الجـــريمـــة الإلكتـــرونيـــة

مقدمـة:

تتيح التكنولوجيا الحديثة القيام بالكثير من الأعمال التي كان يستحيل من قبل إنجازها فلقد وفرت هذه التكنولوجيا في مجال الاتصالات الإلكترونية تحقق التواصل الإنساني وإنجاز المعاملات في سهولة ويسر، وأتاح استخدامها حسن تقديم خدمات الرعاية الصحية وتنمية الملكية الفكرية وغيرها من المجالات.

وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقا للاستخدام التكنولوجي الحديث في مجال الاتصالات ونقل المعلومات وهي تختلف في ذلك كثيراً عن غيرها من الوسائل التقليدية للاتصال و الإعلام وهذا الاختلاف يؤدي إلى أمريـن:

الأول لهو تعدد أوجه استعمالات **هذه الوسائل وتوسعها.**

الثاني هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الاستعمالات غير أن هذه التكنولوجيا قد يساء استعمالها وأن يهدد استخدامها السلامة العامة و المصلحة الوطنية فإن كانت وسائل الاتصال الإلكتروني الحديثة تتيح انجاز المعاملات المالية بشكل سريع وموثوق به أياً كان مكان المتعاملين فإن استعمال هذه الوسائل لا يخلو من المخاطر.

فقد يستغل بعض المجرمين هذه الوسائل في ارتكاب جرائمهم بطريق الاحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم و الحقيقة أن تقنية المعلومات خضعت منذ السبعينيات إلى الرقابة القانونية في مختلف فروع القانون. ما ترتب عنه وجود قانون الكمبيوتر أو قانون تقنية المعلومات، و أول ملامحه الأولى بدأ مع شيوع استعمال الكمبيوتر ولاسيما في الدول المتطورة وانخفاض تكلفته، ولأنه أداء جمع ومعالجة المعلومات فقد كانت أول تحدياته القانونية إساءة الاستخدام على نحو يضر بمصالح الأفراد و المؤسسات ومعه نشأ الارتباط بين القانون و الكمبيوتر.

وفي هذا الإطار فإن أول حالة موثقة لإساءة استخدام الكمبيوتر ترجع إلى عام 1958 وفقا لما نشره معهد" ستانفورد" في الولايات المتحدة الأمريكية.

أما الجهد الدولي فقد تحقق إبتداءاً عام 1968 حيث شهد مؤتمر الأمم المتحدة لحقوق الإنسان (مؤتمر طهران) طرح مخاطر التكنولوجيا على الحق في الخصوصية ، و الذي لحقه إصدار الأمم المتحدة قرارات في هذا الحقل.

الجـــريمـــة الإلكتـــرونيـــة

ومع تطور هذا النوع من الجرائم قامت الدول بتحديث تشريعاتها وقيام دول أخرى بتعديل قوانينها، كما قام المشرع الجزائري بتعديل قانون العقوبات: الصادر بموجب الأمر رقم 156/66 المؤرخ في 1966/06/08 المعدل والمتمم بالأمر رقم 23/06 المؤرخ في 2006/12/20 ج ر رقم 84 المؤرخة في 2006/12/24.

وبذلك تتحدد أهمية دراسة موضوع الجريمة الإلكترونية أو جرائم الكمبيوتر و الانترنت كوسيلة اتصال جماهيرية عالمية لا يمكن تجاهلها وبسبب شعبيتها وانتشارها أصبحت شبكة المعلومات العالمية هذه جزءا مهما من النشاط اليومي لملايين الأفراد في مجتمعاتنا كما أننا في هذا البحث نحاول بشكل مجمل تقديم صورة عامة لطبيعة الجريمة الإلكترونية وأبرز التحديات الأمنية المصاحبة لشبكة الانترنت،وفق منهجية تطمح إلى تقديم الظاهرة الإجرامية على الشبكة كما يتعرض البحث لمجمل التهديدات الأمنية الأكثر وضوحاً على الانترنت، إضافة إلى ذلك يتناول البحث ضمن عرضه لمظاهر التحدي الأمني للشبكة بعض جرائم النشر مثل التشهير و القذف وجرائم انتحال الشخصية ونحو ذلك .

ولتحقيق الهدف من الدراسة سنحاول التعرف على عدد من المفاهيم المرتبطة بهذه الظاهرة وذلك على النحو التالي:

- ❖ تحديد أبرز ملامح الظاهرة الإجرامية في عصر التقنية .
- ❖ التعرف على طبيعة التهديدات الأمنية المصاحبة لشبكة الأنترنت.
- ❖ التعرف على الصور الأكثر شيوعاً لأنماط الجريمة الإلكترونية.
- ❖ التعرف على أبرز الجهود التشريعية في مجال مكافحة الجرائم الإلكترونية.

لذا ستتعرض دراستنا هذه إلى محاور غرضها الايجابي الإطلاع على أهم الإشكاليات المطروحة في الجريمة الالكترونية والتي تتمحور أساسا في الإشكال التالي:

–هل ثمة إدراك حقيقي لمحتوى وحدود ومخاطر الجريمة الالكترونية؟

وان كان ما هي سبل الحد منها؟

والتي من خلالها يتم رصد وفهم وتحليل الظاهرة محل الدراسة وذلك بالوقوف على الخصائص المميزة لها حيث نسعى الى استقصاء التعريفات وطبيعة تلك الجرائم وأنواعها ثم نوضح في الشق الثاني ردة الفعل القانونية اتجاه هذا النوع الجديد من الجرائم. ومن اجل ذلك قسمنا هذه الدراسة إلى فصلين:

الجـــريمـــة الإلكتـــرونيـــة

الفصل الأول: **وهو بعنوان ماهية الجريمة الالكترونية الذي أبرزنا فيه مفهومها واهم الخصائص المميزة لها عن غيرها من الجرائم وما يتميز به مرتكبي هذه الجرائم.**

أما الفصل الثاني: **فهو بعنوان الوسائل المعتمدة في الحد من الجريمة الالكترونية، وفيه أبرزنا الجهود الدولية والقانونية والوسائل التقنية للحد منها كما أبرزنا الاختصاص القضائي والنصوص العقابية على المستوى الوطني.**

الجـــريمـــة الإلكتـــرونيـــة

الفصل الأول: ماهية الجريمة الالكترونية.

إن الحقيقة الثابتة و البسيطة تقول بان الوسائل العلمية التقنية لم تخترع الجريمة بل كانت ضحية لها في 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 و حديثه لا يختلف على بشاعتها و خطرها على المجتمع الإنساني احد، و بمرور حقب التاريخ المختلفة كانت الظاهرة الإجرامية مرادفة للتجمع الإنساني تعكس في أساليبها و أنماطها أحوال و تطورات المجتمع في مختلف النواحي، و في عصر التقنية و ثورة الاتصالات الحديثة تعددت

الجريمة و تنوعت أساليبها مستفيدة من التطور التقني في كافة مناحي الحياة، حيث وظف المجرمون هذه المستحدثات التقنية الحديثة في تطوير أساليبهم بل حتى التقنية ذاتها لم تسلم من الجريمة فمنذ بدايتها ظهر معها ما يعرف بجرائم التقنية أو الجرائم الالكترونية.

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 الالكترونية (المبحث الأول) و استقصاء طبيعتها نظرا لما تتمتع به من خصوصية (المبحث الثاني)

الجـــريمـــة الإلكتـــرونيـــة

المبحث الأول مفهوم الجريمة الالكترونية:

ما كانت جرائم الانترنت من جرائم التقنية العالية أي من الجرائم المستحدثة، وكانت التشريعات العقابية قاصرة عن تناولها، فان كثيرا من المحققين و رجال الضبط في كثير من الدول يواجهون صعوبات أثناء التصدي لتلك الجرائم.فان 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 فان الجرائم الالكترونية هي جرائم العصر الرقمي.[1] و سوف نستقصي تعريفها قانونيا و فقهيا(المطلب الاول) وسنبين خصائصها (المطلب الثاني).

المطلب الأول تعريف الجريمة الالكترونية:

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

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 مجرماً 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 كلّ فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين. وبالتالي فالجرائم الإلكترونية أي فعل ضار يأتيه المواطن عبر استعماله الوسائط الإلكترونية مثل الحواسيب، شبكات نقل المعلومات، شبكة الإنترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموماً.

فمع تطور الانترنت وتوسع استخداماتها وازدياد أعداد المستخدمين لها في العالم (حوالي 1.6 مليار مستخدم يمثلون ربع سكان العالم) أصبحت الانترنت وسطاً ملائماً للتخطيط ولتنفيذ عدد من الجرائم بعيداً عن رقابة وأعين الجهات الأمنية.

[1] انظر نبيلة هبة هروال,الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات– دراسة مقارنة– دار الفكر الجامعي,الإسكندرية, الطبعة الأولى,2007,ص 24.

إذن الجريمة الالكترونية هي استخدام الوسائط الحاسوبية والشبكات وشبكات الإنترنت لارتكاب جريمة أو التخطيط لها.[2]

الفرع الثاني:التعريف الفقهي.

لقد أعطى الفقهاء و الدارسون عددا ليس قليلا من التعريفات تتميز و تتباين تبعا لموضع العلم المنتمية إليه و تبعا لمعيار التعريف ذاته، و قد اجتهدنا في جمع غالبية التعريفات التي وضعت في هذا الحقل.

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

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

تعريف الأستاذ جون فور ستر " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تاديمان بأنها" كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب" .[3]

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

تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث و تبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة الالكترونية" 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.[4]

---

[2] انظر : http://lattakia.org

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

[2] انظر هشام محمد فريد رستم، العقوبات و مخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة،2000، ص 20.

المطلب الثاني خصائص الجريمة الالكترونية

الفرع الأول: مميزات الجريمة الالكترونية عن غيرها من الجرائم.

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

و باستقرائنا لهذا التعريف تتضح لنا الخصائص التي تتميز بها الجرائم الالكترونية فهي جرائم ذات خصائص منفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها و طريقة ارتكابها و هذه الخصائص هي:

1/الحاسب الآلي هو أداة ارتكاب الجرائم الالكترونية:

تعتبر هذه الخاصية من أهم الخصائص التي تميز هذا النوع عن غيرها من الجرائم الأخرى,ذالك لان شبكة الانترنت هي إحدى التقنيات الحديثة التي افرزها تطور الحوسبة,و لذلك فان ارتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي . و يقصد بالحاسب الآلي وفقا للموسوعة الشاملة لمصطلحات الحاسب الالكتروني كل جهاز الكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال و إخراج معلومات و إجراء عمليات حسابية،وهو يتكون من كيانين كيان مادي و معنوي يضم أولهما الأجهزة المادية المختلفة و التي تشمل وحدات الإدخال و الإخراج و التشغيل ،أما الكيان الثاني فيشتمل عل البرمجيات الجاهزة و البيانات و المعلومات المنطقية .[5]

2/الجرائم ترتكب عبر شبكة الانترنت أو عليها:

تعد شبكة الانترنت الحقل الذي تقع فيه الجرائم الالكترونية و دلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم و غيرها من الأهداف التي تكون غالبا الضحية لها إلا انه و بالرغم من كونها الوسيلة

[5]انظر نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات– دراسة مقارنة– دار الفكر الجامعي,الإسكندرية, الطبعة الأولى,2007, الصفحة 35.

لارتكاب الجرائم إلى جانب الحاسب الآلي فإنها كذلك لن تنجو من يد المجرمين لأنها هي الأخرى قد تكون محلا للاعتداءات.[6]

3/مرتكب الجرائم الالكترونية 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 و لذلك 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 .[7]

4/جريمة الانترنت جريمة عابرة للحدود :

لقد سبق و أن ذكرنا أن شبكت الانترنت ذات طابع دولي إذ أنها لا تعترف بتلك الحدود القائمة بين الدول سواء الجغرافية أو السياسية و هذا ما أدى إلى اعتبار أن الجرائم الالكترونية من الجرائم الدولية,و تأخذ 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 انها تاخذ ذلك البعد في الحالة التي يعترفا فيها لمشرع الدولي بان العدوان يمكن إن تقوم به دولة و لو في صيغة التأييد,و تعتبر الجرائم الالكترونية جرائم دولية في الحالة التي يكون احد اطرافها شخصا دوليا,كما انه يمكن ان تكون في مقابل ذلك جريمة وطنية اذ ان لها اثرا إقليميا من حيث ان حجم الأثر المكاني يحتويها كأي جريمة ثانية.[8]

---

[6] انظر نبيلة هبة هروال،نفس المرجع اعلاه ص 36.

[1] انظر نبيلة هبة هروال,الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات– دراسة مقارنة– المرجع السابق،ص38.

[2] انظر نبيلة هبة هروال, نفس المرجع اعلاه ص39.

5/صعوبة إثبات الجرائم الالكترونية:

تعتبر هذه الخاصية من الخصائص المميزة للجرائم الالكترونية عن غيرها من الجرائم نظرا لكونها ترتكب بواسطة او على الانترنت ومن قبل شخص ذو دراية فائقة بها وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة و التخلص من أثارها و بالتالي صعوبة التحقيق فيها و تتبع مرتكبيها و القبض عليهم على غرار الجريمة التقليدية و إلى جانب الأسباب السابقة فانه تعود صعوبة إثبات الجرائم الالكترونية الى:

- صعوبة الإثبات الفني بآثارها إن وجدت.

- يلعب البعد الزمني(اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) و القانوني (أي قانون يطبق) دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب هذه الجرائم.[9]

[9]انظر نبيلة هبة هروال, نفس المرجع السابق ص39.

الفرع الثاني: خصائص مرتكب الجريمة الالكترونية.

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

1/ مرتكب الجريمة الالكترونية من النوابغ:

إن المجرم المعلوماتي هو إجرام الأذكياء و ذلك بالمقارنة بالإجرام التقليدي فهذا المجرم يصنف ضمن نوابغ المجرمين خاصة الأحداث الناجحين منهم و الذين يخشى عليهم من الدخول من مجرد الهواية إلى الاحتراف في أفعال اختراق النظم[10].

2/ مرتكب الجريمة الالكترونية متكيف اجتماعيا:

فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل انه إنسان متكيف اجتماعيا ذالك انه أصلا مرتفع الذكاء و يساعده على ذلك عملية التكيف، و ما الذكاء في راي الكثيرين سوى القدرة على التكيف و لايعني ذلك التقليل من شان المجرم بل أن خطورته الإجرامية تزيد اذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه,و يذكر 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.[11]

---

[10]- انظر عبد الفتاح البيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون ألمعلوماتي)،دارالفكر ا ل الجامعي ، الطبعة الاولى ، الاسكندرية ، 2006 ص 83.

[11]- نظر عبد الفتاح البيومي الحجازي، نفس المرجع اعلاه، ص 84.

3/مرتكب الجريمة الالكترونية 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 الالكترونية مجرم محترف:

ذلك انه لا يسهل على الشخص المبتدئ في حالات قليلة ان يرتكب جرائمه عن طريق الكمبيوتر,فالأمر يقتضي كثيرا من الدقة و التخصص في هذا المجال للتوصل الى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر.

5/مرتكب الجريمة الالكترونية مجرم غير عنيف:

ذلك انه ينتمي إلى إجرام الحيلة فهو لا يلجا إلى العنف في ارتكاب جرائمه و هذا النوع لا يستلزم مقدارا من العنف للقيام به .

وخلاصة القول إن من صفات المجرم انه يتميز بالذكاء و لا يميل إلى استخدام القوى أو العنف كما يتميز بأنه إنسان اجتماعي، فالجرائم الالكترونية لها وجه إنساني بالنظر إلى أن مرتكبها كائن اجتماعي، و لها الوجه الآخر حين نتدبر الآثار المترتبة عليها.[12]

[12] - نظر عبد الفتاح البيومي الحجازي، نفس المرجع السابق، ص 86.

المبحث الثاني: أركان و أنواع الجَرائم الالكترونية.

الجريمة بمصطلحها العام قديم ظهر بظهور البشرية و لكن بشكلها الجديد هي شر يماشي عصر العولمة.ومن المعروف أن الجريمة العادية تتكون من ثلاثة أركان ركن مادي و ركن معنوي و ركن شرعي وهو الحال بالنسبة للجريمة الالكترونية.

وحاليا المجال مفتوح لكل أنواع الجرائم الالكترونية التي يصعب حصرها أو تعدادها نظرا لإزديادها و تنوع أساليبها كلما أمعنا البحث في هذا المجال نجد انه بالتطور التكنولوجي تتطور وتتعدد هذه الجرائم ويصعب تقسيمها.حيث صنفها الفقهاء و الدارسون ضمن فئات متعددة تختلف حسب الأساس و المعيار الذي يستند إليه التقسيم فبعضهم يقسمها إلى جرائم ترتكب على نضم الحاسب الآلي و أخرى ترتكب بواسطته و غيرهم يؤسسها على تعدد الحق المعتدى عليه فتتوزع الجرائم الالكترونية حسب هذا التقسيم إلى جرائم تقع على الأموال و جرائم تقع على الأشخاص.

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

الجـــريمـــة الإلكتـــرونيـــة

المطلب الأول: أركان الجريمة الالكترونية

يقصد باركان الجريمة عناصرها الأساسية التي يتطلبها القانون لقيام الجريمة وهي أركان خاصة وهي التي بنص عليها المشرع بصدد كل جريمة على حدى و أركان عامة وهي الواجب توافرها أي كان نوع الجريمة أو طبيعتها.[13]

و عليه سنقوم بتطبيق الأركان العامة للجريمة العادية على الجريمة الالكترونية.

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.[14]

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 الالكترونية فان النشاط أو السلوك المادي فيها يتطلب وجود بيئة رقمية واتصال بالانترنت، ويتطلب أيضا أن يقوم مرتكب الجريمة بالتجهيز لها فمثلا يقوم مرتكبها بتجهيز الحاسب الآلي و يقوم بتحميل جرائم 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 ولو كان القانون لا يعاقب على الأعمال التحضيرية.[15]

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 لا يعاقب عليها إطلاقاً.[16]

إلا انه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء ,فشراء برامج اختراق و معدات لفك الشفرات و كلمات المرور و حيازة صور دعارة ,فمثل هذه الأشياء تمثل جريمة في حد ذاتها .

---

[13] انظر عبد الله سليمان, شرح قانون العقوبات الجزائري القسم العام, ديوان المطبوعات الجامعية ا' الجزائر الطبعة السادسة2005 ص65.

[14] انظر عبد الله سليمان,المرجع اعلاه ,ص144.

[15] انظر الموقع الالكتروني www.allarab.com

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

والعنصر الثاني هو النتيجة و هي الأثر المادي المترتب عن السلوك الإجرامي ,و تثير مسألة النتيجة الإجرامية في الجرائم الالكترونية مشاكل عدة فعلى سبيل المثال مكان و زمان تحقق النتيجة الإجرامية فلو قام احد المجرمين في أمريكا باختراق خادم احد البنوك في الإمارات فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق.

أما العنصر الثالث فهو العلاقة السببية و هي التي تربط بين الفعل و النتيجة ,و تجدر الإشارة إلى أن جرائم الانترنت تتمثل فيها فكرة النتيجة المحتملة و ذلك راجع إلى طبيعة النشاط التقني الذي قد يترتب عليه نتائج عدة ,فمثلا من يقصد القرصنة و يتحقق معها انتشار الفيروسات فان ذلك يعتبر نتيجة محتملة لذلك العمل ,و إذا كان النشاط المادي يحدث كله في العالم الافتراضي فان النتيجة الإجرامية لها كيان منفصل لكونها تحدث شكل انقسامي مابين حدوثها في العالم المادي جزئيا أو كليا.[17]

الفرع الثاني: الركن المعنوي.

هو الجانب الشخصي أو النفسي للجريمة ,فلا تقوم الجريمة بمجرد قيام الواقعة المادية التي تخضع لنص التجريم بل لابد أن تصدر هذه الواقعة من إرادة فاعلها و ترتبط بها ارتباطا معنويا.[18]

وعناصر الركن المعنوي القصد الجنائي و هو العلم بعناصر الجريمة و إرادة ارتكابها و هما العلم و الإرادة , ففي الجريمة الالكترونية الركن المعنوي هو الحالة النفسية للجاني و العلاقة بين ماديات الجريمة و شخصية الجاني ,حيث برزت مشكلة الركن المعنوي في الجريمة الالكترونية في قضية موريس الذي كان متهما في قضية دخول غير مصرح به على جهاز الحاسب الفدرالي وقد دفع محامي موريس على انتفاء الركن المعنوي الأمر الذي جعل المحكمة تقولً هل يلزم أن يقوم الادعاء باثبات القصد الجنائي في جريمة الدخول الغير مصرح به بحيث تثبت نية المتهم في تحدي الخطر الوارد على استخدام نظم المعلومات في الحاسب و تحقيق خسائر.

أما بالنسبة للقضاء الفرنسي فان منطق سوء النية هو الأعم قي الجرائم الالكترونية, حيث يشترط المشرع الفرنسي وجود سوء نية في الاعتداء على بريد الكتروني خاص بأحد الأشخاص. [19]

---

[17] انظر نبيلة هبه هروال, الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات (داسة مقارنة) دار الفكر الجامعي,الإسكندرية, 2007, ص48-49

[18] انظر عبد الله سليمان, المرجع السابق, ص231.

[19] انظر الموقع الالكتروني www.allarab.com

أما بالنسبة للمشرع الجزائري فقد نص في المادة 394 مكرر2 من جريمة المساس بأنظمة المعالجة الآلية للمعطيات، على انه كل من يقوم عمدا وعن طريق الغش، و هنا فقد تحقق عنصر العلم و الإرادة.[20]

الفرع الثالث: الركن الشرعي.

يعبر عن الركن الشرعي في الجريمة بلاجريمة ولا عقوبة ولا تدابير أمن إلا بنص في القانون .[21]

و الركن الشرعي في الجرائم الالكترونية يعبر عنه بالمعاهدات الدولية و القوانين التي نضمتها كل دولة لمحاربة هذه الجرائم، و في ميدان التنظيم القانوني للانترنت تتنازع المواقف التشريعية منذ منتصف التسعينات وحتى الآن على موقفين:

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

2/أما الثاني فانه يرى الانترنت شانها شان أي مخترع جديد يحتاج إلى تدابير تشريعية تحمي المصالح و تقيم معايير و قواعد تكفل إحداث التوازن بين المصالح المتعارضة من جهة و تتيح مواجهة الآثار و الظواهر السلبية في بيئة الانترنت.

إننا في الوقت الحاضر وبالرغم من موجات التشريع المتتالية في حقل قانون تكنولوجيا المعلومات او قانون الكمبيوتر لا نزال في مقام تغيب فيه أجوبة للعديد من التساؤلات ، وبفعل الطبيعة الخاصة لمعطيات الحاسوب من حيث كونها غير مادية و بفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات و لضمان عدم إفلات الجناة من العدالة و صونا لمبدأ الشرعية الذي يقضي بان لاجريمة و لاعقوبة إلابنص قانوني.[22]

---

[20] انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8- يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

[21] انظر المادة 1 من القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8- يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

[22] انظر يونس عرب، قانون تكنولوجيا المعلومات و المنازعات القانونية في البيئة الرقمية، ورقة عمل، **2007**،

و في 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 قـانون

العقوبات، كخطوة تظهر اهتمام المشرع الجزائري لمثل هذه الجرائم و التمهيد لجرائم أخرى متصلة بنفس الموضوع،و ذلك من

خلال جريمة المساس بأنظمة المعالجة الآلية للبيانات و المعطيات و التي جاء بها المشرع في المادة **394** مكرر إلى المادة **394** مكرر**7** من قانون العقوبات الجزائري.[23]

أما بالنسبة للدول العربية فقد كانت الامارت العربية المتحدة هي أول دولة عربية تصدر قانونا خاصا بمكافحة جرائم المعلومات، حيث اصدر صاحب السمو الشيخ خليفة بن زايد آل نهيان –رئيس دولة الإمارات – القانون الاتحادي رقم **2** لسنة **2006** في شان مكافحة جرائم تقنية المعلومات.

كما أصدرت دولة سلطنة عمان قانونا لمواجهة الجرائم المعلوماتية من خلال التعديل الذي ادخل على قانون الجزاء العماني رقم **7** الصادر عام **1974** بموجب المرسوم السلطاني رقم **2001/72**.

وكمثيلاتها قامت المملكة العربية السعودية تحت إشراف مجلس الوزراء في جلسته يوم الاثنين **7** فيفري **2007** برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز نظام مكافحة الجرائم المعلوماتية، وهو يتضمن **16** مادة.[24]

بما أن الدول الغربية استأثرت منذ البداية بهذا المجال فإنها كانت سباقة هي الأخرى في مجال الحماية المقررة له، و شمل ذلك العديد من دول أوربا و أمريكا،حيث تعتبر دولة السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي و الانترنت، حيث صدر قانون البيانات السويدي عام **1973** الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي.و تبعت الولايات المتحدة الأمريكية السويد حيث شرعت قوانين خاصة بحماية أنظمة الحاسب الآلي

---

[23] انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8- يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

[24] انظر الموقع الالكتروني www.nasb.net

(**1976-1985**)، و تأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي، حيث أقرت قانون مكافحة التزوير و التزييف عام **1981**.

أما النموذج الأوروبي الأكثر تطورا فهي اتفاقية بودابست الاتفاقية الدولية للإجرام المعلوماتي أبرمت بتاريخ **2001/11/08**

من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ **2001/11/23**،[25]

المطلب الثاني: أنواع الجرائم الالكترونية.

صنف الفقهاء والدارسون الجرائم الالكترونية ضمن فئات متعددة تختلف حسب الأساس و المعيار الذي يستند إليه التقسيم، فبعضهم يقسمها إلى جرائم ترتكب على نضم الحاسب الآلي و أخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، و كذا تعدد الحق المعتدى عليه، فتتوزع الجرائم الالكترونية حسب هذا التقسيم إلى جرائم تقع على الأموال و جرائم تقع على الأشخاص.ونجد هذا التقسيم شائعا من خلال الدراسات و الأبحاث الأمريكية، ويلاحظ انه يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء.[26]

الفرع الأول: الجرائم التي تقع على الأشخاص.

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

---

[25] انظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الإنترنت و الحاسب الآلي و وسائل مكافحتها، ،دار الفكر الجامعي،الإسكندرية،2005 ص187،186.

[26] انظر يونس عرب، دليل امن المعلومات و الخصوصية (جرائم الكمبيوتر و الانترنت)، إصدار اتحاد المصارف العربية، الجزء الأول،2001 ،
ص 15.

ا/جريمة انتحال الشخصية:

هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا انه ومع انتشار شبكة الانترنت فقد اخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية و استغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي و ما شابهها من اجل الحصول على بطاقات ائتمانية و غيره، و من خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية و التصرف بحرية تحت اسم مستعار. وغالبا

ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت.[27]

ب/جريمة المضايقة و الملاحقة:

و هو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء و تحديث يطال برامج الحوارات المتبادلة و الدردشة، وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

و جرائم الملاحقة تشمل رسائل تهديد و تخويف و مضايقة و قد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد

العلني، و لا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم و الضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية.[28]

ج/جرائم التغرير و الاستدراج:

هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمي الشبكة، و هي تقوم على عنصر الإبهام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت و

---

[27] انظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي و وسائل مكافحتها، دار الفكر الجامعي، الإسكندرية،2005، ص 42 43.

[28] انظر محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى و الإنترنت،دار الثقافة للنشر و التوزيع، الطبعة الأولى، عمان،2004، ص 45.

التي قد تتطور الى لقاء مادي بين الطرفين، و هذه الجرائم لا تعرف الحدود و لا يمكن حصرها، و هي دون حدود سياسية او اجتماعية اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة و كذلك يقع ضحيتها أي مستخدم حسن النية.[29]

د/جرائم التشهير و تشويه السمعة:

مع انتشار الشائعات و الأخبار الكاذبة التي تطول و تمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية او حتى دينية، و قد ظهرت على شبكة الانترنت بعض المواقع و التي جندت نفسها لهدف واحد هو خدمة تلك الشائعات و الأخبار الكاذبة و ذلك بهدف تشهير و تشويه سمعة تلك الرموز، و كذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم.

وابرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها و نشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة.[30]

هـ/الجرائم المخلة بالأخلاق و الآداب العامة:

إذا كانت شبكة الانترنت تتسم بالعالمية و لا تقتصر على مستخدم دون الآخر، فان ما يتم عرضه من مواد تعد مخلة بالآداب و الأخلاق 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 الالكترونية أو محاولة إغوائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي و دعوتهم إلى القيام بالعمال الفاحشة، و تصوير قاصرين ضمن أنشطة للجنس.

والأعمال الإباحية هي من أشهر الأعمال الحالية و أكثرها رواجا خاصة في الدول العربية و أوربا والدول الآسيوية، و تشمل الجرائم المخلة بالأخلاق و الآداب 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 و دون أي حواجز.[31]

---

[29] انظر الموقع الالكتروني www.arablawinfo.com:

[30] انظر منير محمد الجنبيهي، ممدوح محمد الجنبيهي،المرجع السابق، ص 34.

الفرع الثاني الجرائم التي تقع على الأموال :

هي جرائم الاعتداء على الأموال و التي تهدد الحقوق ذات القيمة المالية و يدخل في نطاق هاته الحقوق الحق ذو قيمة إقتصادية.

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته و ما يرتبط به من أسلاك و ما يتصل به من ملحقات فانه 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 و نظم فان النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي.[32]

أ/جرائم صناعة و نشر الفيروسات:

الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، و لكنها 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 و بالتالي تعطلها عن العمل.

وأما عن بدا عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، و قد تبدأ بمجرد تشغيل لبرنامج الموجودة عليه، و تعتبر هذه الصناعة من أهم جرائم الانترنت و أكثرها اتساعاً وانتشاراً، و يعود 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 احدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في اقل من **9** ساعات عام **2001** .[33]

---

[31]انظر محمد امين احمد الشوابكة،المرجع السابق،ص 114

[32]انظر محمد امين احمد الشوابكة،المرجع أعلاه،ص 136

[33]انظر منير محمد الجنبيهي ممدوح محمد الجنبيهي،المرجع السابق، ص86.

ب/جرائم الاختراقات:

الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير و شبكاتهم الالكترونية،و يتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة و له القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات او الشبكات.

وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول و البعض الأخر لسرقتها، و هذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل بدل مالي للاطلاع عليها. وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، و هو اخطر أنواع الاختراق، ومن ابرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها و معلوماتها وهذه العملية تسمى تغيير وجه الموقع.[34]

ج/جرائم ممارسة القمار:

نظرا لأن القمار قد يكون مصرحا به في بعض البلدان إلا أن الأغلب في البلدان مصرح به و لكن بشكل محدود جدا و في بعض الأماكن السياحية فقط دون أن يكون مصرحا به في الأماكن العادية التي يرتادها الأغلبية من أفراد الشعب، نظرا لأنه يخالف تعاليم الدين في كافة البلاد العربية التي حرم الدين الإسلامي لعبه، ففي الماضي كان لعب القمار يستلزم وجود لاعبين معا على طاولة ليتمكنوا من لعبه ، أما الآن ومع الانتشار شبكة الانترنت على المستوى العالمي فقد أصبح بإمكان اللاعبين

التجمع معا عبر الشبكة ولعب جميع أنواع القمار عليها، وعليه فان انتشار شبكة الانترنت في سلبيات انتشار لعب القمار،و بالتالي فلعب القمار غير مصرح به حتى ولو كان عن طريق الانترنت.[35]

[34] انظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع السابق ، ص 47.

[35] انظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه ، ص 88.

د/جرائم غسيل الأموال:

يعني في بسط صوره هو تحويل المصدر الغير مشروع للأموال إلى مصدر مشروع، فمثلا تحويل الأموال الناتجة عن عمليات غير مشروعة كتجارة المخدرات إلى أموال مصدرها مشروع كتجارة السيارات مثلا. و قد أعطت شبكة الانترنت عدة ميزات لمن يقومون بعمليات غسيل الأموال منها السرعة الشديدة و تخطي الحواجز الحدودية بين الدول و تفادي القوانين التي قد تضعها بعض الدول وتعيق نشاطهم، و أيضا كان لانتشار التجارة الالكترونية 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.[36]

هـ/جريمة تعطيل الأجهزة و الشبكات:

يطال التعطيل أجهزة الحاسب الآلي عبر برامجها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز و الهدف من التعطيل منع الحواسيب و الشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة و تتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها و هو الأمر الذي يعيقها عن تأدية عملها.

و/جريمة النصب و الاحتيال:

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

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

- إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية و استخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، و مرتكبوا الجرائم عبر تلك الوسائل يسهل هروبهم و تواريهم لذلك من الصعب جدا ملاحقتهم و القبض عليهم.[37]

---

[36] نظر منير محمد الجنبيهي ممدوح محمد الجنبيهي، المرجع أعلاه ، ص99-100.

[37] انظر الموقع الالكتروني www.arablawinfo.com

الفصل الثاني: الوسائل المعتمدة في الحد من الجريمة الالكترونية

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

ولاشك في أن التطور الحالي الذي لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل إلكترونية متقدمة ومتعددة قدإنعكس 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 جنائياً قد يكون في منتهى الصعوبة.

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

كما وأن الإثبات الجنائي هو أحد 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 الإلكترونية باستخدام الوسائل الإلكترونية 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: الوسائل القانونيةللحد من الجريمة الإلكترونية.

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

خاصةً سبلاً لمحاربتها إلا أن جرائم العصر الرقمي الجديد أحدثت إشكالاً عاماً يبرز كيفية التعامل مع هاته الجرائم التي أرغمت المشرع القانوني إلى تدارك النقص الهائل ومحاولة ملأه مسايراً في ذلك عدة معايير أهمها التقنية العالية في هاته الجريمة.

فالجريمة الإلكترونية لا تترك أثراً مادياً في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على اتلاف أوتشوية أو إضاعة الدليل في فترة قصيرة، ولاتكفي في هذا النمط من الجرائم إعادة نظام الكمبيوتر وقواعد البيانات وشبكات المعلومات.

وتفصيلا لما سبق سنحاول التطرق إلى الوسائل القانونية للحد من الجريمةالإلكترونية (المطلب الأول)، وتوضيح الإختصاص القضائي و العقوبات المقررة على المستوى الوطني (المطلب الثاني)

المطلب الأول: طرق ووسائل البحث عن الجريمة الإلكترونية.

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

وليس على المحقق الالتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا بمباشرتها جميعاً وإنما يباشر منها ما تميله مصلحة التحقيق وظروفه و يرتبها وفقاً لما تقضى به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جميع الأدلة ما يلي:

أولاً: معاينة مسرح الجريمة المعلوماتية.

ثانياً: التفتيش في مجال الجريمة المعلوماتية.

ثالثاً: الشهادة في الجريمة المعلوماتية.

رابعاً: الخبرة في مجال الجريمة المعلوماتية.

خامساً: الضبط في مجال الجريمة المعلوماتية.[38]

[38] أنظر: منتدى شباب طمرة، قسم الكمبيوتر والأنترنت –"جرائم الكمبيوتر و الأنترنت ":الموقع www.6amra.com

الفرع الأول: معاينة مسرح الجريمة المعلوماتية:

يقصد بالمعاينة فحص مكان أو شيء أو 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 أو 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 أو له حرمة خاصة كانت إجراء تحقيق.

والمعاينة جوازيه لمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها، ولاتتمتع المعاينة فيمجال كشف غموض الجريمة المعلوماتية ينفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك إلى الاعتبارات السالف ذكرها.[39]

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

1-تصوير الحاسب و الأجهزة الطرفية المتصلة به و المحتويات و الأوضاع العامة بمكانه، مع التركيز بشكل خاص على تصوير الأجزاء الخلفية للحاسب ملحقاته ويراعي تسجيل وقت و تاريخ ومكان التقاط كل لصور.

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

3-ملاحظة وإثبات حالة التوصيلات و الكبلات المتصلة بالنظام حتى يمكن أجراء عملية المقارنة و التحليل حين عرض فيما بعد على القضاء.

---

[39] 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

4-عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد 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 و الشرائط و الأقراص الممغنطة، السليمة وير السليمة أو المحطمة وفحصها ورفع البصمات التي قد كون لها صلة بالجريمة المرتكبة.

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

-7إعداد 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 قاعدةsmeac العسكرية و التي تعني الحالة situation الرسالةmission التنفيذيةexécution المداخل والمخارج avenues et aprroach و الاتصالات communication 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، و التنفيذ يعني كيفية أداء المهمة، أما المداخل و لا خارج فإن من المهم معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحسب وفقاً لمكونات طريق التحقيق، بينما يأتي عنصر الاتصال لضمان السرية وسلامة لعامل وتبادل المعلومات أثناء عملية الغارة.[40]

وبعد وصول الفريق إلى مسرح الجريمة يتم التأمين و السيطرة على المكان و البدء في التفتيش على النحو التالي:

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

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

3-تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها و التحفظ 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 الإتصالات.

---

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

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 ان يكون المكان بعيدا عن اجهزة الحاسب الآلي.[41]

الفرع الثاني: التفتيش في مجال الجريمة المعلوماتية:

يعتبر التفتيش اجراء من اجراءات بالتحقيق يتطلب اوامر قضائية لمباشرته، ويهدف للبحث عن الادلة المادية التي ترتبط بالجريمة مدار التحقيق. ولا يشتمل لذاك الادلة الشفوية او القولبة للاتصال الاخيرة بعنصر الشخص الشاهد، ويجري التفتيش

بخصوص جرم تحقق وقوعه ويوجه الى مكان يتمتع بالحرمة او يتجه الى الشخص المشتبه به، ويخضع التفتيش في وجوده واجراءاته التنفيذية الى احكام القانون التي من ايرزها صدور امر التفتيش او مذكراته الكتابية عن الجهة التى حددها القانون، مع بيان الاسباب الموجبة لذلك ومحل التفتيش المخصوص.[42]

وسوف نعالج إجراء التفتيش بالنظر الى أمكانية تفتيش العا لم الرقمي والقيود التي ترد على فرقة التفتيش.

1- مدى قابلية مكونات وشبكات الحاسب الالي للتفتيش:

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

[41] أنظر منتدىجامعة قطر "كلية القانون،": "مراحل إثبات الجريمة الإلكترونية" عن موقع:
http://www.quatar .com. /VB/show heard PHP ?t=20845

[42] . أنظر: احمد الكركي: "التحقيق في جرائم الحاسوب"، عن الموقع
(1) http://www.arablawinfo.com/research -search.asp? Validate=articles& articles ID=158

1-1 مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيئ 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 اذ ان لصفة المكان اهمية خاصة في مجال التفتيش فإذا كانت بموجودة في مكان خاص كمسكن المتهم او أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التى يجوز فيه تفتيش مسكنه وبنفس الضمانات المقررة قانونا في التشريعات المختلفة.[43]

ويجب التمييز داخل المكان الخاص بينما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحايسبا الاخرى أم انها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لايخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في اوعية هذا الظام الاخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التى يستلزمها المشرع لتفتيش هذه الاماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الالي المادية أو كان مسيطر عليها او حائزا عليها ، فإن تفتيشها لايكون الا في الحالات التى يجوز فيها تفتيش الاشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

1-2 مدى خضوع مكونات الحاسب المعنوية للتفتيش :

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاق بشأن جواز تفتيشها حيث يذهب رأي انه اذا كانت الغاية من التفتيش هو ضبط الادلة المادية التى تفيد في كشف الحقيقة فان المفهوم يمتد ليشمل البيانات الالكترونية بمختلف اشكالها.

وفي هذا المعنى نجد أن المادة 251 من قانون الاجراءات الجنائي اليوناني تعطى سلطات التحقيق امكانية القيام (بأي شيئ يكون ضروري لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة اي شيئ بأنها تشمل بالضبط البيانات المخزنة أو المعالجة الكترونيا ، ولذلك فإن ضبط البيانات النخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل اي

[43] أنظر منتدىجامعة قطر " المرجع السابق" عن موقع:
http://www.quatar .com. /VB/show heard PHP ?t=20845

مشكلة في اليونان اذ بمقدور المحقق ان يعطى امرا للخبير بجمع البيانات التى يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية.

وتمنح المادة 487 من القانون الجنائي الكندي سلطة اصدار إذن لضبط اي شيئ طالما تتوفر الأسس معقولة للاعتقاد بأن الجريمة ارتكبت او يشتبه بارتكابها او أن هناك نية بان يستخدم في ارتكاب الجريمة أو انه سوف ينتج دليلا على وقوع الجريمة.

وهكذا يفسر هذا النص بوضوح على انه يسمح بضبط بيانات الحاسب غير المحسوسة، وهناك على النقيض رأي آخر يرى أنه اذا كانت الغاية من التفتيش هي ضبط الادلة المادية التى تفيد في كشف الحقيقة فإن هذا المفهوم المادي لاينطبق على بيانات الحاسب الآلي غير المحسوسة او الملموسة، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة ان يضاف الى هذه الغاية التقليدية للتفتيش عبارة " المواد المعالجة عن طريق الحاسب الآلي او بيانات الحاسب الالي "،وبذلك تصبح الغاية الجديدة من الفتيش بعد هذا التطور التقني الحديث هي " البحث عن الادلة المادية أو أي مادة معالجة بواسطة الحاسب " ، ويرى بعض الفقهاء في فرنسا ان النبضات الالكترونية electronicimpluse او الاشارات الالكترونية الممغنطة لاتعد من قبيل الاشياء المحسوسة وبالتالي لاتعتبر شيئا ماديا بالمعنى المألوف للمصطلح ولذا لايمكن ضبطها.

وفي الولايات المتحدة الامريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصة بالاجراءات الجنائية عام 1970 لتنص على السماح بتفتيش اجهزة الكمبيوتر والكشف عن الوسائط الالكترونية بما في ذلك البريد الالكتروني والبريد الصوتي والبريد المنقول عن طريق الفاكس.

وتتركز أذون التفتيش القياسية الصادرة عند التفتيش في احدى جرائم الكميوتر وبصفة خاصة على ضبط الوثائق المكتوبة اضافة الى اجهزة الكمبيوتر، وتتضمن هذه الوثائق على وجه التحديد : النسخ الضوئية ، مطبوعات الكمبيوتر ، فواتير التلفيون ، سجلات العناوين ، المذكرات والمراسلات.[44]

[44] 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

3-1 مدى خضوع شبكات الحاسب للتفتيش:

ويمكن في الفرض التمييز بين ثلاث احتمالات:

الاحتمال الاول: اتصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان اخر داخل الدولة.

يرى الفقه الألماني بشأن مدى امكانية امتداد الحق في التفتيش اذا تبين ان الحاسب او النهاية الطرفية في منزل المتهم متصلة بجهاز او طرفية في مكان اخر مملوك لشخص غير المتهم، انه يمكن ان يمتد التفتيش في هذه الحالة الى سجلات البيانات التي تكون في موقع اخر استنادا الى مقتضيات القسم 103 من قانون الاجراءات الجنائية الألماني.

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

الاحتمال الثاني: انصال حاسب المتهم بحاسب او نهاية طرفية موجودة في مكان اخر خارج الدولة.

من المتصور طبقا لهذا الاحتمال ان يقوم مرتكبو الجرائم بتخزين بياناتهم في انظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات الادعاء في جميع الادلة، ولمواجهة هذا الاحتمال نص مشروع قانون جريمة الحاسب

الآلي بهولندا انه يجوز لجهات التحقيق مباشرة التفتيش داخل الاماكن وبما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى اذا كانت موجودة في دولة اخرى، ويشترط ان يكون هذا التدخل مؤقتا وان تكون البيانات التي يتم التفتيش عنها لازمة لاظهار الحقيقة (المادة 125).[45]

ووفقا لما جاء بتقرير المجلس الاوربي فان هذا الاختراق المباشر يعتبر انتهاكا لسيادة دولة اخرى ما لم توجد اتفاقية دولية في هذا الشأن، ويؤيد الفقه الالماني ما جاء بتقرير المجلس الاوربي حيث ان السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة اخرى وخرقا للقوانين الثنائية والوطنية الخاصة بامكانية التعاون في مجال العدالة القضائي.

---

[45] أنظر منتدىجامعة قطر "كلية القانون،": "مراحل إثبات الجريمة الإلكترونية" عن موقع:
http://www.quatar .com. /VB/show heard PHP ?t=20845

وقد ايد القضاء الالماني هذا الاتجاه حيث اسفر البحث في احدى جرائم الغش المعلوماتي عن وجود طرفية حاسب في المانيا متصلة بشبكة اتصالات في سويسرا، حيث يتم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الالمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة mutual assistanceRequest for، وقد ساور الاعتقاد الشرطة اليابانية بان مجموعة من المخربين قد استخدمت اجهزة كمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على اجهزة الكمبيوتر في كل من هاتين الدولتين حتى تتمكن من الوصول الى جذور هذه العملية الارهابية .

الاحتمال الثالث : يسمح بالتصنت wireapping والأشكال الخاصة للمراقبة التليفونية في العديد من الدول ، حيث يجيز القانون الفرنسي الصادر في 10 يوليو 1991 اعتراض الاتصالات البعيدة télématique 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 الإلكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي .

2 . ضوابط تفتيش نظم الحاسب الآلي :

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

2 . 1 الضوابط الموضوعية لتفتيش نظم الحاسب الآلي : وتنحصر هذه الضوابط في :

وقوع جريمة إلكترونية : والجريمة الإلكترونية هي كما سبق القول وبشكل عام كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة. وهناك العديد من التشريعات التي حرصت على استحداث نص خاص كما هو الحال بالنسبة للأنظمة القانونية التي تم التطرق سابقا في إطار الجهود الدولية ، سواء المنفردة منها أو الجماعية في مواجهة هاته الجريمة العصرية .

. تورط شخص أو 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 الإلكترونية، 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 نسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفه فاعلا أو شريكا.[46]

توافر أمارات قوية وقرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم، حيث لا يكون التفتيش إلا إذا توفرت لدى المحقق أسباب كافية على أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة المعلوماتية أو أشياء متحصله منها.

محل التفتيش الخاص بنظم الحاسب الآلي هي ل المكونات المادية الحاسب سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش.

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 ومهندسي الصيانة ومديري النظم المعلوماتية [47]

---

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

[47] أنظر: أسامة أحمد المناعسة، جلال محمد الزغبي، صايل فاضل الهواوشة: " جرائم الحاسب الألي والانترنت "، داروائل للنشر ، الطبعةالاولى، 2001
ص: 276/272

2 . 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 :

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 إلكتروني ، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كومبيوتر ، 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 بمنزلهم ، وفي مكان ما من المنزل سنجد النقطة الساخنة جهاز كومبيوتر متصل بخط تليفون أو ربما نجد أكثر من جهاز وأكثر من خط في المنزل الواحد ، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين .

توضع النقطة الساخنة في عهدة فريق يضم اثنين 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 واستصدر إذن التفتيش الخاص بها من القاضي ، فهذا الشخص يعرف تماما الشيء أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماماً ولن نتجاوز إذا ما قلنا أنه هو الذي يقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات

الأسطوانات.... الخ.

أما المسجل فيتولى تصوير كافة الأجهزة والمعدات على ذات الكيفية التي تم ضبطها عليها ، ويقوم المسجل كذلك بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعي أحد المجرمين الماكرين أن الشرطة قد سرقت منزله أثناء التفتيش .[48]

. فريق التفتيش:

هو الفريق المعني بإجراءات التحقيق ، وهو جزء داخل فريق الإغارة الذي يضم بجانب فريق التفتيش و الضبط رجال الحراسات والأمن وقوات الحماية و التأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال و السائقين وخبراء مسرحالجريمة 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 أو براءته منها ، وللشهادة في مجال الإجراءات أهمية بالغة لأن الجريمة ليست تصرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه ويحرص على إخفائه عن الناس [49].

وسماع الشهود كسائر إجراءات التحقيق من الأمور التقليدية للمحقق فله أن يسمع الشهود أو 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 أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعا لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له أو ضده .

---

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

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

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 أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ، ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزا عن الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من أهمها :

. 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 .

– المبرمجون:

وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين :

. الفئة الأولى: وهم مخططو برامج التطبيقات.

. الفئة الثانية : هم 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 .[50]

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

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 الأماكن 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 أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ، ويميل إلى 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 أو 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 الإجراءات 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 .[51]

الفرع الرابع : الخبرة في مجال الجريمة المعلوماتية:

ندب الخبير أو مبررات ندب الخبير وإجراءاته: يرى المحقق في بعض الحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافته العامة عن فهمها ، كتحديد سبب الوفاة أو ساعتها أو فع 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 فان العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية 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 الحاسبات وبرامجها وشبكتها ، كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها.

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة ، وللمحقق في أي وقت إلى 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 على 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 وان 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

[51] منتدى قانون نت ، منتدى القضايا الجنائية خصوصية جرائم الحاسوب و الأنترنت عن موقع www.quanoun.net

الكمبيوتر المطبوعة ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة ، أصلية ، أو صورا من خلال استجواب القائمين على حفظها. [52]

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 الحاسبوب 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 أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها .

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

-أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام .[53]

2 . بيان طرق استخدامه:

- كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو 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 أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها ، مع إثبات أن المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة ؟

الفرع الخامس: الضبط في مجال الجريمة الإلكترونية :

يقصد بالضبط في قانون الإجراءات 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 ، وتتحددطبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر

---

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

[53] انظر عبد الفتاح البيومي الحجازي,مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون ألمعلوماتي), دار الفكر الجامعي,الطبعة الأولى,الإسكندرية'2006' ص305/304.

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 الإجراءات يتحدث في بعض التصرف عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم ، والقبض نظام قانوني يختلف عن ضبط الأشياء .

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك يستوي أن يكون الشيء المضبوط مملوكا للمتهم أو لغيره ، والقاعدة أن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته أن 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 أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة ، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات outprintلأغراض المراجعة أو 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 الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة والورق أربعة أنواع :

- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو 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 أو دفاتر الحسابات وتكون لها علاقة بالجريمة، خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

2. جهاز الحاسب الآليcomputer paraphernalia : 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 الإلكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط والتحريز .

3. ملحقات الحاسب الآلي : من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية cup ، لوحة المفاتيح Keyboard والشاشة monitor / ومع التطورات السريعة التي يمر بها الحاسب الآلي 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 disks and diskettes

مع جهاز الحاسب الآلي للشخص الطبيعي والشخص المعنوي تجد قدرا كبيرا من أقراص الليزر ، علاوة على أن مراكز الحاسب الآلي في الأشخاص المعنوية تجد 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:magnetic tapes

وتستعمل الشرائط الممغنطة عادة للحفظ backup الاحتياطي وقد تكون في مكان بعيد آمن ، كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة .[54]

[54] انظر عبد الفتاح البيومي الحجازي,مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون ألمعلوماتي), المرجع السابق، ص307/306.

المطلب الثاني: الاختصاص القضائي و العقوبات المقررة

الفرع الأول: الاختصاص القضائي:

يقصد بالاختصاص القضائي ولاية أو سلطة الحكم بمقتضى القانون في خصومة معينة معروضة على المحاكم ،وفقدان هذه السلطة يؤدي إلى عدم الاختصاص .

وإذا كان الاختصاص النوعي أو المحلي بالنسبة للقضايا المعروضة على القضاء لا يطرح إشكالا بالنسبة للأشخاص الطبيعية أو المعنوية في الجرائم التقليدية فانه قد طرح عدة مشاكل في مجال الجرائم الالكترونية.

حيث سنقوم بتطبيق المبادئ العامة على هذا النوع من الجرائم لان المشرع الجزائري سكت على الفصل في هذه القضية.

1-الاختصاص النوعي:

يتحدد الاختصاص النوعي للمحتكم وفقا لجسامة الجرم التي حددها القانون على أساس العقوبة المقررة لها، فالجنايات من اختصاص محكمة الجنايات، والجنح من اختصاص محكمة الجنح، والمخالفات من اختصاص محكمة المخالفات.[55]

حيث وضع المشرع الجزائري عقوبات لجريمة المساس بالأنظمة المعالجة الآلية للمعطيات ، لذا ومن خلال الاطلاع على نصوص المواد،[56] فان هذه الجريمة تصنف على إنها جنحة ، ذلك لان العقوبات المقررة لها وفق ما سبق توافقا مع ما اقره المشرع في المبادئ العامة ، حيث نجد إن هذه الجرائم لا تتعدى عقوبتها ثلاث سنوات ، لذلك فان محكمة الجنح تكون ذات ولاية بالنظر فيها

---

[55] أنظر أحمد شوقي الشلقاني مبادئالإجراءات الجزائية في التشريع الجزائري ديوان المطبوعات الجامعية ، الجزائر ،ص 357

[56] المادة 394 مكرر:" يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من "50.000 دج إلى 100.000دج....."

المادة 394 مكرر1:" يعاقب بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من "100.000 دج إلى 5.000.000دج...."

المادة 394 مكرر7:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"

2-الاختصاص المحلي: لا يكفي إن تتحدد المحكمة المختصة بالنظر إلى جسامة الجريمة إذ تتعدد محاكم الدرجة الواحدة ويتعين أيها المختصة بالفصل في الدعوة. وقد وضع المشرع الجزائري ثلاث أماكن لتحديد الاختصاص المكاني:

– محل وقوع الجريمة: ففيها اعتدى على الأمن العام وانتهك القانون وفيها يسهل جمع الأدلة.

محل إقامة احد المتهمين : وهو ماييسر الكشف عن ماضي المتهم وسوابقه وسيما انه قديتعذر تحديد مكان وقوع الجريمة أو تكون قد وقعت في الخارج. ومكان إقامة المتهم هو مكان إقامته المعتاد ، وليس الموطن المختار أو القانوني .

محل القبض على المتهم: وهو ما يجنب السلطة العامة مشقة نقل المتهم إلى مكان وقوع الجريمة واحتمال هربه، فضلا عن إن الجريمة قد تقع في الخارج أو يتعذر معرفة مكان وقوعها أو لا يكون للمتهم محل إقامة.[57]

وبالتطبيق على الجرائم الالكترونية فقد يقع النشاط الإجرامي في مكان وتتحدد النتيجة الإجرامية في مكان آخر ولذلك فان كلا المحكمتين التابع لها المكانين تكون مختصة باعتباره محل وقوع الجريمة.

وإذا كانت الجريمة تتكون من جملة أفعال وقعت في أكثر من مكان كانت جميع المحاكم التي وقعت في دوائرها أفعال التنفيذ مختصة بنظر الدعوة من حيث المكان.

أن ما يثير الأشكال في هذا المجال إن الجريمة الالكترونية ليست موجدة عبر العالم ككل، فكل دولة تقرر قوانين لردع مرتكبي تلك الجرائم.فمن هي المحكمة المختصة ؟ هل هي مكان إدخال البيانات أم استخراجها ؟ وبذلك انقسم الفقه إلى ثلاث اتجاهات

الاتجاه الأول: ويرى أن أولى المحاكم بالاختصاص محاكم دولة تحميل البيانات، فهي مكان ارتكاب الجريمة، وهذا يساعد أكثر على جمع البيانات والأدلة بالإضافة إلى انه مكان واحد بعكس مكان الاستقبال الذي يكون من دول عديدة

الاتجاه الثاني: يرى إعطاء الاختصاص لمكان النتيجة الجريمة لتعدد دول التحميل.

[57] أنظر حميد شوقي الشلقاني: مبادئ الإجراءات الجزائية في التشريع الجزائري نفس المرجع السابق، ص 359/358

الاتجاه الثالث: يرى ان الاختصاص ينعقد لمكان المعتدى عليه فهو المكان الذي تتحقق فيه النتيجة الجريمة ، فهو أكثر تحديدا من موطن التحميل فيجنب المتهم تكاليف باهظة لإجراءات التقاضي كون أن المتهم بريء حتى تثبت إدانته .

الفرع الثاني: العقوبات المقررة.

تناول المشروع الجزائري الجزاءات المقررة لهذا النوع من الإجرام الحديث والتي سماها بالعقوبات الجزائية على جريمة المساس بأنظمة المعالجة الالية.

من خلال القانون 06 /23 المؤرخ في 20 ديسمبر 2006 الذي تضمن في مواده عقوبات ردعية اصلية وتكميلية تطبق على الشخص الطبيعي لمبدأ المسائلة الجزائية له فحددها المشرع في القسم السابع المكرر: المواد 394 مكرر الى 394 مكرر 7 من هذا القانون.

أولا: العقوبات الاصلية:

من خلال استقرائنا للنصوص المتعلقة بالجرائم الماسة بانظمة المعالجة الالية للمعطيات يتبين لنا وجود المتدرج داخل النظام العقابي ،ويحدد الخطورة الاجرامية التي قدرها المشرع لهذه التصرفات ونجد من خلال ثلاث حالات هي:

1-1) الدخول والبقاء في الغش(الجريمة البسيطة):

اعتبرها المشرع جنحة واعطى لها عقوبة طبقا للمادة 394 مكرر من القانون 06 /23 وهي 3 اشهر الى سنة حبس و 50000 الى 100000 دينار جزائري كغرامة مالية كل من يدخل او يبقى عن طريق الغش في كل أو جزءمن منظومة المعالجة الالية للمعطيات او يحاول ذلك.[58]

1-2) الدخول و البقاء بالغش:(الجريمة المشددة).

[58]انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8-يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

هي أخرى يعتبرها المشرع جنحة غير انه ضاعف لها العقوبة في حالة حذف او تغيير للمعطيات المنظومة وذلك باقراره لعقوبة الحبس بين 6 اشهر الى سنتين بغرامة مالية من 50.000 دينار جزائري الى 150.000 دينار جزائري، اذ ترتب عن ذلك التزام بالفعل المعاقب عليه لظروف قد تؤدي الى تنفيذه الا وهي نتائج الدخول او البقاء الغير مشروعة لتخريب نظام الاشغال المنظومة طبقا للمادة 394 مكرر الفقرة 2 من قانون عقوبات جزائية.

1-3) الاعتداء العمدي على المعطيات:

العقوبة المقررة في حالة الاعتداء العمدي على المعطيات داخل النظام طبقا للمادة 394 مكرر 1 من قانون العقوبات هي الحبس من 6اشهر الى 3سنوات وبغرامة من 500.000 د.ج الى 200.000 دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية وازال او عدل بطريقالغش المعطيات التي يتظمها.[59]

اما في حالة الحيازة او افشاء او نشر او استعمال المعطيات المتحصل عليها باحدى الجرائم الماسة بالانظمة المعلوماتية فالعقوبة المقرر هي الحبس من شهرين الى 3 سنوات وبغرامة مالية 1.000.000 دج الى 5.000.000دج طبقا للمادة 394 مكرر 2.**ثانياً: العقوبات التكميلية:** الى جانب العقوبات الاصلية للجريمة التي يقوم بها المجرم الطبيعي فإن المشرع اضاف عقوبات تكميلية طبقا للمادة الـ 394 مكرر من القانون 06/ 23 وهي كالاتي:

2-1المصادرة: تشمل الاجهزة والبرامج والوسائل المستخدمة في ارتكاب احدى الجرائم الماسة بالانظمة المعلوماتية مع مراعاة الغير حسن النية.

2-2 اغلاق المواقع: وهنا الامر يتعلق بالواقع التي تتكون محلا للجرائم المتسة بالانظمة المعلوماتية.

2-3 اغلاق المحل او مكان الاستغلال: هنا يجب ان يتوفرعنصر العلم بالجريمة لصاحبها في المحل مثل اغلاق المقهى الالكتروني الذي ترتكب فيه الجريمة.

[59] انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8-يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

ثالثاً: الظروف المشددة:

نصت المادة 394 مكرر للفقرة 2 و3 على ظرف تشدد به عقوبات جريمة الدخول والبقاء الغير مشروع داخل النظام ويتحقق الظرف عندما ينتج عن الدخول والبقاء اما حذف او تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة ففي الحالة الاولى تتضاعف العقوبة المقررة طبقا للفقرة الاولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة من 6 اشهر الى سنتين وبغرامة من 50.000 الى 150.000 دج. وهذا الظرف المشدد هو ظرف مادي يكفي ان تقوم بينه وبين الجريمةالاساسية وهي جريمة الدخول او البقاء الغير مشروع علاقة سببية للقول بتوافره.

-تتضاعف العقوبة في حالة ان الجريمة استهدفت الدفاع الوطني أوالهيئات او المؤسسات الخاصة للقانون العام.[60]

[60]انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8-يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

المبحث الثاني: الوسائل التقنية والدولية للحد من الجريمة الإلكترونية.

إن ارتباط الأفراد ، بل المنظمات والدول مع بعضها البعض عن طريق شبكة المعلومات العالمية (الإنترنت) ، وازدياد عدد المستخدمين والمستفيدين من خدمات الإنترنت والتي أصبحت خدماتها عابرة للحدود ، فرض على الأفراد والدول على حد سواء ضرورة التفكير بإيجاد طرق وأساليب جديدة لمكافحة جرائم تكنولوجيا المعلومات ، على الصعيد الفردي والدولي.[61]

بيد أن أمر مكافحة الجرائم الإلكترونية لا يخلوا من الصعوبات والمشاكل وعليه لا بد من الاعتراف بأنه بات مؤكدا أن يعرف المجتمع بأنه لا يوجد حل جذري ينصح الالتزام به للوقاية من هذا النوع من الجرائم ، وتأتي الصعوبة هنا نتيجة لتنوع أشكالها، أضف عليه تعدد طرق وأساليب ارتكابها ، زد على ذلك اختلاف دوافع وصفات مرتكبيها ..... الخ.

وبذلك تعد طرق الإثبات العلمية الوسيلة الوحيدة التي يعتمد عليها رجال التحقيق في محاولاتهم لإثبات الجرائم الإلكترونية ، إلا أننا لاحظنا أن المكلفين بالتحقيق ليس لهم أي دور في الوقاية من هاته الجرائم إذ أن دورهم يأتي بعدما تقع الجريمة ويرتكب الجرم .

ولذلك ارتأينا التطرق إلى بعض الوسائل التقنية للحد من وقوع تلك الجرائم (المطلب الأول) كما أن من وسائل الحد التعاون الدولي والتعاون بين الأفراد والمنظمات والشركات والدول وتشريع قوانين على المستوى الوطني، (المطلب الثاني).

[61] انظر :د. عبد الحكيم رشيد توبة: جرائم تكنولوجيا المعلومات، دار المستقبل للنشر و التوزيع، عمان 2009 ص 219

المطلب الأول: الوسائل التقنية.

في ميدان حماية الاتصالات وحماية الكمبيوتر عن إجراءات الوقاية بخدمات الأمن ، ولا يقصد بها الخدمات بالمعنى المعروف وإنما أطلق هذا التعبير جراء نشوء شركات متخصصة بأمن المعلومات تقدم هذه الخدمات وعموما فإن هناك خمسة أنواع أساسية لخدمات الأمن تستهدف حماية خمسة عناصر رئيسية في ميدان المعلومات .

الفرع الأول: خدمات حماية التعريف والسيطرة على الدخول.

– تهدف خدمة حماية التعريف إلى التثبت من الهوية وتحديدا عندما يقوم الشخص بالتعرف عن نفسه ، فإن هذه الخدمة تقوم بالتثبت من أنه هو الشخص نفسه ، ولهذا فإن التعريف يعد من الوسائل التي تحمي من أنشطة التخفي والتنكر ، ومن هنا فإن هناك نوعين من خدمات التعريف الأول تعرف الشخصية وأشهر وسائلها كلمات السر ، وثانيها التعريف بأصل المعلومات كالتثبت من أصل الرسالة .

–تستخدم خدمة السيطرة على الدخول للحماية ضد الدخول غير المشروع إلى مصادر الأنظمة و الإتصالات والمعلومات ، ويشمل مفهوم الدخول الغير مصرح به لأغراض خدمات الأمن والاستخدام غير المصرح به والإفشاء والتعديل والإتلاف وإصدار المعلومات والأوامر الغير مصرح بها. [62]

الفرع الثاني : الخدمات السرية وسلامة المحتوى ومنع الإنكار

– الخدمات السرية تحمي المعلومات من الإفشاء للجهات الغير مصرح لها بالحصول عليها، و السرية تعني بشكل عام إخفاء المعلومات من خلال تشفيرها على سبيل المثال أو من خلال وسائل أخرى كمنع التعرف على حجمها أو مقدارها أو الجهة المرسلة إليها .

– خدمات سلامة المحتوى تهدف إلى الحماية من مخاطر تغيير البيانات خلال عملية إدخالها أو معالجتها أو نقلها ، وتهدف هذه الوسائل أيضا إلى الحماية من أنشطة تدمير المعطيات بشكل كامل أو إلغائها دون تخويل .

–خدمة منع الإنكار تهدف إلى منع الجهة التي قامت بالتصرف من إنكار حصول نقل البيانات أو النشاط من قبلها . [63]

[62] أنظر : يونس عرب ، " الخصوصية وأمن المعلومات في الأعمال اللايلكيو بواسطة الهاتف الخلوي " عن موقع www.arablaw.org.

المطلب الثاني: الوسائل الدولية

إن مكافحة الجرائم الإلكترونية على صعيد مستوى الدولة الوحيدة لن يكون مجديا ، إلا إذا كان هناك تعاون دولي على أكبر قدر من التنسيقات والتعاون بين الدول والمنظمات ، ومن ثم العمل على تنسيق تلك الجهود المبذولة بين كافة دول العالم لتكون هناك أسس ومبادئ وقوانين وثقافة يمكن الاعتماد عليها لخلق مواطن لديه وعي يجنبه عدم الانزلاق وراء دوافعه لارتكاب إحدى الجرائم الإلكترونية .

الفرع الأول: التشريعات على المستوى العربي

-ليس هناك في العالم العربي ما يستحق الوقوف عنده كثيرا ، فإنه للأسف الشديد لا توجد أي دولة عربية قامت بسن قوانين جديدة خاصة بها لتستوعب تلك المستجدات الإجرامية ، فالدول العربية لا زالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي .

ومع ذلك فلا ينتقص الجهد الطيب في عدد من مناطق الاهتمام والتي يمكن تلخيصها فيما يلي :

أ. تشريع الإمارات العربية المتحدة : يعتبر القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، هو الإطار القانوني لمكافحة هذا النوع المستجد من الجرائم ولعل هذا القانون يعتبر من القوانين الريادية الأولى في العالم العربي الذي ينظم مكافحة الجرائم المعلوماتية .[64]

وسوف نقوم بذكر بعض الجرائم التي تعرض لها هذا القانون فمنها :

-جريمة اختراق المواقع والأنظمة الإلكترونية.

-جريمة التزوير لمستندات معترف بها معلوماتيا.

-جريمة التنصت باستعمال الإنترنت أو إحدى وسائل تقنية المعلومات .

- جريمة التهديد باستخدام الإنترنت أو إحدى الوسائل التقنية.

-جريمة انتهاك الحياة الخاصة عن طريق الإنترنت أو إحدى الوسائل التقنية ....

كما قام بوضع قواعد إجرائية وهي أحكام المصادرة والإبعاد ، والسلطات التي تتمتع بصفة الضبط القضائي

---

[63] أنظر : يونس عرب " أمن المعلومات، نفس الموقع أعلاه"

[64] عبد الله عبدالكريم عبد الله ، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)،منشورات الحلبي الحقوقية ، بيروت، 2007ص63

ب . التشريع السعودي : احتلت السعودية المركز السادس عالميا بين الدول التي تنطلق منها الهجمات الإلكترونية نسبة إلى عدد مستخدمي الإنترنت ، وبدأت السلطات في الإعداد لإصدار قانون جديد لمكافحة الجرائم الإلكترونية وذلك بتاريخ 07 فيفري 2007 ويتضمن مشروع القانون 16 مادة .

حيث يتضمن السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 500 ألف ريال أو بإحدى هاتين العقوبتين لكل شخص يرتكب أي من جرائم التنصت على المعلومات المرسلة عن طريق الشبكة العالمية ، كما يتضمن تجريم الدخول غير المشروع للمواقع الإلكترونية لتغيير تصميماته أو تعديله أو إلغائه أو إتلافه، و تصل مدة السجن إلى 10 عشر سنوات والغرامة إلى 5 ملايين ريال في حالة إنشاء مواقع للمنظمات الإرهابية على الإنترنت.

وهذه أمثلة من الجرائم التي جاء بها هذا القانون .

ج . التشريع التونسي: يحدد القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم 83 المؤرخ في 09 أوت 2000 بعض الأحكام الخاصة بجرائم المعلوماتية والإنترنت .

فعلى سبيل المثال الفصل 48 من القانون المشار إليه ينص على أنه يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين ستة أشهر وعامين وبخطية تتراوح بين 1000 و 10.000 دينار أو بإحدى هاتين العقوبتين .

أما بموجب الفصل 49 فإنه يعاقب كل مخالف لأحكام الفصول 25 و 27 و 29 والفقرة الثانية من الفصل 31 والفصل 34 والفقرة الأولى من الفصل 35 من هذا القانون بخطية تتراوح بين 500 و 5000 دينار .[65]

د . التشريع على المستوى الوطني (الجزائر): يتناول المشرع الجزائري هذا النوع من الجرائم من خلال القانون 23/06 الذي تضمن في مواده عقوبات ردعية أصلية وتكميلية تطبق على الشخص الطبيعي والمعنوي حيث يتضمن جريمة المساس بأنظمة المعالجة الآلية لبيانات والمعطيات ، التي جاء بها في المواد من 394 مكرر إلى 394 مكرر 07 من قانون العقوبات الجزائري .[66]

الفرع الثاني: التشريعات على المستوى العالمي.

---

[65] عبد الله عبدالكريم عبد الله ، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)، نفس المرجع السابق، ص85/81

[66] انظر القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8-يونيو1966(ج ر رقم 84 المؤرخة في 24-12-2006)

أ . التشريع السويدي : تعد دولة السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت والحاسب الآلي لتستطيع أن تعاقب المتهمين بارتكاب تلك الجرائم الإلكترونية ،حيث صدر أول قانون خاص بها وسمي بقانون البيانات وقد صدر هذا القانون عام 1973 وقد عالج هذا القانون قضايا الاحتيال عن طريق الإنترنت بالإضافة إلى كونه يشتمل على فقرات عامة من نصوصه لتشمل جرائم الدخول الغير المشروع على البيانات الإلكترونية .[67]

ب . التشريع الأمريكي: كانت هي الدولة الثانية في إصدار قوانين خاصة بها تجرم الجرائم الإلكترونية، حيث شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي (1985 – 1976) وفي عام 1985 حدد معهد العدالة القومي الأمريكي خمسة أنواع من الجرام المعلوماتية وهي :

- جرائم الحاسب الآلي الداخلية .
- جرائم التلاعب بالحاسب الآلي.
- جرائم الحاسب غير المشروع عن بعد .
- دعم العاملات الإجرامية .
- سرقة البرامج الجاهزة والمكونات المادية للحاسب .

وقد خولت وزارة العدل الأمريكية في عام 2000 خمس جهات حكومية للتعامل مع جرائم الإنترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي (FBI).

ج . التشريع البريطاني : هي ثالث دولة تسن قانونا خاص بها لجرائم الإنترنت ، حيث أقرت قانونا لمكافحة التزوير والتزييف عام 1981 الذي تشمل في تعاريف الخاصة تعريف أداة التزوير ، وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى .[68]

د . التشريع الفرنسي : هي من الدول التي اهتمت بتطوير القوانين الخاصة بها للتوائم مع الجرائم التكنولوجية الحديثة (الجرائم الإلكترونية) فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية ، حيث أصدرت

[67] انظر :د. عبد الحكيم رشيد توبة: جرائم تكنولوجيا المعلومات، نفس المرجع السابق، ص 229

[68] انظر :د. عبد الحكيم رشيد توبة: جرائم تكنولوجيا المعلومات ،نفس المرجع أعلاه، ص 230

أول قانون خاص بها في عام 1988 القانون رقم 88/19 والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم كما تم في عام 1994.[69]

الفرع الثالث: المعاهدات والمؤتمرات الدولية.

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة هذا النوع من الجرائم ومنها:

أ/ معاهدة بودابست لمكافحة جرائم الإنترنت : **بتاريخ** 2000/08/20 تقدمت اللجنة الأوربية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر ، وبعد إعداد مسودتها النهائية أقرت لاحقا في بودابست في 2001 وتعرف باتفاقية بودابست .

وتتكون هذه الاتفاقية من مقدمة وأربعة فصول ، فبعد أن استعرضت المقدمة أهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة ، جاء الفصل الأول لتغطية المصطلحات الأساسية (المادة الأولى) وتضمن الفصل الثاني ثلاث أقسام : يضم الأول المواد من 02 – 13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر ، والقسم الثاني ويضم المواد من 14 – 21 وتتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة 22 وهي تتعلق بالاختصاص ، أما الفصل الثالث من الاتفاقية ، فقد تضمن قسمين الأول تحت عنوان المبادئ العامة ويضم المواد من 23 – 28 والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من 29 – 35 ، أما الفصل الخامس فيتضمن الأحكام الختامية ويضم المواد من 36 – 48 .[70]

ب/ القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات : اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة ، والذي كان قد اعتمده مجلس وزراء العدل العرب في دورته التاسعة بالقرار رقم 495- د 19 بتاريخ 2003/10/08 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين ويتكون من 27 مادة .[71]

---

[69] انظر :د. عبد الحكيم رشيد توبة: جرائم تكنولوجيا المعلومات نفس المرجع السابق، ص 231

[70] عبد الله عبدالكريم عبد الله ، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)،منشورات الحلبي الحقوقية ، بيروت، 2007، ص125

[71] عبد الله عبدالكريم عبد الله ، جرائم المعلوماتية و الأنترنت (الجرائم الإلكترونية)، نفس المرجع السابق، ص140

ج/ **المعاهدة الأوربية لمكافحة الجريمة الإلكترونية** : لقد وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوربي على المسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة الدول في مكافحة الجريمة الإلكترونية ، وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس والتوقيع عليها من قبل البلدان المعنية ستلزم الاتفاقية الموقعين عليها بسن الحد الأدنى من القوانين لمواجهة جرائم التقنية العالية. [72]

[72] انظر :د. عبد الحكيم رشيد توبة: جرائم تكنولوجيا المعلوماتنفس المرجع السابق، ص 288

الخاتمة:

بناءا على ما تقدم صار لازما ولكي نحدث تغيير جذريا في مسارنا التاريخي لا بد أن نستوعب عناصر التغيير الفعال لا سيما التي تؤسس طريق المستقبل وبشكل أخص العناصر المستحدثة وإلا فإن العناصر قد تنقلب إلى أزمة حقيقة، إن لم يفهم ويتعامل معها بشكل جيد، ومن هذه التحديات التاريخية الجديدة ظاهرة المعلوماتية التي فرضت نفسها بوصفها عنصر حاسم في صراع الأمم وصياغة المستقبل وامتلاك الغد القريب والبعيد، ويجب أن نفهم جميعا أن هذه الظاهرة سوف نستأصلها إن لم نستوعبها، كما أنها يمكن أن تكون عنصر تغيير بناءا للمستقبل إن استفدنا من جوانبها الايجابية ،وفي ظل هذه الظروف الاتصالية الجديدة باتت تسهيلات وإمكانات خدمات الحاسوب وتطبيقات الانترنت سهلة في مجال التوظيف السلبي لها مسببة هاجسا أمنيا عالميا يتردد صداه في أغلب المجتمعات، ومع الانترنت تجاوزت الجريمة في حجمها وأنماطها الكثير من محددات الجريمة التي صاحبت وسائل الإعلام التقليدية مثل : التشهير والقذف وغيرها من جرائم النشر، حيث نفذت هذه الجرائم التقليدية بأساليب جديدة لتشمل السرقة والنصب والتزوير والاختلاس، عبر شبكات المعلومات والحاسبات وملحقاتها المتجددة كل يوم أو لعل من المهم في مسار العمل المؤسسات المختلفة التي توظف الانترنت وشبكات الحاسوب الاهتمام بإرسال قواعد واضحة لإجراءات أمن هذه الوسائل وتشمل أمن المكان وأمن العاملين ولأمن الأجهزة و البرامج كما يجدر بالمعنيين بالتحقيق و البحث العلمي في الجرائم الإلكترونية إدراك مختلف الأبعاد الاتصالية للشبكة والتفريق بين الجرائم بحسب خصائص كل جريمة و بالتالي تقديم حلول تسهل من مكافحتها و التقليل من آثارها السابية، وبالتالي نتوصل من تمرتا في هذا العرض إلى أن حقيقة الجريمة الإلكترونية عمل أو سلوك غير شرعي ينتظر فرصة فنية للإيقاع بالضحية و أي ثغرة قانونية للإفلات من طائلة العقاب أو حتى إجراء إداري غير مدروس للتغلغل في شبكة إلكترونية مستهدفة وتحقيق غايات تخدمه.

ومن خلال منطلقات وأهداف البحث من خلاصة ما توصلنا إليه يمكن جملة من التوصيات العامة التي قد تساهم في التقليل من الآثار السلبية لكثير من التحولات الأمنية المصاحبة لوسائل الاتصال الحديثة وتندرج هذه التوصيات تحت المحاور الثلاث الآتية والتي قد تفيد مشرعي العالم و الدول العربية بصفة عامة و المشرع الجزائري بصفة خاصة.

ففي مجال التعليم و التدريب نجد إنشاء معهد إقليمي متخصص في التدريب على التحقيق في الجرائم التقنية المعاصرة والنظر تضمين، في مناهج التحقيق الجنائي في كليات ومعاهد

تدريب الشرطة أيضاً تشجيع الباحثين بالدعم المعنوي و المادي لإجراء المزيد من البحوث و الدراسات حول الجرائم المستحدثة وعقد دورات مكثفة للعاملين في حول التحقيق والمرافعات حول الانترنت وتطبيقات الحاسوب والجرائم المرتبطة بها أيضا، خلق ثقافة اجتماعية جديدة تصور جرائم الكترونية على أنها أعمال غير مشروعة مثلها مثال أنماط الجريمة الأخرى والتأكيد على إن مجرم الانترنت يستهدف الإضرار بالآخرين ويستحق العقوبة.

كما نجد في المجال التشريعات والأنظمة إعطاء جرائم تقنية حقها من الأهمية في مؤسسات التشريع الوطنية وإدراجها ضمن التشريعات الوطنية المختلفة، كذلك إدراك أن الجرائم ذات بعد دولي تتطلب الانخراط في الاتفاقيات الدولية والاهتمام بالتعاون الدولي في مجال المكافحة ،وكذلك تعديل بعض التشريعات العالية بما يتلاءم مع طبيعة جرائم الانترنت والتقنية وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات وشرحها لهم بشكل واضح.

أما على مجال الإجراءات الفنية والإدارية ومساعدة شركات التقنية والانترنت في اتخاذ إجراءات أمنية مناسبة سواء من حيث سلامة المنشآت أو ما يختص بقواعد حماية الأجهزة آو البرامج ،كذلك مساعدة شركات إنتاج البرامج في مجال تطوير أنظمة تشغيل، وكذلك برامج الحماية للتحقيق من الاعتماد على الصادرات في هذا المجال، مع ما تحمله من مخاطر محتملة كما يجب وضع سياسات عمل وإجراءات إدارية وفنية واضحة فيما يختص من المعلومات، والحرص على أن يطلع عليها العاملون في الإدارة نأمل في إعطاء أهمية كبيرة للمرونة المالية في شراء العتاد والبرمجيات التي تكفل بناء وصيانة أنظمة وشبكات معلومات متكاملة تتوافر لها الحماية في جميع الأوقات، أيضا عقد اجتماعات دورية لمسؤولين لتحديث تقنية المعلومات ولتبادل الخبرات،فيما يختص بأمن الحاسوب وجرائمه، كما يجب إعادة رسم الأولويات الوطنية مع التأكيد على أن المعلومات في عصر العولمة ثروة وطنية في هذا المجال تستحق كل الجهود والموارد المالية والبشرية للمحافظة عليها .

وأخيرا يجب التنسيق لإنشاء مركز معلومات دولي مشترك يهتم برصد وتحليل جرائم الحاسوب ومعلومات عن المدانين والمشتبه بهم في مجال الجرائم الإلكترونية حيث إن الجريمة الالكترونية لا تحدها حدود وطنية أو قومية.

قائمة المصادر والمراجع

أولاً: قائمة الكتب والمؤلفات

أ- قائمة الكتب والمؤلفات العامة

1- **حميد شوقي الشلقاني**

مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر ، 1996

2 -**عبد الله سليمان,**

شرح قانون العقوبات الجزائري القسم العام , ديوان المطبوعات الجامعية ا' الجزائر الطبعة السادسة 2005

ب- قائمة الكتب والمؤلفات العامة

1-.: **أسامة أحمد المناعسة، جلال محمد الزغبي ،حايل فاضل الهواوشة**

" جرائم الحاسب ألللآلي والانترنت ، دار وائل للنشر ، عمان ، الطبعة الأولى، 2001"

2- جميل عبد الباقي الصغـــــــــــير

القانون الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 1992

3- هدى قشقوش

جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية،القاهرة، 1992

4- هشام محمد فريد رستم

العقوبات و مخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة،2000

5-منير محمد الجنبيهي، ممدوح محمد الجنبيهي

جرائم الانترنت والحاسب الآلي ووسائل مكافحتها ، در الفكر الجامعي ، الإسكندرية، 2005

6-محمد أمين أحمد الشوابكة

جرائم الحاسب الآلي والانترنت-الجريمة المعلوماتية- دار الثقافة للنشر والتوزيع الطبعة الأولى ،2004

7-عبد الفتاح البيومي الحجازي

مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي(دراسة قانونية متعمقة في القانون ألمعلوماتي), دار الفكر الجامعي,الطبعة الأولى,الإسكندرية،2006

8- :د. عبد الحكيم رشيد توبة

جرائم تكنولوجيا المعلومات، دار المستقبل للنشر و التوزيع، عمان ،2009

9-عبد الله عبد الكريم عبد الله

جرائم المعلوماتية والانترنت (الجرائم الإلكترونية) منشورات الحلبي،الحقوقية بيروت ،2007

10- نبيلة هبه هروال

الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات (دراسة مقارنة) دار الفكر الجامعي,الإسكندرية ،2007

11-يونس عرب

دليل امن المعلومات و الخصوصية (جرائم الكمبيوتر و الانترنت)، إصدار اتحاد المصارف العربية، الجزء الأول،2001

ثانيا :النصوص القانونية

القانون 06 -23 المؤرخ في 2006/12/20 – المعدل و المتمم للأمر رقم 156/66 المؤرخ في 08يونيو 1966 –الجريدة الرسمية رقم 84-المؤرخة في 2006/12/24-المتضمن قانون العقوبات.

ثالثا : المواقع الالكترونية على شبكة الانترنت

1-: احمد الكركي: "التحقيق في جرائم الحاسوب"، عن الموقع

? http://www.arablawinfo.com/research -search.asp Validate=articles& articles ID=158

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

http://www.arablawinfo.com/research -search.asp? Validate=articles ID=148

3- منتدى جامعة قطرا"كلية القانون ، التحديات الإجرائية والقانونية في بيئة الانترنت": مراحل إثبات الجريمة الإلكترونية عن موقع:

http://www.quataru .Com. /VB/showtheard PHP ?p=442389#post 442389

موقع: www.allarab.com

law.info.comwww.arab

http://lattakia.org

www.nasf.net

خطة البحث:

المقدمة.

الفصل الأول: ماهية الجريمة الإلكترونية .

المبحث الاول: مفهوم الجريمة الإلكترونية

المطلب الأول: تعريف الجريمةالإلكترونية.

الفرع الأول: التعريف القانوني.

الفرع الثاني: التعريف الفقهي.

المطلب الثاني:خصائص الجريمة الإلكترونية.

الفرع الأول: مميزات الجريمة الإلكترونيةعن غيرها من الجرائم.

الفرع الثاني: خصائص مرتكب الجريمة الإلكترونية.

المبحث الثاني: أركان وأنواع الجرائم الإلكترونية

المطلب الأول: أركان الجريمة الإلكترونية.

الفرع الأول: الركن المادي

الفرع الثاني: الركن المعنوي.

الفرع الثالث: الركن الشرعي.

المطلب الثاني: أنواع الجريمة الإلكترونية.

الفرع الأول: الجرائم التي تقع على الأشخاص.

الفرع الثاني: الجرائم التي تقع على الأموال.

الفصل الثاني: الوسائل المعتمدة في الحدمن الجريمة الالكترونية.

المبحث الأول:الوسائل القانونية للحد من الجريمة الإلكترونية.

المطلب الاول: طرق ووسائل لالبحث عن الجريمة الإلكترونية.

الفرع الأول: معاينة مسرح الجريمة.

الفرع الثاني: التفتيش في مجال الجريمة المعلوماتية

الفرع الثالث : الشهادة في مجال الجريمة المعلوماتية

الفرع الرابع: الخبرة في مجال الجريمة المعلوماتية

الفرع الخامس: الضبط في مجال الجريمة المعلوماتية.