جامعة زيان عاشور _ الجلفة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة بعنوان:

خصوصية جريمة المساس بالأنظمة المعلوماتية في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر في قانون الخاص

تخصص: قانون جنائي خاص

من تقديم:

– صيفية خالد.

_ قشام عمر.

_ لجنة المناقشة :

- د. دروازي عمار..... رئيسا.
- د.جدي نجاة .....مشرفا ومقررا.
- د. حجاج مليكة.....ممتحنا

الموسم الجامعي :2021_2022


بسم الله الرحمن الرحيم

إهـــــداء

* اهدي هذا العمل المتواضع

* الى من هما العمر الاغلى

* اسمهما في حياتي احلى نعمة

* الى اعز واغلى ما في الوجود

* الى جدار القوة ومنبع الحنان الى روح " أمي " رحمها الله.

* الى من حثني على العلم والمعرفة "أبي الغالي" حفظك الله.

* الى شموخ عمري أخواتي واخوتي.

* الى أستاذتي المشرفة حفظك الله.

* الى الاهل والاصدقاء والزملاء والزميلات .

* الى من علموني الحروف ومعانيها معلمون (ت) واساتذة (ت).

* الى كل هؤلاء اهدي عملي المتواضع *

شكر والعرفان

قال رسول الله الكريم عليه أفضل الصلاة وأزكى التسليم " من لم يشكر الناس لم يشكر الله عز وجل"

لذا نحمد الله تعالى حمدا كثيرا طيبا على ما اكرمنا به من اتمام هذه الدراسة.

ثم نتوجه بالشكر الجزيل و عظيم الامتنان و التقدير إلى الدكتورة الفاضلة" جدي نجاة " حفظها الله وأطال في عمرها لتفضلها الكريم بالإشراف علي في هذا البحث فنشكرها على مجهوداتها التي بذلتها معنا في تصويبها لأخطائي وتوجيهاتها القيمة لي.

وكما يسعنا أن نتوجه بالشكر الجزيل الى عاملي وعاملات قسم الحقوق بجامعة الجلفة و إلى كل الذين تمنوا لنا التوفيق و ساعدونا ولو بكلمة طيبة في إنجاز هذا البحث.

صيفية خالد

مقدمة

مقدمة :

الجريمة هو مصطلح قديم المنشأ كان ملازما للإنسان منذ ظهوره وقد تطورت الجريمة بتطور الانسان وبمرور الازمنة و تعاقب الاجيال ، حيث تعتبر الجريمة كل ما يمس امن الفرد و المجتمع او حياة الفرد وكل ما يتعلق بممتلكاته سوآءا المادية او الجسدية .

وبتطور الانسان ظهر ما يعرف بالدولة حيث أصبحت هي من تتولى شؤون الناس وهي من تسن القوانين التي يلتزم بها الفرد و المجتمع بغية تنظيم الحياة العامة ، وتفرض عواقب واجراءات عقابية على كل من يخالف هذه القوانين سوآءا بالسجن أو بفرض غرامات حيث أصدرت تشريعات منها ما هو موضوعي "قانون العقوبات"، الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي "قانون الإجراءات الجزائية "الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان .

غير أنه بتطور الإنسان في شتى الميادين، خصوصا في مجال التقنية، إذ ظهر الحاسب الآلي وشبكة الأنترنت، وغزت هذه الوسيلة جميع المجالات نظرا لما تتسم به من الدقة والسرعة وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المجرمين، وهو الانعكاس السلبي لهذه الثورة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية، فهذه التقنية تسمح بنقل المعلومة صوتا وصورة عبر الأنترنت، وفي أي مكان من العالم، مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم.

ومن هنا ظهر مصطلح جرائم المعلوماتية والتي يستخدم فيها الكمبيوتر لأغراض غير شرعية، مثل سرقة الأموال عن طريق اختراق نظام الكمبيوتر الخاص بمؤسسة أو مصرف معين أو سرقة المعلومات عن طريق اختراق شبكة اتصالات معلوماتية أو يكون الاختراق لأهداف سياسية أو عسكرية أو دينية أو غير ذلك

ومن خلال هذا التمهيد المتواضع و المتعلق بموضوع مذكرتنا التي جاءت بعنوان: "خصوصية جريمة المساس بالأنظمة المعلوماتية في التشريع الجزائري".

أسباب اختيار الموضوع:

التعريف بظاهرة جديدة هي الجريمة المعلوماتية التي بدأت في الظهور والانتشار وارتبطت بتكنولوجيا الحاسبات الآلية مما أسفر عن تميزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم مما يستتبع ضرورة التعامل معها بما يتلاءم من هذه الخصوصية.

ولما كانت هذه الجرائم ترتبط بتقدم المجتمعات فكلما ازداد اعتماد المجتمع على الحاسبات الآلية كلما كان ذلك إيذانا بزيادة معدل جرائم المعلوماتية كان لزاما أن يواكب هذا التقدم فهما كاملا للجريمة المعلوماتية وكيفية مواجهتها سواء من الناحية التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات أو من الناحية القانونية وهي مهمة المشتغلين بالقانون. .

ولقد زاد من أهمية البحث صعوبة تطبيق النصوص التقليدية على هذه الجرائم وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة الجريمة المعلوماتية لذا فإن إدراك ماهية هذه الجريمة واستظهار خصائصها وسمات مرتكبيها ودوافعهم وجزاءاها يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة. ثم ما يزيد من أهمية هذا الموضوع صدور القانون رقم 15/ 4 المعدل والمتمم للأمر رقم66/156.

المتضمن قانون العقوبات الذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية.

وبهذا سنحاول إبراز من خلال طرح الإشكال التالي:

- **إشكالية الدراسة:**

_ هل الترسانة القانونية للمشرع الجزائري كفاية للتصدي للجريمة المعلوماتية وردع مرتكبيها، أم لابد من إعادة النظر في فحوها لتواكب خصوصيات الجريمة المعلوماتية؟

و للإجابة عن هذا التساؤل ارتأينا تقسيم هذا البحث إلى فصلين نتناول في أوله الأحكام العامة للجريمة المعلوماتية بتبيان مفهومها على ضوء التشريعات المقارنة بالإضافة إلى التطرق إلى خصوصيات الجريمة المعلوماتية إلى أن نفضي إلى تحديد أركانها.

- **أهداف الدراسة :**

و الهدف من دراستنا لهذا الموضوع هو إثراء المكتبة وسد النقص في المراجع المتخصصة في هذا المجال، ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها، غير أنه قد واجهتني بعض الصعوبات في إنجاز البحث، كون أن الموضوع له علاقة بالجانب التقني والفني، وهذا ما يستدعي التخصص للإلمام أكثر بالموضوع.

ومن الأسباب الشخصية التي دفعتني للكتابة في هذا الموضوع، هو أنه مجرد اسمها يكتسي جانب من الغموض خصوصا في إطار مكافحتها، فتجعل العقل يفكر في شكل مسرح الجريمة، وطريقة التفتيش وغيرها من الإجراءات، وهذا ما أعطاني دافع للبحث وحب التعرف عليها باعتبارها متعلقة بالعالم الافتراضي، أما الأسباب الموضوعية تتمثل في كون أن الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش، كما أن الجريمة الإلكترونية تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية، حكومة إلكترونية، وهذا ما يساعد على انتشار هذا النوع من الجرائم، وللإجابة على الإشكالية المطروحة، اعتمدت في ذلك على بعض المناهج الملائمة وطبيعة الموضوع.

- **المنهج المتبع:**

المنهج المتبع هو المنهج الإستقرائي وذلك باستقراء وجمع المادة العلمية من مختلف ثم المنهج التحليلي الوصفي إذ قمت بوصف الظاهرة وبيان المفاهيم القانونية الخاصة بها، وتحليل المفاهيم وشرحها بالتفصيل حيث خصصت الفصل الأول الاحكام الموضوعية لجرائم المساس بالأنظمة المعلوماتية بالتطرق إلى مفهومها من خلال تعريفها والدوافع المؤدية لارتكابها وكذا خصائصها و أنواعها، أما الفصل الثاني عالجت فيه مكافحة الجريمة الإلكترونية في القانون الجزائري من الناحية الموضوعية والإجرائية وكذا المساس بأنظمة المعالجة الآلية للمعطيات.

الفصل الأول:

الاحكام الموضوعية لجرائم المساس بالأنظمة المعلوماتية

الفصل الأول: الاحكام الموضوعية لجرائم المساس بالأنظمة المعلوماتية

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشروع للكمبيوتر كأداة الارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به التي ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها لنذهب بالقول أننا أمام عولمة الجريمة، وإن كان في نطاق تطبيق نصوص القانون الجنائي، إلا أنه يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، سواء من حيث محل الجريمة أو أسباب ارتكابها أوصفات المجرم المعلوماتي فالجريمة هنا جريمة معلوماتية تتعلق بالتقنية المعتمدة على المعالجة الالكترونية للمعلومات والبيانات وقبل الدخول في الحديث عن مختلف الإشكالات التي ثارت في خصوص هذا الموضوع من خلال إخضاعها لقانون العقوبات وبعض القوانين التقليدية والخاصة، سنتعرف من خلال هذا الفصل إلى المفاهيم العامة للجريمة المعلوماتية من خلال مبحثين، نتطرق في المبحث الأول إلى مفهوم جريمة المساس بالنظام المعلوماتي وفي المبحث الثاني سنتطرق الى المساس بأنظمة المعالجة الآلية للمعطيات .

المبحث الأول : مفهوم جريمة المساس بالنظام المعلوماتي

من خلال هذا المبحث سأحاول التعرض إلى التعاريف المختلفة لجرائم الماسة بالأنظمة المعلوماتية

نظرا لطبيعتها الخاصة باعتبارها تقع في العالم الافتراضي، على خلاف الجريمة التقليدية التي تقع في الواقع الملموس، وفي هذا المبحث نتطرق الى مطلبين اساسين اولهم تعريف الجريمة الالكترونية واقسامها اما المطلب الثاني فنعرج فيه عن خصائص الجريمة المعلوماتية

المطلب الأول : تعريف الجريمة الالكترونية واقسامها

تعريف الجريمة المعلوماتية تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلى الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات .

الفرع الأول: تعريف الجريمة الالكترونية :

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة المعلوماتية، فهناك عدة تسميات لها منها الجريمة الالكترونية ،المستحدثة[1]، وتحدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه.

أولا: التعريف الضيق للجريمة المعلوماتية :

يعرف الفقيه الفرنسي(Mass)جريمة الكمبيوتر بأنها :" **الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح**"[2] وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال استخدم لهذا التعريف معيارين هما: الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

كما يعرفه أنصار هذا الاتجاه بان الجريمة الإلكترونية بأنها، "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، لملاحقته و تحقيقه من ناحية أخرى." [3]حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط الارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها. وهذا التعريف يضيق بدرجة كبيرة من الجريمة الإلكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة ، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه.

كما يعرفها الفقيهان الفرنسيان (Vivant) و (Le Stant) بأنها: "المجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب "[4] هذا التعريف مستند على احتمال جدارة الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف قانوني وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

وتبقى هذه التعاريف في وجهة نظر من يرودون تضييق تعاريف الجريمة الالكترونية لإعطائها صبغة بسيطة تخول للمتلقي سهولة فهم معنى الجريمة الواقعة على الحاسب الالي او باستعمال مختلف الوسائل التكنولوجية لما تحتوي عليه هذه الظاهرة المستحدثة من تركيز هام في عالمنا الحديث ويبقى راي الفقهاء و رجال القانون هو

[1] عادل يوسف عبدالنبي الشكري، ملتقى بعنوان: الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة، 2008، ص 112.

[2] ابرهيمي سهام، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2004، 2007، ص7.

[3] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة ص 21

[4] Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude. Lamy informatique.1991.n°3445.p1511.

اهم راي يمكن ان يقارب الصواب في مجمل التعاريف المجملة والذين من خلالهم يتم إعطاء وصف دقيق للجريمة المعلوماتية .

ثانيا: الاتجاه الموسع من تعريف الجريمة الالكترونية

ذهب الفقيهان (Michel و Credo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته[1].

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب[2].

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات، أو بيانات، أو برامج، أو محوها، أوكتابتها، أو أي تدخل آخر في مجال إنجاز البيانات، أو معالجتها، وتبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر.

ودائما حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة[3]. أما البعض من الفقهاء يعرفوها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي و شبكة الأنترنت) بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدفة.

---

[1] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1، كلية الحقوق، 2012، 2011، ص6.

[2] سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث ص01/04

[3] كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب،الطبعة 23/21

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا نكون أمام جريمة إلكترونية، كمن يقوم بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك.

أما بالنسبة للتعريف القانوني للجريمة المعلوماتية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04[1] على أنها: "جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية ."

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبني معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمي الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الألية للمعطيات، كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر 07، وترك المجال واسع لإي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية . ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقي عليه القبض من طرف الشرطة الفيدرالية الأمريكية"[2]

[1] القانون رقم 09-04، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج ر العدد 47

[2] جازية سليماني، موقع العربي الجديد، تاريخ الدخول http//www.alaraby.co.uk/media news 09/02/2017

الفرع الثاني : أقسام الجريمة المعلوماتية :

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية[1]. على خلاف هذه الجريمة ، فإن الجريمة المعلوماتية عرفت اختلاف حول تقسيماتها، وذلك بسبب الإختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الإعتداء وتعدد الحق المعتدى عليه[2]. أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها ، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات

وقبل التطرق الى تقسيمات المشرع الجزائري الى الجريمة الالكترونية ناخذ هذه التقسيمات بصفة عامة قبل دراستها من الجانب الجزائري حيث نعدد منها :

ـ **هجمات الحرمان من الخدمات**: يُرمز لها بالرمز(DDoS) ، وتُنفّذ هذه الهجمات باستخدام مجموعات كبيرة من أجهزة الكمبيوتر يُتحكَّم بها عن بُعد بواسطة أشخاص يستخدمون نطاق ترددي مشترك، وتهدف هذه الهجمات لإغراق الموقع المستهدف بكميّات هائلة من البيانات في آن واحد، ممّا يُسبّب بطئاً وإعاقةً في وصول المستخدمين للموقع.

ـ **التصيد الاحتيالي**: يُعتبر هذا النوع من الجرائم الإلكترونية الأكثر انتشاراً، وهو إرسال جماعي لرسائل تصل عبر البريد الإلكتروني تحتوي على روابط لمواقع أو مرفقات ضارّة، وبمجرّد نقر المستخدم عليها فإنّه قد يبدأ بتحميل برامج ضارة بجهاز الكمبيوتر الخاص به.

ـ **مجموعات الاستغلال**: يعرّف هذا النوع على أنّه استخدام برامج مصمّمة لاستغلال أيّ أخطاء أو ثغرات أمنية في أجهزة الكمبيوتر، ويُمكن الحصول على هذه البرامج من شبكة الإنترنت المظلمة، كما يُمكن للقراصنة اختراق مواقع ويب شرعية واستخدامها للإيقاع بضحاياهم.

ـ **مجموعات الاستغلال**: يعرّف هذا النوع على أنّه استخدام برامج مصمّمة لاستغلال أيّ أخطاء أو ثغرات أمنية في أجهزة الكمبيوتر، ويُمكن الحصول على هذه البرامج من شبكة الإنترنت المظلمة، كما يُمكن للقراصنة اختراق مواقع ويب شرعية واستخدامها للإيقاع بضحاياهم.

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، 2002، ط 01، ص 24

[2] رصاع فتيحة، رسالة الماجستير الحماية الجنائية للمعلومات الالكترونية ،جامعة محمد خيضر ، باتنة 2011

ـ **برامج الفدية:** تمنع هذه البرامج صاحب الجهاز من الوصول إلى ملفّاته المخزّنة على محرّك الأقراص الصلبة، ويشترط المجرم على الضحيّة دفع مبلغ ماليّ كفدية لإتاحة استعادة ملفاته التي يحتاجها.

ـ **القرصنة:** تُعرّف القرنصة على أنّها وصول غير شرعي إلى بيانات ومعلومات موجودة على أجهزة الكمبيوتر أو شبكات الإنترنت من خلال استغلال نقاط ضعف وثغرات في هذه الأنظمة.

ـ **سرقة الهويّة:** يحدث هذا النوع من الجرائم عندما يحصل شخص ما على المعلومات الشخصية لشخص آخر بشكل غير قانونيّ ويستخدمها لأغراض غير شرعية مثل الاحتيال والسرقة

ـ **قرصنة البرمجيات:** تُعرّف قرصنة البرمجيات على أنّها إعادة توزيع واستخدام لبرمجيات دون تصريح من الشركة المالكة للبرمجية، وهناك عدّة أشكال لهذه القرصنة كالآتي: إنتاج برمجيات تجارية مزيّفة واستخدام العلامة التجارية للبرمجية الأصلية، تحميل نسخ غير قانونية من البرمجيات. انتهاك اتفاقيات استخدام البرمجيات التي تحدّ من عدد مستخدمي النسخة الواحدة من البرنامج.

أ/ **الفيروس:** وهو برنامج كمبيوتر أو برنامج مرتبط ببرنامج كمبيوتر آخر يُلحق ضرراً مباشراً بنظام الكمبيوتر، وعند تشغيل هذا البرنامج فإنّه سيؤدي إلى ضرر بنظام التشغيل؛ كحذف ملفّات من النظام أو تعطيلها.
ب /**حصان طروادة:** يُعدّ جزءاً خفيّاً في برمجية الكمبيوتر يسرق معلومات المستخدم المهمّة، حيث إنّه يُمكن أن يُراقب ويسرق المعلومات التعريفية للبريد الإلكتروني أثناء محاولة المستخدم الدخول له عبر متصفّح الويب.

ج /**برمجيات أُخرى:** تتضمّن برمجيات الإعلانات، وبرمجيات التجسس، وبرمجيات خبيثة هجينة تضمّ أكثر من نوع من البرمجيات السابقة في الوقت ذاته[1]

أما في نظر التشريع الجزائري فهناك رؤية دقيقة للموضوع ملمة بجميع الجوانب وبناء عليه تم تقسيم الجريمة الالكترونية الى :

أولا ـ الجريمة المعلوماتية المرتكبة باستخدام النظام المعلوماتي:

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار، وسأوضح كل نوع منها في البنود الأتية.

1)ـ الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية:

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

[1] ايمان الحياري ، جرائم معطيات الانظمة المعلوماتية ، منشورات الحاتي الحقوقية 4 ابريل 2022 ،ص 44

أ_ الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية:

يكون النظام المعلوماتي وسيلة للإعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الإختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 0305 الصادر في 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الإختراع[1].

ب_ الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة:

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص أخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني .

2)_ الجريمة الإلكترونية الواقعة على النظم المعلوماتية الأخرى:

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية. بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الإستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة أو استخدام شاشة النظام، أو الإطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الإئتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الإئتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة إئتمانية إنتهت مدة صلاحيتها أو تم إلغاؤها أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة إئتمانية للحصول على السلع والخدمات [2].

[1] سوير سفيان ، جرائم المعلوماتية ، مذكرة لنيل شهادة ماجستير في القانون تخصص علم الاجرام ، جامعة تلمسان ، ص 34-35

[2] سوير سفيان ، جرائم المعلوماتية ، المرجع نفسه، ص 38 .

3/ الجريمة الإلكترونية الواقعة على الأسرار

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[1]، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية .

4/ جريمة المساس بمنظومة معلوماتية.

نصت المادة 394 مكرر 01 من قانون العقوبات رقم

04/15

بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل،

كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها. البند الثالث: أفعال إجرامية أخرى.

جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الأتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر .

[1] سوير سفيان ، مرجع سابق الذكر، ص 54.

المطلب الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه، وهي الآن فيما يعرف بالأنترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية، ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

وسوف نحاول فيما يلي التطرق إلى:

_ بعض السمات الخاصة بالجريمة المعلوماتية والمجرم المعلوماتي ثم سنتناول بالدراسة الدوافع التي أدت به إلى ارتكاب هذه الجرائم[1].

_ خصائص الجريمة المعلوماتية. تتميز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية ببعض السمات الخصائص والتي نوجزها فيما يلي:

الفرع الاول: السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أولا_ خصوصية الجريمة المعلوماتية:

تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى عدة أسباب من بينها:

وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.

فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و18900 جريمة تندرج تحت وصف جرائم الآداب و3 مليون جريمة ضد الأموال، وفي أحدث تقارير مركز شكاوى احتيال الانترنت الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكوى من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الانترنت و814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو

[1] قربوز حليمة ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة تخرج لنيل اجازة المدرسة العليا للقضاء الجزائر 2009 ص 28

الدخول المباشر إلى النظام بشكل مادي مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي[1].

وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية، ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم التقليدية، ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال كانت الخسارة الناجمة عن 8000 حالة سرقة بالإكراه في فرنسا عام 1986 حوالي 561 مليون فرنك الفرنسي، في حين يتضاعف

هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها نسبة 8 مرات عن حالات السرقة بالإكراه.

وفي المقابل فانه، وعلى غرار الآراء التي تتجه إلى القول بأن الجريمة المعلوماتية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها، أو أنه لا يوجد شعور عام بعدم أخلاقية هذه الأفعال، فإنه من الفقهاء من لا يتفقون مع هذه الآراء إذ أن الجريمة المعلوماتية لا تختلف عن غيرها من الجرائم من حيث اعتدائها على مصالح لها أهميتها لدى أفراد المجتمع، ومن ثم تستحق الحماية القانونية كون أن مساس هذه الأفعال بهذه المصالح هو الذي يبرر تجريمها.

ثانيا_ دولية الجريمة المعلوماتية:

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[2].

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي توجد بها المعلومات محل الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[3].

---

[1] نائلة عادل محمد فريد قورة – جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية – منشورات الحاتي الحقوقية 2005، ص 49

[2] نائلة عادل محمد فريد قورة المرجع السابق ص50

[3] لمرجع نفسه، ص 54.

ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "إبرام الاتفاقيات الدولية".

تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق مبدأ ازدواجية التجريم" فيما يتعلق بجرائم المعلوماتية.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. و إن كان المشرع قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون04/15 المعدل والمتمم للأمر66/156.

المتضمن قانون العقوبات. والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين:

المحور الأول: داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

المحور الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرموا المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

الفرع الثاني _ تصنيفات الجريمة الالكترونية:

1)– أنها ترتكب من مجرم غير تقليدي:

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات لا يوجد لها مثيل لدى غيره، كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنده أيضا، فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي ، أي انه متوافق مع مجتمعه و غالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين،

كما أن هذا المجرم إنسان ذكي، إذ أنه يستغل ذكاءه في تنفيذ جريمته، ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا، ويفسر هذا أن هذا المجرم من ذوي المستويات العلمية العالية وما يميز مجرم المعطيات أيضا هي الدوافع التي تدفعه لارتكاب الجريمة، فهي متعددة

ومختلفة فقد تكون السعي لتحقيق الربح وقد تكون الرغبة في الانتقام من رب العمل وقد تكون الرغبة في قهر النظام والتفوق علي وسائل التقنية وتعقيدها . وقد يرتبط الدافع بحب التعلم والاستكشاف، كما قد يرتبط بالسياسة والأيديولوجيا .. إلى غير ذلك من البواعث.

كما يتميز مجرم المعطيات أيضا بفئاته وأنماطه المختلفة وهو ينقسم إلى نوعين رئيسيين: الأول هم الهواة المولعون بالمعلوماتية، والثاني هم محترفو الجرائم المعلوماتية وأساس التمييز بين النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة، بينما هو ساذج لدى النوع الأول لا يتعدى الرغبة في الاستطلاع والاستكشاف، فهو خبيث لدى النوع الثاني، والذي قد يكون ماليا أو سياسيا أو غيره[1]

2)_ صعوبة اكتشاف واثبات الجرائم الإلكترونية:

من المفترض أن اكتشاف هذه الجرائم يتم عن طريق الفحص والتدقيق أو عن طريق الشكاوي التي يقدمها المجني عليهم، والوضع بخصوص جرائم المعطيات بالغ التعقيد في الأمرين معا.

فجهات التحقيق لم تصل إلى تلك المعرفة أو الخبرة التي تملكها حيال التحقيق في الجرائم التقليدية، لأن الأمر يتطلب معرفة واسعة وإحاطة كاملة بهذه التكنولوجيا الحديثة، وتحديث هذه المعارف يوميا، هذا من جهة، ومن جهة أخرى فالضحية في هذه الجرائم تمتنع، في الغالب عن التبليغ عنها وقد يسعى إلى التعتيم على المحققين وتضليلهم حتى لا يكتشفوا هذه الجرائم.

ويفترض إثبات هذه الجرائم الكثير من الصعوبات، فطبيعة هذه الجرائم غير مرئية في الغالب لأنها تتعلق بمعطيات في شكل نبضات أو نبذبات الكترونية، ويسهل على الجاني محو الأدلة المتعلقة بها وتدميرها في وقت وجيز، فضلا عن العقبات التي تشكلها طبيعة هذه الجرائم العابرة للحدود.

لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة وهناك من يشير

إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته 01 % فقط وما تم الإبلاغ عنه إلى السلطات المختصة لم يتعد 15 % من النسبة السابقة، وحتى ما طرح أمام القضاء من هذه الجرائم فان أدلة الإدانة فيه لم تكن كافية إلا في حدود الخمس1/5[2]

3)_ لجرائم الالكترونية للضحية دور مهم فيها:

[1] د. عبد الله حسن محمود ، سرقة المعلومات المخزنة في الحاسب الالي ، دار النهضة العربية ، القاهرة 1998 ص30

[2] نائلة عادل مرجع ، سابق الذكر ص 69

كالمجرم في جرائم المعطيات، فان للضحية أيضا ما يميزها في هذه الجرائم، ذلك أنها تلعب دورا لا يستهان به في أغلبها، هذا الدور قد لا تلعبه الضحية بإرادتها، كما هو الحال عندما تكون شخصيتها غير متجلية أمام الجاني، وذلك عندما لا يرى هذا الأخير أمامه إلا الحاسبات وما تحويه أنظمتها من معطيات دون أن يدرك قيمتها وما قد تمثله في الواقع وكذلك الأمر عندما تلعب العلاقة بين الضحية والجاني دورها في حدوث الجريمة وذلك إذا كان الجاني يعمل لحساب الضحية، لاسيما إذا كان عارفا بخبايا أنظمة الحاسبات والثغرات الأمنية فيها، أو كان مؤتمنا علي ذلك، كأن يكون هو المسؤول عن المركز المعلوماتي فيستغل مركز الثقة الذي يحوزه والألفة التي بينه وبين هذه الأنظمة وذلك ما حدث في إحدى القضايا أن كان الجاني يعمل مستشارا لدى أحد البنوك الكبرى وكان يتمتع بثقة مطلقة[1] .

4)_ الجرائم الالكترونية ناعمة مغرية للمجرمين

إذا كانت بعض الجرائم التقليدية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها فان جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل من علي وسائل الإدخال وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته قد لا ترى بالعين. ونعومة هذه الجريمة وما تدره من أرباح ومن إشباع للفضول عند البعض جعلها من الجرائم المغرية والجذابة للمجرمين

5)_ الجرائم الالكترونية جرائم عابرة للحدود

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحاسبات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان في دولة معينة علي مجني عليه في دولة أخرى في وقت يسير جدا[2].

مكبدة أفدح الخسائر لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت، خاصة في مجال التجارة الإلكترونية.

[1] اسامة احمد المناعسة ، جلال محمد زغبي ، جرائم الحاسب الالي و الانترنت ، دراسة تحليلية مقارنة ، دار وائل للنشر ، عمان الاردن الطبعة الوالى ، 2001 ص 47

[2] محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري ،دار الجامعة الجديدة ، الاسكندرية ،2007 ص159

المبحث الثاني : : المساس بأنظمة المعالجة الآلية للمعطيات

لقد أصبح الاستخدام المتزايد وغير المشروع لتكنولوجيات المعلومات ظاهرة واسعة الانتشار، وهو أمر يقتضي وضع قواعد جزائية لمواجهة هذا النمط المستحدث من النشاط الإجرامي، وتأسيسا على ذلك سن المشرع الجزائري من خلال المنظومة التشريعية قانوني الأول رقم 04-15 المؤرخ في 10 نوفمبر 2004، الذي يجرم من خلاله المساس بأنظمة المعالجة الآلية للمعطيات، والثاني رقم 09-04 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لمواجهة الجريمة المعلوماتية بكافة صورها وأشكالها وذلك من خلال تجريم كل أنواع الاعتداءات التي تستهدف مباشرة أنظمة المعالجة الآلية.

المطلب الاول : مفهوم نظام المعالجة الآلية للمعطيات

نظام المعالجة الآلية للمعطيات عبارة عن مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة [1] وهو تعريف يتفق إلى حد ما بالتعريف الذي جاء به مجلس الأمة الفرنسي سنة 1987 بنصه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط التي يربط بينها مجموعة من العلامات التي تتم عن طريقها تحقيق نتيجة معينة وهي معالجة المعلومات على أن يكون هذا المركب خاضع لنظام المعالجة الفنية".

فهذا التعريف يرتكز على عنصريين أساسيين هما العنصر الأول وهو العنصر المادي والعنصر الثاني وهو العنصر المعنوي، وهما أساس نظام المعالجة الآلية للمعطيات[2]

فنظام المعلومات عبارة عن جهاز يتكون من معدات وبرامج قائمة للمعالجة الآلية للمعطيات الرقمية، وتعتبر معالجة البيانات مجموعة عمليات تطبق على بيانات يتم تسجيلها عن طريق تنفيذ برنامج للمعلوماتية، كما تعتبر معالجة البيانات مجموعة تعليمات يمكن أن يتم تنفيذها عبر الحاسوب للحصول على نتيجة معينة، ويمكن للحاسوب تنفيذ عدة برامج، وفي نظام المعلومات هناك عدة مركبات، بمعنى وحدة المعالجة أو وحدة المعالجة المركزية والمحيط الخارجي، ويعني ذلك أن للحاسوب عدة وظائف معينة يتعامل مع الوحدة المركزية مثل الطباعة والة النسخ والشاشة.[3]

[1] عبد الفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة الالكترونية ، علم المعارف الاسكندرية ،الطبعة الاولى سنة 2009 ، ص 65

[2] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيات الاتصالات الحديثة، دار النهضة العربية ، القاهرة، الطبعة الأولى، سنة 2009، ص277

[3] نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، مذكرة لنيل شهادة الماجستير، جامعة الجزائر 1، سنة 2017، ص28

وعليه فإن نظام المعالجة الآلية للمعطيات عبارة عن تعبير فني تقني، فضلا عن أنه تعبير متطور يخضع للتطورات السريعة في مجال فن الحسابات الآلية، مما صعب على المشرع الجزائري تعريفه، وإنما اكتفى بالنص في قانون العقوبات على المساس .

إلا أن اعتبار أنظمة المعالجة الآلية للمعطيات من قبيل الأموال وإضفاءها نفس المعاملة أثار عدة تساؤلات فظهر اتجاهين، الأول يتمثل في الاتجاه التقليدي الذي يرفض إدراج المعلومات ضمن القيم المالية، والثاني يتمثل في الاتجاه الحديث الذي يدرج المعلومات ضمن القيم المالية.

أولا : الاتجاه التقليدي

يرى هذا الاتجاه أن للمعلومة طبيعة من نوع خاص وبالتالي لا يمكن إدراجها ضمن القيم المالية، ويعلل رأيه بأن الأشياء التي توصف بالقيم هي الأشياء القابلة للاستئثار والحيازة، فالمعلومة ليست لها قيمة مادية وإنما لها طبيعة معنوية، وبالتالي لا تدخل في مجموعة القيم المحمية إلا إذا كانت تحت المواد الأدبية التي تحميها الأنظمة القانونية الخاصة بالحقوق الملكية الأدبية والفنية[1].

ثانيا : الاتجاه الحديث

يذهب هذا الاتجاه إلى إعطاء المعلومة وصفا ذات قيمة، وتبني جانب من الفقه الفرنسي هذا الاتجاه، وفي مقدمته الفقيه pierre catala[2]

فاعتبر هذا الفقيه أن المعلومة في ذاتها تعد قيمة مالية ، وقد شبهها بالسلعة، فهي من إنتاج العمل الإنساني تنتمي إلى من يكسب العناصر الأساسية المكونة لها بالطرق الشرعية، ثم يضعها في المنظومة لتكون صالحة للإطلاع عليها وإرسالها وتبليغها بشكل واضح، فبتوفر هذين الشرطين تصبح المعلومة لها قيمة التملك، وقد اعتمد الفقيه catala على حجتين لتبرير رأيه وإعطاء وصف القيمة على المعلومة وهي: |

– القيمة الاقتصادية التي تمتاز بها المعلومات، حتى تقوم بقيمة نقدية في السوق.

– علاقة الارتباط والتبعية التي تربط المعلومات بالمؤلفة.

نستنتج من كل ما سبق، وحسب الاتجاه الراجح أن للمعلومة قيمة قائمة بذاتها وعليه فهي تخضع للقواعد القانونية الخاصة بحقوق الملكية الأدبية والفنية.

هذا، وباعتبار المساس بأنظمة المعالجة الآلية للمعطيات جزء من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 14، فقد عرف المشرع في القانون رقم 09-04:

[1] ن المساس بأنظمة المعالجة الآلية للمعطيات جاءت في الفصل الثالث المعنون "الجنايات والجنح ضد الأموال"، من القسم الأول المعنون "السرقات وابتزاز الأموال"

[2] فقيه فرنسي تبني هذا الاتجاه الحديث.

المنظومة المعلوماتية بأنها :" أ نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا البرنامج معين.

الفرع الاول : تعريفه في الاتفاقية الدولية للإجرام المعلوماتي

التعاريف على ضوء الاتفاقيات الدولية يعرف خبراء منظمة التعاون الاقتصادي والتنمية نظام المعالجة الآلية للمعطيات بأنه ":كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها [1]."ويتبنى هذا التعريف الفقيه الألماني (Ulrich siehr) يعتمد هذا التعريف على معيارين هما: وصف السلوك، واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

عرف نظام المعالجة الآلية للمعطيات خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية (OECD) [2] 'بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف نظام المعالجة الآلية للمعطيات على النحو التالي: يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك ويقوم إحداهما أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات ويقصد بيانات الكمبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين نظام المعالجة الآلية للمعطيات بأنه: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[3].

عرفت اتفاقية بودابست في المادة الأولى منها بعنوان تعريف خاص بأغراض هذه الاتفاقية منظومة معلوماتية ومعطيات معلوماتية:

1)_ منظومة معلوماتية: "أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها أو ذات صلة بذلك ويقوم أحدها أو أكثر من واحد منها تتبعا للبرنامج بعمل معالج آلية للمعطيات"

2)_ معطيات معلوماتية:

[1] موقع منظمة التعاون الاقتصادي والتنمية ، WWW.0ecd.org

[2] Organisations Economique de commerce et développement

[3] عقد هذا المؤتمر في فيينا في الفترة ما بين (10-17) افريل 2000.

أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل معين جاهز لعملية المعالجة داخل منظومة معلوماتية بما في ذلك البرامج الماسة لجعل منظومة معلوماتية تطبق وظيفة"[1]

يذهب البعض إلى أنة عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها:

1- أن يكون هذا التعريف مقبول و مفهوم على المستوى العالمي.
2- 2- أن يراعي هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.
3- 3- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الاجرامى
4- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية[2]

الفرع الثاني : تعريفه في التشريع الجزائي الجزائري

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريميه لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 04/15 المؤرخ في 2004.11.10 المتضمن تعديل قانون العقوبات[3]، ولكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي وسنبين بصفة موجزة الأفعال التي جرمها المشرع الجزائري بموجب القانون السالف الذكر

1)_جريمة التوصل أو الدخول غير المصرح به:

نصت عليه المادة 394 مكرر من قانون العقوبات بقولها "يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة .فقد أورد المشرع ظرفي تشديد العقوبة الدخول غير المشروع وهما: في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة. وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله "أو يحاول ذلك".[4]

[1] الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ 2001/11/08

[2] أمير فرج يوسف، الجرائم المعلوماتية، ص58

[3] لقانون 04/15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات

[4] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، ص 99

2)_جريمة التزوير المعلوماتي :

نص عليها المشرع في نص المادة 394 مكرر 1 بقوله "يعاقب بالحبس وبالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."[1]

3)_ جريمة الاستيلاء على المعطيات:

نصت عليها المادة 394 مكرر 2 بقولها "كل من يقوم عمدا و بطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

4)_ جريمة إتلاف وتدمير المعطيات :

نص عليها المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات "يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها . وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات.

[1] تنص المادة 394 مكرر2 من قانون العقوبات: "يعاقب بالحبس والغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

– تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم

المبحث الثالث : جرائم المساس بأنظمة المعالجة الآلية للمعطيات

يتم تناقل المعلومات، المعطيات خلال أنظمة معالجة آلية، هاته العمليات تم إخضاعها الحماية قانونية، ضد كل فعل غير مشروع قد يقع عليها، فأصبحت تتمتع بحماية جزائية منصوص عليها قانونا.

هاته الحماية هي ضد كل اعتداء يمكن أن يمس بنظام معالجة آلية للمعطيات، و يمكن أن تكون هذه الاعتداءات إما دخول أو بقاء غير مصرح به، أو تلاعب بمعطيات الحاسب الآلي أو يمكن أن تكون تعامل في معطيات غير مشروعة، و عليه سنتناول في هذا المبحث جميع صور المساس بأنظمة المعالجة الآلية للمعطيات، و المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

المطلب الاول :جريمة الدخول و البقاء غير المصرح به

يعد الاعتداء على نظام المعالجة الآلية للمعطيات عن طريق الدخول أو البقاء غير المصرح به، أول صور من صور المساس بأنظمة المعالجة قد نص عليها المشرع الجزائري في قانون العقوبات من خلال نص المادة 349 مكرر، في الفقرة الأولى منها.

و سيتم تناول هاته الجريمة في ثلاث فروع، الأول بعنوان : الركن الشرعي، و الثاني بعنوان : الركن المادي و الثالث بعنوان: الركن المعنوي .

الفرع الاول : الركن الشرعي (جريمة الدخول و البقاء معا)

لقد عرف الفقيه خالد ممدوح إبراهيم نظام المعالجة الآلية للمعطيات كالآتي" :مجموعة من العناصر المتداخلة و المتفاعلة مع بعضها البعض و التي تعمل على جمع البيانات و المعلومات و معالجتها و تخزينها و بثها و توزيعها بغرض دعم صناعة القرارات و التنسيق و تأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة"[1]، كما عرفه مجلس الشيوخ الفرنسي على انه " :نظام المعالجة الآلية للمعطيات هو كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، و التي تكون كل منها الذاكرة، المعطيات، أجهزة الإدخال والإخراج، أجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نسخة معينة و هي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية[2]

فنظام المعالجة الآلية للمعطيات هو الشرط الأول الذي يجب توافره قبل الانتقال للتحقق من وجود اعتداء عليه أولا، و فيما يخص الدخول و البقاء غير المصرح به في هذا النظام، فإنه جريمة يعاقب عليها المشرع الجزائري، بموجب نص المادة 394 مكرر من خلال العبارة الآتية: "يعاقب بالحبس .... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، فتعد هاته الجريمة أبسط

[1] خالد ممدوح إبراهيم، "التقاضي الإلكتروني"، دار الفكر الجامعي، الإسكندرية، 2009، ص 298

[2] محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري ، دار الجامعة الجديدة ، الاسكندرية ،2007 ص 26

صور جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فبمجرد القيام بفعل "دخول" أو "بقاء" في نظام معلوماتي، بطريقة احتيالية، أي عن طريق الغش، تقوم جريمة الدخول أو البقاء غير المصرح.

أما الاتجاه الثاني فيذهب إلى ضرورة تجريم الدخول و البقاء غير المصرح بهما إلى النظام المعلوماتي، حتى و لو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد فالاتجاه الثاني يرى أن فعلي الدخول والبقاء غير المصرح بهما، لهما تبعات مادية تتمثل في خسائر متعددة، حيث تشير التقديرات إلى أن هناك الآن ما يزيد عن 100 ألف خبير استشاري في المجال المعلوماتي يعملون في أكثر من 20 ألف شركة في العالم و بلغ مجموع ما أنفقته الشركات على خدمات الاستشارة المعلوماتية

4.5 مليون دولار، و كل ذلك من أجل ضمان أمن المبادلات الالكترونية[1].

و يعاقب المشرع الفرنسي على جريمة الدخول و البقاء غير المصرح به، أو كما تسمى أيضا بجريمة الدخول الاحتيالي في الأنظمة المعلوماتية، بموجب نص المادة 323-1 الفقرة الأولى في إطار الفصل الثالث بعنوان "الاعتداء على أنظمة المعالجة الآلية للمعطيات" وجاء نص المادة كما يلي:

Le fait d'accéder ou de se maintenir, 323-1 :

« Article frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60000 € d'amende »

أن المشرع الفرنسي يعاقب بالحبس لمدة عامين و بغرامة قدرها 60000 أورو، كل من يدخل أو يبقى عن طريق الاحتيال في كل أو جزء من نظام المعالجة الآلية للمعطيات، فنلاحظ عدم وجود اختلاف مع ما هو منصوص عليه في التشريع الجزائري الا فيما يخص العقوبة تنص

المادة 02 من اتفاقية بودابست على ما يلي: "..... **عند ارتكابها عن قصد، و ذلك من حيث الدخول على منظومة الكمبيوتر كليا أو على أي جزء منها دون وجه حق، و قد يلزم على الدولة الطرف...**"[2] ، كما تنص المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في فقرتها الأولى على ما يلي: " **الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به**"[3]، فنلاحظ أن كلا الاتفاقيتين قد جرمت فعل الدخول غير المشروع إلى أي نظام معلوماتي، إلا أن اتفاقية بودابست لم تنص على فعل البقاء.

[1] محمود أحمد عبابنة، "جرائم الحاسوب و أبعادها الدولية"، دار الثقافة للنشر و التوزيع، عمان، 2005، ص 81

[2] المادة 323-1، القانون رقم 88-19.

[3] لمادة 06، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

الفرع الثاني : الركن المادي

اولا: الدخول غير المصرح به

تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي، و مدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي و الإحاطة أو السيطرة على المعطيات والمعلومات التي يتكون منها، و فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية و التقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الالكتروني، و يتساوى في هذا المجال إن تم هذا الدخول بطريق مباشر إلى المعلومات أو تم عن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي[1]

و فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، و إنما يتخذ هذا الفعل وصفه الجرمي انطلاقا من كونه قد تم دون وجه حق، أو بمعنى آخر دون تصريح، و من الحالات التي يكون فيها الدخول غير مصرح به إلى النظام المعلوماتي :

دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسؤول عن النظام أو مالكه، و قد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام، إلا أنه يتجاوز التصريح الممنوح له و يدخل إلى كامل النظام أو إلى أجزاء أخرى يحظر عليه الدخول اليها، و هذا الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي، كما أن عدم التصريح بالدخول ينصرف إلى الحالات التي يكون فيها هذا الدخول مشروطا بدفع ثمن محدد، و بالرغم من ذلك يدخل الفاعل إلى النظام دون أن يقوم بتسديد هذا الثمن، أما إذا كان الولوج إلى النظام المعلوماتي بالمجان و كان متاحا للجمهور، ففي هذه الحالة يكون الدخول إليه حق من الحقوق [2].

لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، و لذلك تقع الجريمة بأية وسيلة أو طريقة، فقد يلجأ الجاني إلى التلاعب بعناصر النظام المادية لكي يصل إلى هدفه و هو الدخول، أو يربطه بجهاز تنصت يستطيع من خلاله اختراق النظام أو استقبال المعلومات، كما قد يكون عن طريق برنامج فيروس، مثل فيروس حصان طروادة "Trojan Horse"، أو عن طريق استخدام الرقم الكودي لشخص آخر، أو الدخول من خلال شخص آخر مسموح له بالدخول، أو عن طريق الوصول إلى الرقم الكودي للدخول، أو عن طريق تجاوز نظام الحماية خاصة إذا كان ضعيفا في حالة وجود مثل هذا النظام، و يستوي أن

[1] نهلا عبد القادر، الجرائم المعلوماتية ، دارالثقافة للنشر ، عمان 2008 ، دار النهضة العربية القاهرة

[2] نهلا عبد القادر المومني، المرجع السابق، ص 159

يكون الدخول مباشرة أو بطريق غير مباشر، كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصال التلفزيونية [1]

باختصار، يمكن أن يحصل الدخول دون إذن باختراق النظام المعلوماتي عن طريق الحصول على شفرات خاصة، أو استخدام فيروس يتم دمجه في إحدى البرامج الأصلية للحاسب الآلي كي يعمل كجزء منه، ثم يقوم بتسجيل الشفرات التي يستعملها المستخدمون الشرعيون للدخول إلى الكمبيوتر.

إذن فيما يخص الركن المادي للجريمة: فهو الدخول سواء كان مادي أو معنوي أو بأي طريقة كانت إلى النظام المعلوماتي في جزء منه أو كله و دون أي حق أو ترخيصه، و كما ذكرنا سابقا، فالدخول يعني كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي و يتحقق بالوصول إلى المعلومات و البيانات المخزنة داخل نظام معين دون رضا المسؤول عنه من شخص غير مرخص له باستخدامه[2].

ثانيا: البقاء غير المصرح به:

و هو الفعل الثاني المنصوص عليه في المادة 394 مكرر من قانون العقوبات الجزائري، و يقصد به التواجد في نظام المعالجة الآلية للمعطيات، ضد إرادة صاحب ذلك النظام أو من له سيطرة عليه، فقد يجد شخص نفسه داخل نظام الحاسب آلي عن طريق الخطأ، كما لو كان في طريق للدخول إلى نظام له الحق في الدخول إليه ثم وجد نفسه بسبب خطأ ما كاستخدام شفرة خاطئة على سبيل المثال داخل نظام آخر، و في هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه للخطأ الذي وقع فيه، و قد يستمر في البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مصرح له بالدخول إليه[3].

يتضح الهدف من تجريم البقاء بالنسبة للجاني الذي لم يقصد الدخول عن طريق الغش للنظام، و مع ذلك يبقى داخل النظام و تنصرف إرادته إلى ذلك و الذي كان يمكن أن يغادر النظام.

قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام، وقد يجتمعا، و يكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، و من أمثلة ذلك، إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غبر المشروع إذا توافر لها الركن المعنوي.

و يكون البقاء جريمة أيضا في الحالة التي يستمر فيها الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الرؤية أو الإطلاع فقط، و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التليفونية، و التي

[1] علي عبد القادر القهوجي، "الحماية الجنائية لبرامج الحاسب الآلي"، (بط)، الدار الجامعية، بيروت، 1999، ص 199

[2] خالد ممدوح إبراهيم، "أمن المستندات الالكترونية"،)دط)، الدار الجامعية، الإسكندرية، 2008، ص48

[3] محمد عبيد الكعيبي، "الحماية الجنائية للتجارة الالكترونية، (دط)، دار النهضة العربية، القاهرة، 2010، ص459

يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه، أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة.

قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا، و ذلك في الغرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام و يدخل إليه فعلا، ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا الغرض الاجتماع المادي للجرائم بين الجريمتين و لكن في هذا الغرض تثور مشكلة، "متى تنتهي جريمة الدخول، و متى تبدأ جريمة البقاء؟".

ذهب رأي في الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول فعلا إلى البرنامج، و إن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي عنها جريمة الدخول و تكتمل، و بعد تلك اللحظة تبدأ جريمة البقاء داخل النظام و تنتهي بانتهاء حالة البقاء، و يؤخذ على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة، و لهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، و أخذ على هذا الرأي أيضا صعوبة إثبات علم المتدخل[1].

و لذلك ذهب رأي ثالث إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع او أصبح غير مشروع، فإذا لم ينسحب فإنه يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام، و هذا الرأي و إن كان له وجاهته إلا أنه يفترض وجود جهاز إنذار يقوم بهذه المهمة، و هو إن أمكن توفيره فنيا فإنه لن يكون متاحا إلا للشركات أو المؤسسات الكبيرة فقط.

و لذلك نعتقد أن الرأي الصائب في مثل هذه الظروف، هو الذي يعتبر أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، لأن الغرض يتعلق بدخول غير مشروع، أي مع علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكنا، تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ منذ تلك اللحظة، لأنه يتجول في نظام يعلم مسبقا أن مبدأ الدخول فيه غير مشروع، أو أن مبدأ الاستمرار فيه غير مشروع، و منذ تلك اللحظة، تبدأ جريمة البقاء داخل النظام[2]

[1] عبد القادر القهوجي، المرجع السابق، ص131

[2] عبد القادر القهوجي، المرجع السابق، ص134

الفرع الثالث : الركن المعنوي

جريمة الدخول أو البقاء داخل النظام، جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي، و القصد الجنائي يتكون من علم وإرادة، فيلزم لكي يتوافر الركن المعنوي أن تتجه إرادة ، لجاني إلى فعل الدخول أو البقاء، و أن يعلم الجاني أنه ليس له الحق في الدخول إلى النظام أو البقاء فيه [1]

أولا)_ القصد العام :

تطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما يتطلبه القانون من وقائع لبناء أركان الجريمة، واستكمال عناصرها يتعين أن يشمله علم الجاني، و لكن علم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، و إنما يتعين أن يحيط أيضا بالتكييف الذي تتصف به بعض هذه الوقائع، و تكتسب به أهميتها في نظر القانون، حيث إن عددا من الوقائع التي تقوم بها الجريمة لا يمثل أهمية في نظر القانون إلا إذا اكتسب وصفا معينا، فإن تجرد من هذا الوصف، فقد تجرد من الأهمية القانونية و لم يعد صالحا لتقوم به الجريمة.

و بتطبيق هذه المبادئ العامة على الدخول غير المصرح به إلى نظام الحاسب الآلي، ينبغي أولا أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية تدخل في تكوين هذه الجريمة، فلكي يتوافر القصد الجنائي إذن يجب أن تحيط علم الجاني بعناصر الركن المادي للجريمة، و لعل أول عناصر هاته الجريمة هو موضوع الحق المعتدى عليه (المنصب على نظام الحاسب الآلي لما يتضمنه من معلومات و برامج)، و كما يجب أن يتجه علم الجاني إلى موضوع الحق الذي يناله الاعتداء بارتكاب الجريمة، فإنه يتعين أيضا أن يعلم بخطورة الفعل الذي يقوم به على الحق المعتدى عليه، كما يتطلب القصد الجنائي أيضا أن يتوقع الجاني النتيجة الإجرامية المترتبة على الفعل، و هي الدخول غير المصرح به إلى النظام، و النتيجة التي يجب أن يتوقعها الجاني هي النتيجة بعناصرها التي يحددها القانون، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول[2]

ثانيا)_ القصد الخاص :

هناك بعض النصوص الخاصة ببعض التشريعات المجرمة لفعل الدخول غير المصرح به، تتطلب قصدا خاصا إلى جانب القصد العام، كالقانون الدنماركي الذي يشدد العقوبة متى ارتكب فعل الدخول، بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، و أستراليا، التي تشدد العقوبة لكل من يقوم بفعل الدخول غير المصرح به إلى نظام معلوماتي بنية الإضرار بالغير.[3]

---

[1] عبد القادر القهوجي، المرجع السابق، ص136

[2] نائلة عادل محمد فريد قورة، "جرائم الحاسب الآلي الاقتصادية – دراسة نظرية و تطبيقية –، ط1، منشورات الحلبي الحقوقية، عمان، 2005، ص 365

[3] المرجع نفسه ص 369

كل ما سبق ذكره ينطبق على فعل البقاء غير المصرح به في النظام المعلوماتي، و فيما يخص التشريع الجزائري، ففعلي الدخول و البقاء غير المصرح بهما، يتطلبان نتيجة لا تدخل في عناصر الركن المادي، و التالي فجريمة الدخول و البقاء غير المصرح به هي جريمة قصد عام.

المطلب الثاني : جريمة التلاعب بمعطيات الحاسب الالي

يطلق عليها أيضا اسم "جريمة المساس العمدي للمعطيات"، وهي الجريمة المنصوص عليها في المادة 394 مكرر من قانون العقوبات، و تتمثل هاته الجريمة في القيام بجملة من الأفعال التي تعتبر اعتداءات عمدية على المعطيات، و تتم هذه الاعتداءات باستعمال جملة من الوسائل، و هذا ما سنبينه في هذا المطلب من خلال تقسيمه إلى الفروع التالية: الفرع الأول (الركن الشرعي)، الفرع الثاني (الركن المادي)، الفرع الثالث (الركن المادي)

الفرع الاول : الركن الشرعي

تنص المادة 394 مكرر 1 من قانون العقوبات الجزائري على ما يلي: " يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من500.000 دج إلى 2.000.000 دج

كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش، المعطيات التي يتضمنها "2 ، فنلاحظ أن المشرع الجزائري قد جرم فعل التلاعب بمعطيات الحاسب الآلي، سواء كان ذلك عن طريق الإدخال، التعديل أو الإزالة، و التي يترتب عنها تغيير في حالة المعطيات

أما بالنسبة لاتفاقية بودابست الخاصة بالإجرام المعلوماتي، فقد نصت على جريمة التلاعب بمعطيات الحاسب الآلي في نصوص المواد 04، 08 كالاتي وعلى التوالي: المادة 04 ....." :وذلك من حيث إتلاف، أو إلغاء، أو إفساد أو تغيير أو تدمير البيانات الموجودة بالكمبيوتر دون وجه حق "..... ، المادة 08 ..... " :و ذلك من حيث إحداث خسائر بممتلكات الغير عن طريق:

أ- أية عمليات إدخال برامج تشغيل على الكمبيوتر أو تزويده بمعلومات أو بيانات، أو تبديلها أو تغييرها، أو إلغائها أو تدميرها.

ب- أي نوع من التدخل في طبيعة عمل منظومة الكمبيوتر، بقصد يشوبه التدليس و عدم الأمانة أو بقصد غير شريف للحصول بدون وجه حق على منفعة أو فائدة الكترونية[1]

[1] المادة 08 من اتفاقية بودابست الخاصة بالاجرام الالكتروني 2001

الفرع الثاني : الركن المادي

تقوم جريمة التلاعب بمعطيات الحاسب الآلي المنصوص

عليها في المادة 394 مكرر 01 من قانون العقوبات الجزائري، بإتيان إحدى السلوكات الثلاث الآتية:
الإدخال، التعديل أو الإزالة، و سيتم شرح كل سلوك على حدى فيما يأتي

اولا)_ الادخال :

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت خيالية أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي البطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول، لكي يسحب مبلغا من النقود أكبر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة الائتمان و التي سدد عن طريقها مبلغا اللتاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له، و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان، سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير[1]

ثانيا)_ الازالة / المحو

يقصد بفعل المحو، إزالة جزء من المعطيات المسجلة على دعامة و الموجود داخل النظام أو تحطيم تلك الدعامة، أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة[2]

ثالثا)_ التعديل :

يقصد بفعل التعديل تغير المعطيات الموجودة داخل نظام، و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل، عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات، أو برامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال ، المحو، والتعديل، وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غيرها، حتى لو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات، فلا يخضع لتلك الجريمة فعل نقل البيانات أو التنسيق أو التقريب بينها، لأن كل تلك الأفعال لا تنطوي على إدخال ولا تعديل بالمعنى السابق. ما تجدر الإشارة إليه، أنه لا يشترط اجتماع هذه الصور الثلاث: الإدخال، التعديل، المحو، لقيام الركن المادي، بل يشترط تحقق النتيجة عن قيام إحدى هاته السلوكات غير المشروعة، و المتمثلة في تغير حالة المعطيات [3]

[1] علي عبد القادر القهوجي، المرجع السابق، ص 144
[2] بد الفتاح بيومي حجازي، "الحكومة الالكترونية و نظامها القانوني"، المرجع السابق، ص 365
[3] مال قارة، المرجع السابق، ص122

الفرع الثالث : الركن المعنوي

هو القصد الإجرامي (الجرمي)، أي القيام بالفعل عن علم وإرادة، فاغلب التشريعات الدولية تتطلب توفر هذا القصد لاكتمال الجرم.

اولا)_القصد العام

يتمثل القصد العام في جريمة التلاعب بمعطيات الحاسب الآلي، في كل من الإرادة و العلم، و يجب أن تتجه إرادة الجاني في هاته الجريمة (جريمة التلاعب بمعطيات الحاسب الآلي)، إلى ارتكاب إحدى السلوكات الإجرامية المذكورة سابقا، و المتمثلة في فعل الإدخال، فعل التعديل، فعل الإزالة / المحو، و تعد هذه الإرادة الإجرامية دليلا على خطورة شخصية الجاني، و تعد كذلك جوهر الركن المعنوي، هذا الأخير الذي يمثل ركن المسؤولية الجنائية فإذا انتفى الركن المعنوي كنا بصدد مانع من موانع المسؤولية [1]

ثانيا)_ القصد الخاص :

يقصد بالقصد الخاص في الركن المعنوي لأي جريمة هو وجوب تحقق نتيجة تخرج عن الركن المادي، و فيما يخص جريمة التلاعب بمعطيات الحاسب الآلي، فالقصد الخاص بها لا يتطلب أي نتيجة تخرج عن الركن المادي.

* الإزالة والتعديل : سلوكات عمدية في الركن المعنوي،

* التغيير والحذف : سلوكات غير عمدية في الركن المعنوي.

فالفرق في السلوكات الإجرامية في جريمة الدخول والبقاء غير المصرح به، و السلوكات الإجرامية في جريمة التلاعب بمعطيات الحاسب الآلي، هو أن الأولى ظروف مشددة و الأخرى سلوكات مادية.

و تجدر الإشارة إلى أن الاختلاف بين عقوبة الجريمتين، جريمة الدخول و البقاء غير المصرح به و جريمة التلاعب بمعطيات الحاسب الآلي هو "عنصر العمد"

[1] محمد عبيد الكعبي ، مجلة الحقوق العدد 01 الطبعة الاولى

الفصل الثاني:

مكافحة جرائم المساس بالأنظمة المعلوماتية.

الفصل الثاني : مكافحة جرائم المساس بالأنظمة المعلوماتية في التشريع الجزائري

لوضع حماية جزائية للجريمة المعلوماتية استجابت عدة دول لها، فمثلا الولايات المتحدة الأمريكية التي أصدرت قانون فيدرالي سنة 1984 متعلق بالاحتيال وإساءة استخدام الكمبيوتر، كما أصدرت فرنسا قانون رقم 88/19 الموافق ل 05/01/1988

بشان الغش المعلوماتي، والذي ادمج في قانون العقوبات الفرنسي وأصبح يشكل باب جديد هو الباب الثالث من قانون العقوبات الفرنسي، ثم صدر تعديل جديد لهذا القانون في 01/03/1994

. أما عن التشريعات العربية فقد تبنى المشرع الجزائري في القسم السابع مكرر نصوص الجريمة المعلوماتية أو ما يصطلح عليه بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك بالقانون رقم 06/23 المؤرخ في2006/20/12 المتضمن قانون العقوبات الجزائري.

ونجد المشرع الجزائري لم يتكلم عن الاعتداءات الماسة بمنتجات الإعلام الآلي، والتي تنطوي ضمنها التزوير المعلوماتي وقد شهد العالم مولد أول معاهدة دولية لمواجهة جرائم الكمبيوتر وذلك في سبتمبر 2001 في مدينة بودابست بتوقيع 26دولة من الاتحاد الأوروبي إضافة إلى كندا وجنوب إفريقيا والولايات المتحدة الأمريكية، والحقيقة أن تلك المعاهدة وإن كانت أوروبية المنشأ فهي دولية النزعة فهي مفتوحة للدول الأخرى التي تطلب الانضمام أو الترشح للانضمام لها.[1]

المبحث الأول : العقوبات المقررة على الجرائم الماسة بالانظمة المعلوماتية .

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الحماية الجزائية للمعلوماتية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالمعلوماتية، لذلك سوف نتعرض في هذا المبحث للحماية الجزائية للمعلوماتية من جانبه الموضوعي، من خلال قانون العقوبات ونصوص الملكية الفكرية والصناعية باعتبار المعلوماتية نتاج فكر وإبداع.

المطلب الأول : العقوبات الجزائية المنصوصة التي تعاقب جرائم الانظمة المعلوماتية.

لقد نص المشرع الجزائري في قانون العقوبات على المساس بأنظمة المعالجة الآلية أو ما يعرف بالغش المعلوماتي بموجب التعديل الذي تم بالنسبة لقانون العقوبات بالقانون رقم06/23 المؤرخ في2006/20/12

المتضمن قانون العقوبات الجزائري في قسمه السابع مكرر، والذي شمل المواد من 394مكرر الى 394 مكرر 7، متتبعا في ذلك خطى التشريعات الغربية التي اتجهت في وقت متقدم إلى إصدار تلك النصوص المتعلقة بالجريمة المعلوماتية.

اهم تلك التشريعات نجد التشريع الفرنسي ولا ننسى أول اتفاقية حول الإجرام المعلوماتي التي أبرمت بتاريخ:

[1] أمال قارة، المرجع السابق، ص27_28

08/11/2001

من طرف المجلس الأوروبي. لذلك سنتطرق في الفرع الأول إلى جريمة المساس بأنظمة المعالجة الآلية، أما في الفرع الثاني فهو مخصص للتزوير المعلوماتي الذي لم يتطرق إليه المشرع الجزائري فتمت معالجته من منظور التشريع المقارن[1]

الفرع الاول : جريمة المساس بأنظمة المعالجة الالية للمعلومات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي، وهو الفعل المنصوص والمعاقب عليه في المواد394 مكرر إلى المادة 394 مكرر 7ونجد أن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي قدمت تعريفا للنظام المعلوماتي في مادتها الثانية ، وكذلك عرفها الفقه الفرنسي

وبالعودة إلى قانون العقوبات الجزائري، نجد أن الغش المعلوماتي يأخذ صورتين أساسيتان وهما :

- الدخول في منظومة معلوماتية
- المساس بمنظومة معلوماتية

أولا)_: الدخول في منظومة معلوماتية

ويشمل فعلين هما الدخول و البقاء

1 : جريمة الدخول غير المشروع

تنص المادة 394 مكرر من قانون العقوبات الجزائري والتي تقابلها المادة 323/1 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك ، وتضاعف العقوبة إذ ترتب على الدخول أو البقاء أو حذف أو تغيير معطيات المنظومة أو تخريب النظام.

2: جريمة البقاء غير المشروع

المشرع الجزائري على هذه الجريمة في المادة 394 مكرر من قانون العقوبات الجزائري. المقابلة لنص المادة 323/1من قانون العقوبات الفرنسي. ويقصد بالبقاء، الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أتاء إتاوة.

وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد، كما يجرم البقاء حتى ولو تم بصفة عرضية[1]

[1] أمال قارة، المرجع السابق، ص28

ثانيا)– المساس بمنظومة معلوماتية

تنص المادة 394 مكررة قانون العقوبات الجزائري والذي يقابله في النص الفرنسي المادة 323/3

قانون العقوبات الفرنسي عن "كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[2]

ثالثا)_ صور احرى للغش المعلوماتي :

المادة 394 مكرر 2من قانون العقوبات الجزائري بتجريم الأعمال التالية:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي .

الفرع الثاني : *جريمة التزوير المعلوماتي*

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير، ويلاحظ أن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة 1988 وصدور قانون العقوبات لسنة 1994 عدل المادة 441/ الكي تستوعب بجانب التزوير العادي جريمة التزوير المعلوماتي، حيث نصت بعد تعديلها على :

إن كل تغيير للحقيقة بطريق الغش ....في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر» فالمشرع فصل بذلك بين التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات، حيث أفرد نص خاص، للصورة الأولى بينما احتوى الصورة الثانية في النص العام لجريمة التزوير[3]

وقد تناولت المادة 7 من اتفاقية بودابست جريمة التزوير المتصلة بالحاسوب واعتبرت أن الواقع تعتبر تزويرا إذا تضمنت خلق أو تعديل البيانات أو برامج غير مرخص بإنشائها أو تعديلها،

تصبح لها قيمة مختلفة في الإثبات فيما يتعلق بالمعاملات القانونية التي تقوم على الثقة في المعلومات القائمة على تلك البيانات التي تعرضت للتزوير.

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي ، الطبعة6، دار هومة، الجزائر، ص 445.

[2] د مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006_2009، ص 10

[3] أمال قارة، المرجع السابق، ص47

ونجد المشرع الجزائري لم ينص عن التزوير المعلوماتي لذلك سنتطرق إلى تحديد جريمة التزوير المعلوماتي (الفقرة الأولى) وموقف المشرع الجزائري من التزوير المعلوماتي(الفقرة الثانية)[1]

اولا)_ تحديد جريمة التزوير المعلوماتي

إن موضوع التزوير هو المحرر، الذي لا بد من توافر شروط فيه، تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير، لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير المعلوماتي تقع على المستندات المعلوماتية.

كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي، ووضع نص خاص بالتزوير المعلوماتي يحقق الحماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير، بالمفهوم الجديد للمحررات.

إن النشاط الإجرامي المكون الجريمة التزوير المعلوماتي يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير. وإن تحوير البرنامج أو قواعد البيانات لا يعد تزويرا بل يقع تحت طائلة نصوص قانون حقوق المؤلف والحقوق المجاورة[2].

ثانيا)_ موقف المشرع الجزائري من جريمة التزوير المعلوماتي

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، الذي يعتبر من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن. ونجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد214 الى 229 التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير.

لقد كان من الأفضل لو أضاف المشرع الجزائري نصا خاصا بالتزوير المعلوماتي مثلما قام به المشرع الفرنسي، ونخلص في النهاية أن المشرع الجزائري رغم تداركه من خلال القانون رقم 06/23

الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا أنه أغفل تجريم التزوير المعلوماتي، ولم يتبنى الاتجاه الذي انتهجته التشريعات الحديثة التي قامت بتوسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث ليشمل المستند المعلوماتي

[1] أمال قارة، المرجع السابق، ص 48.

[2] أمال قارة، المرجع السابق، ص42

المطلب الثاني: قواعد الاختصاص المحلي و إجراءات التحقيق الابتدائي

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، فيلزم على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن تنشأ قواعد إجرائية حديثة إلى جانب القواعد الموضوعية، كانت هذه الجرائم المعلوماتية تتميز بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات العملية الإجرائية التي جعلت القواعد الإجرائية التقليدية قاصرة عن مواجهة تلك المشاكل، ولهذا اتجهت بعض التشريعات كالتشريع الانجليزي والأمريكي والجزائري إلى تعديل بعض قواعدها الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية كتلك المتعلقة بالاختصاص المحلي، وإجراءات التحقيق الابتدائي خاصة التي تهدف إلى جمع الأدلة.

وسوف نتناول في هذا المطلب إلى قواعد الاختصاص المحلي (الفرع الأول)، وإجراءات التحقيق الابتدائي (الفرع الثاني)[1].

الفرع الاول : قواعد الاختصاص المحلي

عالج المشرع الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه، وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، لكن لما كانت الجريمة المعلوماتية جرائم عابرة للإقليم، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه، لهذا فان المشرع الجزائري أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة المعلوماتية بموجب القانون

06/22 المؤرخ في 20 ديس مبر 2006 المعدل والمتمم للأمر رقم 66/155

الموافق ل 08يونيو 1966 والمتضمن قانون الإجراءات الجزائية، لهذا سنتطرق لتلك القواعد على النحو التالي:

أولا)–الاختصاص المحلي للنيابة العامة

يحدد الاختصاص المحلي للنيابة العامة وفقا للمادة 37 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي في دائرته القبض على هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر.

[1] أمال قارة، المرجع السابق، ص 55.

وبالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بمكان القبض على هؤلاء الأشخاص حتى ولو تم لسبب أخر لكن لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر فإن المشرع الجزائري بموجب المادة 37فقرة 2 من قانون الإجراءات الجزائية [1]أجاز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة الاختصاص المحاكم الأخرى إلا أنه ترك كيفية تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص[2].

ويتعين على ضابط الشرطة القضائية طبقا للمادة 40مكرر أمن قانون الإجراءات الجزائية الجزائرية[3] أن يبلغوا وكيل الجمهورية لدى المحكمة الكائن لها الجريمة بأصل ونسختين من إجراءات البحث ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة.

والذي يطالب طبقا للمادة 40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة 40مكرر من هذا القانون، وهذه الإجراءات تتعلق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة، والذي يطالب طبقا للمادة 40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص

المحكمة المذكورة في المادة 40مكرر من هذا القانون، وهذه الإجراءات تتعلق بتحريك الدعوى العمومية أو مباشرتها أو رفعها مجرد أن يتبين للنائب العام أن الجريمة تدخل ضمن المحكمة المختصة التابعة لها وهذا مانصت عليه المادة 40مكرر.

ثانيا)_ الاختصاص المحلي لقاضي التحقيق ومحاكم الجنح

1)_الاختصاص المحلي لقاضي التحقيق

يقصد بالاختصاص المحلي القاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق ويتحدد الاختصاص المحلي لقاضي التحقيق طبقا للمادة 40 من قانون الإجراءات الجزائية المكان وقوع الجريمة أو محل إقامة احد هؤلاء الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على احد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر.

---

[1] تنص المادة 2/37 من قانون الإجراءات الجزائية الجزائري على ما يلي ":يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف

[2] مال قارة، المرجع السابق، ص 56

[3] المادة 40مكرر1 من قانون الإجراءات الجزائية الجزائري على ما يلي: "يخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل وبنسختين من إجراءات التحقيق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة"

إلا أن المشرع ألغي في التعديل الجديد الفقرة 2و 3من المادة40، وأصبحت تنص الفقرة2 على انه:" يجوز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، وبالتالي فإن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى لكنه ترك تحديد كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر لاحقا[1]

2)_الاختصاص المحلي لمحاكم الجنح.

يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة 329 من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة، أو بمحل إقامة أحد الأشخاص المتهمين، أو شركائهم، أو بالمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر، غير أن المشرع في التعديل الصادر بموجب القانون 04/14 أضاف فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم[2].

إذن فإن المشرع أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد اختصاص وكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح ولكنه ترك ذلك للتنظيم الذي سيصدر لاحقا والذي يحدد تلك المحاكم التي يمتد إليها الاختصاص، وقرر في المادة 40مكررة[3] أيضا تطبيق القواعد المتعلقة بالدعوى العمومية والتحقيق والمحاكم أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 37،40 ، 329 من قانون الإجراءات الجزائية. والحقيقة أن مشكلة الاختصاص القضائي في الجريمة المعلوماتية تعد من المشكلات العويصة التي تعرقل الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين وتنتج أثارها في مكان أخر داخل الدولة أو خارجها وإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة فأي مكان في هذه الأماكن ينعقد الاختصاص الجنائي لسلطات التحقيق والمحاكمة في الجريمة المعلوماتية.

لكن على المستوى الدولي فان الأمر بحاجة إلى اتفاقيات دولية ثنائية أو جماعية، ولقد شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسوب الآلي، إلا أن ذلك لم يحقق تقدما في معالجة

[1] أمال قارة، المرجع السابق، ص 57.

[2] محمد الأمين البشري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي، ص 372

[3] تنص المادة 40 مكرر من قانون العقوبات الجزائية الجزائري على ما يلي:" تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 37 ،40،329 من هذا القانون، مع مراعاة أحكام المواد من 40مكررا إلى 40مكررة"

الاختصاص القضائي، فلذلك فالحاجة ماسة إلى قوانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في كل المجالات.

الفرع االثاني : إجراءات التحقيق الابتدائي

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشان واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك، والتحقيق مرحلة لاحقة الإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الآخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت[1]

وسوف تقتصر دراستنا على إجراءات جمع الأدلة المادية التي يكون منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل والمنطق، فهي أقوى مفعولا في الاقتناع من الأدلة القولية على أن نخص بالدراسة التفتيش وضبط الأشياء باعتبارهما أهم التحديات الإجرائية لجرائم الكمبيوتر.

أولا)_التفتيش في مجال الجريمة المعلوماتية

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية الجناية أو جنحة تحقق وقوعها في محل وذلك من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة. وإذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية، فما مدى خضوع البرامج والمعلومات كمكونات معنوية للحاسوب للتفتيش ؟وماهي ضوابط تفتيش نظم الحاسوب ؟

1)_ مدى قابلية نظم الحاسوب للتفتيش:

يتكون الحاسوب من مكونات مادية ومكونات معنوية، ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها

[1] محمد الأمين البشري، المرجع السابق ، ص 374.

وعن مرتكبها وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش.

إذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله وبنفس الضمانات المقررة قانونا في التشريعات المختلفة، وبالنسبة للاماكن العامة سواء كانت بطبيعتها كالطرق العامة والشوارع أو كانت بالتخصيص كالمقاهي والمطاعم والسيارات العامة فان الشخص إذا وجد في هذه الأماكن وهو يحمل مكونات مادية للحاسوب أو كان مسيطرا أو حائ ز

ا لها فان التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد[1].

ما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية، كبرامج الحاسوب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض، حيث يذهب رأي أنه إذا كانت الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البرامج والبيانات. وقد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعطيات، وابرز مثال لذلك الفقه الكندي عندما وسع من تفسير المادة 487 من قانون العقوبات الكندي التي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعو اللاعتقاد بأن الجريمة قد وقعت أو يشتبه فيل وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو انه سيتيح دليلا على ارتكاب الجريمة. وهكذا فإن هذا النص يفسر على أنه يسمح بضبط وبتفتيش البيانات وبرامج الحاسب الآلي[2]

2)_ ضوابط تفتيش نظم الحاسب الالي :

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة، ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية :

أ)– الضوابط الموضوعية :

تنحصر هذه الضوابط فيما يلي:

* وقوع جريمة معلوماتية:

[1] عبد الله هلالي، تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، مصر، ص74

[2] كمال عفيفي ، جرائم الكمبيوتر ، لبنان ،منشورات الحلبي الحقوقية ، سنة 2003 ص 366

والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة، وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29 يونيو 1990، وفي فرنسا صدر قانون رقم 88/19 في جينايز 1988 وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.

* اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها

فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلا أو شريكا، بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة، وهذا ما تؤكده المادة 163من قانون الإجراءات الجزائية الجزائري[1] والمادة 77 من قانون الإجراءات الجزائية الفرنسي.

وفي مجال المعلوماتية يمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا[2]

* توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة

فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة، ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

وهكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.

*إجراء التفتيش النظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق:

يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق، أما النيابة

[1] لمادة 163 من قانون الإجراءات الجزائية الجزائري على ما يلي: " إذا رأى قاضي التحقيق أن الوقائع لا تكون جناية أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو أن مقترف الجريمة ما يزال مجهولا، أصدر أمر بألا وجه لمتابعة **المتهم**.

[2] مال قارة، المرجع السابق، ص 59

العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام[1].

[1] عبد الله الهلالي ، تفتيش نظام الحاسب الالي وضمانات متهم المعلوملت ، دراسة مقارنة ، الطبعة الاولى ،القاهرة ، دار النهضة العربية ص 76

المبحث الثاني : جهود التعاون الدولي

تنوعت الجهود الدولية في مكافحة الجريمة الالكترونية حيث تم اتخاذ العديد من الآليات و الإجراءات للحد و التقليل منها إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى المعلوماتية و الاستعمال اللامتناهي للكمبيوتر و الانترنت و سنتطرق إلى إبراز هذه الجهود مع تبيان صعوبة التعاون الدولي للقضاء على هذه الجريمة الدولي العابرة للحدود .

المطلب الاول: الجهود الدولية الغربية

مع تطور تقنية المعلومات، و اهتمام الأنظمة الدولة بموضوع الجرائم المعلوماتية وقعت العديد من الصكوك

و المواثيق الدولية من طرف دول أدركت فعلا مدى الخطورة التي تشكلها هذه الجريمة بوصفها من الجرائم العابر للحدود، فقد يكون الجاني في بلد و المضرور في بلد آخر، و مزود الخدمة في بلد ثالث و المستضيف للموقع و الذي صر منه الفعل المجرم في بلد آخر ومن هنا أثيرت مسألة تطبيق نصوص القانون الجنائي، لذلك سنحاول التطرق إلى المواثيق الدولية لجرائم الكمبيوتر و الانترنت.

الفرع الاول : أهم الصكوك الدولية الخاصة بالجرائم المعلوماتية.

اولا)_ القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر

يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990و قد حث في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز و بتجريم تلك الأفعال جنائيا[1]

و اتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

* ضمان أن الجزاءات و القوانين الراهنة بشأن سلطات التحقيق و الأدلة في الإجراءات القضائية تنطبق على نحو ملائم ، و إدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.

* النص على جرائم و جزاءات و إجراءات تتعلق بالتحقيق و الأدلة حيث تدعو الضرورة للتصدي لهذا الشكل الجديد و المعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو [2]ملائم كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم

[1] عبد الفتاح مراد ،قانون غسل الاموال و اللائحة التنفيذية و القوانين المكملة له ، ص 237

[2] عبد الفتاح مراد– المرجع السابق – ص 238

المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة ، و نصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين و تبادل المساعدة في المسائل الجنائية تنطبق بكل تام على الأشكال الجديدة للإجرام مثل الجرائم الالكترونية ، و أن تتخذ خطوات محددة نحو تحقيق هذا الهدف.

كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير[1]

1- معايير دولية لأمن المعالجة الآلية للبيانات.

2- اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابر للحدود أو ذات الطبيعة الدولية.

3- إبرام اتفاقيات دولية تنطوي على نصوص تنظيم و إجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة المعلوماتية المتصلة فيما بينها و الأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد و حرياتهم و سيادة الدول

ثانيا)_مقررات و توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 1994 البرازيل بشأن جرائم الكمبيوتر.

يمكن اعتبارها انعقد هذا المؤتمر سنة 1994 بالبرازيل حيث نص

على الأفعال المجرمة التي جرائم معلوماتية كالاحتيال، و الغش المرتبط بالكمبيوتر من خلال إتلاف و محو المعطيات ، و أيضا ما يعرف بالتزوير المعلوماتي و يشمل إتلاف و محو البرامج و البيانات و تعطيل

وظائف الكمبيوتر و نظام الاتصالات (الشبكات)، أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن. أما من الناحية الإجرائية فان القرار الصادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية تتمثل فيما يلي[2]

* القيام بإجراء التفتيش و الضبط في بيئة تكنولوجيا المعلومات، و أيضا تفتيش شبكات الحاسب الآلي.

* التعاون الفعال بين المجني عليهم و الشهود و كذا مستخدمي المعلومات من أجل إتاحة استخدام المعلومات للأغراض القضائية.

* اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته و ممارسة الرقابة عليها

[1] عبد الفتاح بيومي حجازي – المرجع السابق – ص 190.

[2] عبد الفتاح مراد– المرجع السابق – ص 242

ثالثا)- اتفاقية برن الدولية لحماية المصنفات الأدبية و الفنية

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 سبتمبر 1886، و المكملة بباريس في ماي 1896، و المعدلة في برلين في 13 سبتمبر 1908، و المكملة ببرن في 20 مارس 1914، و المعدلة بروما في جوان 1928، و بروكسل سنة 1948، و استوكهولم في جويلية 1967، و باريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية.

و بموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية وفقا لما جاء فيها [1]" المتعلقة بالجوانب المتصلة بالتجارة الدولية حيث تسعى الدول TRIPISإضافة إلى اتفاقية "

الأطراف في الاتفاقية إلى تشجيع الحماية الفعالة و الملائمة لحقوق الملكية الفكرية من أجل التخفيف العراقيل التي تعوق التجارة الدولية.

رابعا)- اتفاقية بودابست لمقاومة جرائم المعلوماتية و الاتصالات 2001.

إدراكا من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية "بودابست "نذكر منها: دول أعضاء من الاتحاد الأوروبي ، إضافة إلى كندا، اليابان، جنوب إفريقيا، أمريكا، و جاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الالكترونية و تجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة و تعقب مرتكبيها و المساعدة على الاستدلال عليهم و ضبطهم كما تحدد أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها، كما فصلت الاتفاقية النصوص الجنائية الموضوعية للجريمة و أنواعها كما تشمل جوانب عديدة من جرائم الانترنت من بينها الإرهاب، عمليات تزور بطاقات الائتمان و غيرها.... و تعتبر هذه الاتفاقية أحد محاولة و أكثرها تنوعا من أجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الانترنت.

كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات و أجهزة الشرطة و قطاع الكمبيوتر و قد صاغ نصها عدد من الخبراء القانونين في مجلس أوروبا بمساعدة دول أخرى.

[1] للاطلاع على هذه الاتفاقية أنظر: محمد عد الله أبو بكر سلامة – موسوعة جرائم المعلوماتية "جرائم الكمبيوتر و الانترنت – "المكتب العربي الحديث – الإسكندرية.

خامسا)_ قانون الأونستيرال النموذجي.

اقتناعا من الدول بضرورة منع هذه الجرائم و مكافحتها خاصة و أن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي و الأبعاد الدولي لإساءة استخدام الكمبيوتر و الجرائم المتعلقة به تم صياغة قانون الأونيسترال النموذجي بشأن التجارة الالكترونية، و الآخر بشأن التوقيعات الالكترونية

1)_ قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية

اعتمد هذا النص في 5 جويلية 2001 و ينطبق هذا القانون حيثما تستخدم توقيعات الكترونية [1]خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة،و الحداثة التكنولوجية حيث أنه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الالكتروني و هو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع

جملة من الإجراءات

2)– قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية

تنطبق نصوص هذا القانون على أي نوع من المعلومات التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل الكترونية، و يتم تبادل هذه البيانات من خلال نقلها الكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي و لضرورة توحيد تطبيقه ..[2]

الفرع االثاني : صعوبة التعاون الدولي لمكافحة الجريمة الالكترونية :

لقد قدمت شبكة المعلومات الدولية مجموعة متنوعة و معقدة من الاستخدامات في شتى المجالات السياحية، الثقافية، الاقتصادية، و الأمنية و حتى الشؤون العسكرة الأمر الذي زاد من حالات الاعتداء على خصوصية سرية المعلومات بقصد السرقة، التجسس، القرصنة، و التخريب. حيث أصبح هاجسا لكل دول العالم خاصة بسبب الانتشار الواسع لتبادل المعلومات المشفرة ذات الصلة بالتجسس السياسي أو العسكري أو الصناعي، أو أية نشاطات إجرامية . فنادى البعض بضرورة انشأ وحدات خاصة بمكافحة الجريمة المعلوماتية أسوة بجهات البحث الجنائي الوطنية و الدولية الانتربول)، و ذلك لإثبات الجريمة عند وقوعها و تحديد أدلتها و فاعليها مما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة و تبادل الخبرات و المعلومات حول هذا النوع من الجرائم و مرتكبيها و سبل مكافحتها.

[1] شريف محمد غنام – حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني – دار الجامعة الجديدة – 2007ص 194

[2] عبد الفتاح مراد – المرجع نفسه– ص 424

و رغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك عوائق تحول دون ذلك بل و تجعل من هذا التعاون صعبا، و يمكن إيجاز ذلك في الأسباب التالية[1]

اولا)_ عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج ضمنها ما يسمى: بإساءة استخدام نظم المعلومات الواجب إتباعها، كما انه لا يوجد تعريف محدد للنشاط المفروض أن يتفق

على تجريمة و هذا راجع إلى قصور التشريع ذاته في كافة بلدان العالم و عدم مسايرته السرعة التقدم المعلوماتي ومن ثم الجريمة المعلوماتية.

و ما تجدر الإشارة إليه أن العديد من الدول العربية لم تصدر قانونا يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الكمبيوتر أو عن طريق الانترنت، ولا يزال الخلاف قائما حول أفضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية أم أنه تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك و يتم تجريمها، أم من الأفضل إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية ، حتى أن الأمر لا يتوقف هنا بل يتعداه ، حيث أن عدم اتفاق الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم و ارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة

ثانيا : عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرام ، و حتى في حالة وجودها فان هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم و برامج الحاسب الآلي و شبكة الانترنت، و من ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع و سلطات امن الدول، و يظهر الأثر السلبي في التعاون الدولي و هو ما حاولت الأمم المتحدة الاهتمام به و كذلك بعض البلدان الأوروبية[2].

ثالثا: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة المتعلقة بالجريمة المعلوماتية بين الدول المختلفة خاصة فيما يتعلق بالتحقيق و الحصول على الأدلة لا سيما و أن الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين أمر في غاية الصعوبة فضلا عن صعوبة الحصول على الدليل ذاته.

رابعا : إشكالية الاختصاص في الجرائم الالكترونية كونها تعد من المشكلات التي تعرقل الحصول على الدليل فيها خاصة و أنها من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي و الدول بسبب التداخل و الترابط بين شبكات المعلومات لأن الجريمة قد تقع في مكان معين و تنتج آثارها في مكان آخر.

---

[1] عبد الفتاح بيومي حجازي – المرجع السابق – ص188

[2] شريف محمد غنام ، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني ، داؤ الجامعة الجديدة ،2007 ص194

و ما يلاحظ أن جل التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية لذلك لا مناص من الاتفاقيات الثنائية و الجماعية بين الدول لتسهيل تحقيق جرائم المعلوماتية و رغم إبرام بعض الاتفاقيات إلا أنها لم تف بالغرض في حل مشكلات الاختصاص و تبادل الأدلة الجنائية و تسليم المجرمين. لذلك تبق الحاجة جد ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي و عصر المعلوماتية إن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقا لما جاء في توصية المجلس الأوروبي رقم 13/95 تقتضي التدخل السريع لمد الإجراءات إلى أنظمة كمبيوتر قد تكون موجودة خارج الدولة، و حتى لا يمثل هذا الأمر اعتداء على سيادة دولة معينة أو على أحكام القانون الدولي يجب وضع قاعدة قانونية صريحة تسمح بهذا الإجراء. لذلك فان الحاجة ملحة لاتفاقيات دولية تنظم كيفية اتخاذ هذه الإجراءات كما يجب أن تتوافر إجراءات سريعة و مناسبة و نظم اتصال تسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة و هو ما يوجب تطوير اتفاقيات التعاون الدولي[1].

المطلب الثاني: الجهود الدولية العربية

لا يمكن إنكار ما بذلته الدول العربية من مجهودات في مجال الإجرام المعلوماتي، من أجل مكافحة جميع الجرائم المعلوماتية، سواء كان ذلك عن طريق القوانين، أو الهيئات أو غيرها، و الموجودة على المستوى العربي، كل هاته المجهودات جاءت بغرض حماية الدول من الجرائم الالكترونية خصوصا بعدما تعرضت تلك الدول من أضرار، و ما لحقتها من خسائر بسبب تلك الجرائم.

هاته الجهود سنوضحها من خلال الفرعين الآتيين: الفرع الأول بعنوان "الاتفاقيات والقوانين و الفرع الثاني بعنوان "الهيئات".

الفرع الاول : الاتفاقيات والقوانين

من أبرز الاتفاقيات التي تم إبرامها على المستوى العربي، من أجل مواجهة الجريمة المعلوماتية، هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القائمة على فكرة وجوب تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وقد نصت المادة الأولى منها على ما يلي " :تهدف هذه الاتفاقية إلى تعزيز التعاون و تدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية و مصالحها و سلامة مجتمعاتها و أفرادها"[2].

[1] عبد الفتاح بيومي حجازي- المرجع السابق – ص 192

[2] المادة 01، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

فرواج المعلومات في كل الدول العربية، أدى إلى ظهور عدة ممارسات إجرامية في هذا النطاق، و إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قامت الدول بعدة محاولات لإيجاد سبل تشريعية إجرائية ناجعة لمواجهة هذا النوع من الجرائم المستحدثة.

و من بين هاته الدول مصر، فقد عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة من 25 إلى 28 أكتوبر 1993، و ناقشت موضوع جرائم الكمبيوتر و الجرائم الأخرى في مجال تكنولوجيا المعلومات، من خلال الأبحاث و الدراسات المقدمة من الباحثين و التي دارت حول تحديد أنواع الجرائم المختلفة، و المتعلقة بنظم المعلومات من اعتداء مادي على الأجهزة و الأدوات[1].

لكن، و بالرغم من ذلك، إلا أن مصر لم تعمل على سن قوانين جديدة خاصة بها في هذا المجال ا المعلوماتي و لم تقم حتى بتعديل ما لديها من قوانين، و إنما القانونيين في مصر يحاولون تطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية، و من ذلك على سبيل المثال، اعتبر أن قانون براءات الاختراع ينطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، كما تم تطويع نصوص قانون حماية الحياة الخاصة، و قانون تجريم إفشاء الأسرار، بحيث يمكن تطبيقها

على بعض جرائم الانترنت، و أوكل إلى القضاء الجنائي النظر في القضايا التي ترتكب ضد أو بواسطة النظم المعلوماتية[2].

و على المستوى الوطني، و على غرار باقي الدول، و تطبيق للتوصيات الدولية التي شددت على وجوب النص في القوانين الداخلية و تجريم هذا النوع من الاعتداءات، كذلك فعل المشرع الجزائري بتعديله لقانون العقوبات بموجب المر رقم 04/15 المؤرخ في 10/11/2004 المعدل و المتمم بالأمر رقم 05/155

و الذي افرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، الذي يحوي ثماني مواد من 394 مكرر إلى 394 مكرر 07، أو ما يسمى بجرائم الغش المعلوماتي[3] .

و نشير أيضا إلى جهود المملكة العربية السعودية في مكافحة الجريمة المعلوماتية، فهي الأخرى لا تختلف عن بقية الدول العربية الأخرى، إلا أنها تنطلق أغلب كافة قوانينها من الشريعة الإسلامية، وقضية الجريمة و العقاب في الشريعة، تتسم بوضع متميز بين سائر التقنيات الجنائية المقارنة، حيث

[1] عبد العال الدربي، محمد صادق إسماعيل ، الجرائم الالكترونية النظام القانوني للحماية المعلوماتية ،الطبعة 01 المركز القومي للدراسات القانونية ، القاهرة 2012 ص352

[2] عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات ، الطبعة 01 ، دار المستقبل للنشر والتوزيع ، عمان 2009 ص232

[3] أحسن بوسقيعة، "الوجيز في القانون الجزائي الخاص – الجزء الأول-"، ط18، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2015، ص447.

عالجها الشارع الحكيم في إطار النظام القانوني الشامل المتكامل، الذي يغطي كل جوانب الحياة، ومن أهم ما أصدرته المملكة العربية السعودية في المجال المعلوماتي، نظام حماية حقوق المؤلف بالمرسوم الملكي رقم م/11 في 1410/05/19هـ حيث توضح المادة الثالثة منه، الأنواع المشمولة بالحماية، و ورد في البند العاشر" :برامج الحاسب الآلي"، و أوكل إلى وزارة الإعلام متابعة تنفيذ هذا القرار [1]. يتضح مما سبق، أن البلاد العربية، ليس فيها عمليات عديدة فيما يخص سن قوانين جديدة، و لا حتى تعديل لتلك القوانين، لكي تستوعب جميع الأحداث و المستجدات الجديدة الإجرامية، والتي منها "جرائم تكنولوجيات المعلومات"، وأن ما يوجد فيها هو عملية تطويع للقوانين السابقة، و محاولة إدخال الجرائم الالكترونية تحت بعض نصوصها، ناسين أو متناسين طبيعة هذا النوع من الجرائم، و كذلك حجم الخسائر المادية و النوعية التي تخلفها، و الملابسات أو الغموض الذي يكتشف لحظة ارتكاب الجريمة الالكترونية، وكذلك تناسوا النتائج المترتبة من جراء ارتكاب تلك الجرائم[2]، بذلك يمكن القول أن الدول العربية مازالت متراجعة على المستوى القانوني لباقي الدول الغربية.

الفرع الثاني : الهيئات العربية المستحدثة لمكافحة الجرائم المعلوماتية

أولا)_ المكتب الإقليمي العربي

و هو أحد هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الذي عقد محضر الاجتماع الأول في الجزائر يومي 25 و26 فيفري 2013، تم بموجبه تشكيل فريق العمل حول حماية الأطفال على الانترنت في المنطقة العربية، ويهدف إلى تنسيق الجهود وتوحيد الرؤية في المنطقة العربية، من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل على الانترنت في المنطقة العربية

ثانيا)_ مجلس وزراء العدل العرب

1)_ تعريفه : تعريفه وأهدافه

أنشئ مجلس وزراء العدل العرب في سبتمبر 1981

و هو احد المجالس الوزارية المتخصصة العاملة في نطاق جامعة الدول العربية و يهدف إلى:

- تقوية و تعميق التعاون العربي في المجالات القانونية و القضائية و تنمية تبادل الخبرات و الكفاءات، و تأهيل الأطر القانونية والقضائية و كفالة تخصصها بما يحقق قدرتها على مواكبة التطور و النظر فيما يستجد من قضايا و منازعات، و العمل على تأكيد الضمانات لاستقلال القضاء و صون حرمته،

[1] عبد الحكيم رشيد توبة، المرجع السابق، ص 233

[2] عبد الحكيم رشيد توبة، المرجع السابق، ص 232

- دعم و متابعة الجهد المشترك لتوحيد التشريعات العربية وفق أحكام الشريعة الإسلامية السمحاء مع الأخذ بالاعتبار ظروف المجتمع في كل قطر عربي، و وضع الخطط و المناهج لتحقيق هذا الهدف و العمل على تنفيذها.
- العمل على تطوير الأنظمة القضائية و توحيدها، و المهن القانونية، و تحسين أسلوب العمل بالمحاكم، كل هاته الهداف نصت عليها المادة الثانية من النظام الأساسي لمجلس وزراء العدل العرب[1]

دوارته :

نصت المادة السابعة من النظام الأساسي لمجلس وزراء العدل العرب على ما يلي " :يعقد المجلس دوراته العادية و الاستثنائية في مقر جامعة الدول العربية أو في أية دولة عربية بناء على دعوة منها و موافقة المجلس كما نصت المادة الثامنة من نفس النظام على ما يلي " :يعقد المجلس اجتماعا دوريا مرة كل عام بناء على دعوة من الأمين العام للجامعة خلال شهر نوفمبر، و له أن يعقد اجتماعات استثنائية بقرار منه أو بناء على طلب إحدى الدول الأعضاء و موافقة أغلبية أعضائه"[2]

أهم القوانين والقرارات الصادرة عنه في المجال المعلوماتي

أ)_ قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها:

وهو أحد أهم القوانين الصادرة عن مجلس وزراء العدل العرب في مجال الجريمة المعلوماتية فقد تضمن هذا القانون جملة من المصطلحات المتعلقة بالجريمة المعلوماتية، كما نظم الأحكام المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما نتناول أيضا الاحكام المتعلقة بالشروع و الاتفاق / المساهمة في هاته الجرائم، كما جرم في مضمونه مختلف الاعتداءات المرتكبة عن طريق الشبكة المعلوماتية أو أي نظام معلوماتي، و هو ما نصت عليه المادة 16 كالآتي: "كل من اعتدى على أي من المبادئ أو القيم الدينية أو السرية أو حرمة الحياة الخاصة عن طريق الشبكة

المعلوماتية أو أحد أجهزة الحاسب الآلي و ما في حكمها، يعاقب بالحبس مدة لا تقل عن ..... "[3]

ب)– القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة:

وهو أحد القوانين العربية الاسترشادية المعتمدة من طرف مجلس وزراء العدل العرب في المجال الالكتروني، وقد تضمن موضوع "حجية الكتابة والمحررات والتوقيع الالكتروني"، وقد أشار إلى تعريف مصطلح "المعاملات الالكترونية" في نص المادة الأول منه بقوله: " المعاملات الالكترونية

[1] لنظام الأساسي لمجلس وزراء العدل العرب، الصادر في 04 سبتمبر 1982، المعدل بالقرار رقم 159/ د8-22 / 04/1992 المادة 02

[2] لمادة 08، النظام الأساسي لمجلس وزراء العدل العرب

[3] المادة 16، النظام الأساسي لمجلس وزراء العدل العرب

هي كل إجراء أو مجموعة من الإجراءات تتم بين طرفين أو أكثر بوسيلة الكترونية بقصد إنشاء التزامات متبادلة أو على طرف واحد و تتعلق بالتزام مدني أو تجاري أو إداري [1]، وغيرها من النصوص القانونية الأخرى التي تضمنت كل ما يتعلق بالمحررات الالكترونية و التوقيع الالكتروني

ج)_ القانون العربي الاسترشادي للمعاملات والتجارة الالكترونية:

تضمن هذا القانون في مضمونه عدة مواضيع، أهمها "رسالة البيانات"[2]، "العقود الالكترونية "[3]الدفع الالكتروني"، إضافة إلى العقوبات المقررة في حال مخالفة ما ورد فيها من التزامات.

[1] القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، الصادر في 27 نوفمبر 2008، المادة 01.

[2] رسالة البيانات: عرفه قانون الأنسيترال النموذجي بشأن التجارة الالكترونية الصادر في 16 ديسمبر 1996، في المادة الثانية منه، بقولها " :يراد بمصطلح "رسالة بيانات المعلومات التي يتم إنشاؤها أو إرسالها أو لاستلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية، أو البريد الالكتروني، أو البرق أو التلكس أو النسخ البرقي

[3] عرفه قانون الأونسيترال النموذجي بشأن التجارة الالكترونية في المادة الثانية منه بقولها " :يراد بمصطلح "تبادل البيانات الالكترونية "نقل المعلومات الكترونيا من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات "

خاتمة

خاتمة:

في خاتمة دراستنا التي كانت تحت عنوان " خصوصية جريمة المساس بالأنظمة المعلوماتية في التشريع الجزائري " تمكنا من تحديد جملة من النتائج على النحو التالي:

_ إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعيا صريحا، من هذا المنطلق استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات"، وكذلك تقررت عقوبات للاعتداء على أنظمة المعلومات في قانون حماية حقوق المؤلف رقم 05/03، وبذلك حاول المشرع الجزائري أن يضع قواعد تتناسب وخصوصية الجريمة المعلوماتية.

_ أظهر البحث أن هناك صعوبة تكتنف الدليل بالنسبة للجريمة المعلوماتية سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلى عمليات فنية وعلمية وحسابية معقدة، كما أن طبيعته قد تكون غير مرئية، كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه وقد يتم ذلك عن طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة.

_ أظهر البحث أن هناك قصورا واضحا في الكثير من التشريعات الموضوعية والإجرائية في مواجهة ظاهرة الجريمة المعلوماتية، فمازال الكثير من هذه الجرائم تخضع للنصوص التقليدية وهو ما يترتب عليه الاعتداء على مبدأ الشرعية من جهة أو إفلات الكثير من الجناة من العقاب.

_ أظهر البحث كذلك أنه رغم التدخل التشريعي الموضوعي إلا أن هناك قصورا في التشريعات الإجرائية، ذلك أنه ما يزال يقف في حمايته للحرية الشخصية وحرمة الحياة الخاصة من الوسائل الالكترونية متجاهلا بذلك الإجراءات الضرورية للحصول على الدليل في الجريمة المعلوماتية ومعتمدا دائما على الإجراءات التقليدية، خاصة منها التفتيش والخبرة.

_ أظهر البحث كذلك تأثر قانون الإجراءات الجزائية في إثبات المسائل المتعلقة بالجريمة المعلوماتية وقوانين غير عقابية كالقانون التجاري والقانون المدني بظهور الشيكات الالكترونية والمحررات الالكترونية فيكون إثباتها بذلك مع الأدلة التي تتفق مع طبيعتها وعليه توجب تطوير هذه التشريعات الأخيرة غير العقابية كي تتسع نصوصها لهذه العمليات الالكترونية وتتجاوب مع الثورة الرقمية التي نعيشها اليوم.

وفي الأخير يجب أن يتلاءم تعريف الجريمة المعلوماتية مع فكرة عالمية المعلومات والاتصالات، بحيث يكون متفقا عليه على المستوى العالمي خاصة مراعاة التطور التكنولوجي الحاصل يوما عن يوم، ويجب توضيح الدور الذي يقوم به الحاسب الآليفي ارتكاب الجريمة.

وكمجل التوصيات من هذه الدراسة المتواضعة :

- يمكننا القول أن الجريمة الالكترونية اخدت ابعاد عالمية خصوصا مع توفر وسائل التكنولوجيا وسهولة الوصول اليها.
- تحصين المنظومات الدفاعية بالاستثمار في هذا المجال والتصدي لاي هجومات محتملة
- توعية الجيل الصاعد بمخاطر التكنولوجيا و وضغ الرقابة اللازمة عليها
- الاستشراف في هذا المجال بتكوين اطارات مختصة في هذا المجال
- تبادل الخبرات مع الدول التي تسبقنا في هذا المجال
- الامضاء على اتفاقيات اقليمية ودولية تنص على تجريم هذا النوع من الممارسات ووضع قوانين ردعية.

قائمة المصادر

والمراجع

قائمة المراجع:

- **الكتب:**

ـــ كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب،الطبعة 23/21.

ـــ عبد الله حسن محمود ، سرقة المعلومات المخزنة في الحاسب الالي ، دار النهضة العربية ، القاهرة 1998.

ـــ أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، 2002، ط 01.

ـــ اسامة احمد المناعسة ، جلال محمد زغبي ، جرائم الحاسب الالي و الانترنت ، دراسة تحليلية مقارنة ، دار وائل للنشر ، عمان الاردن الطبعة الوالى ، 2001

ـــ محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري ،دار الجامعة الجديدة ، الاسكندرية ،2007

ـــ عبد الفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الجريمة الالكترونية ، علم المعارف الاسكندرية ،الطبعة الاولى سنة 2009

ـــ عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيات الاتصالات الحديثة، دار النهضة العربية ، القاهرة، الطبعة الأولى، سنة 2009

ـــ أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة

ـــ خالد ممدوح إبراهيم، "التقاضي الإلكتروني"، دار الفكر الجامعي، الإسكندرية، 2009

ـــ محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الالي في القانون الجزائري ، دار الجامعة الجديدة ، الاسكندرية ،2007

ـــ محمود أحمد عبابنة، "جرائم الحاسوب و أبعادها الدولية"، دار الثقافة للنشر و التوزيع، عمان، 2005، المادة 323-1، القانون رقم 88-19.

ـــ نهلا عبد القادر، الجرائم المعلوماتية ، دارالثقافة للنشر ، عمان 2008 ، دار النهضة العربية القاهرة

ـــ علي عبد القادر القهوجي، "الحماية الجنائية لبرامج الحاسب الآلي"، (بط)، الدار الجامعية، بيروت، 1999.

ـــ خالد ممدوح إبراهيم، "أمن المستندات الالكترونية"، (دط)، الدار الجامعية، الإسكندرية، 2008

ـــ محمد عبيد الكعبي، "الحماية الجنائية للتجارة الالكترونية، (دط)، دار النهضة العربية، القاهرة، 2010

_ نائلة عادل محمد فريد قورة، "جرائم الحاسب الآلي الاقتصادية – دراسة نظرية و تطبيقية –، ط1، منشورات الحلبي الحقوقية، عمان، 2005.

_ عبد الله الهلالي ، تفتيش نظام الحاسب الالي وضمانات متهم المعلوملت ، دراسة مقارنة ، الطبعة الاولى ،القاهرة ، دار النهضة العربية

_ شريف محمد غنام – حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني – دار الجامعة الجديدة – 2007

_ محمد غنام ، حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني ، داؤ الجامعة الجديدة 2007،

_ عبد العال الدريبي، محمد صادق إسماعيل ، الجرائم الالكترونية النظام القانوني للحماية المعلوماتية ،الطبعة 01 المركز القومي للدراسات القانونية ، القاهرة 2012

_ عبد الحكيم رشيد توبة، جرائم تكنولوجيا المعلومات ، الطبعة 01 ، دار المستقبل للنشر والتوزيع ، عمان 2009

_ أحسن بوسقيعة، "الوجيز في القانون الجزائي الخاص – الجزء الأول–"، ط18، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2015.

- **المقالات والمداخلات:**

_ سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث .

_ رصاع فتيحة، رسالة الماجستير الحماية الجنائية للمعلومات الالكترونية ،جامعة محمد خيضر ، باتنة 2011

_ ايمان الحياري ، مقالة لمجلة الموضوع الالكترونية ، 4 ابريل 2022

_ نائلة عادل محمد فريد قورة – جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية – منشورات الحاتي الحقوقية 2005

_ محمد عبيد الكعبي ، مجلة الحقوق العدد 01 الطبعة الاولى

_ أحسن بوسقيعة، الوجيز في القانون الجزائي ، الطبعة6، دار هومة، الجزائر

_ عبد الله هلالي، تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، مصر

_ كمال عفيفي ، جرائم الكمبيوتر ، لبنان ،منشورات الحلبي الحقوقية ، سنة 2003

- **الرسائل والأطروحات:**

_ عادل يوسف عبدالنبي الشكري، بحث بعنوان: الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة، 2008.

_ برهيمي سهام، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2004، 2007،

_ حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة

_ طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1، كلية الحقوق، 2012، 2011.

_ سوير سفيان ، جرائم المعلوماتية ، مذكرة لنيل شهادة ماجستير في القانون تخصص علم الاجرام ، جامعة تلمسان

_ قربوز حليمة ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة تخرج لنيل اجازة المدرسة العليا للقضاء الجزائر . 2009

_ نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، مذكرة لنيل شهادة الماجستير، جامعة الجزائر 1، سنة 2017

_ المساس بأنظمة المعالجة الآلية للمعطيات جاءت في الفصل الثالث المعنون "الجنايات والجنح ضد الأموال"، من القسم الأول المعنون "السرقات وابتزاز الأموال".

_ مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006_2009

- **النصوص القانونية:**

_ المادة 06، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

_ المادة 08 من اتفاقية بودابست الخاصة بالاجرام الالكتروني 2001

_ المادة37/2 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف

_ المادة 40مكرر1 من قانون الإجراءات الجزائية الجزائري على ما يلي: "يخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل وبنسختين من إجراءات التحقيق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة"

_ محمد الأمين البشري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي

_ المادة 40 مكرر من قانون العقوبات الجزائية الجزائري على ما يلي:" تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد 37 ،40،329 من هذا القانون، مع مراعاة أحكام المواد من 40مكررا إلى 40مكررة".

_ مادة 163 من قانون الإجراءات الجزائية الجزائري على ما يلي: " إذا رأى قاضي التحقيق أن الوقائع لا تكون جناية أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو أن مقترف الجريمة ما يزال مجهولا، أصدر أمر بألا وجه لمتابعة المتهم

_ النظام الأساسي لمجلس وزراء العدل العرب، الصادر في 04 سبتمبر 1982، المعدل بالقرار رقم 159/ د8-22 / 04/1992 المادة 02.

_ القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، الصادر في 27 نوفمبر 2008، المادة 01

- **المواقع الالكترونية:**

_WWW.0ecd.org

الفهرس

الفهرس

إهداء

شكر وتقديم

مقدمة 1

الفصل الاول : خصوصية جريمة المساس بالأنظمة المعلوماتية في التشريع الجزائري.. 4

المبحث الأول : مفهوم جريمة المساس بالنظام المعلوماتي 4

المطلب الاول: تعريف الجريمة الالكترونية واقسامها 4

الفرع الاول: تعريف الجريمة الالكترونية 5

الفرع الثاني: أقسام الجريمة الالكترونية 8

المطلب الثاني: خصائص الجريمة المعلوماتية 12

الفرع الأول: السمات الخاصة بالجريمة المعلوماتية 12

الفرع الثاني: تصنيفات الجريمة الالكترونية 14

المبحث الثاني: المساس بأنظمة المعالجة الآلية للمعطيات 17

المطلب الأول: مفهوم نظام المعالجة الآلية للمعطيات 17

الفرع الاول: تعريفه في الاتفاقية الدولية للإجرام المعلوماتي 19

الفرع الثاني: تعريفه في التشريع الجزائي الجزائري 20

المبحث الثالث: جرائم المساس بأنظمة المعالجة الآلية للمعطيات 22

المطلب الأول: جريمة الدخول و البقاء غير المصرح به 22

الفرع الاول: الركن الشرعي 22

الفرع الثاني : الركن المادي 24

الفرع الثالث : الركن المعنوي 27

المطلب الثاني: جريمة التلاعب بمعطيات الحاسب الالي 28

الفرع الاول : الركن الشرعي 28

الفرع الثاني : الركن المادي 29

الفرع الثالث : الركن المعنوي 30

الفصل الثاني: مكافحة جرائم المساس بالأنظمة المعلوماتية 31

المبحث الاول : العقوبات المقررة على الجرائم الماسة بالانظمة المعلوماتية.....31
المطلب الاول: العقوبات الجزائية المنصوصة التي تعاقب جرائم الانظمة المعلوماتية.....31
المطلب الأول: جمالية الآليات الإيقاعية في معلقة امرئ القيس.....31
الفرع الاول : جريمة المساس بأنظمة المعالجة الالية للمعلومات..... 32
الفرع الثاني : جريمة التزوير المعلوماتي.....33
المطلب الثاني: قواعد الاختصاص المحلي و إجراءات التحقيق الابتدائي..... 35
الفرع الاول: قواعد الاختصاص المحلي.....35
الفرع الثاني:: إجراءات التحقيق الابتدائي:.....38
المبحث الثاني : جهود التعاون الدولي.....41
المطلب الاول: الجهود الدولية الغربية.....42
الفرع الاول : أهم الصكوك الدولية الخاصة بالجرائم الالكترونية.....42
الفرع االثاني : صعوبة التعاون الدولي لمكافحة الجريمة الالكترونية.....45
المطلب الثاني: الجهود الدولية العربية.....47
الفرع الاول : الاتفاقيات والقوانين.....47
الفرع الثاني : الهيئات العربية المستحدثة لمكافحة الجرائم المعلوماتية.....49
الخاتمة.....52
قائمة المصادر والمراجع.....54