائري الذي نص عليه في المادة 236 من قانون الإجراءات الجزائية بقوله " يقوم الكاتب تحت إشراف الرئيس بإثبات سير المرافعات ولاسيما أقوال الشهود وأجوبة المتهم ويوقع الكاتب على مذكرة الجلسة ويؤشر عليها الرئيس في ظرف ثلاثة أيام التالية لكل جلسة على الأكثر"، ونص المشرع المصري عليه في المادة 272 من قانون الإجراءات الجنائية المصري "يجب أن يحرر محضر بما يجري في جلسة المحاكمة ويوقع على كل صفحة منه رئيس المحكمة وكاتبها في اليوم التالي على الأكثر..."، كما عنت التشريعات أيضا بتفصيل ما ينبغي أن يشتمل عليه محضر الجلسة من تاريخ الجلسة، علنية أو سرية الجلسة، أسماء القضاة والكاتب وعضو النيابة وكذا الخصوم ومحاميهم، وأسماء الشهود وكذا التصريحات التي جاء بها الشهود و أقوال الخصوم والطلبات المقدمة من قبلهم، وجميع ما تم من إجراءات خلال الجلسة، ولم تستوجب ذكر جميع هذه البيانات في محضر الجلسة، فإغفال أيا منها لا يترتب عليه بطلانه، طالما لا يؤدي إلى الحيلولة بين المحضر وأداءه لدوره الإجرائي الذي أناطه به القانون في إعطاء صورة صحيحة ووافية عن إجراءات المحاكمة، وإذ اغفل المحضر بيانا ولكن ذكره الحكم سواء في ديباجته أو في منطوقه، اعتبر كما لو كان واردا في المحضر نفسه، ولم يكن محل لأن يعاب على المحضر إغفاله هذا البيان، ويعد ذلك تطبيقا لمبدأ أن " المحضر و الحكم يكمل كل منهما الأخر" [61] ص913 .غير أن إغفال تحرير محضر الجلسة من أصله يؤدي إلى بطلان المحاكمة وبطلان الحكم الناجم عنها.

2.2.3.2.إجراءات سير المحاكمة في الجرائم المعلوماتية

لا تختلف إجراءات سير المحاكمة في الجرائم المعلوماتية عن الإجراءات المتبعة في غيرها من الجرائم، غير أن ارتباط الجرائم المعلوماتية بتقنيات ومصطلحات فنية وعلمية قد تشكل صعوبة في وجه القضاة أثناء نظرهم في الدعاوى المتعلقة بهذا النوع من الجرائم ،وهذا ما أدى بالبعض إلى الدعوة إلى ضرورة أن تسبق مرحلة المحاكمة مرحلة تحضيرية يتم من خلالها توضيح ما قد يكتنف هذه الجرائم من غموض.

1.2.2.3.2.تحضير إجراءات المحاكمة في الجرائم المعلوماتية

يرى البعض[49] ص374 أن التحضير للمحاكمة في الجرائم المعلوماتية يكتسي أهمية بالغة، فتقديم المعلومات العلمية ومصطلحات التقنية العالية أمام المحاكم وشرحها للقضاة تشكل صعوبة بالغة لدى المحققين وأعضاء النيابة، وترك مهمة الشرح والتقديم لخبراء الحاسوب الآلي كلية، تفقد القضية الجنائية عناصرها القانونية، و لذلك يرون أنه من الضروري أن تتبع في تحضير إجراءات المحاكمة في الجرائم المعلوماتية الخطوات التالي:

◆الخطوة الأولى: ويقوم بها المحقق وهي إجراءات تلخيص القضية وتعبئة النماذج والاستمارات الخاصة بملف القضية وإعداد ورقة حصر التهم وصياغة سيناريو الجريمة كما كشفتها التحريات والأدلة المتوفرة.

◆الخطوة الثانية: وهي اللقاء بين المحقق وخبراء الحاسوب الآلي الذين أسهموا مع المحقق في إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية، وفي هذا اللقاء يتم حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بينة أو قرينة، كما يقوم المحقق في هذه المرحلة بشرح الجوانب القانونية للخبراء والتأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة التي ينوي محاكمة المتهم بموجبها.

◆الخطوة الثالثة: في هذه الخطوة يلتقي المحقق بممثل الاتهام أو وكيل النيابة الذي يتولى مهمة الادعاء أمام القضاء، وذلك لشرح أبعاد الفصل الإجرامي وتمكين ممثل الادعاء من صياغة التهمة المناسبة والاتفاق حول عناصر وأركان الجريمة وترتيب الأدلة لإثبات كل ركن أو عنصر من الجريمة موضوع الاتهام، ومن الضروري في هذه المرحلة التيقن من مدى إلمام ممثل الاتهام بالتقنيات والبرامج ذات العلاقة بالحاسوب الآلي موضوع القضية .

◆الخطوة الرابعة: في هذه المرحلة يتم اللقاء بين المحقق وممثل النيابة وخبراء الحاسوب الآلي لترتيب المصطلحات الفنية المستخدمة أثناء إجراءات المحاكمة، مع ضرورة الاتفاق حول تلك المصطلحات وكيفية استخدامها والمرافعات التي قد ترد أثناء الاستجواب، حتى تطمئن الأطراف على أن هناك لغة موحدة بينهم لا تقبل الشك أو الخطأ، علما أن المتهم في مثل هذه القضايا على دراية بمصطلحات الحاسوب الآلي ومن حقه أن يجادل بما لديه من علم ومعرفة للدفاع عن نفسه، كما انه من الضروري مراعاة أي خلاف ينشب بين ممثل النيابة العامة وخبراء الحاسوب الآلي أمام المحكمة، لأن ذلك قد يطيح بجميع الأدلة الفنية التي تقوم

عليها التهمة، إذ أن الشك يفسر لصالح المتهم ومن السهل إثارة الشكوك في مجال تقنيات الحاسوب الآلي المفتوحة على جميع أبواب المعرفة .

◆الخطوة الخامسة: وهي مرحلة وضع سيناريو المحاكمة ويقصد بالسيناريو ترتيب الأحداث والوقائع والعمليات الفنية التي تشكل الجريمة مع توفر عناصر القصد الجنائي و إظهار مبررات علاقة المتهم الذي سيمثل أمام المحكمة بالفعل الإجرامي موضوع الاتهام، ويشمل وضع السيناريو أسلوب الإخراج القانوني بالكيفية التي تنساب بها الحقائق المؤكدة إلى عقل القاضي .

ومن جانبنا نرى انه وان كانت مثل هذه الخطوات تكتسي أهمية كبيرة في الجرائم المعلوماتية نظرا لتعقديها والغموض الذي يكتنفها، فإن أهميتها لا تقل عن غيرها من الجرائم، فالتحضير للمحاكمة من شأنه أن يكفل التنسيق الجيد بين جهات التحقيق والحكم من اجل الوقوف على حقيقة أي واقعة و كشف خباياها.

2.2.2.3.2.سير إجراءات المحاكمة في الجرائم المعلوماتية

إن سير إجراءات المحاكمة في الجرائم المعلوماتية كغيرها من الجرائم ، تختلف تبعا للمحكمة المنظورة أمامها الدعوى المتعلقة بها.فقد تكون الجريمة المعلوماتية جنحة فتنظر الدعوى بشأنها أمام محكمة الجنح والمخالفات وقد تكون الجريمة المعلوماتية جناية فتنظر الدعوى بشأنها أمام محكمة الجنايات، وقد يكون المتهم بالجريمة المعلوماتية حدثا فتنظر الدعوى أمام محكمة الأحداث. وسنقتصر على بيان إجراءات سير المحاكمة في الجريمة المعلوماتية وفقا للتشريع الجزائري الذي قد تنظر الدعاوى المتعلقة بجرائم معلوماتية في ظله ،إما أمام محكمة الجنح و المخالفات إذا كان المتهم بالجريمة شخصا بالغا أو إما أمام محكمة الأحداث إذا كان المتهم بها حدثا.

1.2.2.2.3.2.إجراءات سير المحاكمة في الجرائم المعلوماتية أمام محكمة الجنح

تسري إجراءات المحاكمة في الجرائم المعلوماتية أمام محكمة الجنح و المخالفات وفقا للقواعد العامة المقررة لسير الإجراءات أمامها [105]، و التي يمكن اختصارها فيما يلي :

◆الإعلان عن بدء الجلسة

تبدأ المحكمة جلستها بالإعلان عن افتتاحها ثم المناداة على أطراف الدعوى من متهمين و ضحايا و كذا شهود و مسؤولين مدنيين إن وجدوا، ليتم التأكد من حضورهم أو غيابهم و يتحقق الرئيس من هوية المتهم و يعرفه بالإجراء الذي تمت من خلاله إحالته على المحكمة حيث تقضي المادة 343 من قانون الإجراءات الجزائية «يتحقق الرئيس من هوية المتهم و يعرف بالإجراء الذي رفعت بموجبه الدعوى للمحكمة، كما يتحقق عند الاقتضاء من حضور أو غياب المسؤول بالحقوق المدنية أو المدعي المدني و الشهود..."

◆ بدء إجراءات التحقيق

تبدأ إجراءات التحقيق باستجواب المتهم ومناقشته تفصيلا في التهمة المنسوبة إليه و مواجهته بالأدلة القائمة ضده ، و ذلك إما لتنفيذها أو الاعتراف بها، و لرئيس المحكمة توجيه ما يراه ضروريا من أسئلة للمتهم، كما يجوز ذلك للنيابة العامة، وكذا للمدعي المدني و للدفاع، و في هذه الحالة توجه الأسئلة من خلال الرئيس، حيث تنص المادة 224 من قانون الإجراءات الجزائية الجزائري "يقوم الرئيس باستجواب المتهم قبل سماع الشهود و يتلقى أقواله ، و يجوز للنيابة العامة توجيه أسئلة إلى المتهم كما يجوز ذلك للمدعي المدني و للدفاع عن طريق الرئيس» . و بعد استجواب المتهم يتم سماع المدعي المدني و يتلقى الرئيس تصريحاته بشأن ظروف الجريمة المرتكبة و الضرر اللاحق به، و بعدها تسمع شهادة الشهود حيث يلتزم كل منهم بالإدلاء بما لديه من معلومات حول الواقعة المرتكبة و ذلك بعد تأديتهم اليمين القانونية، و يتم الاستماع أولا لشهود الإثبات ثم يتم الاستماع لشهود النفي .

بعد الانتهاء من سماع الشهود ، يعرض الخبراء الموجه لهم استدعاء للحضور للجلسة ، نتائج ما قاموا به من أعمال فنية ككيفية قيامهم بعملية استخلاص الدليل المعلوماتي و نقله إلى دعامة مادية و غير ذلك من الأعمال، و ذلك بعد أدائهم اليمين القانونية المقررة. و يجوز للرئيس إما من تلقاء نفسه أو بناء على طلب النيابة العامة أو الخصوم أو محاميهم توجيه أسئلة للخبراء و ذلك في حدود مهمتهم المنجزة.

◆ المرافعات

تبدأ المرافعات بسماع المدعي المدني أو محاميه حيث يقدم هذا الأخير طلباته المتمثلة في التعويض عن الضرر اللاحق به، بعد ذلك تتقدم النيابة العامة بطلباتها سواء الكتابية أو

الشفوية و التي ترمي إلى تحقيق العدالة، ثم يقدم محامي المتهم مرافعته دفاعا عن المتهم سواء بالسعي إلى تفنيد التهمة عن موكله و من ثم طلب البراءة، أو طلب تخفيف الحكم، و للمدعي المدني و النيابة العامة دائما حق الرد، ثم تترك للمتهم و محاميه الكلمة الأخيرة .

◆الإعلان عن تاريخ الحكم

يعلن الرئيس عن انتهاء المرافعات فيقرر إما إصدار الحكم في الحال، أو يحدد تاريخا للنطق بالحكم .

2.2.2.2.3.2.إجراءات سير المحاكمة في الجرائم المعلوماتية أمام محكمة الأحداث

تتم محاكمة المتهم الحدث في جريمة معلوماتية وفقا للإجراءات المقررة لمحاكمة هذه الفئة و التي خصها المشرع بإجراءات يطغى عليها طابع من البساطة و المرونة في التطبيق، و يمكن تلخيصها فيما يلي :

◆سرية الجلسة

تتم محاكمة الحدث في جلسة سرية سواء بمكتب أو في غرفة المشورة، و ذلك حفاظا على سمعته حيث تنص المادة 461 من قانون الإجراءات الجزائية الجزائري «تحصل المرافعات في سرية و يسمع أطراف الدعوى و يتعين حضور الحدث بشخصه و يحضر معه نائبه القانوني و محاميه، و تسمع شهادة الشهود إن لزم الأمر بالأوضاع المعتادة».

◆بدء التحقيق

بعد أن يتأكد القاضي من هوية الحدث ، يخبره بالتهمة المنسوبة إليه و يستفسره فيها و في الظروف التي أدت به إلى ارتكابها ، و سماع الحدث لا يكون إلا بحضور نائبه القانوني الذي هو إما احد والديه أو وصيه أو متولي حضانته ، كما يقوم القاضي بسماع هذا الأخير و يستفسره عن ظروف الحدث و طبعه و نفسيته و عن كل ما قد يؤدي إلى الوقوف عن الأسباب التي أدت إلى جنوحه، ثم بعد ذلك يقوم القاضي بسماع الطرف المدني و كذا الشهود و ذلك بالأوضاع العادية لسماعهم .

◆المرافعات

إن تعيين محام للحدث وجوبي سواء تم تعيينه من قبل الحدث أو نائبه القانوني، أو تم تعيينه تلقائيا من قبل المحكمة، فحضور المحامي مع الحدث ضروري، و تسري المرافعات بالأحوال العادية لسيرها حيث يتم سماع المدعي المدني أو محاميه، و من ثم تقدم النيابة العامة طلباتها، فيقدم الدفاع مرافعاته و للمدعي المدني و النيابة حق الرد على دفاع المتهم الحدث، و تبقى الكلمة الأخيرة للمتهم الحدث و محاميه، غير انه لا يسمح بحضور المرافعات إلا لشهود القضية و الأقارب القريبين للحدث ووصيه أو نائبه القانوني و أعضاء النقابة الوطنية للمحامين و ممثلي الجمعيات أو الرابطات أو المصالح أو الأنظمة المهتمة بشؤون الأحداث و المندوبين المكلفين بالرقابة على الأحداث المراقبين و رجال القضاء.

◆الإعلان عن الحكم

رغم أن المشرع قرر سرية جلسة محاكمة الحدث ، إلا أن هذه السرية لم تشتمل صدور الحكم .حيث يصدر الحكم في جلسة علنية و بحضور الحدث .

3.3.2.شروط قبول الأدلة المعلوماتية و حجيتها في الإثبات

إن الأدلة المعلوماتية إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات أو الراسم، و إما أن تكون مخرجات غير ورقية أو الكترونية كالأشرطة و الأقراص الممغنطة و اسطوانات الفيديو و الأقراص الضوئية و غيرها من الأشكال الالكترونية غير التقليدية، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به[94] ص183، و تعتبر هذه الأدلة الأساس الذي يعتمد عليه القضاء في إثبات الجريمة المعلوماتية . لكن و لكونها تعتبر شكلا جديدا من الأدلة المطروحة على القضاء – من غير المخرجات الورقية – فإن أول ما يثار بشأنها هو مدى إمكانية قبولها كأدلة لإثبات الجرائم المعلوماتية، و هل لها حجية في الإثبات ؟ هذا ما سنحاول الإجابة عليه في هذا المطلب،الذي سنقسمه إلى فرعين، نتطرق في الفرع الأول إلى شروط قبول الأدلة المعلوماتية، ثم نتناول في الفرع الثاني حجية هذه الأدلة في الإثبات.

1.3.3.2.شروط قبول الأدلة المعلوماتية

يشترط لقبول الأدلة المعلوماتية أمام المحاكم أن تتوافر ضوابط معينة يلتزم بها القضاة لتحاشي سوء التصرف و لدعم و حماية حقوق الأطراف و غيرها من الحقوق محل الاحترام، و هذه الضوابط مدارها أصل البراءة و ما يتفرع عنه من نتائج و آثار[1]ص69،70، والتي تتمثل فيما يلي:

1.1.3.3.2.أن تكون الأدلة المعلوماتية مشروعة

يشترط لقبول الأدلة المعلوماتية أن تكون مشروعة، و يقصد بذلك ضرورة اتفاق الإجراء الذي تم الحصول من خلاله على الدليل المعلوماتي مع القواعد القانونية و الأنظمة الثابتة في وجدان المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر و فقط على مجرد المطابقة مع القاعدة القانونية التي ينص عليها المشرع، بل يجب أيضا مراعاة إعلانات حقوق الإنسان و المواثيق و الاتفاقيات الدولية، قواعد النظام العام و حسن الآداب في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها المحكمة العليا [106] ص105،106، و قد أشار المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد في البرازيل في الفترة من 4 إلى 9 سبتمبر 1994 في قراره الصادر حول القواعد الإجرائية في بيئة جرائم الحاسوب، على أن الانتهاكات غير المشروعة لحقوق الإنسان التي يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون [107] ص314 ، و لقد صادقت لجنة الوزراء التابعة للمجلس الأوربي في 1981/01/28 على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، و من المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة و كاملة و دقيقة، و مستمدة بطرق مشروعة . [94] ص189

و على ذلك فإن القاضي ليس له أن يستند في حكمه على دليل معلوماتي تم الحصول عليه بطرق غير مشروعة. و من أمثلة الطرق غير المشروعة أو غير النزيهة التي يمكن أن تستخدم في الحصول على الأدلة المعلوماتية، إكراه المتهم (ماديا أو معنويا) من أجل فك شفرة الدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملف البيانات المختزنة، أو الاستجوابات المنهكة لقوى المتهم المعلوماتي، كأن يستدعى للتحقيق معه لمدد طويلة بغية معرفة معلومات معينة حول قاعدة بيانات أو نظام إدارة قواعد البيانات أو قنوات إرسال البيانات[68]

ص111، كما تعتبر من الطرق غير المشروعة في الحصول على الأدلة المعلوماتية قيام ضباط الشرطة القضائية بعمليات مراقبة الكترونية دون الحصول على إذن مسبق من السلطات المختصة.

إن كل دليل معلوماتي تم الحصول عليه بطرق غير مشروعة يجب على القاضي استبعاده، حتى و لو كان هذا الدليل، دليلا صارخا على إدانة المتهم المعلوماتي، وفي هذا الشأن ذهب المشرع الانجليزي إلى توسيع قاعدة استبعاد الدليل الجنائي الذي تم الحصول عليه بطريقة غير مشروعة . فوفقا له فإن كل دليل قد تم التوصل إليه مباشرة أو بطريقة غير مباشرة و كان متضمنا اعتداء على الحقوق الأساسية للمواطن يتعين استبعاده من جلسة المرافعات، حتى و لو كان دليلا ملائما أو موضوعيا يتصل بموضوع النزاع مباشرة يثبته أو يساهم في إثباته . [1] ص128،129

2.1.3.3.2.أن تكون الأدلة المعلوماتية يقينية

يشترط لقبول الأدلة المعلوماتية أن تكون هذه الأدلة مبنية على الجزم واليقين بعيدة عن الظن والتخمين، ذلك انه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، وهذا الجزم واليقين ليس مطلقا بل نسبيا فقط، فالمطلوب أن يبني القاضي عقيدته على أساس احتمالات ذات درجة عالية من الثقة لا يهزها أو يناقضها احتمال أخر.[1] ص85

ويمكن للقاضي أن يصل إلى اليقين والجزم من خلال ما يعرض عليه من أدلة مستخرجة من الحاسوب والانترنت، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، فيحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه، فكأن القاضي يصل إلى هذا اليقين من خلال نوعين من المعرفة :أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة وتفحصها، وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه الأدلة والملابسات التي أحاطت بها، فإذا لم ينته القاضي إلى الجزم بنسبة الفعل أو الجريمة المعلوماتية إلى المتهم المعلوماتي تعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي. [1] ص90،91

هذا وتشترط بعض التشريعات شروطا معينة ليقينية الأدلة المستمدة من الحواسب والانترنت، كقانون البوليس والإثبات في بريطانيا لسنة 1984، حيث يشترط ليقينية الأدلة

المعلوماتية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، أما في كندا فإن الرأي السائد في الفقه هو اعتبار مخرجات الحاسوب من أفضل الأدلة[94] ص191، وهو ذات ما ذهبت إليه بعض قوانين الولايات في أمريكا، حيث قضت أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد أفضل الأدلة المتاحة لإثبات هذه البيانات، وبالتالي يتحقق مبدأ يقينية الأدلة المعلوماتية، بيد أن هذا لم يمنع القضاء الأمريكي من استبعاد هذه المخرجات إذا كانت ناتجة عن حاسوب لا يؤدي وظائفه بصورة سليمة أو كان القائم عليه لا تتوافر فيه الثقة والطمأنينة.[1] ص95

ويقرر الفقه الياباني قبول الأدلة المستخرجة من الحاسوب و التي تم تحويلها إلى صورة مرئية سواء كانت هي الأصل أم كانت نسخا مستخرجة عن هذا الأصل، ففي هذه الحالة يتحقق اليقين الذي ينبني عليه الحكم الجنائي، كما يمكن أن يتحقق اليقين لهذه المخرجات أيضا من خلال التقارير التي يقدمها الخبراء. [94] ص191

أما على مستوى تشريعاتنا العربية فنجد المشرع الأردني يعتبر من خلال المادة 21 من قانون المعاملات الالكترونية المؤقت رقم 85 لسنة 2001 نظام المعالجة الالكتروني مؤهلا لإثبات تحويل الحق في السند بشرط أن تكون النسخة المعتمدة من السند محددة بصورة غير قابلة للتغيير وأن تدل النسخة المعتمدة من السند على اسم الشخص الذي تم سحب السند لمصلحته. [94] ص192

3.1.3.3.2.أن يتم مناقشة الأدلة المعلوماتية في الجلسة

إن اقتناع القاضي لا يجوز أن يبنى إلا على الأدلة التي عرضت في الجلسة و تمت مناقشتها، فمناقشة هذه الأخيرة في الجلسة توضح حقيقتها وتجلى غموضها وتكشف للمحكمة العناصر التي تكون منها قناعتها[97] ص172، كما أن استناد القاضي على دليل لم يطرح بالجلسة وليس له أصل ثابت بأوراق الدعوى يعني أن عمله يعتبر ابتداعا وانتزاعا للخيال[108]ص35. وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة، ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحواسب الآلية وأيضا بالنسبة لشهود الجرائم المعلوماتية الذين قد سبق وأن سمعت أقوالهم في التحقيق الابتدائي، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة، كذلك فإن خبراء

الأنظمة المعلوماتية على اختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحاكم لمناقشتهم أو مناقشة تقاريرهم التي خلصوا إليها إظهارا للحقيقة وكشفا للحق. [1] ص104

وقد اشترطت جل التشريعات وجوب مناقشة الأدلة في الجلسة، و من بينها المشرع الجزائري و ذلك من خلال الفقرة الثانية من المادة 212 من قانون الإجراءات الجزائية السالفة الذكر، كما نص عليه المشرع المصري من خلال المادة 302 من قانون الإجراءات الجزائية "..ومع ذلك لا يجوز له أن يبني حكمه على دليل لم يطرح أمامه بالجلسة.."

وتجدر الإشارة إلى أن مناقشة الأدلة المعلوماتية تحتاج إلى خبرة فنية ومعرفة بتقنيات الحاسوب الآلي، وهنا تظهر أهمية تدريب القضاة الذي نوهنا عنه فيما سبق، فمن شأن هذا التدريب أن يساعد القضاة على المناقشة الجيدة والبناءة للأدلة المعلوماتية على اختلاف أنواعها ومفرداتها.

2.3.3.2.حجية الأدلة المعلوماتية في الإثبات

إن حجية الأدلة المعلوماتية هي قيمة ما تتمتع به بأنواعها المختلفة الورقية أو الالكترونية والمصغرات الفيلمية من قوة استدلالية على صدق نسبة الفعل الإجرامي لشخص معين أو كذبه[1] ص22. وتختلف حجية الأدلة المعلوماتية من دولة إلى أخرى تبعا لنظام الإثبات المعتمد في كل منها. وتكشف الدراسات على وجود ثلاث أنظمة رئيسية للإثبات نظام الأدلة القانونية، نظام حرية الإثبات أو الاقتناع الذاتي للقاضي، ونظام الإثبات المختلط.

1.2.3.3.2.حجية الأدلة المعلوماتية في ظل نظام الأدلة القانونية

تكون الأدلة في نظام الأدلة القانونية محصورة ومحددة مسبقا من المشرع ولا يجوز للقاضي أن يخرج عليها أو يبني حكمه على خلافها، وبالتالي تكون قوتها الإثباتية محددة، فإذا ما توفرت شروط الدليل بالشكل الذي حدده المشرع وجب على القاضي أن يبني اقتناعه ويؤسس حكمه على أساس هذا الدليل، حتى و إن لم يكن مقتنعا به شخصيا، وعند عدم توافر الشروط المطلوبة قانونا يكون كذلك القاضي ملزما ببناء اقتناعه وتأسيس حكمه على أساس عدم قيام الدليل على الادعاء وإن كان القاضي مقتنعا تماما بثبوت الادعاء[26] ص85،و في ذلك بلا شك تقييد لسلطته التقديرية.

إن نظام الأدلة القانونية من شأنه في الكثير من الأحيان التقليل من أهمية الدليل المستمد من الحاسوب، خاصة و أن هذا النظام يعمل بقاعدة "الدليل الأفضل" أو "قاعدة المحرر

الأصلي"، و التي مؤداها انه لا يجوز قبول صورة للمستند أو المحرر إذا كان من الممكن الحصول على الأصل، و هو ما يقتضي إلغاء الدليل الثانوي لمحتوى المستند و تأسيسا على ذلك يشترط في الدليل الذي يقدم إلى ساحة القضاء أن يكون دليلا أصليا ، فالأصل يفضل على الصورة أو النسخة المطابقة . [1] ص94

و على ذلك فإن قبول الأدلة المعلوماتية كأدلة صالحة للإثبات أمام القضاء، قد يثير الكثير من الشكوك عندما تكون في صورة مخرجات للحاسوب، و ذلك باعتبار أن الإشارات الالكترونية و النبضات الممغنطة التي تعتمد عليها الحواسب الآلية في تشغيلها ليست مرئية للعين البشرية ، الأمر الذي لا يتأتى معه للقاضي مناظرتها أو وضع يده على الدليل الأصلي، و ما يقدم إليه من وثائق أخرجها الحاسوب- رغم أهميتها لنجاح الملاحقة الجنائية- يمكن الاعتراض على قبولها بدعوى أنها نسخ لأصول، مما يجعلها دليلا ثانويا و ليس أصليا. [7] ص387

و من الدول التي تتبنى هذا النظام المملكة المتحدة، و التي أصدرت قانونا للشرطة و الإثبات الجنائي سنة 1984 حوى تنظيما محددا لمسألة قبول مخرجات الحاسوب كأدلة إثبات في المواد الجنائية، حيث قضى بأن المستند الناتج عن الحاسوب الآلي لا يقبل كدليل، إذا لم يستكمل باختبارات الثقة المنصوص عليها في القسم 69 من هذا القانون، و التي يمكن بلورتها في ضرورة عدم وجود سبب معقول يدعو إلى الاعتقاد بأن مخرج الحاسوب غير دقيق أو أن بياناته غير سليمة. كما أوجبت أن يكون الحاسوب الناتج عنه هذا المخرج يعمل بكفاءة و بصورة سليمة[1] ص53. بمعنى أن قبول المستند الناتج عن الحاسوب في ظل هذا القانون يتوقف على مدى تطابقه مع المعلومات التي يتضمنها الحاسوب الآلي.

2.2.3.3.2.حجية الأدلة المعلوماتية في ظل نظام الإثبات الحر

نظام الإثبات الحر أو ما يسمى بنظام الاقتناع الذاتي للقاضي يقوم على أساس حرية الإثبات حيث يكون للقاضي سلطة تقديرية واسعة في تقدير الأدلة و قبولها، و لا سلطان عليه في ذلك إلا ضميره، و بذلك فله أن يبني قناعته على أي دليل طرح أمامه بالجلسة بشرط أن يكون هذا الدليل مشروعا.غير أن الملاحظ أن التعامل بالأنظمة المعلوماتية أصبح يفرض منطقا لا يتماشى و حرية القاضي أمام الدليل في الدعاوى العامة، فللأنظمة المعلوماتية دقة رقمية و مخارج، لا يمكن دحضها إلا بالمعطيات التي تناقضها.

ويمكن القول أنه و في ظل هذا النظام فإن حجية الأدلة المعلوماتية لا تثير أية صعوبات، فالدول التي تتبنى هذا النظام لا تتردد عموما في طرح الأدلة المعلوماتية أمام المحاكم ولا تجد صعوبة في قبولها . و من بين هذه الدول الجزائر حيث تنص الفقرة الأولى من المادة 212 من قانون الإجراءات الجزائية "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لإقناعه الشخصي" ، فالقانون الجزائري يعتمد مبدأ الإثبات الحر كأصل ونظام الأدلة القانونية كاستثناء، فلا يوجد ما يحول دون قبول الأدلة المعلوماتية في ظله طالما أنها لا ترد ضمن الاستثناءات المقررة.

و في فرنسا كذلك فإن حجية الأدلة المتحصلة من الحاسوب، على المستوى الجنائي لا تبدو مسألة ملحة أو عاجلة في نظر الفقهاء هناك، فالأساس هو حرية الأدلة و حرية القاضي في تقدير هذه الأدلة، و يدرس الفقه الفرنسي هذه الحجية تحت طائلة نطاق قبول الأدلة الناشئة عن الآلة آو الأدلة العلمية مثل أجهزة التصوير و أشرطة التسجيل وأجهزة التصنت [1] ص196

3.2.3.3.2.حجية الأدلة المعلوماتية في ظل النظام المختلط

يقوم النظام المختلط على تحديد المشرع سلفا لأدلة الإثبات التي يجوز للقاضي الاستناد إليها عند إصداره لحكمه في الدعوى التي ينظرها، مع منحه الحق في تقييم كل دليل على حدى، و تقرير كفايته للحكم بالإدانة، حيث أن المشرع لا يقوم بتحديد قيمة كل دليل في الإثبات أو إنما يترك هذا الأمر للقاضي يقدره بكامل سلطته التقديرية[7] ص393. ومن التطبيقات التشريعية الآخذة بهذا النظام نجد المشرع الياباني الذي حصر طرق الإثبات المقبولة في أقوال المتهم، أقوال الشهود و القرائن و الخبرة . أما بالنسبة لأدلة الحاسوب و الانترنت، فيقرر الفقه الياباني أن السجلات الالكترونية غير مرئية في حد ذاتها ، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية و مقروءة عن طريق محتويات الطباعة لمثل هذه السجلات، و في مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب و الانترنت سواء كانت هي الأصل أم كانت نسخة من هذا الأصل. [1] ص62

هذا و يلجأ البعض في الفقه الياباني و سايره البعض في الفقه المصري إلى حيلة يتم من خلالها التوصل إلى إمكانية قبول الأدلة المستمدة من الحاسوب الآلي في إثبات وقائع الدعاوى التي تتناول الجرائم المعلوماتية، و المتمثلة في التفرقة بين وسائل الإثبات و طرق

الإثبات المترتبة، فمن حيث وسائل الإثبات يرون أنها محددة على سبيل الحصر، أما طرق الإثبات فهي متنوعة و تتزايد يوما بعد يوم مع التقدم العلمي و التكنولوجي. [7] ص395

و على الرغم ما قد تثيره حجية الأدلة المعلوماتية في بعض الأنظمة القانونية من صعوبات، إلا أن هناك من ذهب إلى القول أن هذه الأدلة (خاصة الرقمية منها)، لا تثير أية صعوبات أمام المحاكم، و أرجع ذلك للأسباب التالية: [52] ص128،127

◆الثقة التي اكتسبها الحاسوب و الكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف المجالات.

◆ارتباط الأدلة الجنائية المعلوماتية (الرقمية) و آثارها، بالجريمة موضوع المحاكمة.

◆وضوح الأدلة المعلوماتية و دقتها في إثبات العلاقة بين الجاني و المجني عليه أو بين الجاني و السلوك الإجرامي .

◆إمكانية تعقب آثار الأدلة المعلوماتية و الوصول إلى مصادرها بدقة .

◆قيام الأدلة المعلوماتية على نظريات حسابية مؤكدة لا يتطرق إليها الشك، مما يقوي من يقينية الأدلة المعلوماتية.

◆الأدلة المعلوماتية يدعمها – عادة – رأي خبير، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة و فحصها و تقييمها و عرضها أمام المحاكم وفق شروط وقواعد نظمها القانون و اقرها القضاء.

و من جانبنا نرى أن هذا الرأي صائب نوعا ما ، فطبيعة الأدلة المعلوماتية و كونها تطبيق من تطبيقات الأدلة العلمية يجعلها تكتسي نوعا من الموضوعية و المصداقية، و لكن و على الرغم من ذلك فإن الأمر لا يخلو من الصعوبات، و ذلك راجع لحداثة هذا النوع من الأدلة التي أصبح القضاة و لعدم معرفتهم الجيدة بها يخشون التعامل معها، مما يجعل أمر قبولها يعتمد على مدى تفهم القاضي لها و مدى قدرته على الربط بينها و بين موضوع الجريمة المعلوماتية المرتكبة .

خاتمـــــــــة

باتت الثورة المعلوماتية السمة التي تميز العصر ، فالعالم اليوم يمر بلحظة انبهار محاولا استيعاب فوائد هذه الثورة الهائلة، التي أثرت في الفكر الإنساني. فقد أصبح استخدام الأنظمة المعلوماتية المقياس الذي يحدد مدى تطور الشعوب و تقدمها، حيث أحدثت هذه الثورة نقلة فريدة من نوعها، انتقلت بالشعوب من طور الركود و البطء في ممارسة الأنشطة المختلفة إلى طور المرونة و السرعة و الديناميكية و الحركة، نحو أداء الخدمات المرفقية و الوظيفية و المؤسساتية و تبادل المعلومات بشكل سهل و بسيط، وكذا الربط بين الأفراد و الجماعات و الشركات داخل المجتمع الدولي و كأنهم ينتمون إلى بلد واحد،فضلا عن تقريب المسافات و لغة الحوار و ممارسة المعاملات بكافة أنواعها عن طريق الشبكات المعلوماتية الدولية و الداخلية.

هذه الثورة المعلوماتية و رغم فوائدها التي لا تعد و لا تحصى، ألقت بمسؤولية كبيرة على عاتق أجهزة العدالة الجنائية التي باتت عاجزة عن استيعاب ما أفرزته هذه الثورة من جرائم لم تألف التعامل معها من قبل نظرا للطبيعة الخاصة التي تميزها و ارتباطها بشكل أساسي بالتقنيات المعلوماتية، التي ما فتئت أن ظهرت حتى أصبحت بعض الجهات و الأفراد تتسابق في التفنن في استخدامها من أجل تحقيق أهداف إجرامية، حيث أصبحت هذه التقنيات وسيلة جديدة في أيدي مجرمي المعلوماتية،المعروفين بمهارتهم و ذكائهم و إلمامهم بتقنيات الحاسوب الآلي و برمجياته و لغاته من أجل ارتكاب أخطر جرائمهم.

أمام هذا كله أصبحنا أمام معادلة غير متكافئة،طرفاها، أجهزة عدالة جنائية غير مؤهلة كما يجب للقيام بدورها في ظل التطورات المتلاحقة و المتسارعة للتقنيات المعلوماتية و في ظل غياب المعرفة التقنية لديها، و مجرمون معلوماتيون لهم من الخبرة والمهارة و المعرفة الفنية ما يؤهلهم لارتكاب جرائمهم دون إمكانية الاستدلال عليهم وبالتالي نشهد حاليا قفزة غير معقولة في ارتكاب الجرائم المعلوماتية، يقابلها ركود غير معهود في أجهزة العدالة الجنائية التي لا زالت في ثبات و غفلة.

و عليه و بناء على ما سبق، تطلب الأمر أن نتقدم بنتائج ما وصلنا إليه من خلال هذا الجهد المتواضع الذي قمنا به في سبيل التصدي لموضوع شديد الحساسية و في حاجة دائمة

للدراسة و التحليل بفعل ارتباطه بالتطور المستمر لتكنولوجيا المعلومات ، و يمكن بلورة هذه النتائج فيما يلي:

✓أن الجرائم المعلوماتية أصبحت تشكل نمطا خطيرا من الجرائم،التي يقوم النشاط الإجرامي فيها على استخدام تقنية الحاسوب الآلي بشكل مباشر أو غير مباشر كوسيلة أو هدف لتنفيذ الفعل المنشود.

✓ أن ارتباط الجرائم المعلوماتية بالتقنية المعلوماتية، جعل منها جرائم ذات طبيعة خاصة، تتميز عن غيرها من الجرائم التقليدية، سواء من حيث ماهيتها، و من حيث مرتكبيها وحتى من حيث ضحاياها.

✓أن تنامي ظاهرة الجرائم المعلوماتية بما تتميز به من طبيعة خاصة، أفرز جملة من التحديات على الصعيد الإجرائي، تجسدت في المقام الأول في مجموعة من العوائق التي أثرت في إثباتها.

✓أن عوائق إثبات الجرائم المعلوماتية متعددة و متنوعة، منها ما تعلق بالجريمة ذاتها، و منها ما تعلق بأدلتها، و منها ما تعلق بالعامل البشري فيها.

✓أن ما تثيره الطبيعة الخاصة بالجرائم المعلوماتية من عوائق في حقل إثباتها أصبح يستدعي التعامل معها وفق ما يتناسب وطبيعتها.

✓أن ما تتوفر عليه أجهزة العدالة الجنائية من مهارات قانونية، لم يعد يكفي لوحده لإثبات الجرائم المعلوماتية، و إنما أصبح الأمر يتطلب توفر مجموعة من المهارات الفنية من حيث التعرف على الحواسب الآلية و ملحقاتها، و معرفة أساسيات عمل الشبكات و مصطلحاتها، وغير ذلك من المعارف الفنية التي ترتبط ارتباطا وثيقا بالجرائم المعلوماتية.

✓أن إثبات الجرائم المعلوماتية، أصبح يستدعي و بشدة إعداد البرامج التدريبية المتخصصة الكفيلة بتلقين الجهات القائمة على إثبات الجرائم المعلوماتية، فنيات البحث والتحري و التحقيق و الحكم في هذا النوع المستحدث من الجرائم.

✓أن أجهزة العدالة الجنائية لم تعد قادرة لوحدها، على إثبات هذا النوع من الجرائم، و إنما أصبح من الضروري أن تساند هذه الأخيرة جهات خاصة تكون عونا لها كأجهزة شرطة

متخصصة للبحث و التحري في الجرائم المعلوماتية، و كذا فريق للتحقيق في هذا النوع من الجرائم .

✓أن وسائل التحقيق التقليدية لم تعد كافية لوحدها لإثبات هذا النوع من الجرائم، و إنما أصبح و لابد من تزويد أجهزة العدالة الجنائية بمجموعة من الأجهزة و البرمجيات الفنية التي تساعد في تحديد نوع الجريمة و توقيت ارتكابها و مصدرها و شخصية مرتكبيها، و كذا استرجاع الأدلة المتعلقة بها.

✓أن الإجراءات التقليدية أصبحت قاصرة عن إثبات الجرائم المعلوماتية المتميزة بسهولة ارتكابها وسرعة محوها، فأصبح الأمر يتطلب اتخاذ إجراءات تتلاءم و طبيعة هذه الجرائم، خاصة فيما يتعلق بإجراءات الضبط و التفتيش و المعاينة.

✓أن الأدلة المعلوماتية ما هي إلا تطبيق من تطبيقات الدليل العلمي بما تتميز به من موضوعية وحياد و كفاءة، ولهذا فلا يجب أن تثير أية صعوبة عند تقديمها كأدلة إثبات في الجرائم المعلوماتية.

✓أن الوصول إلى الحكم السديد في الجرائم المعلوماتية، أصبح يتوقف على مدى قدرة القاضي على مناقشة الدليل المعلوماتي، المناقشة العلمية الصحيحة التي تقوم على مدى تفهم القاضي لفحوى التقدم العلمي في مجال التقنية المعلوماتية و مدى قدرته على الربط بين الدليل المعلوماتي و الجريمة المرتكبة.

و على ذلك يمكن القول أن مجمل ما تم التوصل إليه من خلال هذه الدراسة، أن نظم و قواعد الإثبات التقليدية قاصرة على إثبات ما يقع من جرائم معلوماتية، فضلا على أن الفكر الأمني و القضائي غير ملائم لعملية إثبات الجرائم المعلوماتية، بل أصبح الأمر يحتاج إلى رجل أمن معلوماتي، و محقق معلوماتي، و قاض معلوماتي. لهذا ارتأينا أن نختم هذه الدراسة بمجموعة من التوصيات، لعلها تساهم و لو بقدر ضئيل في حل بعض المشكلات التي لمحناها في ثنايا هذه الدراسة، وتتمثل هذه التوصيات فيما يلي:

✓توعية مستخدمي الانترنت و الحاسوب الآلي و موظفي المصارف و المراكز العلمية، حول خطورة الجرائم المعلوماتية و ضرورة الحماية منها من جهة ،و أهمية الإبلاغ عنها و الإرشاد إلى مرتكبيها من جهة أخرى.

✓ضرورة تدريب و تأهيل الكوادر الأمنية و سلطات التحقيق و القضاء على كيفية التعامل مع هذا النوع من الجرائم، و تحقيق التعاون مع التقنيين أصحاب الخبرة و التخصص في المجالات المعلوماتية، و ذلك من خلال عقد دورات تدريبية بشكل دوري و دائم للاستفادة من خبراتهم و إرشاداتهم، بدءا من مرحلة جمع الاستدلالات إلى مرحلة التحقيق و انتهاء بمرحلة المحاكمة، و ما تتطلبه من خبرة و شهادة في المجال المعلوماتي.

✓العمل على إنشاء وحدات متخصصة للبحث و التحري و التحقيق في الجرائم المعلوماتية، و استقطاب المتميزين من ذوي الخبرة و التخصص للتحقيق في الجرائم المعلوماتية، بالإضافة إلى استقطاب الكوادر الوطنية من المتخصصين في الحاسوب الآلي، و تدريبهم للعمل كخبراء حاسوب جنائيين.

✓تزويد أجهزة العدالة الجنائية بالأجهزة و الوسائل و البرمجيات الضرورية للتحقيق في الجرائم المعلوماتية و تدريبها على كيفية التعامل بها و استخدامها .

✓ضرورة إعادة النظر في القوالب الإجرائية الحالية و تحديثها و استكمالها بما يتلاءم و طبيعة الجرائم المعلوماتية و تعقيدها، و ذلك على النحو الذي يحقق متطلبات الإثبات في الجرائم المعلوماتية.

✓تخصيص مقررات بالكليات العلمية لدراسة الجرائم المعلوماتية و أنواعها و طرق إثباتها و تطوير نظم الحماية منها.

✓تزويد مقرات و أقسام الشرطة بوصلات ارتباط بالانترنت لاستخدامها من قبل الضباط للتعود على التعامل مع خدمات الانترنت المختلفة، و الاطلاع على المستجدات في مجال الحاسوب بشكل عام و الجرائم المعلوماتية بشكل خاص، مع الاهتمام بوضع الضوابط الأمنية المناسبة لتأمينها من الهجمات الخارجية تحت إشراف متخصصين في أمن الحاسوب و الشبكات.

✓ضرورة تكثيف الجهود الدولية بوضع اتفاقيات دولية تستمد منها التشريعات الجنائية الداخلية ضوابط نصوصها، لتحقيق تنظيم جنائي إجرائي، كتطوير أدلة الإثبات بما يتلاءم مع هذا الشكل الجديد من الإجرام، بالإضافة إلى ضرورة تنظيم إجراءات التفتيش و ضبط المعلومات المتبادلة عبر شبكة الانترنت، و تسليم مجرمي المعلوماتية، و تبادل الخبرات و الأبحاث القائمة في هذا المجال .

✓العمل على عقد المزيد من الندوات العلمية و المؤتمرات حول العلاقة بين المعلوماتية و القانون .

✓تبادل الخبرات و المعلومات، و إبرام الاتفاقيات مع الدول المختلفة للتعاون على مكافحة الجريمة المعلوماتية ، و ذلك لتضييق الخناق على العابثين بالتعامل من خلال الشبكة المعلوماتية.

مـــــــــــلاحق

ملحـــــــــق رقم 01

القانون رقم 09- 04 المؤرخ في 05 أوت 2009 المتضمن القــواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

الفصـــــــل الأول

أحكـــام عامـــــــــــة

الهدف

المادة 01: يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .

المصطلحات

المادة02: يقصد بمفهوم القانون ما يأتي:

أ- الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال **:** جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

ب- منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين .

ج- معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها .

د- مقدمو الخدمات:

1- أي كيان عام أو خاص يقدم لمستعملي خدماته ، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

2- و أي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

هـ -المعطيات المتعلقة بحركة السير : أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، و الوجهة المرسل إليها، و الطريق الذي يسلكه ، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة.

و- الاتصالات الالكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.

مجال التطبيق

المادة03: مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون ،وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية.

الفصل الثاني

مراقبة الإتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادة04: يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

ج- لمقتضيات التحريات و التحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية المتبادلة .

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة .

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة " أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد و ذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها .

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 الاعتداءات على أمن الدولة و مكافحتها، و ذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير .

الفصل الثالث

القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادة05: يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية في الحالات المنصوص عليها في المادة4 أعلاه، الدخول، بغرض التفتيش، و لو عن بعد، إلى:

أ- منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية .

في الحالات المنصوص عليها في الفقرة"أ" من هذه المادة، 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 السلطات القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل .

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها .

حجز المعطيات المعلوماتية

المادة06: عندما تكتشف السلطات التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و أنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية .

غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات .

الحجز عن طريق منع الوصول إلى المعطيات

المادة07: إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول

إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها ، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة .

المعطيات المحجوزة ذات المحتوى المجرم

المادة08: يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة ، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك .

حدود إستعمال المعطيات المتحصل عليها

المادة09: تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادة10: في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم يد المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطة المذكورة .

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق .

حفظ المعطيات المتعلقة بالحركة السير

المادة11: مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال .

ج- الخصائص التقنية و كذا تاريخ ووقت ومدة كل اتصال.

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها .

هـ - المعطيات التي تسمح بالتعرف على المرسل إليه و المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها .

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة و كذا تلك التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه .

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، و يعاقب الشخص الطبيعي بالحبس من ستة(06) أشهر إلى (05) سنوات و بغرامة من 50.000 دج إلى 500.000 دج .

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات .

تحدد كيفيات تطبيق الفقرات 1و2و3 من هذه المادة، عند الحاجة ، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الأنترنت"

المادة12: زيادة على الالتزامات المنصوص عليها في المادة11 أعلاه، يتعين على مقدمي خدمات "الأنترنت" ما يأتي :

أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن .

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

إنشاء الهيئة

المادة 13: تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته .

تحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق التنظيم .

مهام الهيئة

المادة14: تتولى الهيئة المذكورة في المادة13 أعلاه، خصوصا المهام الآتية:

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلامو الاتصال و مكافحته .

ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية.

ج- تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال وتحديد مكان تواجدهم .

الفصل السادس

التعاون و المساعدة القضائية الدولية

الاختصاص القضائي

المادة15: زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني .

المساعدة القضائية الدولية المتبادلة

المادة16: في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون و كشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني .

يمكن في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعـــة بمـــا في ذلك أجهزة الفـــــــاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط كافية للتأكد من صحتها .

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادة17: تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة و الاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل .

القيود الواردة على طلبات المساعدة القضائية الدولية

المادة18: يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام .

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادة19: ينشر هذا القانون في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية .

ملحق رقم (2)

تطبيقات قضائية في الجرائم المعلوماتية

مجريات التحري و التحقيق في قضية سرقة بطاقات ائتمانية و الدخول على مواقع غير مصرح بها في مصر

أولا: تحريات الإدارة العامة لمباحث الأموال

الإدارة العامة لمباحث الأموال العامة

ادارة مباحث الأموال العامة بغرب الدلتا

محرر بتاريخ 2006/06/17م الساعة 11م

بمعرفتنا نحن العقيد /.....المفتش بالإدارة

أثبت الأتي

في إطار الجهود التي تبذلها الإدارة العامة لمباحث الأموال العامة في مجال مكافحة جرائم تزوير المسندات البنكية و بطاقات الدفع الالكتروني ،فقد سبق أن وردت معلومات سرية مفادها قيام بعض الشباب من مدينة الإسكندرية بممارسة نشاط إجرامي في مجال تزوير بطاقات الدفع الالكتروني و استعمالها في الاستيلاء على أموال البنوك المصرية و الأجنبية.

أكدت التحريات السرية للسادة مفتش إدارة مباحث التزييف و التزوير و إدارة غرب الدلتا صحة و جدية ما ورد من معلومات و أفادت التحريات بقيام كل من :

1- .....مواليد 1968/01/24 و المقيم 03 شارع .....- محطة الرمل – الاسكندرية.

2- .....مواليد 1983/03/12 و المقيم 20 شارع .....- محرك بك- و له إقامة أخرى بإتحاد ملاك برج الصيادلة بطريق 14 مايو بجوار مديرية الأمن الجديدة – سموحة- سيدي جابر.

3- .....السن 25 سنة – ومقيم 02 شارع .....ميامي – بدائرة قسم المنتزه.

و ذلك بممارسة نشاط إجرامي واسع في مجال تزوير المستندات البنكية و بطاقات الدفع الالكتروني و استعمالها في الاستيلاء على أموال البنوك المصرية و الأجنبية و كذلك الاستيلاء على بضائع و سلع من خلال الدخول على الشبكة الدولية للاتصالات " الأنترنت" و استعمال تلك البطاقات. و قد أكدت التحريات بأنه الثلاثة المذكورين يحوزون و يحرزون بمساكنهم في الصناديق الموضحة مستندات و بطاقات ائتمان مزورة و بضائع و سلع متحصلة من تلك الجريمة و الأجهزة و الأدوات المستعملة في التزوير.

و اقفل المحضر على ذلك عقب إثبات ما تقدم و بعرضه على السيد الأستاذ وكيل النائب العام للتكرم بالإطلاع و الإذن بضبط المتحرى عنهم الثلاثة المذكورين و تفتيش مساكنهم الموضحة لضبط ما بحوزتهم من مستندات و أوراق بنكية مزورة و بطاقات ائتمان و دفع الكتروني مزورة و الأدوات و الأجهزة المستعملة في تزويرها في تلك الجريمة و ضبط أية أشياء أخرى تظهر عرضا حال التفتيش و تعد حيازتها جريمة قانونا و كذلك الإذن بضبط متحصلات الجريمة المشار إليها.

ثانيا:إذن النيابة العامة بالقبض و التفتيش

في الثامن عشر من شهر جوان عام ألفين و ستة

و في تمام الواحدة و النصف صباحا بمقر النيابة

نحن(.....) وكيل نيابة شرق الاسكندرية الكلية

بعد الاطلاع على محضر التحريات المسطر خلفه بمعرفة العقيد /..... المفتش بالإدارة العامة لمباحث الأموال العامة – غرب الدلتا- و حيث أن ما وردته يعد جريمة حالة و قائمة يتعين ضبط مرتكبيها و بعد الاطلاع على الدستور و القوانين و الحريات العامة- لذلك-

نأذن للعقيد /..... المفتش بالإدارة العامة لمباحث الأموال العامة -لغرب الدلتا- أو من ينوبه أو يعاونه من مأموري الضبط القضائي المختصين قانونا بضبط و تفتيش شخص و مسكن المتحرى عنهم و الواردة أسماءهم وكذا عناوينهم و المؤشر اسم كل منهم بتوقيعنا بالمداد، و ذلك لضبط ما يحوزه أو يحرزه كل منهم من مستندات و أوراق بنكية مزورة و بطاقات ائتمانية و دفع الكتروني مزورة و الأدوات و الأجهزة المستخدمة في تزويرها، و كذا ما قد يظهر عرضا أثناء التفتيش و تعد حيازته أو احرازه جريمة يعاقب عليها القانون. على أن يتم هذا البند لمرة

واحدة فقط و موعد تمامه أربعة أيام من ساعته و تاريخه و يحرر محضر بما تم من إجراءات إيجابا و سلبا و يعرض في الحالة الأولى على النيابة المختصة فور الضبط رفق محرره.

2006/06/18 وكيل النيابة الكلية

(توقيع)

ثالثا:محضر الشرطة

الإدارة العامة لمباحث الأموال العامة

إدارة مكافحة جرائم التزييف و التزوير

تحرر بتاريخ 2006/06/18 جنح العطارين الساعة 8:50 مساءا

بمعرفتنا نحن الرائد /.....المفتش بالإدارة

أثبت الآتي

حيث ورد للإدارة بلاغ أنتربول واشنطن بشأن قيام المدعو/..... بارتكاب وقائع احتيالية على العديد من التجار أصحاب المحلات التجارية بالولايات المتحدة الأمريكية حيث تمكن من اختراق العديد من المواقع الالكترونية على شبكة الانترنت و سرق منها بيانات بطاقات ائتمانية خاصة بأشخاص أمريكيين الجنسية و استخدام تلك البيانات المسروقة في الدخول على مواقع التجار الأمريكيين على شبكة الانترنت و انتحل شخصية أصحاب البطاقات و طلب منهم شراء بضائعهم على أن تسدد قيمة البضائع من حسابات البطاقات الائتمانية المسروقة بياناتها.

حيث قام هؤلاء التجار بإرسال البضائع المشتراة و هي عبارة عن كتب و مجلات وبرامج كمبيوتر و أسطوانات و أشياء أخرى ذات قيمة إلى المذكور أعلاه ،الذي قام باستلامها من مكاتب البريد بمصر حيث تم اكتشاف تلك الوقائع حال رفض أصحاب البطاقات سداد قيمة تلك البضائع لعدم قيامهم بتلك العمليات أو طلبها و أنها تمت بالأسلوب الاحتيالي المشار إليه .

و التي أمكن للجانب الأمريكي تحديده و تحديد الشخص القائم على ذلك النشاط و هو المدعو/.....و ذلك بعدما تمكنوا من التتبع الفني للرسائل المرسلة من مصر إلى التجار الأمريكيين بمعرفة المتهم المذكور.

و حيث أسفرت التحريات التي قمنا بإجرائها بالاشتراك مع إدارة مكافحة جرائم الأموال العامة بغرب الدلتا عن صحة ما جاء بالبلاغ المشار إليه و أن المذكور هو وراء ارتكاب تلك الواقعة ،وأنه سبق ضبطه و اتهامه في قضيتين مماثلتين مقيدتين برقمي 42899 لسنة 2005 جنح الرمل،1703 لسنة 2006 إداري قسم الجيزة،و انه يزاول نشاط تزوير البطاقات الائتمانية و سرقة بياناتها و استخدامها في الاحتيال على الشركات المصرية و الأجنبية و الاستيلاء على بضائعهم من خلال شبكة المعلومات الدولية " الانترنت" ،حيث أن المذكور يعد من العناصر الإجرامية النشطة في مجال القرصنة على شبكة الانترنت.

كما أضافت التحريات بأن أشخاص آخرين يزاولون نفس النشاط ، ارتكبوا وقائع مماثلة بأساليب عديدة أخرى .... . و بعرض محضر بما توصلت إليه التحريات أذنت للسيد العقيد/..... المفتش بإدارة مكافحة جرائم الأموال بغرب الدلتا أو من ينوبه أو ينتدبه أو يعاونه من مأموري الضبط القضائي المختصين قانونا بضبط و تفتيش شخص و مسكن المتحرى عنه المذكور و المقيم سكنا بالعقار رقم 03 شارع/.....بمحطة الرمل بالطابق الأخير ، دائرة قسم شرطة العطارين الإسكندرية.

توجهت مأمورية من ضباط الإدارة العامة لمباحث الأموال العامة برئاسة السيد العقيد /..... تحت كل من السيد المقدم /.....و المقدم مهندس/.....المفتش بالإدارة ، وقوة من الشرطة السريين بسيارة الإدارة إلى مسكن المتحرى عنه لتنفيذ إذن النيابة العامة و نظرا لإلمام السيد العقيد /.....بطبيعة المنطقة و قاطنيها ،قد قام سيادته بتأمين المأمورية عقب انتدابنا لتنفيذ إذن النيابة العامة .و بالصعود إلى شقة المأذون بتفتيشه و الذي تبين وجوده بالشقة ، و بالإفصاح له عن شخصيتنا و طبيعة مأموريتنا و إذن النيابة العامة بتفتيش شخصه و مسكنه ،عثرنا داخل حجرة نومه الخاصة على ما يلي:

1- ثمانية إخطارات بوصول طرود من الخارج باسم المذكور صادرة عن الهيئة القومية للبريد (مكتب المنشية).حيث قرر المذكور حال مناقشته أن تلك الإخطارات خاصة بوصول طرود من الخارج له، و أن تلك الطرود عبارة عن بضائع و كتب و برامج تمكن من الاستيلاء عليها بعدما احتال على التجار أصحاب الشركات الأجانب، و قدم إليهم بيانات بطاقات ائتمانية منتحلا شخصية أصحابها و ذلك لخصم قيمة تلك البضائع من حساباتها " موضوع بلاغ أنتربول واشنطن".

2- العديد من الكتب و القواميس و البرامج الكمبيوترية و التي تمكن المتهم من الحصول عليها بإتباعه الأسلوب الإجرامي الوارد بالبلاغ و بالتحريات ،و حيث أقر المتهم حال مناقشته، بأن تلك البضائع جزء من البضائع التي تمكن من الاستيلاء عليها بالأسلوب الإجرامي المشار إليه، وأنه في طريقه لإعادة بيع تلك البضائع و الكتب و الحصول على مقابلها النقدي مثل البضائع الأخرى التي تمكن من الاستيلاء عليها بذات الأسلوب الإجرامي و التي قام ببيعها.

3- مبلغ نقدي قدرة ثمانية مئة و خمسون جنيها أقر المذكور بأنها من متحصلات نشاطه المؤثم المشار إليه.

4- جهاز كمبيوتر بمشتملاته عبارة عن:

أ- وحدة تحكم مركزي ماركة Ghost .

ب- لوحة مفاتيح ماركة Pyeniun.

ج- ماوس(فارة) بدون علامة تجارية.

د- شاشة ماركة GTX.

هـ- عدد واحد اسطوانة (سي-دي).

و- موزع شبكات خاص بالاتصال بشبكة الانترنت ماركة Speed touch.

ز- كاميرا رقمية خاصة بالاستعمال على شبكة الانترنت ماركة CREATIVE.

ولم يسفر التفتيش عن ثمة مضبوطات أخرى.

و بمواجهة المذكور بما جاء ببلاغ انتربول واشنطن و ما أسفرت عنه التحريات و اسفر عنه الضبط و التفتيش أقر بارتكابه واقعة بلاغ انتربول واشنطن، و وقائع أخرى مماثلة بدول أجنبية أخرى بخلاف أمريكا، كما أقر بمزاولته النشاط المؤثم الوارد بالتحريات و سبق ضبطه في وقائع مماثلة و اقر بحيازته للمضبوطات المشار إليها و أنها من متحصلات نشاطه.

و بسؤاله عن كيفية حصوله على بيانات البطاقات الائتمانية التي تمكن من سرقتها و استخدامها في الاحتيال على أصحاب المحلات التجارية بالعديد من الدول الأجنبية و الحصول على بضائعهم أقر أنه نظرا لما لديه من خبرة عالية في مجال استخدام الحاسب الآلي و كيفية اختراق المواقع الالكترونية الخاصة بالشركات و البنوك و الأشخاص، فقد تمكن من

الحصول من تلك المواقع التي استطاع اختراقها ،على بيانات البطاقات الائتمانية و البيانات الشخصية لأصحابها.

و أضاف أنه تمكن أيضا من الحصول على أرقام بطاقات ائتمانية خاصة بأجانب عن طريق تخليق الأرقام، بأن يحصل على رقم بطاقة صادرة عن أحد البنوك و يقوم بتخليق منها مجموعة من الأرقام و ذلك باستخدامه برنامج خاص بذلك ،و أضاف بأن جهاز الكمبيوتر الخاص به و المضبوط محمل عليه ذلك البرنامج ،و المواقع التي كان يخترقها و بيانات البطاقات الائتمانية التي قام باستخدامها في الاستيلاء على البضائع و كذا مواقع التجار الأجانب التي كان من خلالها يخاطبهم منتحلا شخصية صاحب البطاقة و يمدهم ببيانات البطاقة والتي يتم بموجبها إرسال البضائع له.

و عليه فقد قمنا بضبط المذكور و التحفظ على المضبوطات و العودة إلى ديوان الإدارة و تحرر محضر بما تم من إجراءات.

ملحوظة1: أرفق بالمحضر صورة ضوئية من إذن النيابة العامة المشار إليه حيث تم إرفاق أصل الإذن بالمحضر المحرر بشأن واقعة ضبط وتفتيش شخص المتهم/.....ـــ تمت الملحوظة ـــ

ملحوظة 2: تم تحريز إخطارات وصول الطرود الصادرة عن الهيئة القومية للبريد و عددهم ثمانية المثبتين بالمحضر و المضبوطين بمسكن المتهم/..... و ذلك بوضعهم داخل مظروف وشمع عليه في عدد من المواضع بخاتم بصمته /.....ـــ تمت الملحوظةـــ

ملحوظة 3: تم تحريز الكتب و برامج الكمبيوتر و القواميس المضبوطة بمسكن المتهم المذكور و ذلك بوضعهم داخل كرتونه و شمع عليها بالشمع الأحمر في عدد واحد موضع بخاتم يقرأ ذات البصمة/.....ـــ تمت الملحوظةـــ

ملحوظة 4: تم وضع المبلغ النقدي المضبوط و قدره ثمانية و خمسون جنيه داخل مظروف مفتوح ـــ تمت الملحوظةـــ

ملحوظة 5:تم تحزيز وحدة التحكم المركزي المضبوطة بوضعها داخل كرتونه و شمع عليها بالشمع الأحمر في عدد واحد موضع بخاتم يقرأ ذات البصمةـــ تمت الملحوظة

ملحوظة 6: تم تحريز الشاشة و لوحة المفاتيح و الماوس و موزع الشبكات و الكاميرا و (الهارد ديسك) و الاسطوانة المضبوطين وتم وضعهم جميعا داخل كرتونه، لفت بدوبارة و شمع عليها بالشمع الأحمر في عدد واحد موضع بخاتم يقرأ ذات البصمة ــ تمت الملحوظة ــ

ملحوظة 7: تم عرض الأجهزة المضبوطة على السيد المقدم مهندس/.....لفحصها و إعداد تقرير بنتيجة الفحص لإرفاقه بالمحضر- تمت الملحوظة-

و عليه أقفل المحضر عقب إثبات ما تقدم و يعرض لقيده برقم أحوال في النيابة بالمتهم و الإحراز للاطلاع و التصرف فيها.

ثالثا: تقرير الفحص الفني

وزارة الداخلية

الإدارة العامة لمباحث الأموال العامة

إدارة مكافحة جرائم التزييف و التزوير

تقرير فحص فني

بمعرفتنا نحن مقدم مهندس/.....- المفتش بوحدة الفحص المعملي بالإدارة – قمنا بتاريخ الأحد الموافق ل 2006/06/18 بفحص الأجهزة المضبوطة بيانها كالأتي:

جهاز كمبيوتر يتكون من :

1- وحدة تحكم تحمل علامة تجارية تقرأ Ghost .

2- شاشة كمبيوتر تحمل علامة تجارية تقرأ CTX.

3- لوحة مفاتيح تحمل علامة تجارية تقرأ Premium.

4- ماوس بدون علامة تجارية.

5- كاميرا رقمية تستخدم في الاتصال بشبكة الانترنت ماركة Creative.

6- موزع شبكات يستخدم في الاتصال بشبكة الانترنت ماركة Speed touch.

7- عدد واحد أسطوانة كمبيوتر CD.

و بفحص محتويات الملفات المخزنة على جهاز الكمبيوتر تبين أنه يوجد بداخل المجلد الرئيسي "D" مجلد فرعي أخر باسم " Program files" بداخله مجلد فرعي باسم " Ccverify" بداخله ملف باسم " ccverifier .exe" ،و بفتحه تبين أنه برنامج خاص بفحص أرقام بطاقات الائتمان و التأكد من صحتها.

و بفحص محتويات الملفات الموجودة داخل الاسطوانة المضبوطة (1) تبين أنه يوجد بداخلها مجلد باسم" Trench" و بفتحه تبين أنه يوجد بداخله الملفات الأتية:

1- ملف باسم " 50visa credit card members 2002" يوجد بداخله العديد من أرقام بطاقات الائتمان .

2- ملف باسم "alfando" يوجد بداخله بيانات بطاقات ائتمان و تشمل (رقم البطاقة و اسم صاحبها و تاريخ الانتهاء و الحد الائتماني و البنك المنسوب إليه البطاقة).

3- ملف باسم " Ice- cvv2.text" يوجد بداخله أيضا العديد من بطاقات الائتمان المشابهة للبند السابق.

4- ملف باسم " mathuat.text" يوجد بداخله بيانات العديد من بطاقات الائتمان .

5- كما يوجد تسعة ملفات باسم " cc2.text" إلى " cc10.text" ويوجد أيضا بداخلها العديد من البيانات الكاملة لبطاقات ائتمانية .

و بفحص جميع بيانات بطاقات الائتمان الموجودة بداخل الملفات السابقة ،تبين أنه يمكن استخدام البطاقات " السارية" التي لم ينتهي تاريخ الانتهاء الخاص بها ، في جميع أنواع عمليات الشراء عبر شبكة الانترنت ،و كذلك يمكن استخدامها في تحويل مبالغ مالية من رصيد صاحب البطاقة الأصلي من خلال مواقع تحويل الأموال الموجودة على شبكة الانترنت، حيث أن البيانات الموجودة في الملفات السابق ذكرها تشتمل على جميع البيانات المطلوب إدخالها على موقع تحويل الأموال لإتمام عملية تحويل المبالغ المالية من رصيد صاحب البطاقة الأصلي إلى مستخدم تلك البيانات المسروقة.

هذا و بعد الانتهاء من فحص جميع محتويات جهاز الكمبيوتر و الملفات الموجودة داخل الاسطوانة قمنا بإغلاق الجهاز إغلاق طبيعي.

و هذا تقرير فني بنتيجة الفحص. مقدم مهندس/

ثانيا:الإرسالية

وزارة الداخلية

الادارة العامة لمباحث الاموال العامة

السيد/مأمور قسم شرطة العطارين

تحية طيبة ...و بعد

نتشرف بأن نرسل لسيادتكم رفقة الحرس المحضر رقم (3ح)الإدارة في تاريخ 2006/06/18 عدد أربعة أحراز موضحة بالمحضر و مبلغ ثمانية مئة و خمسين جنيه و المتهم /.....للتكرم لقيد و عرض المتهم و الأحراز على النيابة العامة تنفيذا لما تأشر عليه المحضر في هذا الخصوص.

و تفضلوا سيادتكم بقبول فائق الاحترام

2006/06/19 م

مدير ادارة

مكافحة جرائم الأموال بغرب الدالتا

(.....)

رابعا: الإحالة على المحكمة

في 05/ 2006/12

نحن/..... وكيل النيابة

بعد الاطلاع على الأوراق و ما تم فيها من تحقيقات

أولا:تفيد الأوراق جنحة ،بالمادة 336 من قانون العقوبات ، و المواد 48، 2/20 ،2/68 من القانون 143 لسنة 1993 ، و المادتين 1،23 فقرة اولى بند (ب) و فقرة أخيرة من القانون رقم 15 لسنة 2004 من قانون التوقيع الالكتروني.

ضـــــــد

.....

لأنه في تاريخ سابق على 2006/06/18 بدائرة قسم العطارين

1- توصل إلى الاستيلاء على المنقولات المبينة وصفا و قيمة بالأوراق و المملوكة لأجانب غير معلومين و كان ذلك بالاحتيال لسلب بعض ثرواتهم باستعمال طرق احتيالية من شأنها ايهامهم بحصول ربح و همي و اتخاذ أسماء كاذبة.

2- ارتكب تزويرا بمحرر الكتروني و ذلك بطريق التعديل و انتحال أسماء مالكي بطاقات ائتمان على النحو المبين بالاوراق.

3- لم يحمل بطاقة تحقيق شخصية حال كونه من رعايا جمهورية مصر العربية و جاوز السادسة عشر من العمر.

ثانيا: تقدم الاوراق لجلسة 2007/01/09.

وكيل النيابة

مجريات المحاكمة في أول قضية قرصنة الكترونية في الجزائر

أولا : بدء الجلسة

بدأت الجلسة بالمناداة على المتهم " ع. ي"،21 سنة طالب بالسنة الثالثة ثانوي، المقيم بحي بوزوران بباتنة ، حيث قام القاضي بالتحقق من هويته و أحاطه علما بالتهمة المنسوبة إليه و هي تهمة البحث والتجميع و النشر و الاتجار في معلومات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية الفعل المعاقب عليه بالمادة 394 مكرر 2 من قانون العقوبات.

ثانيا:بدء التحقيق

بعد التحقق من هوية المتهم، تم البدء باستجوابه من قبل القاضي و كذا النيابة العامة حيث تمحورت الأسئلة حول مكتب التحقيقات الفدرالي الأمريكي و الأتراك و الروس و الانجليز و كبرى الشركات الأمريكية الخاصة بتطوير منظومات حماية المواقع الالكترونية و القرصنة و بيع وشراء المعلومات عبر العالم الافتراضي (الانترنت) عن طريق المساومة و الابتزاز، و أجاب المتهم بكل ثقة على ما وجه له من الأسئلة مفندا التهمة المنسوبة إليه، موضحا انه كان فقط يقوم ببيع أنظمة معلومات خاصة بحماية المواقع الالكترونية و يقوم بخدمات إشهارية لصالح أصحاب المواقع الراغبة في ذلك، نظير تلقيه أموال مقابل هذه الخدمات ،غير أن القاضي كان يؤكد في كل مرة، أن المتهم يقوم بالدخول إلى مواقع شركات أمريكية و يستولي على معلوماتها السرية، قبل أن يساومها من جديد بدفع أموال مقابل استرجاع تلك المعلومات ، كما أكد القاضي أن المتهم يقوم ببيع تلك المعلومات لقراصنة من استراليا و أوروبا الغربية، روسيا و تركيا، وهو ما أكدته الخبرة المنجزة من طرف الشرطة العلمية و التي تلى تفاصيلها شرطي خبير ،قال أن المتهم و باستعمال بريده الالكتروني الحامل لاسم مستعار يعني بالعربية "القبعة البيضاء" قام باقتحام شركة "ساف نات وورك" الأمريكية المختصة في توفير الحماية لمختلف المواقع الالكترونية ، و استولى على معلومات سرية لزبائنها و ساوم القائمين على الشركة بدفع مقابل مالي نظير استرجاع تلك المعلومات ، و أن المتهم كان يقوم ببيع معلومات خاصة بزبائن مواقع أخرى مقابل مبالغ مالية ترسل إليه عن طريق حوالات بريدية عبر مؤسسة "وستون يونيون" العالمية .

ثالثا :المرافعات

ممثل الحق العام و في مرافعته أشار إلى تواجد عدة مواقع شركات أمريكية اقتحمها الهاكر الباتني ، ذكر منها ثلاث مواقع و انه عرض بيع 2000 معلومة ، المعلومة بـ 8 دولار ، و ذلك خلال أطوار الفخ المنصوب له من قبل الجهات المختصة ، و أضاف وكيل الجمهورية بمحكمة الجنح بباتنة أن هذه الجريمة تعتبر سابقة من نوعها أمام القضاء الجزائري و أن القانون يجرم أفعالها و أن ما قام به المتهم يدخل في إطار التهمة الموجهة إليه، ملتمسا في الأخير إدانته بسنتين حبس نافذ.

أما عن دفاع المتهم المتكون من محامين ، فقد ركزا في مداخلتهما على انعدام أركان الجريمة من ركن مادي و معنوي ، كما رفض احد المحامين الخبرة التي أتت بها العدالة ، حيث قال انه من الطبيعي أن تكون الخبرة ضد المتهم في هذه الحالة مطالبا رئيس الجلسة تسجيل إشهاد ، رفض من قبل القاضي ، مضيفا إلى أن موكله أخطأ بالدخول إلى الشبكة العنكبوتية، لكنه لم يقم البتة بقرصنة مواقع أمريكية أو بيع معلوماتها، ملتمسا من هيئة المحكمة البراءة لموكله.

رابعا : صدور الحكم

تمت إدانة المتهم بعام حبس نافذة و 50 ألف دينار جزائري غرامة إلى جانب مصادرة الأشياء المحجوزة.

قائـــمة المراجـــع

1.هلالي عبد اللاه أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الأولى،دار النهضة العربية، القاهرة ،1997.

2.محمد سامي الشوا،الغش المعلوماتي كظاهرة إجرامية مستحدثة،المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ،من 25 الى 28 أكتوبر 1993.

3.Jean Claude Berreville,Le particularisme de la preuve en droit pénal douanier, Thèse Lille,1966 .

4.محمد علي العريان ،الجرائم المعلوماتية ، دار الجامعة الجديدة للنشر، الأزاريطة، 2004.

5. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى ، منشورات الحلبي الحقوقية، بيروت ،2005.

6.أيمن عبد الله فكري ، جرائم نظم المعلومات ، دار الجامعة الجديدة للمنشورات، الإسكندرية، 2007.

7.فتوح الشادلي ، عفيفي كامل عفيفي ، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، منشورات الحلبي الحقوقية ، لبنان ، 2003.

8.يونس عرب، جرائم الكمبيوتر و الانترنت ،بحث مقدم لمؤتمر الأمن العرب، أبو ظبي ، من 10الى 12 فيفري2002.

9.أحمد خليفة الملط، الجرائم المعلوماتية،الطبعة الثانية ،دار الفكر الجامعي، الإسكندرية، 2006.

10.محمد أمين الشوابكة ، جرائم الحاسوب و الأنترنت (الجريمة المعلوماتية) ، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، عمان ،2007.

11.Nidal El Chaer ,La Criminalité informatique devant la justice pènale ,Edition juridique Sader ,Liban ,2004.

12.أسامة أحمد المناعسة،جلال محمد الزعبي، صايل فاضل الهواوشة،جرائم الحاسب الآلي و الانترنت،الطبعة الأولى ، دار وائل للنشر، عمان ، 2001.

13.هدى حامد قشقوش ، جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ، من 25 الى 28 أكتوبر 1993.

14.محمد احمد عبابنة ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة للنشر والتوزيع ، عمان، 2005.

15.اليوسف عبد العزيز،التقنية في الجرائم المستحدثة،بحث منشور ضمن كتاب الظواهر الاجرامية المستحدثة وسبل مواجهتها،منشورات أكاديمية نايف للعلوم الامنية، الرياض،1999.

16.شنيتي حفيظة، الجريمة المعلوماتية كفاءات عالية و إمكانيات متطورة لمواجهة الظاهرة،مجلة الشرطة ، عدد خاص، الجزائر، جويلية 2009.

17.جعفر حسن جاسم الطائي،جرائم تكنولوجيا المعلومات،الطبعة الأولى ، دار البداية، عمان، 2007.

18.خالد ممدوح ابراهيم،أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية،2008.

19.عبد الفتاح مراد ،موسوعة مصطلحات الكمبيوتر و الانترنت ، دار الكتب و الوثائق المصرية ،مصر،(دون سنة).

20.سامي منصور ، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية ، المنشورات الحقوقية صادر، بيروت ، 2006.

21.علاء الدين محمد شحاتة ، رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ، من 25 إلى 28 أكتوبر 1993.

22. محمد حماد مرهج الهيتي ، جرائم الحاسوب ، الطبعة الأولى، دار المناهج للنشر و التوزيع، عمان ،2006.

23.علي عبد القادر القهواجي، الحماية الجنائية لبرامج الحاسب ، دار الجامعة الجديدة للنشر و التوزيع، الإسكندرية،1997 .

24.نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري ،دار الهلال للخدمات الإعلامية، الجزائر، 2005.

25.محمد أبو بكر سلامة ، جرائم الكمبيوتر و الانترنت،منشأة المعارف، الإسكندرية،2006.

26.سيدي محمد البشير،دور الدليل الرقمي في إثبات الجرائم المعلوماتية،رسالة ماجستير في العلوم الشرطية،أكاديمية نايف العربية للعلوم الأمنية، ، الرياض، 2010.

27.عبد الفتاح بيومي حجازي ،الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر،2005.

28.نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى،دار الثقافة للنشر و التوزيع، عمان ،2008.

29.عبد الفتاح بيومي حجازي ،جرائم الكمبيوتر و الانترنت في التشريعات العربية، الطبعة الأولى، دار النهضة العربية ، القاهرة ،2009.

30.فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري ، بحث مقدم إلى الملتقى المغاربي حول القانون و المعلوماتية ،أكاديمية الدراسات العليا بليبيا، أكتوبر 2009.

31.علي عبد القادر القهواجي ، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت،1999.

32.محمد أمين الرومي ، جرائم الكمبيوتر و الانترنت ، دار المطبوعات الجامعية، الإسكندرية، 2003 .

33.أيمن عبد الحفيظ ،الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية،(دون دار نشر)،2005.

34.خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.

35.يحي بن محمد ابو مغايض ، الأبعاد الإستراتيجية في مواجهة الجرائم المعلوماتية، بحث مقدم للملتقى العلمي لمكافحة الجرائم المعلوماتية ، الرياض ، من 12 إلى 14 أكتوبر 2009.

36.محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، من 25الى 28 أكتوبر 1993.

37.محمود محمد حسين المرزوقي، جرائم الحاسوب ، المجلة العربية للفقه و القضاء، عدد 28،مصر،2003.

38. مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية (ما هيتها ،مكافحتها)، دار الكتب القانونية ، مصر ،2005.

39.سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت ،دار الفكر الجامعي، الإسكندرية، 1999.

40.بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية ، 2008.

41.فوزية عبد الستار، شرح قانون العقوبات ، الطبعة الخامسة ، دار النهضة العربية ، القاهرة، 1991.

42.Philippe Rosè ,La criminalité informatique, deuxième édition, Edition Dahleb ,1995.

43.Mohamed Buzubar, La criminalité informatique sur l’internet , journal of law , vol 26 ,Koweït ,March 2002.

44.حسن طاهر داوود، جرائم نظم المعلومات، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000 .

45.تركي بن عبد الرحمن المويشير،التحقيق في الجرائم المعلوماتية ، ورقة عمل مقدمة للملتقى العلمي لمكافحة الجرائم المعلوماتية ،الرياض ،من 12 إلى 14 أكتوبر 2009.

46.عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي ، الطبعة الأولى ، دار النهضة العربية، الإمارات العربية المتحدة ،2001.

47.عبد الفتاح بيومي حجازي ، الإثبات الجنائي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية ، مصر،2001.

48.عمر محمد بن يونس، التحكم في جرائم الحاسوب وردعها ،مؤسسة آدم للنشر والتوزيع، مالطا ،2005.

49.محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي والانترنت ،المجلة العربية للدراسات الأمنية والتدريب ،عدد 30 ، السعودية، نوفمبر 2000.

50.عبد الله عبد الكريم عبد الله ،جرائم المعلوماتية و الانترنت ،الطبعة الأولى ، منشورات الحلبي الحقوقية ، لبنان،2007.

51.كمال احمد الكركي، التحقيق في جرائم الحاسوب ، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، الإمارات العربية المتحدة، من 26 إلى 28 أفريل 2003.

52.محمد الأمين البشري، الأدلة الجنائية الرقمية مفهومها و دورها في الإثبات، المجلة العربية للدراسات الأمنية و التدريب، المجلد 17،العدد33، السعودية،2001.

53.ممدوح عبد الحميد عبد المطلب ، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية،مصر، 2006.

54.موسى مسعود أرحومة ،الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية ، بحث مقدم للمؤتمر المغاربي الأول حول المعلوماتية والقانون ، طرابلس، من 28 إلى 29 أكتوبر 2009.

55.عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الكتب القانونية و دار شتات للنشر والبرمجيات،مصر،2007.

56.علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، الإمارات العربية المتحدة، من 26 إلى 28 أفريل 2003 .

57.محمد حماد مرهج الهيتي ، التكنولوجيا الحديثة و القانون الجنائي، دار الثقافة ، عمان، 2004.

58.عبد المحسن بدوي محمد أحمد، الجرائم المعلوماتية، مجلة الأمن و الحياة ، عدد 335 ، السعودية،2010.

59.منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي، الإسكندرية ،2005.

60.عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة ، الجزائر،2005.

61.محمود نجيب حسيني ، شرح قانون الإجراءات الجزائية ، الطبعة الثالثة، دار النهضة العربية، القاهرة ،1995.

62.انظر نص المادة 16و19من قانون الإجراءات الجزائية.

63.نبيلة هبة هروال،الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى ، دار الفكر الجامعي، الإسكندرية ،2006.

64.Christiane Feral-Schuhl, Cyber Droit , 3éme édition , Dalloz Dunod, Paris, 2002.

65.أنظر المادة 13في الملحق رقم 01 ص 163.

66.انظر المادة 14 في الملحق رقم 01 ص 163.

67. مصطفى إبراهيم عيسى ، جرائم العصر، مجلة الأمن و الحياة ،عدد340، السعودية، 2010 .

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

69. محمد بن نصير محمد السرحاني، مهارات التحقيق الفني في جرائم الحاسوب و الانترنت ، رسالة ماجستير في العلوم الشرطية ، جامعة نايف العربية للعلوم الأمنية ، الرياض، 2004.

70. محمد أبو العلا عقيدة ، شرح قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ،القاهرة،2001 .

71. محمد زكي أبو عامر ، الإجراءات الجنائية ، الطبعة السابعة ، دار الجامعة الجديدة، الإسكندرية، 2005.

72.Eoyhan Casey, Hand Book of computer crime investigation, second edition,Academic press,Britain,2003.

73.Catherine H.conly, Organizing of computer crime investigation and prosecution, institute of justice ,Washington.

74.أنظر محضر الشرطة في الملحق رقم 02 ص 167.

75. معراج جديدي ، الوجيز في الإجراءات الجزائية مع التعديلات الجديدة ، (بدون دار النشر)، الجزائر،2004.

76. أبو العلا علي أبو العلا النمر ، الإثبات الجنائي ، الطبعة الثانية ، دار النهضة العربية ، القاهرة، 1991.

77. محمد أبو العلا عقيدة، التحقيق وجمع الأدلة في الجرائم الالكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، الإمارات العربية المتحدة ،من 26 إلى 28 أفريل .2003

78.احمد إبراهيم الكفاوين، إجراءات التحقيق في الجرائم المعلوماتية ، ورقة عمل مقدمة للملتقى العلمي لمكافحة الجرائم المعلوماتية ، الرياض، من 12الى 14 أكتوبر 2009.

79.أنظر المادتين 10و 11 في الملحق رقم 01 ص 162،161.

80. مصطفى محمد موسى ،المراقبة الالكترونية عبر شبكة الانترنت ،الطبعة الأولى، دار الكتب والوثائق القومية المصرية ، مصر ،2003.

81.أنظر المادة 03 في الملحق رقم 01 ص 158.

82. أنظر المادة 04 في الملحق رقم 01 ص 158 .

83.معجب بن معدي الحويقل، المرشد للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض ،2003.

84. عبد الكريم الردايدة ،الجامع الشرطي في إجراءات التحقيق الجنائي و أعمال الضابطة العدلية ،الطبعة الأولى، دارالبراع، عمان ، 2006.

85. جيلالي بغدادي، التحقيق (دراسة مقارنة)،الطبعة الأولى، الديوان الوطني للأشغال التربوية ،الجزائر، 1999.

86. أحمد أبو الروس ،التحقيق الجنائي والتصرف في الأدلة الجنائية ،دار المطبوعات الجامعية، الإسكندرية، 1992.

87. عبد الرحمان محمد العيسوي، سيكولوجية المحقق الجنائي، مجلة الأمن والحياة، عدد 327، السعودية،2009.

88.Dictionnaire encyclopédique bilingue de la micro- informatique, Microsoft press, France.

89.Lance Spitzner, Honypots : Traking Hackess, Pearson éducation ,boston,2003.

90.سليمان منجع العنزي، وسائل التحقيق في جرائم نظم المعلومات،رسالة ماجستير في العلوم الشرطية ،كلية الدراسات العليا، أكاديمية نايف العربية للعلوم الأمنية ، الرياض، 2003.

91. أبو الوفا محمد أبو الوفا،المواجهة الإجرائية للجرائم المعلوماتية، مداخلة ضمن ندوة جرائم المعلومات،الإمارات العربية المتحدة، في 24 نوفمبر 2010.

92. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف المسماوي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية،بحث مقدم للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب لشرعي ، الرياض، من 12الى 14 نوفمبر2007.

93. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، الطبعة السابعة، دار النهضة العربية ،القاهرة ،1993.

94. علي حسن محمد الطوالبة،التفتيش الجنائي على نظم الحاسوب و الانترنت،الطبعة الأولى،عالم الكتب الحديث، الأردن، 2004.

95. معتصم خميس مشعشع ، إثبات الجريمة الالكترونية ، مداخلة ضمن ندوة جرائم تقنية المعلومات ، الإمارات العربية المتحدة ، في 24نوفمبر2010.

96.هلالي عبد اللاه أحمد ، التزام الشاهد بالإعلام في الجرائم المعلوماتية ، دار النهضة العربية، القاهرة، 1997.

97.حسن يوسف مصطفى مقابلة، الشرعية في الإجراءات الجزائية، الطبعة الأولى، الدار العلمية الدولية للنشر والتوزيع ودار الثقافة للنشر والتوزيع،عمان، 2003.

98. صالح سالم جودة، القاضي الطبيعي، دار النهضة العربية، القاهرة ،1997.

99. أحمد فتحي سرور ، الشرعية الدستورية و حقوق الإنسان في الإجراءات الجنائية، طبعة معدلة ، دار النهضة العربية ، القاهرة ،1995 .

100. مداولة المجلس الأعلى للقضاء المجتمع في دورته العادية الثانية يوم 23 ديسمبر 2006 المتضمنة مدونة أخلاقيات مهنة القضاة .

101. مدونة القيم القضائية المغربية الصادرة عن الودادية الحسينية للقضاء في شهر أفريل 2009.

102. محمد السيد عرفة ، تدريب رجال العدالة وأثره في تحقيق العدالة ، بحث ضمن أبحاث المؤتمر الدولي للقضاء والعدالة ، الجزء الثاني، الطبعة الأولى، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.

103. عوض محمد، قانون الإجراءات الجنائية، الجزء الثاني، (بدون دار نشر)، الإسكندرية، 1995.

104. نصر الدين مروك، محاضرات في الإثبات الجنائي، الجزء الأول، دار هومة، الجزائر، 2003.

105.أنظر الملحق رقم 02 ص 175.

106. أحمد فتحي سرور ، الشرعية و الإجراءات الجنائية، دار النهضة العربية ، القاهرة، 1997.

107. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت ، دار المطبوعات الجامعية، الإسكندرية، 2008 .

108. رمزي رياض ،سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة) ، دار النهضة العربية، القاهرة ، 2004.