الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الدكتور الطاهر مولاي – سعيدة –
كلية الحقوق والعلوم السياسية
قسم : الحقوق

الحماية الإجرائية والموضوعية للجريمة المعلوماتية

مذكرة لنيل شهادة الماستر:

تخصص : قانون جنائي

من إعداد الطالب :

☐ شيباني عبد الكريم.

تحت إشراف الأستاذ :

• بومدين أحمد

أعضاء اللجنة المناقشة

- الأستاذ ..... مشرفا.
- الأستاذ ..... رئيسا.
- الأستاذ ..... عضوا مناقشا.
- الأستاذ ..... عضوا مناقشا.

الموسم الجامعي 2015-2016

كن عالما فإن لم تستطع فكن متعلما فإن لم

تستطع فأحب العلماء

تشكرات

الشكر لله الذي خلق الكون فنظمه و خلق الإنسان فكرمه، فالق الحب و النوى منزل التوراة و الإنجيل و الفرقان.

- **كما نتقدم بالشكر للأستاذ المشرف " بومدبن أحمد " و نتقدم له بكل امتنانا و ذلك نظرا لتشجيعه و توجيهاته القيمة.**
- **كما لا يفوتنا أن نشكر كافة عمال الإدارة .**

إهـــــداء

إلى التي عجز القلم عن بيان فضلها إلى من وضعت الجنة تحت قدميها و أعزما أملك في الوجود إليك والدتي

إلى الذي لا تكفي الكلمات لذكر فضله علي إلى الذي أعطاني كل شيء و لم يرد جزاءا و شكورا إلى الذي انار لي دربي والدي

إلى الأستاذ المشرف "د. **بومدين أحمد**

مقدمة عامة

مقدمة:

- لئن كانت الألة هي محور تقدم الذي حصل في القرن الماضي فإن المعلومات هي محور تقدم في عصرنا هذا و الذي سمي بإسمها " عصر المعلومات" .

و لم يعد يخفى على أحد ما أصبحت تمثله هذه المعلومات من أهمية، حتى باتت سلعة متناولت فهي قد غزت مختلف جوانب الحياة و إرتبطت بمختلف الأنشطة و الأعمال و لقد بات إلزاما على كل مجتمع ينشد التطور و الإزدهار أن يولي لها الإهتمام و أن يحقق لها التدفق و الإنسياب مما يكفل الإستفادة القصوى منها.

لقد أتاحة هذه التكنولوجيا القيام بكثير من الأعمال التي كان يستحيل من قبل إنجازها فلقد وفرت هذه التكنولوجيا في مجال الإتصالات الإلكترونية و تحقق التواصل الإنساني و الإنجاز المعاملات في سهولة و ييسر و ذلك من خلال الشبكات المتطورة التي أصبحت تتسم بصورة عالية جدا و تحول كما هائلا من المعلومات المتدفقة بين أماكن متفرقة من العالم في ثوان معدودات، هذا و قد زاد الإقبال على هذه الشبكات و أهمها شبكة الإنترنيت .

لكن إن كان هذا هو الجانب المشرق لما يسمى بالمعلوماتية فإن هذه الأخيرة و ككل تطور قد حملت بين طياتها جانبا مضلما

أفرزته إستعمالها لأغراض غير مشروعة و هو ما يسمى بالجريمة المعلوماتية هذه الجريمة إلتبست بلباس المعلوماتية و إتسمت بها من سمات ما تقدمه من تطور ، فتغيرت عن غيرها من الجرائم بخصائص و تقنيات عديدة.

و بذلك تتحدد أهمية دراسة موضوع الجريمة المعلوماتية أو جرائم الكمبيوتر و الأنترنيت كوسيلة للإتصال الجماهيري العالمي لا يمكن تجاهله بسبب شعبيته و إنتشاره أصبحت شبكة المعلومات العالمية جزءا من النشاط اليومي لملايين الأفراد في مجتمعاتنا، هذا ما أدى بالبعض إستغلال هذه الوسائل في إرتكاب جرائمه الغش المعلوماتية، و جوهر المعلوماتية هو المعلومات و التي تدخل إلى الحاسب الىلي و تحول إلى المعطيات بعد معالجتها و تخزينها و قد جرمة هاته الأفعال التي تشكل أدوانا على المعطيات و هذه الجرائم تقع على الأشخاص و على الأموال و هناك أيضا جرائم تعرف بالدخوا أو البقاء الغير المصرح به لأنظمة المعالجة الآلية لمعطيات و كذا جريمة التلاعب بالمعطيات.

فما هي ما هية الجريمة المعلوماتية ؟ و ما هي الجرائم الواقعة على هاته المعطيات؟ و ما هي أهمية هذه الحماية الإجرائية و الجنائية؟ و هل وضع المشرع الجزائري تجريم لأفعال هذه الجريمة؟

كل هذه الإشكاليات سنحاول الإجابة عليها في بحثنا هذا.

أما أهمية هذه الدراسة و سبب إختياري لهذا الموضوع هو التعريف بظاهرة جديدة يزداد إنتشارها يومنا بعد يوم و نأمل أن نسلط الضوء على هذا الموضوع بما يساعد على التعرف أليه و لو شيئا قليلا.

و من الصعوبات التي إعترضت طريق الباحث خلال قيامه بهذا البحث العلمي و حداثة هذا الموضوع، إذ أنه من المواضيع الغضة التي لم يشدو عودها بعد لأنه جزء من الجريمة المعلوماتية، و نتيجة لذلك فقد قل الباحثون في هذا المجال و قلة مراجعهم خاصة في العالم العربي.

أما في ما يخص منهج الدراسة في بحثنا هذا المنهج التحليلي و يتمثل في القيام بتحليل هذه الجريمة موضوع الدراسة .

و قد حاولنا ايضا في مراحل هذا البحث العلمي على المقارنة في مختلف التشريعات و عرضنا مختلف الآراء الفقهية حول الجريمة المعلوماتية.

لقد قسمنا هذا البحث إلى فصلين: خصصنا الفصل الأول للكلام حول ما هية الجريمة المعلوماتية بمفهومها الفقهي و القانوني و خصائصها و ما ميزها عن الجرائم الأخرى.

فيه نتكلم الخصائص المجرم المعلوماتي بالاإضافة ايضا إلى أركان هذه الجريمة.

أما الفصل الثاني: فقد خصصناه للحديث عن الحماية الإجرائية للمعلومات الإلكترونية و تطورها على الصعيد الوطني و الدولي.

و كذا الحماية الجنائية للمعلومات الإلكترونية لموجب النصوص المستحدثة للمشرع الجزائري و ماقرر لها من جزاءات و أنهينا هذا البحث بخاتمة تضمنت أهم ما توصلنا إليه.

الفصل الأول

ماهية الجريمة المعلوماتية

الفصل الأول : ماهية الجريمة المعلوماتية

إن الحقيقة الثابتة والبسيطة تقول بأن الوسائل العلمية التقنية لم تخترع الجريمة بل كانت ضحية لها في معظم الأحوال ، معظم الأحوال ، حيث أن هذه الوسائل تعرضت لسوء الاستغلال من قبل كثيرين عبر التاريخ ومن الثابت أيضا أن معظم المجرمين قد وظفوها ضمن أدواتهم المختلفة لخدمة النشاطات الإجرامية التي يقومون بها .

أما الجريمة فهي ذاتها الجريمة في قديم التاريخ وحديثة لا يختلف على بشاعتها وخطرها على المجتمع الإنساني أحد وبمرور حقب التاريخ المختلفة كانت الظاهرة الإجرامية مرادفة للتجمع الإنساني تعكس في أساليبها وأنماطها أحوال وتطورات المجتمع في مختلف النواحي ، وفي عصر التقنية وثورة الاتصالات الحديثة تعددت .

الجريمة وتنوعت أساليب مستفيدة من التطور التقني في كافة مناحي الحياة ، حيث وظف المجرمون هذه المستحدثات التقنية الحديثة في تطوير أساليبهم بلى حتى التقنية ذاتها لم تسلم من الجريمة فمنذ بدايتها ظهر معها ما يعرف بجرائم التقنية أو الجرائم المعلوماتية .

وبالنظر إلى حداثتها هل يمكن القول أن هاته الجريمة حازت على غرار الجرائم التقليدية على مفهوم متفرد بالنظر إلى طبيعتها القانونية ؟

وبناءا على ذلك سوف نحاول الكشف عن تعريف الجريمة المعلوماتية (المبحث الأول) واستقصاء طبيعتها نظرا لما تتمتع به من خصوصية (المبحث الثاني) .

المبحث الأول مفهوم الجريمة المعلوماتية :

ما كانت جرائم الانترنت من جرائم التقنية العالية أي من الجرائم المستحدثة ، وكانت التشريعات العقابية قاصرة عن تناولها ، فإن كثيرا من المحققين ورجال الضبط في كثير من الدول يواجهون صعوبات أثناء التصدي لتلك الجرائم ، فإن هذا النوع من الجرائم قد يطال المعرفة ، الاستخدام الثقة ، الأمن ، الربح ، المال ، ومع هذا كله فهي لا تطال حقيقة غير المعلومات ، لكن المعلومات بأشكالها المتباينة في البيئة الرقمية تصبح شيئا فشيئا معرفة بذلك المعلوماتية هي جرائم العصر الرقمي [1]وسوف نستقضي تعريفها قانونيا وفقهيا (المطلب الأول) وسنبين خصائصها (المطلب الثاني) .

المطلب الأول : تعريف الجريمة المعلوماتية :

مع دخول الحاسوب والانترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها ، حيث سنقوم بتعريفها قانونيا وفقهي .

الفرع الأول : التعريف القانوني

تعرف الجريمة في القوانين الوضعية بأنها كل فعل يعاقب عليه القانون أو امتناع عن فعل يقضي به القانون ولا يعتبر الفعل أو الترك جريمة إلا إذا كان مجرما في القانون ، ويحدد القانون الوضعي عقوبات محددة للمخالفات بمعنى أنه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لا يعتبر جرم .

من ناحية أخرى الجريمة هي كل فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين وبالتالي فالجرائم المعلوماتية ، أي فعل ضار يأتيه المواطن عبر استعماله الوسائط

[1] انظر نبيلة هبة هروال ، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الأولى 2007 ص 24 .

الالكترونية مثل الحواسيب ، شبكات نقل المعلومات ، شبكة الانترنت ، أو الاستخدامات غير قانونية للبيانات الحاسوبية أو الالكترونية عموما .

فمع تطور الانترنت وتوسع استخداماتها وازدياد أعداد المستخدمين لها في العالم) حوالي 1.6 مليار مستخدم يمثلون ربع سكان العالم) أصبحت الانترنت وسطا ملائما للتخطيط ولتنفيذ عدد من الجرائم بعيدا عن رقابة و أعين الجهات الأمنية ، إذن الجريمة المعلوماتية هي استخدام الوسائط الحاسوبية والشبكات الانترنت أو التخطيط لها .

الفرع الثاني : التعريف الفقهي

لقد أعطى الفقهاء والدارسون عددا ليس قليلا من التعريفات تتميز وتتباين تبعا لموضع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته ، وقد اجتهدنا في جمع غالبية التعريفات التي وضعت في هذا الحقل .

فمن التعريفات التي تستند إلى موضوع الجريمة أو أحيانا إلى أنماط السلوك على التحريم ، تعريف الأستاذ ROSENBALT بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقة " أو هي كما عرفها الفقيه سولارز " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات.

أما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة فإن أصحابها ينطلقون من أن الجرائم المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة ، ومن هذه التعريفات :

تعريف الأستاذ جون فورستن " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ويعرفها ناديمان بأنها " كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب"[1] .

ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل .

[1] انظر هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن ، دار النهضة العربية ، القاهرة 1992 ص 120 .

تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية " أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها.

كما عرفها الأستاذ " دافيد تومسن " أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي [1].

المطلب الثاني : خصائص التحقيق الجريمة المعلوماتية

الفرع الأول : مميزات الجريمة المعلوماتية عن غيرها من الجرائم

تعتبر الجرائم المعلوماتية النوع الشائع من الجرائم إذ أنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى ارتكابها ويمكن تعريف تلك الجرائم بأنها الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الانترنت وبواسطته شخص على دراية فائقة بهما .

وباستقرائنا لهذا التعريف تتضح لنا الخصائص التي تتميز بها الجرائم المعلوماتية فهي جرائم ذات خصائص منفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها وهذه الخصائص هي :

1/ الحاسب الآلي هو أداة ارتكاب الجرائم المعلوماتية :

تعتبر هذه الخاصية من أهم الخصائص التي تميز هذا النوع عن غيرها من الجرائم الأخرى ، ذلك لأن شبكة الانترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة ، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي ، ويقصد بالحاسب الآلي وفقا للموسوعة الشاملة لمصطلحات الحاسب الالكتروني كل جهاز الكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال وإخراج معلومات وإجراء عمليات حسابية ، وهو يتكون من كيانين كيان مادي ومعنوي يضم أولهما

[1] أنظر هشام محمد فريد رستم العقوبات ومخاطر جرائم المعلوماتية ، دار النهضة العربية ، القاهرة 2000 ص 20.

الأجهزة المادية المختلفة والتي تشمل وحدات الإدخال والإخراج والتشغيل ، أما الكيان الثاني فيشتمل على البرمجيات الجاهزة والبيانات والمعلومات المنطقية [1] .

2/ الجرائم ترتكب عبر شبكة الانترنت أو عليها :

تعد شبكة الانترنت الحقل الذي تقع فيه الجرائم المعلوماتية وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم وغيرها من الأهداف التي تكون غالبا الضحية لها إلا أنه وبالرغم من كونها الوسيلة لارتكاب الجرائم إلى جانب الحاسب الآلي فإنها كذلك لن تنجو من يد المجرمين لأنها هي الأخرى قد تكون محلا للاعتداءات[2].

3/ مرتكب الجرائم المعلوماتية هو شخص ذو خبرة :

تتطلب هذه الجرائم على غرار الجرائم التقليدية الحرفية الفنية العالية سواء عند ارتكابها أو عند العمل على عدم اكتشافها ، أي يجب أن يكون ذلك الشخص خبيرا بالقدر اللازم بأمور الحوسبة ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي ، فإن الشرطة تبحث أولا عن خبراء الكمبيوتر عند ارتكاب هذا النوع من الجرائم[3] .

4/ جريمة الانترنت جريمة عابرة للحدود :

لقد سبق وأن ذكرنا أن شبكت الانترنت ذات طابع دولي إذ أنها لا تعترف بتلك الحدود القائمة بين الدول سواء الجغرافية أو السياسية وهذا ما أدى إلى اعتبار أن الجرائم المعلوماتية من الجرائم الدولية ، وتأخذ بعدا دوليا من حيث إمكانية أن يكون العمل الإجرامي عبر الانترنت ذو طبيعة عالمية ذلك حينما ترتكب داخل الدولة إلا أنها تمتد إلى خارج تلك الأخيرة مما يعني خضوعها لأكثر من قانون جنائي ، كما أنها تأخذ ذلك البعد في الحالة التي يعترفا فيها المشرع الدولي بأن العدوان يمكن أن تقوم به دولة ولو في صيغة التأييد ، وتعتبر الجرائم المعلوماتية جرائم

---

[1] انظر نبيلة هبة هروال ، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الأولى 2007 ص 35 .

[2] أنظر نبيلة هبة هروال ، نفس المرجع أعلاه ص 36 .

[3] انظر نبيلة هبة هروال ، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، المرجع السابق ص 38 .

دولية في الحالة التي يكون أحد أطرافها شخصا دوليا ، كما أنه يمكن أن تكون في مقابل ذلك جريمة وطنية إذ أن لها أثرا إقليميا من حيث أن حجم الأثر السكاني يحتويها كأي جريمة ثانية[1] .

5/ صعوبة إثبات الجرائم المعلوماتية :

تعتبر هذه الخاصية من الخصائص المميزة للجرائم المعلوماتية عن غيرها من الجرائم نظرا لكونها ترتكب بواسطة أو على الانترنت ومن قبل شخص ذو دراية فائقة بها وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة والتخلص من أثارها وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها والقبض عليهم على غرار الجريمة التقليدية وإلى جانب الأسباب السابقة فإنه تعود صعوبة إثبات الجرائم المعلوماتية إلى:

- صعوبة الإثبات الفني بآثارها إن وجدت .

- يلعب البعد الزمني (اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي قانون يطبق) دورا مهما في تشتيت جهودا التحري والتنسيق الدولي لتعقب هذه الجرائم [2] .

الفرع الثاني : خصائص مرتكب الجريمة المعلوماتية :

إن المجرم المعلوماتي ليس له نموذج محدد بل هناك عدة نماذج للمجرمين قد يستخدمون الكمبيوتر في جرائمهم وقد يقومون بأفعال إجرامية ضد الكمبيوتر نفسه ، فلهذا نجد صعوبة في تحديد سمات معينة لمرتكب الجريمة الالكترونية ويرجع ذلك إلى تعدد الجرائم وتنوعها ، ورغم ذلك فإن مرتكبها بالنسبة للمجموعة التقليدية هو شخصية مستقلة بذاتها فهو من جهة مثال منفرد للمجرم الذكي وهو من جهة أخرى اجتماعي بطبيعته وكذلك يتميز بصفات خاصة تميزه عن غيره من مرتكبي الجرائم الواردة في قانون العقوبات ، فمن السمات العديدة لمرتكب الجريمة المعلوماتية .

[1] أنظر نبيلة هبة هروال ، نفس المرجع أعلاه ص 39

[2] أنظر نبيلة هبة هروال ، نفس المرجع أعلاه ص 39

1/ مرتكب الجريمة المعلوماتية من النوابغ :

إن المجرم المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي فهذا المجرم يصنف ضمن نوابغ المجرمين خاصة الأحداث الناجحين منهم والذين يخشى عليهم من الدخول من مجرد الهواية إلى الاحتراف في أفعال اختراق النظم[1].

2/ مرتكب الجريمة المعلوماتية متكيف اجتماعيا :

فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل إنه إنسان متكيف اجتماعيا ذلك أنه أصلا مرتفع الذكاء ويساعده على ذلك عملية التكيف ، وما الذكاء في رأي الكثيرين سوى القدرة على التكيف ولا يعني ذلك التقليل من شأن المجرم بل أن خطورته الإجرامية تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه ، ويذكر كذلك أن الإجرام المعلوماتي تمخض عنه عوامل مستحدثة في أذهان مرتكبيه حيث لجأ العديد منهم إلى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتية [2].

3/ مرتكب الجريمة المعلوماتية مجرم متخصص :

فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم .

4/ مرتكب الجريمة المعلوماتية مجرم محترف :

ذلك أنه لا يسهل على الشخص المبتدئ في حالات قليلة أن يرتكب جرائمه عن طريق الكمبيوتر فالأمر يقتضي كثيرا من الدقة والتخصص في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر .

5/ مرتكب الجريمة المعلوماتية مجرم غير عنيف :

[1] انظر عبد الفتاح البيومي الحجازي ، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي) دار الفكر الجامعي ، الطبعة الأولى ، الاسكندرية 2006 ص 83 .

[2] نظر عبد الفتاح البيومي الحجازي ، نفس المرجع أعلاه ، ص 84 .

ذلك أنه ينتمي إلى إجرام الحيلة فهو لا يلجأ إلى العنف في ارتكاب جرائمه وهذا النوع لا يستلزم مقدارا من العنف للقيام به .

وخلاصة القول إن من صفات المجرم أنه يتميز بالذكاء ولا يميل إلى استخدام القوى أو العنف كما يتميز بأنه إنسان اجتماعي ، فالجرائم الالكترونية لها وجه إنساني بالنظر إلى أن مرتكبها كائن اجتماعي ، ولها الوجه الآخر حين نتدبر الآثار المترتبة عليها [1] .

[1] نظر عبد الفتاح البيومي الحجازي ، نفس المرجع أعلاه ، ص 86

المبحث الثاني : أركان وأنواع الجرائم المعلوماتية :

الجريمة بمصطلحها العام قديم ظهر بظهور البشرية ولكن بشكلها الجديد هي شر يماشي عصر العولمة ومن المعروف أن الجريمة العادية تتكون من ثلاثة أركان ركن مادي وركن معنوي وركن شرعي وهو الحال بالنسبة للجريمة المعلوماتية وحاليا المجال مفتوح لكل أنواع الجرائم المعلوماتية التي يصعب حصرها أو تعدادها نظرا لازديادها وتنوع أساليبها كلما أمعنا البحث في هذا المجال نجد أنه بالتطور التكنولوجي تتطور وتتعدد هذه الجرائم ويصعب تقسيمها ، حيث صنفها الفقهاء والدارسون ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم فبعضهم يقسمها إلى جرائم ترتكب على نضم الحاسب الآلي وأخرى ترتكب بواسطته وغيرهم يؤسسها على تعدد الحق المعتدى عليه فتتوزع الجرائم المعلوماتية حسب هذا التقسيم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص .

وبناءا على ما تقدم فإننا سوف نتطرق في مبحثنا هذا إلى أركان الجريمة المعلوماتية (المطلب الأول) ثم سوف نخوض في أنواع الجرائم التي تقع على الأشخاص وعلى الأموال 'المطلب الثاني) .

المطلب الأول : أركان الجريمة المعلوماتية :

يقصد بأركان الجريمة عناصرها الأساسية التي يتطلبها القانون لقيام الجريمة وهي أركان خاصة وهي التي ينص عليها المشرع بصدد كل جريمة على حدى وأركان عامة وهي واجب توافرها أي كان نوع الجريمة أو طبيعتها ، وعليه ستقوم بتطبيق الأركان العامة للجريمة العادية على الجريمة المعلوماتية[1].

[1] أنظر عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام ، ديوان المطبوعات الجامعية ، الجزائر الطبعة السادسة 2005 ص65 .

الفرع الأول الركن المادي :

الأصل أن القانون لا يعاقب على النوايا مهما كانت شريرة مادامت محبوسة في نفس الجاني فالقانون يعاقب على الأفعال المادية التي تصدر من الجاني [1]

وعليه تكمن عناصر الركن المادي في السلوك الإجرامي فهو الأفعال التي يقوم بها المجرم فهذا الفعل قد يكون بالإيجاب أو السلب . و بتطبيق هذا الركن على الجرائم الإلكترونية فان النشاط أو السلوك المادي فيها يتطلب وجود بيئة رقمية و اتصال بالانترنت ، و يتطلب أيضا أن يقوم مرتكب الجريمة بتجهيز لها فمثلا يقوم مرتكبها بتجهيز الحاسب الآلي و يقوم بتحميل الجرائم الاختراق أو أن يقوم بإعداد هذه البرامج بنفسه و كذلك يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة .

لكن كل جريمة تستلزم وجود أعمال تحضيرية و في الحقيقة يصعب الفصل بين العمل التحضيري و البدء في النشاط الإجرامي في الجرائم الالكترونية حتى و لو كان القانون لا يعاقب على الأعمال التحضيرية .

حيث تنص المادة 31 من القانون 06-23 المحاولة في الجنحة لا يعاقب عليها إلا بناءا على نص صريح في القانون . و المحاولة في المخالفة عليها إطلاقا.[2]

إلا انه في مجال التكنولوجية المعلومات الأمر يختلف بعض الشيء ، فشراء برامج اختراق و معدات لفك الشفرات و الكلمات المرور و حيازة صور دعارة ، فمثل هذه الأشياء جريمة في حد ذاتها .

والعنصر الثاني هو النتيجة وهي الأثر المادي المترتب عن السلوك الإجرامي ، وتثير مسألة النتيجة الإجرامية في ، الجرائم الالكترونية مشاكل عدة فعلى سبيل المثال مكان وزمان تحقق

[1] أنظر عبد الله سليمان ، المرجع أعلاه ص144 .

[2] انظر القانون 06 – 23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66- 156 المؤرخ في 8-نيونيو 1966 (ج.ر رقم 84 المؤرخة في 24-12-2006).

النتيجة الإجرامية فلو قام أحد المجرمين في أمريكا باختراق خادم أحد البنوك في الإمارات فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أو توقيت بلد البنك المسروق .

أما العنصر التالي فهو العلاقة السببية وهي التي تربط بين الفعل والنتيجة وتجدر الإشارة على إلا أن الجرائم الانترنت تتمثل فيها الفكرة النتيجة المحتملة ذلك راجع إلى طبيعة النشاط التقني الذي قد يترتب عليه نتائج عدة فمثلا من يقصد القرصنة ويتحقق معها انتشار الفيروسات فإن ذلك يعتبر نتيجة محتملة لذلك العمل ، وإذا كان النشاط المادي يحدث كله في العالم الافتراضي فإن نتيجة الإجرامية لها كيان منفصل لكونها تحدث شكل إنقسامي ما بين حدوثها في العالم المادي جزئيا أو كليا [1].

الفرع الثاني : الركن المعنوي :

هو الجانب الشخصي أو النفسي للجريمة فلا تقوم ، الجريمة بمجرد قيام الواقعة المادية التي تخدع لنص التجريم بل لابد أن تصدر هذه الواقعة من إرادة فاعلها وترتبط بها ارتباطا معنويا .[2]

وعناصر الركن المعنوي القصد الجنائي وهو العلم بعناصر الجريمة وإرادة ارتكابها وهما العلم والإرادة ، ففي الجريمة المعلوماتية الركن المعنوي هو الحالة النفسية للجاني والعلاقة بين ماديات الجريمة وشخصية الجاني ، حيث برزت مشكلة الركن المعنوي في الجريمة المعلوماتية في قضية موريس الذي منهما في قضية دخول غير مصرح به على جهاز الحاسب الفدرالي وقد دفع محامي موريس على انتقاء الركن المعنوي الأمر الذي جعل المحكمة تقول هل يلزم أن يقوم الادعاء بالثبات القصد الجنائي في جريمة الدخول الغير مصرح به بحيث تثبت نية المتهم في تحدي الخطر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر .

[1] انظر نبيلة هبة هروال ، الجوانب الإجرامية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، دار الفكر الجامعي ، الاسكندرية ، الطبعة الأولى 2007 ص 48-49 . .

[2] أنظر عبد الله سليمان ، المرجع أعلاه ص 231 .

أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو الأعم في الجرائم الالكترونية ، حيث يشترط المشرع الفرنسي وجود سوء النية في الاعتداء عللا بريد الكتروني خاص بأحد الأشخاص .

أما بالنسبة للمشرع الجزائري فقد نص في المادة 394 مكرر 2 من جريمة المساس بأنظمة المعالجة الآلية للمعطيات ، على أنه كل من يقوم عمدا وعن طريق الغش ، وهنا فقد تحقق عنصر العلم والإرادة [1].

الفرع الثاني : الركن الشرعي

يعبر عن الركن الشرعي في الجريمة بلا جريمة ولا عقوبة ولا تدابير أمن إلا بنص في القانون[2]

والركن الشرعي في الجرائم الالكترونية يعبر عنه بالمعاهدات الدولية والقوانين التي تضمنها كل دولة لمحاربة هذه الجرائم وفي ميدان التنظيم القانوني للانترنيت تتنازع المواقف التشريعية منذ منتصف التسعينات وحتى الآن على موقفين :

1/ أحدهما يصر على وجوب أن يكون التنظيم القانوني في إطار الحد الأدنى وبأضيق مدى منعا لأية قيود على بيئة الانترنت التي يضعها أصحاب هذا الرأي بأنها البيئة الديمقراطية والإبداعية والمتفتحة ، والتي لا تستقيم مع القيود التي تحد من هذه السمات .

2/ أما الثاني فإنه يرى الانترنت شأنها شأن أي مخترع جديد يحتاج إلى تدابير تشريعية تحمي المصالح وتقيم معايير وقواعد تكفل إحداث التوازن بين المصالح المتعارضة من جهة وتتيح مواجهة الآثار الظواهر السلبية في بيئة الانترنت .

إننا في الوقت الحاضر وبالرغم من موجات التشريع المتتالية في حقل قانون تكنولوجيا المعلومات أو قانون الكمبيوتر لا تزال في مقام تغيب فيه أجوبة للتعديد من التساؤلات ، وبفعل

[1] أنظر القانون 06-23 المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966رج رقم 84 المؤرخة في 24-12-2006

[2] أنظر المادة 1 06-23 المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966رج رقم 84 المؤرخة في 24-12-2006

الطبيعة الخاصة لمعطيات الحاسوب من حيث كونها غير مادية وبفعل ما آثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات ولضمان عدم إفلات الجناة من العدالة وصونا لمبدأ الذي يقضي بأن لا جريمة ولا عقوبة إلا بنص قانوني [1].

وفي ظل كل هذا سنت العديد من دول العالم قوانين جنائية خاصة أو عدلت قوانين العقوبات لديها بما يكفل مواجهة الجرائم الالكترونية حيث بالنسبة للمشرع الجزائري فقد تدارك الفراغ القانوني في مجال حماية المال المعلوماتي من خلال استحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 06-23 المتضمن تعديل القانون العقوبات كخطوة تظهر اهتمام المشرع الجزائري لمثل هذه الجرائم والتمهيد لجرائم أخرى متصلة بنفس الموضوع ، وذلك من خلال جريمة المساس بأنظمة المعالجة الآلية للبيانات والمعطيات والتي جاء بها المشرع في المادة 394 مكرر إلى المادة 394 مكرر 7 من قانون العقوبات الجزائري [2].

المطلب الثاني : أنواع الجرائم المعلوماتية :

صنف الفقهاء والدارسون [3]الجرائم المعلوماتية ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم ، فبعضهم يقسمها إلى جرائم ترتكب على نضم الحاسب الآلي وأخرى ترتكب بواسطته وبعضهم بصفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة ، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء ، وكذا تعدد الحق المعتدى عليه ، فتوزع الجرائم المعلوماتية حسب هذا التقسيم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص ونجد هذا

[1] أنظر يونس عرب ، قانون تكنولوجيا المعلومات والمنازعات القانونية في البيئة الرقمية ، ورقة العمل 2007 .

[2] أنظر القانون 06-23 المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966رج رقم 84 المؤرخة في 24-12-2006 .

[3] أنظر منير محمد الجنبيهي ممدوح محمد الجنبيهي ، جرائم الانترنت والحاسب الآلي وسائل مكافحتها ، دار الفكر الجامعي ، الاسكندرية 2005 ص 187-186 .

التقسيم شائعا من خلال الدراسات والأبحاث الأمريكية ، ويلاحظ أنه يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء[1].

الفرع الأول : الجرائم التي تقع على الأشخاص

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث ، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي ، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية في صيانة الشرف...

جريمة انتحال الشخصية :

هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية ، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على شبكة المعلوماتية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره ، ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار ، وغالبا ما يتحصل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت [2]

ب/ جريمة المضايقة والملاحقة :

وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث بطال برامج الحوارات المتبادلة فالدردشة ، وهي عبارة عن مساحات معروفة في الفضاء المعلوماتية تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض ، ، وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد .

[1] أنظر يونس عرب ، دليل أمن المعلومات والخصوصية (جرائم الكمبيوتر والانترنت) إصدار اتحاد المصارف العربية الجزء الأول 2001 ص 15 .

[2] أنظر منير محمد الجنبيهي ممدوح محمد الجنبيهي ، جرائم الانترنت والحاسب الآلي وسائل مكافحتها ، دار الفكر الجامعي ، الاسكندرية 2005 ص 42-43 .

العلي ولا تتطلب الجريمة المرتكبة عبر الانترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية [1].

ج/ جرائم التغرير والاستدراج :

هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمي الشبكة ، وهي تقوم على عنصر الإتهام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والتي قد تتطور إلى لقاء مادي بين الطرفين ، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها ، وهي دون حدود سياسية أو اجتماعية إذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية .

د/ جرائم التشهير وتشويه السمعة :

مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية ، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص ينشر الشائعات عنهم .

وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية ، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة[2].

[1] أنظر محمد أمين احمد الشوابكة ، جرائم الحاسوب الأولى والانترنت ، دار الثقافة للنشر والتوزيع ، الطبعة الأولى ، عمان 2004 ص 45 .

[2] أنظر منير الجنبيهي ، ممدوح محمد الجنبيهي ، المرجع السابق ص 34 .

ه/ الجرائم المخلة بالأخلاق والآداب العامة :

إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر ، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر .

وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة و إفسادهم عبر الوسائل المعلوماتية أو محاولة إغوائهم لارتكاب هذه الأنشطة ، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالعمال الفاحشة ، وتصوير قاصرين ضمن أنشطة للجنس .

والأعمال الإباحية هي من أشهر الأعمال الخالية وأكثرها رواجا خاصة في الدول العربية وأوربا والدول الأسيوية ، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز[1].

الفرع الثاني : الجرائم التي تقع على الأموال :

هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية .

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فإنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول ، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي[2].

[1] أنظر محمد أمين أحمد الشوابكة ، المرجع السابق ص 114 .

[2] أنظر محمد أمين أحمد الشوابكة ، المرجع أعلاه ص 136 .

أ/ جرائم صناعة ونشر الفيروسات :

الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي ، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل .

وأما عن بدا عملها فيتحدد طبقا لأسلوب تصميمها ، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها ، وقد تبدأ بمجرد تشغيل لبرامج الموجودة عليه ، وتعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشارا ، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي " فون نيو مان" على صعيد الحاسب الآلي دون الانترنت ، ومن أشهرها فيروس رسائل الحب ، فيروس الدودة الحمراء ، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في أقل من 09 ساعات عام 2001 [1] .

ب/ جرائم الاختراقات :

الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم المعلوماتية ، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسيات أو الشبكات .

وتختلف أسباب الاختلاف أهداف المخترق ، فمنهم من اخترق أجهزة البعض أو مواقعهم لمجرد فضول والبعض الآخر لسرقتها وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلومتهم التي قد يكونون قد عرضوها مقابل بدل مالي للإطلاع عليها ، وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير ، وهو أخطر أنواع الاختراق ، ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع[2].

[1] أنظر منير الجنبيهي ، ممدوح محمد الجنبيهي ، المرجع السابق ص 86

[2] أنظر منير الجنبيهي ، ممدوح محمد الجنبيهي ، المرجع السابق ص 47

ج/ جرائم ممارسة القمار :

نظرا لأن القمار قد يكون مصرحا به في بعض البلدان إلا أن الأغلب في البلدان مصرح به ولكن بشكل محدود جدا وفي بعض الأماكن السياحية فقط دون أن يكون مصرحا به في الأماكن العامة التي يرتادها الأغلبية من أفراد الشعب ، نظرا لأنه يخالف تعاليم الدين في كافة البلاد العربية التي حرم الدين الإسلامي لعبة ، ففي الماضي كان لعب القمار يستلزم وجود لاعبين معا على طاولة ليتمكنوا من لعبة ، أما الآن ومع انتشار شبكة الانترنت على المستوى العالمي فقد أصبح بإمكان اللاعبين التجمع معا عبر الشبكة ولعب جميع أنواع القمار عليها ، وعليه فإن انتشار شبكة الانترنت في سلبيات انتشار لعب القمار ،و بالتالي فلعب القمار غير مصرح به حتى ولو كان عن طريق الانترنت[1].

د/ جرائم غسيل الأموال :

يعني في بسط صورة هو تحويل المصدر الغير للأموال إلى مصدر مشروع ، فمثلا تحويل الأموال الناتجة عن عمليات غير مشروعة كتجارة المخدرات إلى أموال مصادرها مشروع كتجارة السيارات مثلا ، وقد أعطت شبكة الانترنت عدة مميزات لمن يقومون بعمليات غسيل الأموال منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها بعض الدول وتعيق نشاطهم ، وأيضا كان لانتشار التجارة المعلوماتية عبر شبكة الانترنت خير المعين لهؤلاء القائمين على عمليات غسيل الأموال ، نظرا لسرعة الاتفاق على الصفقات و إتمامها من خلاله دون أن تكون في معظم الأحيان تحت رقابة قانونية صارمة[2] .

ه/ جريمة تعطيل الأجهزة والشبكات :

يطال التعطيل أجهزة الحاسب الآلي عبر برامجها ، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية

[1] أنظر منير الجنبيهي ، ممدوح محمد الجنبيهي ، المرجع أعلاه ص 88

[2] أنظر منير الجنبيهي ، ممدوح محمد الجنبيهي ، المرجع أعلاه ص 99-100

عملها دون أن تتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها وهو الأمر الذي يعيقها عن تأدية عملها .

و/ جريمة النصب والاحتيال :

أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها ، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف النصب والاحتيال ومن بينها:

- خرق التعاملات عبر طرق احتيال جديدة ثم ابتكارها ، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت .

- إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا ، ومرتكبوا الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم و القبض عليهم .

الفصل الثاني

آليات الحماية القانونية والجنائية للجريمة المعلوماتية

إن التقدم العلمي له تأثيره البالغ على القانون وعلى الواقع الذي يطبق عليه هذا القانون ولكي تتحقق الفائدة المرجوة من هذا القدم، فإن القانون يجب ألا ينفصل عن الواقع الذي يفرزه ويطبق عليه، بل يجب أن يكون متجاوبا معه ومتطور بتطوره.

ولاشك في أن التطور الحالي الذي لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة قد إنعكس أثره عن الجرائم التي تمخضت عن ذلك، بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها، ومن حيث المحل التي تقع عليه من حيث الجناة الذين يرتكبونها على النحو السابق الإشارة إليه، بحيث يمكن القول أن الأساس في خطر هذه الجرائم يكمن في أنها تجمع بين الذكاء الاصطناعي والذكاء البشري مما جعل إثباتها جنائيا قد يكون في منتهى الصعوبة.

فالتطور الحالي الذي إنعكس أثره على قانون العقوبات قد انعكس اثره أيضا على قانون الاجراءات الجزائية، بحيث أن هذا القانون الأخير قد لا يطبق بسبب عجز القانون الأول عن استيعاب الجرائم المستحدثة التي ترتكب بالوسائل الالكترونية.

كما وان الإثبات الجنائي هو احد الموضوعات الهامة لهذا القانون، فقد تأثر بدوره بالتطور الهائل الذي لحق الأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة، الأمر الذي يتعين معه تغيير النظرة إلى طرق الإثبات الجنائي لكي تقترب الحقيقة العلمية في واقعها الحالي من الحقيقة القضائية.

فإثبات الجرائم التي تقع على العمليات المعلوماتية باستخدام الوسائل الالكترونية سيتأثر بطبيعة هذه الجرائم، وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع.

وبناءا على ذلك هل يمكن القول بوجود الحماية القانونية داخل البيئة الرقمية؟

المبحث الأول : اجراءات التحري وجمع الأدلة في الجريمة المعلوماتية

لقد خالفت الجريمة المعلوماتية النمطية الواحدة التي تمتاز بها الجرائم التقليدية في طبيعتها الكلية والتي رصدت التشريعات القانونية الإجرائية.

خاصة سبلا لمحاربتها إلا أن جرائم العصر الرقمي الجديد أحدثت إشكالا عاما يبرز كيفية التعامل مع هاته الجرائم التي أرغمت المشرع القانوني إلى تدارك النقص الهائل ومحاولة ملأه مسايرا في ذلك عدة معايير أهمها التقنية العالية في هاته الجريمة.

فالجريمة المعلوماتية لا تترك أثرا ماديا في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على اتلاف او تشويه أو إضاعة الدليل في فترة قصيرة، ولا تكفي في هذا النمط من الجرائم إعادة نظام الكمبيوتر وقواعد البيانات وشبكات المعلومات.

وتفصيلا لما سبق سنحاول التطرق إلى الوسائل واجراءات الكشف عن الجريمة (المبحث الأول) المعلوماتية وتوضيح الحماية الجنائية للمعلومات الالكترونية على الصعيدين الوطني والدولي (المبحث الثاني).

المطلب الأول : طرق ووسائل البحث في الجريمة المعلوماتية

مراحل جمع الادلة كما حددها القانون هي : المعاينة، الخبراء، التفتيش، وضبط الأشياء، ومراقبة المحادثات وتسجيلات وسماع الشهود الاستجواب والمواجهة.

وليس على المحقق الالتزام باتباع ترتيب معين مباشرة هذه الاجراءات بل هو غير ملزم أساسا بمباشرتها جميعا وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقضي به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جميع الأدلة ما يلي:

أولا : معاينة مسرح الجريمة المعلوماتية.

ثانيا : التفتيش في مجال الجريمة المعلوماتية.

ثالثا : الشهادة في الجريمة المعلوماتية.

رابعا : الخبرة في مجال الجريمة المعلوماتية.

خامسا : الضبط في مجال الجريمة المعلوماتية[1].

الفرع الأول : معاينة مسرح الجريمة المعلوماتية :

يقصد بالمعاينة فحص مكان أو شيء او شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء حقيق لإثبات ما بالجسم من جراح أو على الثياب من دماء أو ما بها من مزق أو ثقوب.

ويلاحظ أن المعاينة قد تكون إجراء تحقيق او استدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأفراد فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن او له حرمة خاصة كانت إجراء تحقيق.

والمعاينة جوازية لمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم او لم يطلبوها، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك إلى الاعتبارات السالف ذكرها[2].

وحتى أصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات أهمها ما يلي:

1- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بشكل خاص على تصوير الأجزاء الخلفية للحاسب ملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل الصور.

2- الهناية البالغة بالطريقة التي تم بها إعداد النظام الآثار الالكترونية، وبوجه خاص التسجيلات الالكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو النظام أو الموقع أو الدخول معه في الحوار.

[1] أنظر : منتدى شباب طمرة، قسم الكمبيوتر والأنترنت – "جرائم الكمبيوتر والأنترنت" : الموقع www.6amra.com.
[2] أنظر : عبد الله حسين محمود، " إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" عن موقع :
http://www.arablawinfo.com/research-search.asp?Validate=articles.ID=148

3- ملاحظة وإثبات حالة التوصيلات والكبلات المتصلة بالنظام حتى يمكن إجراء عملية المقارنة والتحليل حين عرض فيما بعد على القضاء.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتاكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.

5- التحفظ على محتوى سلة المهملات من الأوراق الملقاة والممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة، السليمة وغير السليمة او المحطمة وفحصها ورفع البصمات التي قد كون لها صلة بالجريمة المرتكبة.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.

إعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل التحرك، مع الأخذ في الاعتبار قاعدة سماك العسكرية والتي تعني الحالة الرسالة التنفيذية المداخل والمخارج والاتصالات هي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيه وعدد المتورطين فيه، أما الرسالة فهي تحدد الهدف من الغارة، والتنفيذ يعني كيفية أداء المهمة، أما المداخل والمخارج فإن من المهم معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقا لمكونات طريق التحقيق، بينما يأتي عنصر الاتصال لضمان السرية وسلامة لعامل وتبادل المعلومات أثناء الغارة[1].

وبعد وصول الفريق إلى مسرح الجريمة يتم التأمين والسيطرة على المكان والبدء في التفتيش على النحو التالي:

1- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإعارة وذلك عن طريق إغلاق الطرق والمداخل.

[1] أنظر : نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات – دراسة مقارنة – دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2007، الصفحة 220.

2- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة، ورصد الاتصالات الهاتفية من وإلى مكان الإغارة مع إبطال أجهزة الهاتف النقال.

3- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ على الأشخاص الموجودين.

4- تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد موقعها بأسرع فرصة ممكنة، وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملف file server لتعطيل حركة الاتصالات.

5- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من اتلاف المعلومات من على البعد أو من جهاز آخر داخل المبنى.

6- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدا عن اجهزة الحاسب الآلي[1].

الفرع الثاني : التفتيش في مجال الجريمة المعلوماتية

يعتبر التفتيش اجراء من اجراءات التحقيق يتطلب أوامر قضائية لمباشرته، ويهدف للبحث عن الأدلة المادية التي ترتبط بالجريمة مدار التحقيق. ولا يشتمل لذلك الأدلة الشفوية أو القولية للاتصال الأخيرة بعنصر الشخص الشاهد، ويجري التفتيش بخصوص جرم تحقق وقوعه ويوجه إلى مكان يتمتع بالحرمة او يتجه إلى الشخص المشتبه به، ويخضع التفتيش غي وجوده وإجراءاته التنفيذية إلى أحكام القانون التي من أبرزها صدور أمر التفتيش أو مذكراته الكتابية عن الجهة التي حددها القانون، مع بيان الأسباب الموجبة لذلك ومحل التفتيش المخصوص[2].

[1] أنظر : منتدى جامعة قطر "كلية القانون" : " مراحل إثبات الجريمة الالكترونية" عن موقع :
heard PHP?t=20845http://www.quatar.com/VB/show
[2] أنظر : أحمد الكركي : " التحقيق في جرائم الحاسوب"، عن الموقع :
? Validate=article&articles ID=158 (1)http://www.arablawinfo.com/research-search.asp

وسوف نعالج إجراء التفتيش بالنظر إلى إمكانية تفتيش العالم الرقمي والقيود التي ترد على فرقة التفتيش.

1- مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

يتكون الحاسب الآلي من مكونات مادية ، مكونات منطقية، كما أن له شبكات اتصال بعدية سلكية ولا سلكية سواء على المستوى المحلي او المستوى الدولي، فهل تخضع هذه المكونات للتفتيش؟

1-1 مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها للاجراءات القانونية الخاصة بالتفتيش، وبعبارة أخرى فإن جواز التفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه وهل هو مكان عام أم مكان خاص إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيه تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة[1].

ويجب التمييز داخل المكان الخاص بينما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحياسب الأخرى ام انها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لا يخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للاماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية او كان مسيطر عليها او حائز عليها، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

[1] أنظر : منتدى جامعة قطر "كلية القانون" : " مراحل إثبات الجريمة الالكترونية" عن موقع :
heard PHP?t=20845http://www.quatar.com/VB/show

2-1 مدى خضوع مكونات الحاسب المعنوية للتفتيش

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأي أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها.

وفي هذا المعنى نجد أن المادة 251 من قانون الاجراءات الجنائي اليوناني تعطى سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروري لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشمل بالضبط البيانات المخزنة أو المعالجة الكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أي مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية.

وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر الأسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه بارتكابها أو ان هناك نية بأن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة[1].

2-2- مدى خضوع شبكات الحاسب للتفتيش :

ويمكن في الفرض التمييز بين ثلاث احتمالات :

الاحتمال الأول : اتصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان آخر داخل الدولة :

يرى الفقه الألماني بشأن مدى امكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، إنه يمكن أن يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الاجراءات الجنائية الألماني.

[1] أمين فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية لكلية حقوق مصرية، الاسكندريةن 2008، ص 219-224.

كما نص مشروع قانون جرائم الحاسب الآلي في هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود.

الاحتمال الثاني : اتصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان آخر خارج الدولة.

من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات الادعاء في جميع الأدلة، ولمواجهة هذا الاحتمال نص مشروع قانون جريمة الحاسب الآلي بهولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الاماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دولة أخرى، ويشترط أن يكون هذا التدخل مؤقتا وان تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة 125)[1].

الاحتمال الثالث : يسمح بالتصنت والأشكال الخاصة للمراقبة التليفونية في العديد من الدول.

حيث يجيز القانون الفرنسي الصادر في 10 يوليو 1991 اعتراض الاتصالات البعيدة بما في ذلك شبكات تبادل المعلومات، ويجوز لقاضي التحقيق في هولندا أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة متورطا فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الالكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي.

3- ضوابط تفتيش نظم الحاسب الآلي:

يمكن تقسيم ضوابط تفتيش نظم الحاسب الآلي إلى نوعين موضوعية وشكلية :

3-1 الضوابط الموضوعية لتفتيش نظم الحاسب الآلي : وتنحصر هذه الضوابط في :

وقوع جريمة الكترونية : والجريمة الالكترونية هي كما سبق القول وبشكل عام كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة. وهناك العديد من

[1] أنظر : منتدى جامعة قطر "كلية القانون" : " مراحل إثبات الجريمة الالكترونية" عن موقع :
heard PHP?t=20845http://www.quatar.com/VB/show

التشريعات التي حرصت على استحداث نص خاص كما هو الحال بالنسبة للأنظمة القانونية التي تم التطرق سابق في إطار الجهود الدولية، سواء المنفردة منها أو الجماعية في مواجهة هاته الجريمة العصرية.

- تورط شخص او أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيه :

ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة الالكترونية، سواء بوصفه فاعلا لها أو شريكا فيها وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، كذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد مسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلا أو شريكا[1].

وتشمل المكونات المادية للحاسب وحدة الإدخال ووحدة الذاكرة الرئيسية ووحدة الحساب والمنطق ووحدات الإخراج وأخيرا وحدات التخزين الثانوي.

كما تنقسم المكونات المعنوية للحاسب الآلي إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقا لاحتياجات العميل، ويستلزم الحاسب بمكوناته سالفة الذكر مجموعة من الأشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسب وخبراء البرامج، سواء كانوا مخططي برامج تطبيقات أم كانوا مخططي برامج نظم ومحليين ومهندي الصيانة ومديري النظم المعلوماتية[2].

3-2 الضوابط الشكلية لتفتيش نظم الحاسب الآلي :

ويمكن إجمال مثل هاته الضوابط فيما يلي:

الأسلوب الآلي لتنفيذ التفتيش في نظم الحاسب الآلي حيث الريادة في ذلك كانت للنظام الأمريكي وذلك على النحو التالي:

[1] أنظر : عبد الله حسين محمود، " إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" عن موقع : http://www.arablawinfo.com/research-search.asp?Validate=articles&ID=148.

[2] أنظر : أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة : " جرائم الحاسب الآلي والانترنت" ، دار وائل للنشر، الطبعة الأولى، 2001، ص : 272-276.

تقتحم قوات الشرطة القضائية المكان بصورة سريعة ومن كافة منافذه في آن واحد وذلك باستخدام القدر الأعظم من القوة، بافتراض أن هذا التكتيك يقلل من احتمالية وقوع إصابات بين صفوف رجال الشرطة.

يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر المتواجدة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل الكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كمبيوتر، ودائما ما تكون غرفة المعيشة ويوضعوا تحت حراسة مشددة، وفي هذه الخطوة يتم تقديم التفتيش الصادر من النيابة إليهم ويتم تحذيرهم بأن كافة أقوالهم ستحسب عليهم منذ هذه اللحظة وقد تؤخذ بمثابة دليل إدانة ضدهم، ودائما ما سنجد لدى العديد منهم الكثير من الحديث وخاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث بمترلهم، وفي مكان ما من المترل سنجد النقطة الساخنة جهاز كمبيوتر متصل بخط تلفون أو ربما نجد أكثر من جهاز وأكثر من خط في المترل الواحد، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين.

توضع النقطة الساخنة في عهدة فريق يضم إثنين من العملاء (مكتشف ومسجل)، ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريبا متقدما على نظم المعلومات، وغالبا ما يقوم بهذا الدور العميل المعني بالقضية والذي عاصرها منذ البداية واستصدار إذن التفتيش الخاص بها من القاضي، فهذا الشخص يعرف تماما الشيء او الأشياء التي يبحث عنها ويتفهم طبيعتها تماما ولن نتجاوز إذا ما قلنا أنه هو الذي يقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الأسطوانات ...الخ.

- **فريق التفتيش** :

هو الفريق المعني بإجراءات التحقيق، وهو جزء داخل فريق الإغارة الذي يضم بجانب فريق التفتيش والضبط رجال الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والسائقين وخبراء مسرح لجريمة العادية الملائمين لجريمة موضوع التحقيق.

الفرع الثالث : الشهادة في مجال الجريمة المعلوماتية

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم او براءته منها، وللشهادة في مجال الاجراءات أهمية بالغة لأن الجريمة ليست تصرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه وبحرص على إخفائه عن الناس[1].

وسماع الشهود كسائر إجراءات التحقيق من الأمور التقليدية للمحقق فله ان يسمع الشهود او يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك إلى فطنة المحقق والأصل أن يطلب الخصوم سماع من يرون من الشهود، غير أن للمحقق أن يجيبهم إلى طلبهم أو يرفضه وله أن يدعو لشهادة من يقدر أن لشهادته أهمية بل له أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه، ومن المبادئ المستقرة أن الشاهد لا يرد ولو غلب على الظن انه لن يتحرى الصدق في شهادته سواء كان ذلك راجعا لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له او ضده.

1- المقصود بالشاهد في الجريمة المعلوماتية:

الشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، الذي تكون لديه معلومات جوهرية او هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن ادلة الجريمة داخله، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزا عن الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من اهمها :

القائم على تشغيل الحاسب الآلي:

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.

[1] أنظر : منتدى جامعة قطر "كلية القانون" : " مراحل إثبات الجريمة الالكترونية" عن موقع :
heard PHP?t=20845http://www.quatar.com/VB/show

- **المبرمجون :**

وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين :

- الفئة الأولى : وهم مخططو برامج التطبيقات.
- الفئة الثانية : هو مخططو برامج النظم.

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخططو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج[1].

المحللون :

المحلل وهو الشخص الذي يحلل ويقوم بتجميع البيانات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما سمي بمخطط تدفق البيانات واستنتاج الاماكن التي يمكن ميكنتها بواسطة الحاسب.

2- التزامات الشاهد المعلوماتي:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟

هناك اتجاهان بهذا الصدد :

- **الاتجاه الأول** : ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات او الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى

[1] عبد الله حسين محمود، "المرجع السابق" عن موقع :
ID=148.http://www.arablawinfo.com/research-search.asp?Validate=articles

هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب.

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

- **الاتجاه الثاني** : ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية، ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهاداتهم (المواد 62، 109، 138) من قانون الاجراءات الجنائية الفرنسية، ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة[1].

الفرع الرابع : الخبرة في مجال الجريمة المعلوماتية

ندب الخبير أو مبررات ندب الخبير وإجراءاته : يرى المحقق في بعض الأحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافته العامة عن فهمها، كتحديد سبب الوفاة أو ساعتها أو رفع بصمة وجدت في مكان الجريمة أو فحص سيارة لبيان ما فيها من خلل وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظرا لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج متعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات عملية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة، لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها، ويمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحسابات وبرامجها وشبكتها، كذلك لا يوجد خبير قادر على التعامل مع كافة انماط الجرائم التي تقع عليها أو ترتكب بواسطتها.

[1] منتدى قانون نت، منتدى القضايا الجنائية خصوصية جرائم الحاسوب والأنترنت عن موقع www.quanoun.net

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة، وللمحقق في أي وقت إلى أن ينتهي التحقيق أن يندب من يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب خبير، كما أنه يحدد للخبير مهمته والميعاد الذي يقدم فيه تقريره وعليه أن يحلفه اليمين على أن يبدي رأيه بالذمة وهذا الإجراء جوهري يترتب علي إغفاله بطلان عمل الخبير، والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه والاستثناء يتم ذلك في غيابه.

وللخصوم حق الحضور أثناء عمل الخبير ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش أمرا سهلا حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء، وهذه المستندات مثل : أدلة عمل النظام، سجلات إدارة الكمبيوتر، وثائق البرامج، السجلات، صيغ مدخلات البيانات والبرامج، وكذلك صيغ مخرجات الكمبيوتر المطبوعة ويتم التخطيط على هذه المستندات ويمكن تحديدها ما إذا كانت كاملة، أصلية، او صورا من خلال استجواب القائمين على حفظها[1].

وبالطبع فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمرا بالغ التعقيد ويحتاج إلى وجود خبير، وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي :

1- تحديد وصف الحاسوب :

- تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعية التي يستخدمها، بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير ... الخ.

- طبيعة بيئة الحاسب او الشبكة من حيث تنظيم ومدى تركيز او توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وامكنة اختزانها.

- الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

[1] عبد الله حسين محمود، "إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" عن موقع :
http://www.arablawinfo.com/research-search.asp?Validate=articles.ID=148

- أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام[1].

2- بيان طرق استخدامه :

- كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة او تدميرها أو إلحاق ضرر بالأجهزة؟

- كيف يمكن عند الاقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير أن يلحقها تلف؟

- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا امكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب او النظام أو الشبكة أو الدعامة الممغنطة؟

الفرع الخامس : الضبط في مجال الجريمة الالكترونية

يقصد بالضبط في قانون الاجراءات وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق، وتتحد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال.

1- محل الضبط :

الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق، وإذا كان قانون الاجراءات يتحدث في بعض التصرف عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف عن ضبط الأشياء.

[1] أنظر : عبد الفتاح البيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية، 2006، ص 304-305.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك يستوي أن يكون الشيء المضبوط مملوكا للمتهم او لغيره، والقاعدة أن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته ان يكون مفيدا في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه.

والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات الجرائم الحاسب الآلي ونسبتها إلى المتهم هي :

1- الورق : كثير من الجرائم الواقعة على المال او على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها غي الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة او التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة، وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدرا كبيرا من الأوراق في وقت قصير، عليه يعتبر الورق من الادلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة والورق أربعة أنواع :

- اوراق تحضيرية يتم إعدادها بخط اليد كمسودة او تصور للعملية التي يتم برمجتها.
- أوراق تالفة تتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.
- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.
- أوراق أساسية وقانونية محفوظة في الملفات العادية او دفاتر الحسابات وتكون لها علاقة بالجريمة، خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

2- جهاز الحاسب الآلي : وجود جهاز حاسب آلي مهم للقول بأن هناك جريمة، ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة، وخبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الالكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحرير.

3- ملحقات الحاسب الآلي : من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية، لوحة المفاتيح، والشاشة، ومع التطورات السريعة التي يمر بها الحاسب الآبي نجد إضافات جديدة مثل المودم والماوس والسماعات و "السير فر"، وإذا كنا بصدد الحديث عن الأجهزة الكبير فإننا نجد أن أشكالها تتغير باستمرار خاصة من حيث الحجم والهيكل، ومن الضروري إطلاع العاملين في مجال التحقيق على مختلف أجهزة الحاسب الآلي فور ظهورها.

4- أقراص الليزر :

مع جهاز الحاسب الآلي للشخص الطبيعي والشخص المعنوي نجد قدرا كبيرا من أقراص الليزر، علاوة على أن مراكز الحاسب الآلي في الأشخاص المعنوية نجد فيها الآلاف من الأقراص قد تكون على غلاف القرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد في مكان ما أقراص الليزر ولا تجد معها أجهزة حاسب آلي ومع ذلك يعد جزءا من جريمة الحاسب الآلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

5- الشرائط الممغنطة :

وتستعمل الشرائط الممغنطة عادة للحفظ الاحتياطي وقد تكون في مكان بعيد آمن، كما يقوم البعض بإيداعها في خزائن البنوك التجارية او مراكز التوثيق الحكومية الآمنة[1].

المطلب الثاني: الدليل الرقمي في الجريمة المعلوماتية:

يتمتع الدليل الرقمي بصفة الحداثة ، فهو من الأدلة الحديثة التي أفادها التطور التقني و هو ايضا ذو طبيعة خاصة من حيث الوسط الذي ينشأ فيه و الطبيعة التي يبدو عليها، و لذى فإننا سنتطلع في هذا المطلب إلى التعريف بالدليل الرقمي.

[1] أنظر : عبد الفتاح البيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي (دراسة قانونية متعمقة في القانون المعلوماتي)، المرجع السابق، ص 306-307.

- **التعريف بالدليل الجنائي بشكل عام:**

الدليل في اللغة: هو المرشد ، و ما يتم به للإرشاد، و ما يستدل به، و الدليل هو الدال و جمع الأدلة[1] و كذلك يعني تأكيد الحق بالبينة و البينة هي الدليل أو الحجية

- **الدليل في المصطلح القانوني:**

هو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها وم المقصود بالحقيقية بهذا الصدد: هو كل ما يتعلق بالإجراءات و الوقائع المعروضة عليه بإعمال حكم القانون عليها.[2]

الفرع الأول: ما هية الدليل الرقمي

هو الدليل المؤخوذ من أجهزة الكمبويتر و هو يكون في شكل مجالات و نبضات مغناطيسية أو كهربائية ممكن تجميعها و تحليلها بإستخدام برامج التطبيقات و تكنولوجيا و هي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال و الرسوم و ذلك من أجل إعتماده أمام أجهزة نفاذ و تطبيق القانون[3] و يعرف الدليل الرقمي بأنه:

مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجمميعها و تحليلها لإستخدام برامج و تطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.

[1] د. جميل صليبا، المعجم الفلسفي، بيروت، دار الكتاب اللبناني، ط1، 1980، ص23

[2] د.ناصر إبراهيم محمد زكي، سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة" ، رسالة دكتوراة جامعة الأزهر، كلية الشريعة و القانون، 1978، ص211

[3] د.ممدوح عبد الحميد عبد المطلب، زوبيدة محمد قاصي، عبد الله عبد العزيز، النموذج المقترح لقواعد إعتماد الدليل الرقمي للإثبات في جرائم الكمبيوتر، منشور ضمن أعمال مؤتمر"الأعمال المصرفية و الإلكترونية" نضمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة و غرفة التجارة و الصناعة دبي في الفترة من 10 - 12 /2003/05، المجلد الخامس، ص2273

و ترجع تسمية الدليل الرقمي لأن البيانات داخل الوسط الإفتراضي سواءا كانت صور أو تسجيلات أو نصوص تأخذ شكل أرقام على هيئة الرقمين (1 أو 0) و يتم تحويل هذه الأرقام عند عرضها لتكون في شكل صور أو مستند أو تسجيل[1]

الفرع الثاني:خصائص و مميزات الدليل الرقمي:

- **خصائص الدليل الرقمي:**

1-يعتبر الدليل الرقمي دليلا غير ملموس أي هو ليس دليلا ماديا (فهو تكون في مجالات مغناطيسية أو كهربائية...)

2-يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية [2]

3-إن فهم مضمون الدليل الرقمي يعتمد على إستخدام أجهزة خاصة بتجميع و تحليل محتواه و لذلك ما لا يمكن تحديد و تتحليل محتواه بواسطة تلك الأجهزة و يمكن إعتباره دليلا رقميا .

مميزات الدليل الرقمي :

1 - يتميز الدليل الرقمي بصعوبة محوه او تحطيمه ، اد حتى في حالة محاولة اصدار امر بازالة دليل فمن الممكن اظهاره من خلال داكرة الالة اللتي تحتوي دلك الدليل .

2- ان محاولة الجاني محو الدليل الرقمي بداتها تسجل عليه كدلك ، حيث ان قيامه بدلك يتم تسجيله بداكرة الالة و هو ما يمكن استخراجه و استخدامه كدليل ضده .

[1] د.عبد الفتاح بيومي الحجازي، دليل الرقمي و التزوير في جرائم الكمبيوتر و الأنترنيت، دراسة معمقة في جرائم الحاسب الآلي و الأنترنيت، بهجات للطباعة و التجليد، مصر، 2010

[2] د. علي محمود عي حمودة، الأدلة المتحصلة للوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مقدم ضمن أعمال مؤتمر العلمي الأول حول جوانب القانونية و الأمنية و العمليات الإلكترونية نضمته أكاديمية شرطة دبي، في الفترة من 26 إلى 28 -2003/04 دبي، ص22

3- ان الطبيعة الفنية دليل رقمي تمكن اخضاعه لبعض البرامج و التطبيقات للتعرف على ما ادا كان قد تعرض للعبث و التحريف .

الفرع الثالث : مشروعية الدليل الرقمي

يقصد بمشروعيته الوجود ان يكون الدليل معترف به ، بمعنى ان يكون القانون يجيز للقاضي الاستناد اليه لتكوين عقيدته للحكم بالادانة ، فهناك اتجاهان رئيسان ، الاول نظام الادلة القانونية ، و الثاني نظام الاثبات الحر .

اولا : نظام الادلة القانونية ففوفقا لهدا النظام فان المشرع هو اللدي يحدد حصرا للادلة اللتي يجوز للقاضي اللجوء اليها في الاثبات ، كما حدد القيمة الاقناعية لكل دليل بحيث يقتصر دور القاضي على مجرد فحص دليل للتاكد من توافر الشروط اللتي حددها القانون[1] ، فلا سبيل للقاضي في تقدير القيمة الاقناعية للدليل ، و لدا سمي هدا النظام بنظام الاثبات القانوني او المقيد حيث ان القانون قيد القاضي بقائمة من الادلة اللتي حددت قيمتها الاثباتية ، و هدا النظام ينتمي للنظم دات الثقافة الانجلوسكسونية ، مثل المملكة المتحدة " بريطانيا" و الولايات المتحدة الامريكية ، و لدا فان النظم اللتي تتبنى هدا النظام لا يمكن في ظلها الاعتراف بالدليل الرقمي باية قيمة اثباتية ما لم ينص القانون عليه صراحة ضمن قائمة ادلة الاثبات .

و تطبيقا لهدا الفهم نص قانون الاثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي و حدد قيمته الاثباتية اتفاقا و طبيعة النظام القانوني في بريطانيا .[2]

و يمكن ان يعاب على نظام الاثبات القانوني ان من شانه تقييد القاضي على نحو يفقده سلطته في

[1] د.هلالي عبد الإله أحمد ، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة ، ب.ط أو دار نشر، 1999 ، ص49

[2] د.علي محمود علي حمودة، مرجع سابق ذكره، ص30

الحكم مما يتفق مع الواقع ، فيحكم في الكثير من الاحيان مما يخالف قناعته اللتي تكونت لديه من ادلة لا يعترف بها دلك فيصبح القاضي كالالة في اطاعته لنصوص القانون و لذلك فإن هذا النظام بدا ينحصر نطاقه حتى في الدول التي تعتبر أكثر إقناعا لها، فنجد بريطانيا مثلا قد بدأ تخفف من علوائه، حيث ظهر فيها ما يعرف بقاعدة الإدارة دون أدنى شك و التي مفادها أن القاضي يستطيع أن يكون عقيدته من اي دليل إن لم يكن من ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته .[1]

ثانيا: نظام الإثبات الحر:

يسود نظام الإثبات الحر في ظل الأنظمة اللاتينية، و وفق لهذا النظام يتمتع القاضي الجنائي في تكوين قناعته فله أن يبني هذه القناعة على اي دليل و إن لم يكن منصوص عليه بل إن المشرع في هذا النظام لا يحفل بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، و القاضي هو الذي يختار من بين ما يطرح عليه و ما يراه صالحا للوصول إلى الحقيقة و هو في ذلك يتمتع بمنطلق الحرية لقبول الدليل أو رفضه إذا لم يطمأن إليه، فالمشرع في هذا النظام لا يتدخل في تحديث القيمة الإقناعية للدليل فعلى الرغم من توفر شروط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الإقتناع، و لذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل إنحصار دور المشرع .[2]

[1] د. هلالي عبد الإله أحمد، حجية الخرجات، مرجع سابق، ص91
[2] نفس المرجع، ص29 و ما بعدها

في هذا النظام لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على إعتبار أن المشرع لا يعهد عنه سياسة النص على قائمة أدلة الإثبات و لذلك فإن مسألة قبول الدليل الرقمي لا ينال منها سوى مدى إقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه بالتقدير القضائي.

الفرع الرابع:حجية الدليل الرقمي أمام القضاء الجنائي

إن مجرد الحصول على الدليل الرقمي و تقديمه للقضاء لا يكفي بإعتماده كدليل للإدانة إن الطبيعة الخاصة بالدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على الدليل صادقة في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة، و لذلك تثور فكرة الشك في مصداقياتها كأدلة الإثبات الجنائي، فهل من شأن ذلك غستبعاد الدليل الرقمي من دائرة الإثبات الجنائي لتعارضه و قرينة البراءة؟

في ضل النظم القانونية التي تعتمد النظام اللاتيني في اللإثبات - كالنظام القانون الليبي - فإن القاضي يملك سلطة واسعة في تقديم الدليل من حيث قسمته التدليلة ، فللقاضي قبول الدليل أو رفضه و هو يعتمد في ذلك على مدى إقتناعه الشخصي بذلك الدليل و هذا المعنى هو ما نصت عليه المادة 275 من قانون الإجراءات الجنائية الليبي.[1]

إن سلطة القاضي الجنائي في تقدير الدليل لا يمكن ان يتوسع في شانها بحيث يقال إن هذه السلطة تتمتد لتشمل الأدلة العلمية ، فالقاضي بثقافته القانونية لا يمكن إدراك الحقائق المتعلقة باصالة الدليل الرقمي فضلا عن ذلك فإن هذا الليل يتمتع من حيث قوته التدليلية بقيمة غثباتية قد تصل إلى

[1] د.أحمد الصادق الجهاني ، محاضرات ألقيت على طلبة الدراسات العليا، كلية القانون ، جامعة قار يونس،2003-2004، غير منشور تنص المادة 275 على أنه: "يحكم القاضي في الدعوة حسب العقيدة التي تكونت لديه بكامل حريته، و مع ذلك لا يجوز له أن يبلي حكمه على إي دليل لم يطرح أمامه في الجلسة."

اليقين، فهذا هو شأن الأدلة العلمية عموما و لكن هذا لا يناقض ما سبق أن قدمناه من أن الدليل الرقمي هو موضع شك من حيث سلامته من العبث و من ناحية صحة الإجراءات المتعبة في الحصول عليها من ناحية أخرى حيث يشك في سلامة الدليل الرقمي من ناحيتين:

الأولى : الدليل الرقمي من الممكن خضوعه للعبث للخروج به من نحو يخالف الحقيقة و من ثم فقد يقدم هذا الدليل معبرا عن واقعة معينة صنع اساسا لأجل التعبير عنها خلافا للحقيقة، و ذلك دون أن يكون في إستطاعة غير المتخصص إدراك ذلك العبث فالتقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة و يسر بحيث يظهر و كأنه نسخة أصلية في تعبيرها عن الحقيقة .

الثانية: و إذا كانت نسبة الخطأ الفني في الحصول على الدليل الرقمي نادرة للغاية إلا أنها تضل ممكنة، و يرجع الخطأ في الحصول على الدليل الرقمي لسببين :

1-الخطأ في إستخدام الأدات المناسبة في الحصول على الدليل الرقمي و يرجع ذلك الخلل في الشفرة المستخدمة أو بسبب إستخدام مواصفات خاطئة.

2-الخطأ في إستخلاص الدليل، و يرجع ذلك إلى إتخاذ قرارات لإستخدام الأدات تقل نسبة صوابها عن 100% و يحدث هذا غالبا بسبب وسائل الإختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التي تم تقيمها .

و من ذلك فإننا نخلص إلى أن الشك في الدليل الرقمي لا يتعلق بمضمونه كدليل، و إنما بعوامل مستقلة عنه و لا كنها تؤثر في مصداقيته

المبحث الثاني : الحماية الجنائية للمعلومات الالكترونية

لقد ألقت الثورة المعلوماتية بظلالها على قوانين العقوبات، خاصة في تلك الدول التي استفادت من ثمار هذه الثورة، ووجب عليها في الوقت ذاته أن تتلاقى عيوبها وما اوجدته من جرائم فتاكة، تصدت لها قوانين العقوبات وعاقب عليها والملاحظ في هذا المجال أنه كلما كان الاعتماد أكبر على التقنية المعلوماتية، لهذا ترى أن الدول المتقدمة معلوماتيا كانت السباقة في مجال التجريم المعلوماتي، وسنتناول فيما يلي التطور الذي مر به كل من التشريع الجزائري والفرنسي والمصري في هذا المجال .

المطلب الأول : تطور الحماية الجنائية على الصعيد الداخلي (الوطني)

الفرع الأول : القانون الجزائري

لقد شهد العالم في الآونة الأخيرة تطورا مذهلا وسريعا في مجال المعلوماتية ولقد تسارعت وتيرة الاعتماد على هذه الأخيرة في شتى مناحي الحياة، حتى باتت ضرورة لا يمكن الاستغناء عنها، وأصبحت مقياسا لتطور الدول ، والجزائر ليست بمنأى عن هذا القول المعلوماتي، وهي إن لم تبلغ مصاف الدول المتقدمة فإنها قد تأثرت بهذه الثورة المعلوماتية سلبا وايجابا، فقد تأثرت بما جرته هذ الثورة من ألوان جديدة من الاجرام لم تشهده البشرية من قبل ارتبطت ارتباطا وثيقا بالحاسب الآلي وما حواه من معلومات.

هذه الجرائم طالت مصالح جديدة غير تلك التي يحميها قانون العقوبات، فبدت الحاجة شديدة لوضع نصوص جديدة، و لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات، ولقد جاء في عرض هذا التعديل " أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها وان الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات وان هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات وسوف يمكن لا محالة من مواجهة بعض أشكال الاجرام الجديد وكان التعديل بموجب القانون رقم 04-15

المؤرخ في 10 نوفمبر سنة 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي أفرد القسم السابع مكرر منه تحت عنوان :" المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمن ثمانية (08) مواد (من المادة 394 مكرر وحتى المادة 394 مكرر 07) ونص على عدة جرائم هي :

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات.
- الدخول أو البقاء المؤدي إلى ترتيب نظام أشغال المنظومة.
- الدخول أو البقاء المؤدي إلى حذف نظام أشغال المنظومة.
- إدخال أو إزالة أو التعديل معطيات بطريق الغش في نظام المعالجة الآلية.
- تصميم او بحث أو تجميع أو توفير او نشر او الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إنشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصلة من إحدى الجرائم المنصوص عليها في هذا القسم.

كما شددت العقوبة إلى الضعف إذا استهدفت الجريمة الدفاع الوطني أو المؤسسات العمومية، وشددت عقوبة الغرامة على الشخص المعنوي إلى خمس مرات للحد الأقصى المقررة للشخص الطبيعي، وذلك بعد اقرار المواد 18 مكرر، 18 مكرر1، و 51 مكرر من التعديل نفسه لمسؤولية الشخص المعنوي بوجه عام.

كما عاقبت تلك المواد على الاشتراك في مجموعة أو إنفاق يتألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم.

ونص هذا التعديل أيضا على عقوبة مصادرة وسائل ارتكاب الجريمة واغلاق المواقع التي تكون محلا لها، واغلاق المحل والمكان الذي ارتكبت فيه الجريمة. كما عاقب التعديل أيضا الشروع في جرائم هذا القسم.

وكانت مواجهة الجريمة المعلوماتية إحدى بنود اتفاق يؤسس الشراكة بين الجزائر والاتحاد الأوربي، عقد بتاريخ 22 أفريل 2002 وتضمنت ذلك المادة 86 منه[1].

الفرع الثاني : في القانون الفرنسي

كانت أولى المحاولات لمد سلطان القانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل وذلك سنة 1985، عندما تقدم بمشروع قانون عقوبات جديد أضاف بموجبه بابا رابعا للكتاب الثالث بعنوان :" الجرائم في المادة المعلوماتية" « Les infractions en matière informatique » يتكون من ثمانية مواد (من 1/307 إلى 8/307) تناولت بالتجريم الموضوعات التالية :

- التقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي عمدا.
- استخدام او نقل او انتاج برنامج او معطيات او أي عنصر من عناصر النظام بدون موافقة من لهم الحق.
- تخريب او تعييب كل جزء من النظام المعالجة الآلية للمعلومات او عرقلة أداءه لوظيفته.
- الحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق استخدام غير المشروع لنظام المعالجة الآلية للمعلومات.

لكن هذا الشروع لم يجد سبيله للتطبيق[2] ، أما المحاولة التي كانت لها النجاح فقد كانت في الخامس من أغسطس عام 1986 عندما تقدم النائب « Jacques » ونواب آخرون إلى الجمعية الوطنية باقتراح مشروع قانون الغش المعلوماتي « Fraude informatique » ، هذا الاقتراح حاول تعديل وتطويع بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الامانة والتزوير والاتلاف والاخفاء، وذلك لشمل العدوان المعلوماتي، وحدث أن تعددت مناقشات هذا المشروع في البرلمان الفرنسي، فوصلت إلى ثلاثة أمام الجمعية

[1] أنظر : Accordeurs méditerranéen établissant une association entre la communauté europ-europ-eene états membres, donepart, et la république Algérienne Démocratique et Populaire, d'autre. http ://www.dunepart-part.22Averil2002 fothman.Free.Fr/accmultitxt/eur/eur-evromed/dz-evromed.html.

[2] أنظر : R.Gassion Op-Cit, noorp.op وأنظر : كذلك د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا- بحيث مقدم لمؤتمر القانون والكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات، دولة الامارات العربية المتحدة، 2000، ص 39.

الوطنية مرتين أمام مجلس الشيوخ، وطال امدها حتى استغرقت عاما ونصف العام، وأسفرت في النهاية عن قانون اختلف تماما عن ذلك المشروع الذي قدم اول مرة، بل تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل عام 1985[1].

- تم اقرار هذا القانون وإدماجه في قانون العقوبات الفرنسي، ليشكل الباب الثالث من الكتاب الثالث من القسم الثاني منه، وهذا الكتاب يتعلق بالجنايات والجنح المتعلقة بأحد الناس، وأصبح الباب الثالث متعلقا بجرائم المعلوماتية، وذلك في المواد 2/462 إلى 9/462، تضمن النص على الجرائم التالية :

* الدخول او البقاء غير المشروع في نظام معالجة الآلية للمعطيات او في جزء منه وتشدد العقوبة في حالة محو او تعديل المعطيات الموجودة داخل النظام أو افساد وظيفته.

* إدخال معطيات في النظام او محو او تعديل المعطيات الموجودة فيه عمدا أو بدون مراعاة حقوق الغير، سواء تم ذلك بطرقة مباشرة او غير مباشرة.

كل فعل من شأنه أن يعرقل او يفسد عمدا او بدون مراعاة حقوق الغير أداء النظام الوظيفية.

* تزوير المستندات المعالجة آليا أيا كان شكلها، واستعمال هذه المستندات.

* الشروع في ارتكاب الجرائم السابقة.

* الاتفاق الجماعي على ارتكاب الجرائم السابقة.

- أما المحطة التالية من محطات التجريم المعلوماتي فكانت عام 1994، عندما تم تعديل قانون العقوبات الفرنسي، وقد استخدم هذا التعديل مصطلح الغش في الجرائم السابقة واستغنى عن مصطلح "دون مراعاة حقوق الغير"، كما أن هذا التعديل مس المادة 1/441 فطور من جريمة التزوير المعلوماتي، لتصبح جريمة تزوير المستندات المعلوماتية واستعمالها بعدما كانت جريمة من نطاق جرائم الاعتداء على نظام المعالجة الآلية للمعطيات لاختلاف المصلحة المحمية فيها عن المصلحة في تلك الجرائم، فهي في هذه الأخيرة مصلحة صاحب الحق في النظام او من له حق

[1] راجع د. أحمد حسام تمام، الجرائم الناشئة عن استخدام الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار 2000، ص 261.

السيطرة عليه، بينما في جريمة التزوير المعلوماتي الجديد هي الثقة العامة في المستندات ذات القيمة القانونية أيا كان شكلها[1] وقد تضمن هذا التعديل المواد من 1/323 إلى 7/323.

كما أن هذا التعديل قد أقر مسؤولية الشخص المعنوي، بعدما كان الفقهاء والقضاء الفرنسيين منقسمين بشأنها، سبب سكوت قانون العقوبات الفرنسي سنة 1810 عن هذا الموضوع بعدما كان قانون 1670 يقر هذه المسؤولية[2] ، وظل هذا الجدل قائما حتى صدور قانون العقوبات لسنة 1994 الذي أقر المسؤولية للشخص المعنوي.

وبعد عشر سنوات من هذا التعديل جاء تعديل آخر لقانون العقوبات الفرنسي عام 2004، وقد أضاف الشرع بموجبه جريمة أخرى هي جريمة التعامل في وسائل يمكن أن ترتكب بها جريمة، او تلك الوسائل التي تصلح لأن ترتكب بها جريمة الدخول او لبقاء غير المصرح بهما أو جريمة التلاعب بالمعطيات او جريمة إعاقة او إفساد أنظمة المعالجة الآلية للمعطيات وقد نصت على هذ الجريمة المادة 3/323-1.

الفرع الثالث : في القانون المصري

لا يحوي قانون العقوبات المصري نصوصا تحمي معطيات الحاسب الآلي. او تحمي المال المعلوماتي عموما، والمشرع المصري لا يحمي من البيانات إلا أنوعا معينة، دون ان يولي اعتبارا لطريقة معالجتها، تقليدية كانت أو آلية، هذه البيانات تحميها قوانين خاصة، وتتعلق بما يلي:

- بيانات الأحوال المدنية.
- البيانات الضريبية واقرار الكسب غير المشروع (مكنون ضرائب رقم 157 لسنة 1981).
- بيانات التعداد والاحصاءات السكانية (القرار الجمهوري بالقانون رقم 35 لسنة 1960 والمتعلق بالاحصاء والتعداد، والمعدل بالقانون رقم 21 لسنة 1982).

[1] انظر : R.Gassin.op.cit noo9p.op وأنظر كذلك : د. محمد سامي الشوا. ثورة المعلومات وانعكاسات على قانون العقوبات، دارالنهضة العربية، القاهرة 1998، ص 200، وانظر كذلك : د. علي عبد القادر القهوجي، التزوير المعلوماتي في جرائم الكمبيور والأنترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة ، 2001، ص 116، وانظر د.احمد حسام طه تمام، المرجع السابق، ص 422.

[2] د. أحمد حسام طه تمام، المرجع السابق، المكان نفسه.

- بيانات حسابات البنوك والمعاملات المتعلقة بها (قرار رئيس الجمهورية بالقانون رقم 205 لسنة 1990).

وقد حاول البعض قياس البيانات او المعلومات الشخصية التي تتم معالجتها بواسطة أجهزة الحاسب الآلي تم تحفظ في بنوك المعلومات بعض البيانات السابقة، كتلك المتعلقة بالتعداد والاحصاءات السكانية وعارضهم البعض الآخر[1] كما حوال آخرون تطبيق نص المادة 310 من قانون العقوبات المصري وبخاصة الحماية سر المهنة على حالة إفشاء المعلومات للشخصية التي يتم معالجتها الكترونيا وتخزن في بنوك المعلومات، وعارضهم جانب آخر[2] لكن يجدر الذكر ان ثمة مشروع لقانون التجارة الالكترونية بمصر، تم اعداده بمعرفة مركز المعلومات، ودعمه مجلس الوزراء، لم تقدمه الحكومة بعد، تضمن تجريما للعديد من الأفعال التي تمس معطيات الحاسب الآلي[3] وفيما يلي الجرائم التي تنص عليها هذا المشروع :

- كشف مفاتيح الشيفر المودع بمكتب التشفير أو فض معلومات مشفرة في غير الأحوال المصرح بها.
- استخدام التوقيع الالكتروني او محوه او التعديل فيه أو في مادة التحرر الالكتروني دون موافقة كتابية مسبقة من صاحب الحق.
- الدخول بطريق الغش او التدليس على نظام معلومات او قاعدة بيانات بصورة غير شرعية.
- منع أو حيازة او الحصول على نظام معلومات او برامج لإعداد توقيع الكتروني دون موافقة صاحب الشأن.
- تزوير او تقليد محرر او توقيع الكتروني مزور أو شهادة مزورة باعتماد توقيع الكتروني.
- استخدام نظام او برنامج للحيلولة دون اتمام المعاملات التجارية بالوسائل الالكترونية وذلك بالتعديل فيها أو محو بياناتها أو إفشائها أو تدميرها او تعطيل أنظمتها.

[1] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة ، القاهرة، 1998، ص 17.
[2] د.علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة (الحاسب الالكتروني، الكمبيوتر، الأنترنت) ، بدون ناشر، 2004.
[3] نص الشرع المشار إليه لدى . د. هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية ، 2000.

- إذاعة أو تسهيل إذاعة استعمال – ولو في غير علانية- لمحرر أو توقيع الكتروني او فض شفرته دون مسوغ قانوني او موافقة صاحب الشأن، وتشدد عقوبة هذه الجريمة إذا كان فاعلها أمينا على المحرر او التوقيع الالكتروني بمقتضى صناعته او وظيفته او كان من العاملين.
- الادخال العمدي او بإهمال لفيروس إلى نظام معلوماتي بدون موافقة مالك النظام أو حائزه الشرعي.

وقد تراوحت عقوبات الجرائم السابقة الذكر الحبس أو الحبس مع الشغل والغرامة ومصادرة الأجهزة والأنظمة والبرامج المستخدمة في ارتكاب الجرائم ، مع غرامة بضعف ما عاد على المحكوم عليه من الربح او الفائدة من وراء الجريمة.

ورغم أهمية هذا الشروع في سد فراغ قانوني كبير إذا تم اعتماده، إلا أنه لم ير النور بعد.

المطلب الثاني : الحماية الجنائية على الصعيد ادولي

إن الاجرام المعلوماتي في تزايد مستمر يوما بعد يوم، ولقد اتسع نطاقه كثيرا إثر الانتشار الواسع للحاسبات الآلية وشبكات الاتصال الخاصة بها خاصة شبكة الانترنت ومنح كثيرا من مالجال الذي يمكن لهذه الجرائم أن تحدث أثرا فيه، إضافة إلى صعوبة إثباتها وملاحقة مرتكبيها، إذ أنها جرائم عابرة للحدود أو ذات طابع دولي[1].

جعل كل دولة تقف بمفردها عاجزة عن التصدي لها، هذا الوضع استدعى من الدول أن تلم شملها وتوحد جهودها في مواجهة هذا الاجرام.

فتحركه من خلال العديد من المنظمات الدولية والاقليمية لابرام الاتفاقيات بهذا الخصوص، وسوف نعرض فيما يلي الدور الذي لعبته كل من الأمم المتحدة والاتحاد الأوربي، ومجلس وزراء العدل العرب في هذا المجال.

[1] الطابع الدولي لهذه الجرائم لا يعني كونها من الجرائم الدولية التي يتناولها القانون الدولي الجنائي، فهي جرائم داخلية، ولو كانت جرائم عالمية، راجع د. عمر الفاروق الحسيني للمشكلات الهامة في الجزائر المتصلة بالحاسب الآلي وأبعادها الدولية، طبعة 2، دار النهضة العربية، القاهرة، 1995.

الفرع الأول : دور الأمم المتحدة

تبذل الأمم المتحدة جهودا كبيرة في سبيل تعزيز العمل المشترك بين أ'ضاء المنظمة من أجل التعاون في مواجهة الجرائم المعلوماتية، وذلك من خلال اشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، أو من خلال الوكلات والمنظمات العاملة تحت لوائها، كالمنظمة العالمية للملكية الفكرية [1]« WIPO ».

ففيما يخص مؤتمرات منع الجريمة، فقد كلف المؤتمر السابع المنعقد في ميلانو عام 1985 لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي واعداد تقرير يعرضه على المؤتمر الثامن، ولقد أكد هذا الأخير على ضرورة الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الحركة، وأشار إلى مسألة الخصوصية واختراقها بالاطلاع على البيانات الشخصية المخزنة داخل النظام للحاسب الآلي، وضرورة اعتماد ضمانات لصون سريتها. كما أكد على ضرورة تشجيع التشريعات الحديثة التي تتناول هذه الجرائم بصفتها نمطا من انماط الجريمة المنظمة، ويمكن اجمال توصيات مؤتمر هافانا لعام 1990 في المبادئ التالية[2] :

1- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسية.
2- تحسين أمن الحاسب الآلي والتدابير المنعية.
3- اعتماد اجراءات تدريب كافية للموظفين والوكلات المسؤولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
4- تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.
5- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.
6- زيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص 155.
[2] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

أما المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين والمنعقد في القاهرة عام 1995 فقد أوصى بوجوب حماية الإنسان في حياته الخاصة وفي ملكيته الفكرية من تزايد مخاطر التكنولوجيا، ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الاجراءات المناسبة[1].

وقد أوصى المؤتمر العاشر المنعقد في بودابست بالمجر عام 2000 بوجوب العمل الجاد على الحد من جرائم الحاسب الآلي المتزايدة والمعتبرة نمطا من انماط الجرائم المستحدثة والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة[2].

وإضافة إلى هذه المؤتمرات لا يكفي ما تلعبه المنظمة العالمية للملكية الفكرية، كإحدى الوكالات المتخصصة التابعة للأمم المتحدة، من دور في مجال محاربة القرصنة المعلوماتية وحماية البرامج.

الفرع الثاني : دور المجلس الأوربي

لقد بدل ومازال المجلس الأوربي يبدل جهودا كبيرة في مواجهة جرائم المعطيات والحاسب الآلي، عموما وفي 28 يناير 1981 تم توقيع اتفاقية تحت اشرافه، تعلقت بحماية الأشخاص في مواجهة المعالجة الالكترونية للمعطيات الطبيعية الشخصية[3].

ولقد أصدر المجلس العديد من القواعد التوجيهية في هذا المجال، تضمنت وجوب تجريم العديد من السلوكيات كالغش المعلوماتي وتزوير المعلومات وسرقة الأسرار المخزنة والتوصل غير المصرح به وسرقة منفعة الحاسب، كما تضمنت العديد من الاجراءات الفنية لتجنب الوصول غير المرخص به إلى المعلومات المخزنة كحماية كلمة السر المستخدمة في النهايات الطرفية وحماية الأوامر الخاصة بالتشغيل وترميز المعلومات الشخصية وأسماء من تتعلق بهم[4].

[1] محمود أحمد عبابنة، المرجع السابق، ص 158.
[2] المرجع نفسه، ص 159.
[3] د. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة ، القاهرة، 1998، ص 83.
[4] د. أسامة عبد الله قايد، المرجع السابق، ص 84.

واهم ما قام به المجلس في هذا المجال هو اشرافه على اتفاقية بودابست الموقعة في 23 نوفمبر 2001، وقد جاء في المذكرة التفسيرية لهذه الاتفاقية ما يلي[1] :

" هناك سمة بارزة في تكنولوجيا الاتصالات عن بعد .... كذلك يكفي أن يتم إدخال البيانات إلى شبكة معينة من خلال عنوان المرسل إليه حتى تصبح متوافرة لأي شخص يريد الدخول إليها.

كما أن الاستخدام العام للبريد الالكتروني ووصول الجمهور لمواقع الويب عبر شبكة الانترنت من امثلة هذا التطور الذي قلب أوضاع مجتمعنا.

ومن خلال الاتصال بخدمات الاتصالات والمعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى "الفضاء المعلوماتي" الذي يستعمل أساسا لأغراض شرعية ولكن يمكن أن تخضع لسوء الاستخدام، إذ هناك احتمال لاستخدما شبكات الحاسب والمعلومات الالكترونية في ارتكاب أعمال إجرامية.

وعلى ذلك يجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة استخدام إمكانيات الفضاء المعلوماتي. وان يعمل على ردع هذه الأفعال الاجرامية.

وتتكون هذه الاتفاقية من ثمانية وأربعين مادة، موزعة على أربعة أبواب يعالج الباب الأول منها استخدام المصطلحات، ويناول الباب الثاني الاجراءات الواجب اتخاذها على المستوى القومي، ويضم ثلاثة أقسام : اولها للقانون العقابي المادي أو الموضوعي، وثانيها للقانون الاجرائي، وثالثها للاختصاص القضائي.

أما الباب الثالث فقدتم تخصيصه لدراسة التعاون الدولي وهو يشمل على قسمين : أولهما : المبادئ العامة، وثانيها الاحكام الخاصة وأخيرا يأتي الباب الرابع الذي يتعرض للشروط الختامية، وقد تم التمهيد لهذه الأبواب الأربعة بافتتاحية او مقدمة.

وقد شملت الاتفاقية في شقها الموضوعي النص على تسع جرائم موزعة على أربع فئات[2] :

[1] د. هلالي عبد الله أحمد ، الجوانب الموضوعية والاجرامية لجرائم المعلوماتية على ضوء اتفاقية بودابيست الموقعة في 23 نوفمبر 2001، دار النهضة الغربية ، القاهرة، 2003، ص 23.

[2] د. الهلالي عبد الله أحمد، المرجع السابق، ص 30-32.

الفئة الأولى : الجرام ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية وقد تناولتها المواد من 02 إلى 06 كما يلي:

- المادة 02 : الولوج غير القانوني.
- المادة 03 : الاعتراض غير القانوني.
- المادة 04 : الاعتداء على سلامة البيانات.
- المادة 05 : الاعتداء على سلامة النظام.
- المادة 06 : اساءة استخدام أجهزة الحاسب.

الفئة الثانية : الجرائم المعلوماتية (الجرائم المتصلة بالحاسب) وتناولتها المادتان 07 و 08 كما يلي :

- المادة 07 : التزوير المعلوماتي.
- المادة 08 : الغش المعلوماتي.

الفئة الثالثة : الجرائم المتصلة بالمحتوى، وتناولتها المادة 09 والتي تنص على الجرائم المتصلة بالمواد الاباحية الطفولية.

الفئة الرابعة : الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة وقد نصت عليها المادة 10.

وقد تناولت المادة 11 الشروع والاشتراك، وتناولت المادة 12 مسؤولية الأشخاص المعنية، وتناولت المادة 13 الجزاءات والتدابير.

الفرع الثالث : الدور العربي

يعتبر اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد كقانون نموذجي بموجب قرار رقم 229 لسنة 1996، يعتبر الأهم عربيا في مجال مواجهة جرائم المعطيات والحاسب الآلي عموما، وبالرجوع إلى الباب السابع من القانون والخاص بالجرائم ضد الأشخاص، نجد قد حوى فصلا خاصا بالاعتداء على حقوق الأشخاص الناتج عن الجذاذات والمعالجات المعلوماتية وذلك في المواد من 461 إلى 464، حيث أشارت المواد الثلاث الأولى فيها إلى وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية

وكيفية الاطلاع عليها، أما المادة 464 فعاقبت على الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية المعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتاد، وتغير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية، وسرقة المعلومات[1].

وللجمعية المصرية للقانون الجنائي دورا في هذا المجال، فقد عقدت مؤتمرها السادس بالقاهرة عام 1993 حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات والذي أكد على عالمية هذه الجرائم وضرورة تكاثف الجهود لمكافحتها، ووجوب تعديل نصوص قانون العقوبات التقليدية أو إضافة نصوص جديدة، نظرا لعجز نصوص القائمة عن مواجهة هذه الجرائم، وأوصى المؤتمر بالتعاون الدولي في هذا المجال لاسيما في مجال الإنابة القضائية وتسليم المجرمين وتنفيذ الاحكام، كما اوصى بوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات وطرق الاستدلال والتحقيق وجمع الأدلة في الجرائم المتعلقة بها[2]

[1] د. محمود أحمد عبابنة، المرجع السابق، ص 170.
[2] المرجع نفسه، ص 172.

خاتمة

الحماية الجنائية التي تخيرها المشرع في تدخله هذا عدة مصالح تتعلق بمعطيات الحاسب الآلي و بسط حماية عليها، و هذه المصالح هي سرية هذه المعطيات و سلامتها و تكاملها و كذا إتاحتها أو وفرتها فحماية لمصلحة السرية جرم المشرع الدخول أو البقاء الغير المصرح به داخل أنظمة المعالجة الآلية للمعطيات، بغض النظر عما إذا كان النظام يتمتع بالحماية الفنية أم لا و المشرع في هذا جرم كل دخول إلى النظام سواء أدى هذا الدخول إلى نتيجة معينة أم لم يؤدي و لا يستند إلى تصريح و لتكامل هذه الحماية من طرف المشرع قد قام بتجريم التلاعب الغير مصرح به بتعديل أو إزالة المعطيات موجودة داخل نظام المعالجة الآلية أي قام بتجريب كل ما يؤدي إلى تغير حالة المعطيات بغير تصريح.

و إمعانا في الحماية و رغبة المشرع في قطع دابر هذه الجريمة و التصدي لها فقد جرم أيضا الإتفاق على إرتكاب إحدى الجرائم الشابقة إذا تجسد في أعمال مادية و ذلك نظرا لما يشكله الإتفاق الجنائي من خطورة، إضافة إلى ذلك فقد جرب المشرع الشروع في تلك الجرائم إذا قدر فعلا خطورتها لأن نظام الشروع إلا في الجنح الخطيرة.

هذا و قد شدد المشرع العقوبة إذا إرتكبت تلك الجرائم من شخص معنوي و كذلك شدد العقوبة إذا إرتكبت هاته الجرائم على مؤسسة الدفاع الوطني أو إحدى المؤسسات العمومية لما يشكله هذا من تهديد لأمن الوطن و المصالح العامة.

و نحن في هذا البحث نرى أن المشرع الجزائري قد راعى لحمايته الجنائية أهم المصالح المتعلقة بالمعطيات و قد غطى بهذا جانبا كبيرا من الجريمة المعلوماتية و إن الحماية الجنائية لا تقل أهمية و لا

كفاءة عما توصلت إليه التشريعات الدول المتقدمة كانت سابقة في هذا المجال (و ذلك من خلال إضراب إتفاقية أوروبية و دولية للتصدي لهذه الجريمة) لأن هذه الخطوة التي قام بها المشرع مهمة في الوقت الراحل و ذلك لما تؤول إليه هذه التكنولوجيا من التطور الذي يتزايد كل يوم و هذا لا يحول دون غستمرار هذه الإعتداءات بتقنيات عديدة و متجددة

قائمة المصادر و المراجع

قائمة المصادر و المراجع:

- .أحمد حسام، طاه تمام، الجرائم الناشئة عن إستخدام الحماية الجنائية للحاسب الآلي، دراسة مقارنة، 2000
- أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة و بنوك المعلومات، دار النهضة، القاهرة، 1998.
- أمين فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنيت، دار المطبوعات الجامعية لكلية الحقوق المصرية، الإسكندرية، 2008.
- جميل صليبة، معجم الفلسفي بيروت، دار الكتاب اللبنلني، ط1، 1980
- عبد الباسط خلافن الحماية الجنائية لوسائل الإتصال الحديثة، (الحاسب الإلكتروني، الكمبيوتر، الأنترنيت)ب.د.ن ، 2004
- عبد الفتاح البيومي الحجازي مكافحة جرائم الكمبيوتر و الأنترنيت في القانون العربي نموذجي (دراسة مقارنة متعمقة في القانون المعلوماتي) دار الفكر الجامعي، ط1، الإسكندرية ، 2006
- علي عبد القادر القهواجي، التزوير المعلوماتي في جرائم الكمبيوتر و الأنترنيت، دار الكتب القانونية، المحة الكبرى، القاهرة، 2001.
- محمد أمين، أحمد الشوابكة، جرائم الحاسب الآلي و الأنترنيت، دار الثقافة للنشر و التوزيع، ط1، عمان ، 2004.

- محمد سامي، الشوة، ثورة المعلومات و إنعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998
- محمود أحمد عبابنى، جرائم الحاسب و أبعادها الدولية، دار الثقافة للنشر و التوزيع، عمان الأردن، 2005
- منير محمد الجنبيهي ممدوح الجنبيهي، جرائم الأنترنيت و الحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005
- ناصر غبراهيم محمد زكي، سلطة القاضي الجنائي، في تقدير الأدلة، دراسات مقارنة، رسالة دكتوراة، جامعة الأزهر، كلية الشريعة و القانون، 1978
- نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنيت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ط1، 2007
- هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992
- هشام محمد فريد رستم، العقوبات و مخاطر المعلوماتية، دار النهضة العربية، القاهرة، 2000
- هلالي عبد الله أحمد، جوانب الموضوعية و الإجرائية للجرائم المعلوماتية على ضوء إتفاقية بوداباست الموقعة في 23-11-2001، دار النهضة العربيةن القاهرةن 2003

- هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسات مقارنة، ب..ط، ب.د.ن، 1999
- يونس عرب، قانون تكنولوجيا المعلومات و المنازعات القانونية البيءة الرقمية، ورقة عمل ، 2013

قائمة الكتب و المؤلفات العامة:

- عبد الله سليمان، شرح قانون العقوبات الجزائري، قسم العام، ديوان المطبوعات الجامعية، الجزائر، ط06، 2005
- أنظر القانون 06-23 المؤرخ في 2006/12/20 المعدل و المتمم للأمر رقم 66 - 156 المؤرخ في 8 يوليو 1966 (ج.ر رقم 84 المؤرخة في 12/24 2006) المتضمن قانون العقوبات.

مؤتمرات علمية:

- د.ممدوح عبد الحميد عبد المطلب، زبيدة محمد قاسي، عبد الله عبد العزيز، نموذج المقترح لقواعد الإعتماد الدليل للإثبات الجرائم الكمبيوتر، منشور ضمن أعمال، مؤتمر "الأعمال المصرفية و الإلكترونية" نظمته كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، و غرفة التجارة و الصناعة، دبي، في الفترة من 10-12 /2003/05المجلد الخامس، ص2237

- د. علي محمود علي حمودة، الأدلة المتصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي ، مقدم ضمن أعمال المؤتمر العلمي الأول حول جوانب الأمنية و القانونية للعمليات الإلكترونيةنظمته أكاديمة الشرطة، دبي في الفترة من 26-2003/04/28، دبي

المواقع الإلكترونية:

عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات عن موقع

http////WWW.arablawinfo.com/reasearch-search.asp ?validité=articlesID=148

منتدى جامعة قطر كلية القانون، التحديات الإجرائية و القانونية في بيئة الأنترنيت، مراحل إثبات الجريمة الإلكترونية، الموقع

http ::/www.quataru.com/VB/showtheardPHP ?p=442389#post442389

الفهرس

الفهرس