جامعة 20أوت 1955 سكيكـــدة
كليـــة الحقـــوق والعلوم السياسية
قـــسم الحـــقـــوق

جريمة المساس بأنظمة المعالجة الآلية للمعطيات

مذكرة مكملة لنيل شهادة الماستر تخصص -قانون جنائي-

من تقديم الطالب (ة): إيمان حـــروج

المشـــرف: بوغاغة ياسمينة

لجنة المناقشـــة:

1- الأستاذ الدكتور فليغـــة نور الدين رئيسا

2- الأستاذة بوغاغة ياسمينة مشرفا ومقررا

3- الأستاذ بوصيدة فيصل مناقشـــا

دورة جـــوان 2014

بسم الله الرحمن الرحيم

شكر وعرفـــان

الحمد لله الذي أعانني على انجاز هذا العمل

حمدا يليق بجلال وجهه وعظيم سلطانه

أتقدم بخالص شكري إلى

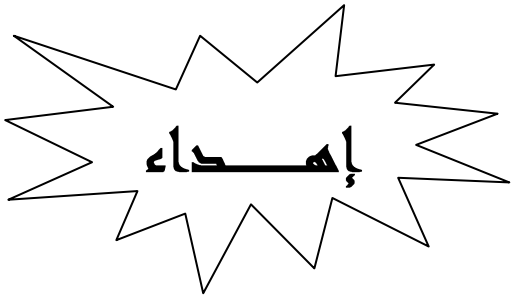
الأستاذة بوغاغة ياسمينة على رحابة صدرها وسعة بالها بأن تحمل مشقة الإشراف على هذا العمل

كما لا يفوتني أن أوجه خالص امتناني إلى:

الأستاذ بوغاغة إبراهيم على كل المجهودات الجبارة التي بدلها معي.

كل التبجيل والشكر الجزيل- سلفا- للأساتذة الكرام أعضاء لجنة المناقشة على تكبدهم مهمة معاينة وتقييم هذا العمل.

وإلى كل من أمدني بيد المساعدة ولو بالكلمة الطيبة شكرا لكم جميعا.



أصل البداية فكرة، وأصل الفكرة دوافع وما أصعب تجسيد الأفكار على أرض الواقع.

أهدي نتاج هذا الجهد وعصارة هذا العمل إلى كل الذين ساعدوني على جعل الفكرة واقعا وأخص بالذكر أعز الناس إلى قلبي:

* إلى التي أهدتني نور الحياة وسقتني من نفقات حبها ورعايتها ورسمت معي أحلام حياتي والدتي الحبيبة أطال الله في عمرها وأدامها لي تبعا صافيا أمحو به كدر الأيام.

* إلى الذي استلهمت منه معنى الثبات وزرع في قلبي حب العلم ووضع بين جنباتي القوة والعزيمة والدي العزيز، عرفانا بفضله ووفاء لعهده أطال الله في عمره.

* إلى زوجي الغالي تقديرا واحتراما.

* إلى إخوتي وأخواتي وفقهم الله.

* إلى الكتكوتة ابنة أختي نريمان حفظها الله ورعاها.

إيمـــان

مقــدمة

الجريمة ظاهرة اجتماعية تتواجد بتواجد الإنسان والمجتمع وتتطور بتطورهما، ولا شك أن المجرمين كما- رجال الأمن- يحاولون الاستفادة من هذا التقدم التقني خاصة وأننا في عصر ثورة المعلومات وتقدم العلوم الحديثة والتكنولوجيا المتطورة، و تبعا لذلك فإنه من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس قاصرا على الأسباب التقنية فقط بل يحدث دوما وبصفة مستمرة فالمجرم والجريمة في تقدم وتجدد مستمر فمجرم الأمس ليس كمجرم اليوم، وبالتالي فجريمة الأمس ليست كجريمة اليوم، وقد تمخضت ثورة المعلومات والتكنولوجيا المتقدمة عن وسائل اتصالات متطورة جعلت العالم قرية الكترونية مفتوحة للعموم، ألغت معها الحدود الجغرافية والسياسية للدول، وهذه التقنية الخاصة بنظام نقل المعلومات السريع أو ما يعرف بالإنترنت ليست سيئة في حد ذاتها بل هي سلاح ذو حدين فيمكن أن تسخر للخير والمنفعة كما يمكن أن تسخر للشر والمضرة.

ومع شيوع الإنترنت، تزايدت جرائم الكمبيوتر واستغلال الكمبيوتر والشبكات في الأنشطة الإجرامية وهي تدق أجراس الخطر لتنبيه مجتمعات العصر الراهن إلى حجم المخاطر والخسائر الناتجة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات، معلومات، برامج مكافحة أنواعها....) يرتكبها أشخاص أذكياء يمتلكون أدوات المعرفة التقنية التي يستخدمونها في الاعتداء على الحق في الخصوصية

المعلوماتية على معطيات الكمبيوتر المخزنة وعلى المعلومات المنقولة عبر نظم وشبكات الإنترنت.

ومع أن الإجرام المعلوماتي لم يتخذ في الواقع الجزائري بعد، والواقع العربي كتلك الأبعاد التي اتخذها في الدول المتقدمة، إلا أن ذلك لا ينفي ضرورة التصدي لبوادره كي لا يستفحل مع وتيرة النمو المتسارع الذي تشهده دول عربية عدة، ومن بينها الجزائر في استخدام النظم المعلوماتية، حيث بادر المشرع الجزائري توجيه الأنظار إلى طائفة من الأفعال في بيئة المعالجة الآلية للبيانات تقتضي مصلحة المجتمع الملحة إدخالها في دائرة التجريم والعقاب.

أهمية الموضوع :

– يرجع دراسة هذا الموضوع للتعريف بظاهرة جديدة هي:" جريمة المساس بأنظمة المعالجة الآلية للمعطيات " التي بدأت بالظهور والانتشار، وارتبطت بتكنولوجيا متطورة هي تكنولوجيا الحاسبات الآلية، حيث تتميز بخصائص تختلف عن غيرها من الجرائم مما يستطيع ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية.

– كون هذه الجرائم ترتبط بتقدم المجتمعات وذلك من خلال زيادة اعتماد المجتمع على الحاسبات الآلية كما زاد معدل جريمة المساس بأنظمة المعالجة الآلية للمعطيات

ولمواجهتها سواء من الناحية القانونية وهو عمل المتخصصين في مجال تكنولوجيا المعلوماتي أو من الناحية القانونية وهي مهمة المشتغلين بالقانون.

– ثم ما يزيد من أهمية الموضوع صدور القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات والتي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية كذلك صدور القانون 04/09 المـــــــؤرخ في 05أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بغرض الكشف عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات ومرتكبيها.

– وتكمن أهمية هذه الدراسة في أنه وعلى الرغم من أن ظهور صناعات البرامج لا زال حديثا إلا أنها اكتسحت جل مجالات الحياة بما فيها الحياة العادية للفرد فضلا عن دورها الفعال في المجالات العملية بشتى أشكالها إدارية ، اقتصادية، تعليمية،....وغيرها وهذا ما زاد من أهمية هذا النوع من الصناعة مما كان سببا في بروز الأهمية القصوى إلى حماية هذه البرامج جنائيا وذلك لردع المخالفات التي قد تقع عليها وكذلك سدا للفراغ القانوني الذي قد يحدث إثر ذلك ، كما أن حماية هذه البرامج له أثر في الدفع بعجلة الابتكار، وذلك لأنها تضمن لمنتجي هذه البرامج الحصول على مقابل إنتاجهم أو مقابل تفجير ملكاتهم ببزوغ مجال آخر من مجالات التأليف والازدهار الفكري.

دوافع اختيار الموضوع:

لا يخفى أن لاختيار أي موضوع بحثي من دوافع محركة ذاتية لدى الباحث وأخرى موضوعية.

الدافع الذاتي:

هو نابع من إيماننا بالعدالة وضرورة احترام وحماية القيم الاجتماعية جنبا إلى جنب مع احترام حقوق الإنسان، وإيماننا بأن أساليب الإجرام يتطور مع تطور أساليب مكافحته وتقدم التكنولوجي هذا ما أدى إلى ظهور جريمة المساس بأنظمة المعالجة الآلية للمعطيات وكون النصوص التقليدية ليست فعالة لمواجهة هذا النوع من الإجرام.

وكذلك ميولنا الشخصية للبحث والخوض في موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات كونها خطر يهدد الأمن ولابد من التصدي لها لأنها في تطور وتزايد مستمر.

الدافع الموضوعي:

يستمد من أهمية هذا النوع من الإجرام الذي يتميز بطابعه العابر للحدود واختلاف أفعاله الإجرامية وطبيعة أدلته عنه في الإجرام التقليدي.

وما شجعنا أكثر للخوض في هذا البحث هو حداثة الموضوع في التشريع الجزائري بجوانبه الموضوعية والإجرائية، وقد واجهتنا ندرة المراجع الوطنية التي تبحث في الموضوع وافتقار مكتبتنا الوطنية لمثل هذا البحث، وهو أمر لم يثنينا عن تبنيه كموضوع بحثي وإضافة إثراء لهذه المكتبة.

أهداف اختيار الموضوع:

- تسليط الضوء على حداثة هذا النوع من الإجرام وخطورته وزيادة انتشاره وتطوره مع تطور التقنيات التكنولوجية.

- تنبيه الباحثين إلى دراسة هذه الجريمة في مختلف جوانبه كونها تتميز بالاتساع وصعوبة وغرابة مصطلحاتها عن رجال القانون.

صعوبات الدراسة:

- تكمن الصعوبة في تطبيق النصوص التقليدية على هذه الجرائم وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة هذه الجريمة، لذا فإن إدراك ماهيتها وخصائصها والطبيعة الموضوعية لها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم وأنواعهم وأركانها وأدلة إثباتها وطبيعة الدليل المعلوماتي الذي يختلف عن الدليل التقليدي وجزاءاتها يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة، وإذا كان مجتمعنا الجزائري تأثر بعد بشكل ملموس فعلا بمخاطر هذا النمط المستجد من الإجرام، فإن خطر الجريمة المعلوماتية المحتمل في بيئتنا يمكن أن يكون كبيرا باعتبار أن الجاهزية التقنية والتشريعية والأدائية (استراتيجيات حماية المعلوماتية) لمواجهتها ليست بالمستوى المطلوب وإن لم تكن غائبة تماما.

- صعوبة بعض المصطلحات المتعلقة بالجريمة.

الإشكالية:

وفيما يخص الإشكالية الأساسية فتتمثل في إبراز المشاكل القانونية التي ظهرت بظهور المعلوماتية في نطاق القانون الجنائي وقانون الإجراءات الجزائية، خاصة فيما يتعلق منها بطبيعة المال المعلوماتي باعتباره مالا معنويا، في حين أن الحماية الجزائية للمعلوماتية تقتصر في أغلب الدول على المال المادي، وقصور قواعد الإجراءات الجزائية في مواجهة الإجرام المعلوماتي خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق.

والذي سنعالج موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات من خلال الإشكالية الرئيسية:

– ما طبيعة جريمة المساس بأنظمة المعالجة الآلية للمعطيات؟ وهل تختلف عن غيرها من الجرائم المنصوص عليها في قانون العقوبات؟

أما الإشكاليات الفرعية هي:

– كيف عالج المشرع الجزائري موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات؟

– هل تفي النصوص التقليدية للحد من هذا النوع من الجرائم؟ أم يلزم تعديل هذه النصوص بما يتلاءم مع التطور التقني للمعلوماتية؟

المنهج المتبع:

من أجل دراسة هذا البحث ضرورة استعمال بعض المناهج العلمية من خلال الاعتماد على المنهج الوصفي لبيان ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات، واستعمال المنهج التحليلي لتحليل أحكام النصوص القانونية التي تناولت هذا النموذج الإجرامي بالخصوص مواد قانون العقوبات وقانون الإجراءات الجزائية، وأحكام القانون 15/04 المعدل والمتمم لقانون العقوبات، وكذلك أحكام القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبعض النصوص في القوانين المقارنة.

الخطة المتبعة ومبرراتها:

لابد من الاعتراف أن الإجابة عن الإشكالية التي يطرحها موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالمعطيات والتي نكتشفها بصدد ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات وخصائصها وموضوعها ودور الحاسوب فيها وأركان الاعتداء على أنظمة المعالجة الآلية للمعطيات والاعتداءات على منتوجات الإعلام الآلي.

لذلك ارتأينا أن تكون نقطة الانطلاق من عنوان رسالتنا "جريمة المساس بأنظمة المعالجة الآلية للمعطيات" وعلى هذا الأساس فإن الموضوع محل البحث ستتم دراسته في إطار القانون الجنائي الخاص باعتبارنا سنتعرض للجريمة ببعض جوانبها وأركانها وسبل مواجهتها وإثبات الجريمة والجزاءات المقررة لها.

لهذا الغرض قسمنا موضوع البحث إلى فصلين، نتعرض في الفصل الأول لماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات باعتبارها جريمة مستحدثة ومتميزة عن باقي الجرائم التقليدية، وله مبحثين، المبحث الأول نتناول فيه مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات، أما المبحث الثاني فنتناول فيه أركان جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

أما الفصل الثاني فنتناول فيه قمع هذه الجريمة وقسمناه هو الآخر إلى مبحثين، خصصنا المبحث الأول لدراسة القواعد الإجرائية لمكافحة الجريمة، أما المبحث الثاني نتناول فيه كيفية إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات والجزاءات المقررة لها.

الفصل الأول

ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تعد جريمة المساس بأنظمة المعالجة الآلية للمعطيات من أحدث الجرائم التي لم يتوقعها المجتمع البشري، مما أدى إلى إثارة ضجة في الأوساط الفقهية بخصوص ماهيتها وخصائصها واختلاف مرتكبيها ودوافع ارتكابهم لها، وموضوعها ودور الحاسوب فيها والأفعال المجرمة التي تدخل في نطاقها كون هذه الجريمة ظاهرة إجرامية تستهدف استخدام التطورات التكنولوجية بدلالتها التقنية الواسعة[1].

لذلك ارتأينا التعرض في الفصل الأول والذي تم تقسيمه إلى مبحثين، لنتطرق في المبحث الأول لمفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات وخصائصها وأنواع مرتكبيها ودوافع ارتكابهم للجريمة وموضوعها ودور الحاسوب في الجريمة، أما المبحث الثاني لدراسة أركان جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

المبحث الأول

مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات

لقد ذهب البعض بأن جرائم الحاسبات لا يوجد مصطلح موحد للدلالة عليها، فالبعض يطلق عليها بجريمة " الغش المعلوماتي" والآخر يطلق عليها " جريمة المساس

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2007، ص35.

بأنظمة المعالجة الآلية للمعطيات" والآخر يطلق عليها " ظاهرة الاختلاس المعلوماتي" والآخر يطلق عليها " جناح المعلوماتية"، مما صعب إيجاد تعريف موحد باعتبار أن هذه الظاهرة حديثة نسبيا، مما يخشى معه حصرها في نطاق محدد[1].

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر، منشأة المعارف، الإسكندرية، د. ط، ص18.

المطلب الأول

مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات وخصائصها

تقتضي دراسة مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات التطرق في هذا المطلب بالبيان والتوضيح ضمن فرعين، الأول تخصصه لتعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات، أما الفرع الثاني فنخصصه لتحديد خصائصها.

الفرع الأول

تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تعرف الجريمة شرعا بأنها" إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم معاقب على تركه، أو هي فعل أو ترك فعل نصت الشريعة على تحريمه والعقاب عليه"[1].

أما التعريف القانوني للجريمة " هي كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية[2].

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، د. ط، 2007، ص37.

[2] g. Stéfani,g. le vasseur, b. bauloc : droit général Dalloz,17éme édition p.5.

أحسن بوسقيعة ، الوجيز في القانون الجزائي العام، ، دارهومة، الجزائر، الطبعة العاشرة ،2011، ص27. راجع: منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم، عنابة، د. ط، 2006، ص83.

هذا فيما يخص تعريف الجريمة، وقبل التطرق إلى تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات(للمعلوماتية) كان لابد من توضيح معنى المعلوماتية.

أولا: تعريف المعلوماتية.

المعلوماتية أو علم المعلوماتية Science Informatics or Information وهو عبارة عن العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها واختزانها، واسترجاعها ثم بتفسيرها وإعادة بثها أو تحويلها واستخدامها، والبحث في تمثيل المعلومات في النظم الطبيعية والصناعية و الإدارية واستخدام الرموز والأكواد في نقل الرسالة والتعبير عنها بكفاءة، وكذلك دراسة أساليب معالجة المعلومات كالأنظمة المعلوماتية ونظم البرمجة، ونظرا لهذا المفهوم فإن المعلوماتية " كعلم" لها صلة بالكثير من العلوم الأخرى ولعل أهمها علوم الأنظمة المعلوماتية Cybernetie وعلوم المكتبات والتوثيق، وأيضا بعلوم اللغويات، والإحصاء والرياضيات والإدارة وبحوث العمليات ونظريات النظم والاتصال والقانون[1].

ومصطلح المعلوماتية هي المعالجة الآلية للمعطيات وهي ترجمة من اللغة الفرنسية لكلمة informatique وتعني تكنولوجيا و معالجة وإرسال المعلومات بواسطة الكمبيوتر[2].

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الثانية، 2006، ص78.

[2] مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، د. ط، 2010، ص19.

وإن أول من استعمل هذا المصطلح هو ميخالوفAI. Mikhaïlov مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي، وقد سماه " بعلم المعلومات العلمية"، ثم ذاع استخدامه بعد ذلك على مستوى جغرافي واسع بمفاهيم متباينة حتى أحصى له البعض أكثر من ثلاثين تعريفا مختلفا في الكتابات المتخصصة في علم المعلومات[1].

ولقد شاع استعمال كلمة المعلوماتinformation منذ خمسينات القرن الماضي في مجالات مختلفة وسياقات شتى مما جعل لها في الاستعمال الدارج مفاهيم متنوعة.

فالمعلومة لغويا مشتقة من كلمة علم ودلالتها فيها، وتدور حول المعرفة التي يمكن نقلها واكتسابها، وإشارتها قريب في اللغة الفرنسية إلى فحوى عمليات الاتصال التي تستهدف نقل وتوصيل إشارة أو رسالة أو الإعلام عنها واتخاذ وظيفتها في نقل المعارف. Transfert de connaissance

والمعلومات في اللغة الانجليزية والألمانية والروسية تعني كلمة information اللاتينية الدالة بحسب الأصل على شيء للإبلاغ والتوضيح على علمية Process الإبلاغ أو النقل أو التوصيل وهو نفس ما يعنيه لفظ Ximxi المقابل لها في اللغة الصينية.

[1] سامي علي حامد، المرجع السابق، ص35.

أما اصطلاحا فهناك مئات من التعريفات التي أدلى بها باحثون من تخصصات وثقافات مختلفة لفهم وإدراك المعنى المراد بمصطلح "المعلومات" إذا ما استخدم الاتصال العلمي بغير تحديد[1].

وحتى هذه اللحظة لا يوجد تعريف قانوني يعطي تعريفا جامعا مانعا للمعلومة عدا التعريف المشار إليه في القانون الفرنسي الصادر في 29 جويلية 1982 بشأن الاتصالات السمعية والبصرية، وهو أو تعريف عام للمعلومة، وقد عرفها بأنها " رنين صور الوثائق والبيانات أو الرسائل من أي نوع"[2]، ويعرف الأستاذ كاتالا (Catala) المعلومة بأنها " رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير[3]ويعرفها البعض الآخر بأنها" رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى"[4].

وتتميز المعلومة بخصائص، فلا بد أن تكون المعلومة محددة، وإذا انعدم التحديد فلا تكون المعلومة محل حماية، فالأستاذ كاتالا (Catala) يرى" أن المعلومة هي أولا تعبير وصياغة مخصصة لتبليغ رسالة وهي من ثم قابلة للتبليغ بواسطة علامات مختارة لكي تنقل رسالة للغير"، ولا بد أن تكون المعلومة مبتكرة فإذا كانت شائعة يسهل الرجوع إليها من قبل الكافة فلا تكون مبتكرة، ولا تكون محل للحماية، وأن تكون المعلومة سرية كونها هي سبب حيازتها وأي اعتداء عليها هو فعل يستحق العقاب كسر تركيب الدواء وأسرار

[1] أحمد خليفة الملط، المرجع السابق، ص73.

[2] مسعود خثير، المرجع السابق، ص15.

[3] Pierre Catala «la propriété de l'information» cité parf. Toubal, le logiciel-analyse juridique FUDUL.L.G.D.J.1986. P127.

[4] أحمد خليفة الملط، المرجع السابق، ص74.

شركة تجارية من حيث رأس مالها، كذلك لا بد أن يكون هناك استئثار بالمعلومة، بمعنى حيازة المعلومة من شخص بحيث يصبح هو المتصرف الوحيد فيها، وهناك من يشترط أن تكون المعلومة معالجة آلية لكي تخضع للتجريم ويقصد بها العمليات المتعددة والتي تتم بصفة آلية على معلومات لكي تتحول إلى معطيات عن طريق معالجتها داخل نظام آلي[1].

ففي أو السبعينات ازدهرت صناعة جديدة حيث أطلق عليها بصناعة المعلومات وأصبحت مصدرا للثروة وتتصف بعظمة التعقيد التقني والتدقيق وضخامة ما يستثمر فيها من أموال وأصبحت مقياسا لتقدم الأمم ومصدرا للقوة الاقتصادية والسياسية والعسكرية ومورد لا يقل ولا ينضب وتتزايد دوما ولا تتناقص بالاستخدام، ولا تستهلك ولا ترتبط بالزمان والمكان وتتفاعل مع التطور، وهي في الحقبة المعاصرة مفتاح للموارد الأخرى وسلعة وخدمة تباع وتشترى ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كل جوانب الحياة المعاصرة وأصبح توفيرها وحسن استغلالها من الأسس الضرورية لدفع عجلة التقدم في الأمم والمجتمعات وصار تدفقها وانسيابها بمثابة النبض والعصب لجهود التنمية والتحديث والرقى المعرفي والحضاري، وبات الوعي بأهميتها مظهرا ومقياسا لتقدم الدول.

[1] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، د. ط، 2004، ص42.

وفي الأخير أن المعلوماتية هي علم المعالجة العقلية للمعلومات باستخدام آلات تعمل ذاتيا.

"la science du traitement rationnel par des machines automatiques d'information notamment"[1]

وإن هذا التعريف للمعلوماتية هو الأقرب إلى الصحة حيث يضع المشكلة في مكانها الصحيح إذ يتضمن المعلومات التي يتم تجميعها بمعرفة الإنسان والتي تتمتع بالتحديد والابتكار والسرية والاستئثار والمجمعة عن طريق شبكات المعلومات ويتم معالجتها آليا وفقا للأنظمة المعلوماتية[2].

ثانيا: التعريفات المختلفة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

لم يضع المشرع الفرنسي تعريفا قانونيا واضحا وشاملا للجريمة المعلوماتية حيث تولى رجال الفقه مهمة تعريفها، في حين أن المشرع الجزائري وعلى خلاق المشرع الفرنسي فلم يضع تعريفا لها إلا مؤخرا من خلال المادة 2 الفقرة الأولى من القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق لـــ 5 أوت 2009 المتضمن " القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها " والذي دخل حيز النقاد بموجب الجريدة الرسمية/ العدد 147 الصادرة بتاريخ 16 أوت 2009 وتجدر الإشارة أن التعريف الذي ورد في هذا القانون جاء حسب رأينا عاما وخالي من

[1] سفيان سوير، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، تلمسان، 2011، ص11.

[2] أحمد خليفة الملط، المرجع السابق، ص73-81.

أي دقة تقنية حيث اكتفى المشرع بها على أنها كل الجرائم سواء المتعلقة بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب ويكون ارتكابها باستعمال منظومة معلوماتية أو أي نوع آخر من نظم الاتصال الالكتروني حسب مضمون الفقرة (أ) من القانون السالف الذكر وبالتالي سنتعمق أكثر لتعريف هذا النوع الخاص من الجرائم في نظر مختلف فقهاء القانون بعد تحديد المصطلحات القانونية التقنية المرتبطة بها[1].

أ – تحديد مصطلحات المستخدمة للدلالة على جريمة المساس بأنظمة المعالجة الآلية للمعطيات:

فابتداء من اصطلاح إساءة استخدام الكمبيوتر مرورا باصطلاح احتيال الكمبيوتر، جريمة المساس بأنظمة المعالجة الآلية للمعطيات، فاصطلاحا جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية ..... وغيرها إلى جرائم الهاكرز أو الاختراقات، فجرائم الإنترنت وجرائم نظم المعلومات .....وأخيرا سيبركريم Cyber crime[2].

ومن خلال الأبحاث والدراسات التي أجريت بشأن تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات والكتابات التي تناولها البعض أنه لا يوجد مصطلح موحد للدلالة عليها وذلك خشية حصرها في مجال ضيق يمكن أن يضر بها ولكن بات من الضروري

[1] نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي، جامعة قسنطينة، 2013، ص ب.

[2] محمد محمود المكاوي، الجوانب الأخلاقية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية، مصر الطبعة الأولى، 2010، ص24. راجع: نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، د. ط، 2008، ص49.

أن يوضع تعريفا لها يشمل العناصر الأساسية التي تسمح بتحديدها[1]، هذا ما أدى إلى تباين الآراء الفقهية لتعريفها فهي متفاوتة فيما بينها ضيقا واتساعا ويمكن تصنيفها إلى أربع فئات التالية[2]:

- تعريفات مرتكزة حول وسيلة ارتكاب الجريمة
- تعريفات مرتكزة حول موضوع الجريمة
- تعريفات مرتبطة بتوافر المعرفة بتقنية المعلومات
- تعريفات مختلفة ومتنوعة

1- تعريفات مرتكزة حول وسيلة ارتكاب الجريمة

أي أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر كوسيلة لارتكابها، فيعرفها الفقيه الألماني تيدمانTiedemain بأنها" كل أشكال السلوك غير المشروع" أو الضارب بالمجتمع" الذي يرتكب باستخدام الحاسب.

كذلك التعريف الذي أقره المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف جريمة المساس بأنظمة المعالجة الآلية للمعطيات " بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"، بوجه عام الجرائم المعلوماتية قد تكون سرقة أو غسيل أموال وتحويلها من حساب لآخر، تدمير

[1] أحمد خليفة الملط، المرجع السابق، ص83.

[2] سامي علي حامد عياد، المرجع السابق، ص38.

المعلومات أو الاحتيال أو تزوير البطاقات الشخصية أو بطاقات الائتمان أو باستخدام البريد الالكتروني، واستخدام صور القذف والإساءة للمجني عليهم بالذم أو التشهير والتقاط الرسائل المفتوحة وكذلك البطاقات الالكترونية المتبادلة بواسطة البريد الالكتروني[1].

ويعرفها كذلك مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب Computer crime بأنها "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[2].

وهناك من يعرفها بأنها" كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية[3]. أو تعريفها " تلك الجريمة التي يكون قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسب"، أو بعبارة أخرى:" تلك الجرائم التي يكون دور الحاسب فيها ايجابيا أكثر منه سلبيا"[4].

وإن التعاريف المعتمدة على الوسيلة المستخدمة في ارتكابها قد تم نقدها مفاده أنه لكي تعرف الجريمة يجب الرجوع إلى العمل الأساسي المكون لها وليس فحسب، إلى الوسائل المستخدمة لتحقيقه " وليس لمجرد أن الحاسب قد استخدم في الجريمة، كما يقول فريق آخر أن تعتبرها من الجرائم المعلوماتية[5].

---

[1] زيدان زيبخة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، د. ط، 2011، ص43.

[2] سامي علي حامد عياد، المرجع السابق، ص38. راجع: أحمد خليفة الملط، المرجع السابق، ص84.

[3] **www.droit-dz.com/forum**، تاريخ التصفح 18مارس2014 الساعة00 11h صباحا. راجع: أحمد خليفة الملط، المرجع السابق، ص85.

[4] محمد محمود المكاوي، المرجع السابق، ص29.

[5] سامي علي حامد عياد، المرجع السابق، ص39.

2- تعريفات مرتكزة حول موضوع الجريمة:

يرى واضعو هذه التعريفات أن النظام المعلوماتي ليس أداة لارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات بل هي التي تقع على النظام أو داخل نطاقه.

وقد عرفها روزنبلات Rosanblatt وخبراء آخرين بأنها" كل نشاط غير مشروع موجه إما لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الأنظمة أو المحمولة أو المتبادلة عن طريقها " بمعنى أنها كل سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات أو بتحويلها[1].

وتعرفها الدكتورة هدى قشقوش بأنها" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[2].

فلقد حاول هذا التعريف تجاوز الوقوع في المنزلقات، إلا أنه جاء في الوقت ذاته عام يفقد التعريف ذاته مقدرته على بيان أركان الجريمة وتحديد الأفعال المنطوية تحتها، وإن هذه التعريفات لا تستند في الحقيقة إلى موضوع الجريمة بالمعنى القانوني الذي هو محل الاعتداء، وإنما ركزت على أنماط السلوك الإجرامي وأبرزتها متصلة بالموضوع لا الموضوع ذاته[3]، وقد تم نقد هذه التعاريف المعتمدة على المعيار الموضوعي للجريمة

[1] نسرين عبد الحميد نبيه، المرجع السابق، ص56.

[2] عادل غرام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة غبر الوسائط الالكترونية، دار الثقافة ، عمان، الطبعة الأولى، 2011، ص39.

[3] نسرين عبد الحميد نبيه، المرجع السابق، ص57 .

كون محل الجريمة ليس المال إلا في الأحوال التي يستخدم فيها الكمبيوتر وسيلة لارتكاب جرم استيلاء على مال[1].

3- تعريفات مرتبطة بتوافر المعرفة بتقنية المعلومات:

تقوم على أساس سمات شخصية لدى مرتكب الفعل، وهي تحديد سمة الدراية والمعرفة التقنية من هذه التعريفات، تعريف دافيد ثومسون David thompson بأنها" أية جريمة يكون متطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب، ومن هذه التعريفات أيضا تعريف سولانز A.Solanz تحت هذا النمط " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[2]، وعرفتها وزارة العدل الأمريكية معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها العام 1979م بأنها:" أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها[3].

ويمكننا القول بأن شرط المعرفة التقنية، شرط شخصي متصل بالفاعل وقد لا تتوافر لدى بعضهم المعرفة بتقنية المعلومات كونها يرتكب جزء كبير منها من قبل مجموعة تتوزع أدوارهم بين التخطيط والتنفيذ والتحريض والمساهمة[4].

4- تعريفات مختلفة ومتنوعة:

تشير هذه التعريفات أن مصطلح " جريمة الحاسب" متعلق بالمعرفة بالحاسب أو استخدامه شرطا ضروريا لارتكابها، والقول كذلك بأن ما يسمى بجريمة الحاسب يتضمن

[1] المرجع نفسه، ص59 .

[2] أحمد خليفة الملط، المرجع السابق، ص86.

[3] محمد محمود المكاوي ، المرجع السابق، ص30.

[4] نسرين عبد الحميد نبيه، المرجع السابق، ص59.

تقريبا أي ضرب من النشاط الموجه ضده، أو المنطوي على استخدام " نظام الحاسب"[1]، وعند فريق آخر هي أية واقعة تتضمن ثنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب، هذا التعريف بين لنا الهدف من وراء ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات وهو الحصول على مكسب[2].

أما التعريف البلجيكي من طرف خبراء متخصصون في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية"O E C D" بأنها" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[3].

وقد عبر خبراء المنظمة الأوربية للتعاون الاقتصادي عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات بأنها " كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"[4].

وباستقرائنا لمختلف التعريفات نجد أن تعريف منظمة التعاون الاقتصادي والتنمية (O E C D) الخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها بأن الجرائم المعلوماتية هي" كل فعل أو امتناع من شأنه الاعتداء على الأموال

[1] سامي علي حامد عياد، المرجع السابق، ص41.

[2] **www.droit-dz.com/forum**، المرجع السابق، تاريخ التصفح 22 مارس 2014 الساعة 03h 00 مساءا.

[3] عبد الله عبد الكريم عبد الله، المرجع السابق، ص15.

[4] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، د. ط ، 2009، ص6.

المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1] يتسم بالوضوح وذلك للأسباب التالية:

- تحديد ماهية السلوك الإجرامي للجريمة التي تقع به، إذ شمل كل من الفعل الايجابي والسلوك السلبي المتمثل في الامتناع.

- تعريف واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة الجرائم التقنية وذلك لربطه بين الجريمة وأي تدخل للتقنية المعلوماتية بصفة مباشرة أو غير مباشرة.

- يتيح إمكانية التعامل مع التطورات المستقبلية التقنية إذ بنصه على "تدخل التقنية المعلوماتية" يفتح المجال لكامل صور هذه التقنية القديمة والجديدة والمستقبلية.

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هذه الجريمة.

وقد اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وعرفها بموجب أحكام المادة 02 من قانـــــــــون 09-04 على أنها " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[2].

[1] أحمد خليفة الملط، المرجع السابق، ص87.

[2] سفيان سوير، المرجع السابق، ص15.

ومن خلال استقراء التعريف المعتمد من طرف المشرع الجزائري يمكن استخلاص الملاحظات الآتية:

- أنه اصطلح على الجرائم المعلوماتية بتسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- أن المشرع الجزائري اصطلح على الجرائم الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر07 وترك مجال واسع لأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

- المشرع الجزائري لم يحدد صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية.

- أن هذا التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الالكترونية يندرج تحت مصطلح المنظومة المعلوماتية ذلك أن المشرع عرف هذه الأخيرة بموجب أحكام المادة 02 من القانون 04/09 على أنها" نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

وحسب رأينا فإن تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات الأقرب إلى الصواب هو كل اعتداء على النظام المعلوماتي أو كل اعتداء يتم باستخدام النظام المعلوماتي وكان له دور رئيسي في السلوك المجرم[1].

[1] سفيان سوير، المرجع نفسة، ص16- 17.

وترجع أهمية الجهود المبذولة لوضع تعريف لهذه الجريمة إلى أهمية مساعدة المحقق الجنائي على معرفة أركان الجريمة وعناصرها وفقا للقانون، ورسم خطته عند جمعه للأدلة المعلوماتية[1].

الفرع الثاني

خصائص جريمة المساس بأنظمة المعالجة الآلية للمعطيات

نظرا لوقوع هذه الجريمة في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء عبارة عن نبضات الكترونية، فإننا أمام ظاهرة إجرامية ذو طبيعة خاصة ذات صلة بما يعرف عن البعض بالقانون الجنائي المعلوماتي، ووقوع هذه الجرائم في بيئة المعالجة الآلية للبيانات يستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي يتوافر فيه إمكانيات لتصحيحها، تعديلها، محوها، تخزينها،استرجاعها، وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولا بد من فهم الجاني لها كما في حالة التزوير والتقليد مثلا، وكذلك نتعامل مع مفردات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء[2].

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009، ص113.

[2] عفيفي كامل عفيفي، المرجع السابق، ص21.

ونظرا لارتباط جريمة المساس بأنظمة المعالجة الآلية للمعطيات بجهاز الحاسوب وشبكة الإنترنت والتي تتميز بالطابع الخاص عن الجرائم التقليدية لصعوبة كشفها واثبات الجريمة الأولى دون الثانية وذلك للأسباب الآتية[1].

أولا: جريمة المساس بأنظمة المعالجة الآلية للمعطيات جريمة عابرة للحدود[2]

تؤثر جريمة المساس بأنظمة المعالجة الآلية للمعطيات على أماكن متعددة في دول مختلفة في آن واحد مما يثير صعوبة تحديد الدولة صاحبة الاختصاص القضائي وحول تحديد القانون الواجب التطبيق.

ثانيا: صعوبة اكتشاف جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تتميز بصعوبة كشفها ويتم اكتشاف معظمها إن لم يكن جميعها بالصدفة البحتة والدليل على ذلك كما يؤكد البعض أنه لم يكتشف إلا بنسبة 1% فقط منها وإن 15% منها تم الإبلاغ عنها، وإن خمس النسبة الأخيرة هي التي يصدر فيها أحكام بإدانة مرتكبيها[3].

ثالثا: صعوبة إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات

[1] نهلا عبد القادر المومنى، الجرائم المعلوماتية، دار الثقافة ، عمان، د. ط، 2008، ص50.

[2] من القضايا التي لفت النظر إلى البعد الدولي لجرائم الحاسبات الآلية، قضية مرض نقص المناعة المكتسبة(الايدز) لعام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من البرامج تحتوي على نصائح لمرض نقص المناعة لكن في حقيقته كان يحتوي على فيروس حصان طروادة الذي يقوم بتعطيل جهاز الحاسوب عن العمل. راجع: سفيان سوير، المرجع السابق، ص20.

[3] عفيفي كامل عفيفي، المرجع السابق، ص22.

إن اكتشاف جريمة المساس بأنظمة المعالجة الآلية للمعطيات أمر ليس بالسهل، ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعوبات.

رابعا: أسلوب ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تتطلب الجرائم التقليدية نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما في جريمة السرقة ....الخ، فإن الجرائم المعلوماتية لا عنف لها ولا جثث لقتلى ولا آثار للدماء أو اقتحام من أي نوع وإنما تحتاج إلى القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

خامسا: جريمة المساس بأنظمة المعالجة الآلية للمعطيات تتم عادة بتعاون أكثر من شخص

تتم عادة جريمة المساس بأنظمة المعالجة الآلية للمعطيات بتعاون أكثر من شخص على ارتكابها إضرار بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود لشخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج مؤسسة المجني عليه لتغطية عملية التلاعب وتحويل المكاسب إليه.

سادسا: خصوصية مجرمي المعلوماتية وضحاياها ونوعية جرائمهم

كما تتميز جريمة المساس بأنظمة المعالجة الآلية للمعطيات بخصائص كذلك مرتكب هذه الجريمة أو ما يسمى بالمجرم المعلوماتي، وهو ليس شخصا عاديا كما هو الحال في الجريمة التقليدية وإنما هو شخص ذو مهارات تقنية عالية، من خلال قدرته على استخدام خبراته في اختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسب بشكل غير مشروع، وهذا ما يبين لنا تطور أعمال الإجرام، وانتقالها من عالم المجرمين البؤساء إلى عالم مجرمي المهارات المعلوماتية من ذوي الياقات البيضاء والسمات الخاصة[1].

أ- من حيث الجناة

إذا كان المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الحاسبات الآلية فلا بد أن يكون إنسانا اجتماعيا يحيا وسط المجتمع يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية وأيضا فلا بد أن يكون شخصا محترفا يتمتع بقدر كبير من الذكاء[2]، ويختلف الإجرام المعلوماتي (الالكتروني) عن الإجرام التقليدي من حيث أن المجرم في هذا الشأن يحيا وسط مجتمع ويمارس في المجال المعلوماتي، أو غيره من المجالات الأخرى أي أنه إنسان اجتماعي ولا يستعمل

[1] عمر عيسى الفقي، الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، د. ط ، 2006، ص15.

[2] محمد أمين الرومي، المرجع السابق، ص23.

القوة أو العنف وتطبيقا لذلك فمختلف الجرائم المعلوماتية ترتكب بدوافع[1]مختلفة، وسوف نتعرض لها من خلال ثلاثة عناصر هي[2]:

العنصر الأول: الدوافع الشخصية لارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات

ويمكن رد هذه الدوافع إلى دوافع مادية ودوافع ذهنية أو نمطية:

أ- **الدوافع المادية:** تعتبر الدوافع المادية من أهم البواعث على ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات لما تحققه من ثراء فاحش والدليل على ذلك ماحدث في فرنسا 1986م حيث كان العائد من ارتكاب جناية سرقة مع حمل السلاح هو 70.000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670000 فرنك فرنسي[3] وهناك بحث أجرته إحدى المجالات المتخصصة بخصوص موضوع " الأمن المعلوماتي" ومن خلاله ما ذكره الأستاذ باركر Parker تبين أن:

- 34% من جرائم الغش المعلوماتي من أجل اختلاس الأموال
- 23% من أجل سرقة المعلومات
- 19% من أجل الإتلاف

[1] ليلى لفويلي، الجريمة الالكترونية، مذكرة لنيل شهادة الماستر في القانون(اختصاص قانون العقوبات والعلوم الجنائية)، جامعة قسنطينة، 2013، ص19.

[2] أحمد خليفة الملط، المرجع السابق، ص88.

[3] Rose Philippe la criminalité informatique que saie je ? 1 er édition, Puf, 1988, P 490.

- 15% من أجل سرقة وقت الآلة

وهناك من يرجع ارتكابهم للجرائم المعلوماتية إلى الديون الناتجة عن المشاكل العائلية أو الخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في مثل هذه الحالات فالغاية تبرر الوسيلة.

ب- دوافع ذهنية أو نمطية

وذلك من خلال رغبة مرتكب الجرائم المعلوماتية في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوايا آثمة، وذلك راجع إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب تلك الجرائم.

العنصر الثاني: الدوافع الخارجية

هناك مواقف يتأثر الإنسان بها ويستسلم للمؤثرات والدوافع الخارجية بارتكابه بعض الجرائم المعلوماتية وتتمثل في:

أ - دافع الانتقام

يلجأ البعض إلى ممارسة الجرائم المعلوماتية إذا ما شعروا بالظلم وانتابتهم الرغبة في الانتقام من أشخاص أو جهات في محيطهم الاجتماعي أو في العمل[1]، كقيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات وديون المنشأة[2].

حيث شهدت 107 جريمة الكترونية في سنة 2013 بدافع الغيرة والانتقام اللذان فجرا الشبكة العنكبوتية لدى الجزائريين، حيث كشف نائب مدير القضايا الاقتصادية والمالية بمديرية الشرطة القضائية عميد أول للشرطة عن تسجيل 107 قضية، أي بزيادة 60 جريمة مقارنة بسنة 2012[3].

ب- دافع جنون العظمة أو الطبيعة التنافسية

وذلك من خلال العاملين داخل المنشأة لإظهار قدراتهم الفنية لإدارة المنشأة حتى ينافس زملائه للوصول إلى المراكز المرموقة.

ت- دافع التعاون والتواطؤ على الأضرار

[1] محمد محمود المكاوي، المرجع السابق، ص53.

[2] أحمد خليفة الملط، المرجع السابق، ص90.

[3] جريدة الخبر، الصادرة بتاريخ 03 مارس 2014 عدد7361.

هذا النوع يحدث من متخصص في الأنظمة المعلوماتية وهو كثير التكرار في الجرائم المعلوماتية حيث يقوم بالجانب الفني من المشروع وآخر من المحيط أو خارج مؤسسة المجني عليه لتغطية عمليات التلاعب وتمويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.

ث- دافع التهديد

يحدث هذا النوع نتيجة الوقوع تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة.

العنصر الثالث: دوافع خاصة بالمنشأة

بعض الدوافع تخص الشخص المسؤول عن المركز المعلوماتي بالمنشأة حيث يمكنه وضعه الوظيفي من استغلال منصبه إذا ما شاء لمصلحته ،وبعض المتخصصين يعتقدون في تقنية الأنظمة المعلوماتية أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية استخدام الأنظمة وبرامجها لأغراض شخصية أو للتنافس الفكري فيما بينهم أو بممارسة بعض الهوايات الدائرة في فلك التقنية، مما أدى إلى تمادي بعضهم إلى استخدام الأنظمة بصورة غير مشروعة تصل إلى حد ارتكاب جرائم خطيرة بالمنشأة لمصلحته الخاصة وهذا ما يسمى بأغراض النخبة[1].

[1] أمال قارة، الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة الماجستير، جامعة الجزائر، 2002، ص26.

ومثال ذلك في أن مستشار لدى إحدى البنوك الكبرى يدعى ستانلاي ريفكين (Stanley Rifkin) كان يتمتع بثقة مطلقة من جانب البنك وسمحت له اختصاصاته بالولوج إلى مفتاحين إلكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك إلى آخر وقد تمكن بفضل معالجته الآلية للمعلومات وتأقلمه الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث ومن خلاله استطاع تحويل 10 مليون دولار إلى حساب بنكي مفتوح باسمه في سويسرا وألقى القبض عليه وصدر ضده حكم بالسجن لمدة ستة(06) سنوات[1].

بالإضافة إلى دافع التجسس والإرهاب، فيما يتعلق بالتجسس، ليس المقصود به التجسس على الدول الأخرى، وإنما يقصد به التجسس على المنافسين، وذلك من خلال الحصول على المعلومات المتعلقة بإستراتيجية عمل المؤسسة المنافسة، أما فيما يتعلق بالإرهاب تستخدم الجماعات الإرهابية الدولية الشبكات المعلوماتية بهدف نشر أفكارها.

وقد أظهرت دراسة حديثة أجرتها جمعية المحامين الأمريكيين حول إساءة استخدام الحاسب أن تحقيق الربح السريع للكسب المالي هو السبب الشائع الأول وراء إتيانه وأن التحدي الذهني هو العامل الشائع الثاني الذي يقف وراءه، وأن معظم من يسيئون استخدام الحاسب 77% يكونون من داخل منظمة المجني عليه، وأن معدل الخسارة المادية الناجمة عن الحالة الوحيدة لإساءة استخدام الحاسب تتراوح ما بين 2 و10 مليون دولار[2].

[1] أحمد خليفة الملط، المرجع السابق، ص91.

[2] أمال قارة، المرجع السابق، ص26.

حيث بلغ عدد مستخدمي الإنترنت في الجزائر عام 2000 نحو 50000 مستخدم، في حين ارتفع هذا العدد ليصل عام 2008 إلى 000 500 3 مستخدم، وبذلك تقع الجزائر في المرتبة الرابعة بين الدول العربية في استخدام الإنترنت بين عامي 2000 و2008 وذلك قياسا على تعداد سكان الجزائر[1].

وبناءا على ما تقدم يمكن أن نقسم مجرمي المعلوماتية Cyber criminals إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة(07) أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هذه الطوائف فيما يلي[2].

- **الطائفة الأولى:"المازحون Pranksters"** هم الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليه، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).

- **الطائفة الثانية:"المخترقون Hackers "** هم الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح بهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

---

[1] عادل عزام سقف الحيط، المرجع السابق، ص284.

[2] سفيان سوير، المرجع السابق، ص30- 31.

- **وتتضمن الطائفة الثالثة:"الماكرين المخترقون Malicieuse Hackers**" أشخاص هدفهم إلحاق خسائر بالمجني عليه دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترعي فيروسات الحاسبات الآلية وموزعيها.

- **أما الطائفة الرابعة : "محللو المشاكل الخاصة Personnel Problem Solvers**" فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ويكون الهدف من ورائها إيجاد حلول لمشكلات مادية تواجههم ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية وغالبا ما يكون المجني عليه مؤسسة مالية.

- **وتشمل الطائفة الخامسة: " مجرمي المهنة Career Criminals** " هم مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.

- **أما الطائفة السادسة: " المتطرفونAdvocates Extreme** " فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي.

- **وأخيرا الطائفة السابعة:" مجرمي الإهمال The Criminels Negligent** " تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية في أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح، ففي نيوزيلندا على سبيل المثال قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة لهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ[1].

هذا بالإضافة إلى وجود بعض حالات الغش غير المعلن عنها لان ضحايا الجرائم المعلوماتية عندما يعلمون بها فإنهم يفضلون عدم إفشاء الفعل حفاظا على سمعتهم التجارية ومكانتهم المرموقة[2].

ب- من حيث المجني عليهم

يقع من المتصور ضحية هذه الجرائم جميع الأشخاص سواء الطبيعية منها أو المعنوية العامة والخاصة طالما كانت تستخدم الحاسب الإلكتروني في ممارسة أنشطتها سواء الاقتصادية منها أو الاجتماعية أو حتى السياسية والعسكرية.

[1] سفيان سوير، المرجع نفسه، ص 31.

[2] سامي علي حامد عياد، المرجع السابق، ص59.

ويلاحظ أنه من الصعب تحديد نطاق ضحايا هذه الجرائم على وجه الدقة وذلك راجع إلى أن هؤلاء الضحايا لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل وفي هذه الحالة يرون أنه من الحكمة عدم الإبلاغ عنها وبالتالي لا يرغب أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضده انتهاكا ما، وهذا السلوك السلبي يعتبر مغريا لمرتكبي هذه الجرائم للاستمرار في نشاطهم مما يلاحظ أن هذا النوع من الجرائم يوجه بصفة رئيسية إلى البنوك.

وبالتالي هذه الجرائم تستهدف في الواقع المؤسسات المالية أو المؤسسات التي تسيطر على ما يعرف" بالقيم الرأسمالية" وبالتالي فالهدف الأول لهذه الجرائم يتمثل في التمرد وتليها المعلومات باعتبارها الطريق إلى اقتصاد السوق ويمكن من خلالها بناء صناعة راسخة وحديثة، ونظرا لأهمية المعلومات يسعى المنتمون لمجتمع الأعمال بكل ما أوتوا من قوة من أجل الحصول عليها سواء بالطرق المشروعة أو غير المشروعة الأمر الذي حدا بالبعض إلى التقرير بوجود سوقين لشراء المعلومات إحداها شرعي والثاني يطلق عليه" السوق السوداء" للمعلومات الذي يرتبط بالجانب الأكبر من الجرائم التي تستهدف الأنشطة الاقتصادية والاجتماعية للمجتمع، ويمكن أن يتحقق بالنسبة للمعلومات المالية التي تتصل بالوضع المالي والإداري وتداول رؤوس الأموال والاستثمارات في المنشآت الاقتصادية سواء كانت عامة أو خاصة.

ويمكن أن يتحقق كذلك بالنسبة للمعلومات التجارية والصناعية التي تتعلق بالأبحاث المتعلقة بالسوق والمشروعات الاستثمارية والصناعة والإنتاج والتجارة والتوزيع، وأيضا

بالنسبة للمعلومات الشخصية المخزنة في ذاكرة الحاسب الالكتروني للجهات التي يتعامل معها الشخص الطبيعي ومن شأن إنشائها تهديد أو انتهاك الحياة الخاصة، وعلى نظيرها المعلومات المخزنة في ذاكرة الحاسبات الموجودة لدى البنوك والمحامين والأطباء ومراكز البوليس والنقابات المهنية والأحزاب السياسية، ويمكن أن يتحقق هذا النوع من الإجرام كذلك بالنسبة للمعلومات العسكرية وهي المعلومات التي يكثر الطلب عليها وخاصة من الدول الأجنبية والقوى المعادية مما يجعلها أكثر رواجا في سوق المعلومات السوداء[1].

ت- من حيث نوعية الجرائم

تختلف الجرائم بحسب المحل الذي ترد عليه فقد ترد على الذمة المالية للغير أو المعلومات أو المكونات المادية للنظام سواء بنسخها أو إفشائها أو الاستيلاء على المكونات المادية أو الاعتداء على النظام المعلوماتي بإتلافه أو محوه أو جعله غير صالح للاستعمال، أو نظام التشغيل مما يؤدي إلى عرقلة استعمال الجهاز وقد يستخدم الحاسب كأداة سلبية أو ايجابية.

المطلب الثـــــاني

موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات ودور الحاسوب في الجريمة

[1] أمال قارة، المرجع السابق، ص28.

تقتضي دراسة موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات ودور الحاسوب فيها تقسيم هذا المطلب إلى فرعين، نتناول في الفرع الأول موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات، أما الفرع الثاني فنخصصه لدراسة دور الحاسوب في الجريمة.

الفرع الأول

موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات

قد ترتكب الجريمة على الحاسب الالكتروني نفسه سواء على مكوناته المادية أو غير المادية وقد يستخدم الحاسب ذاته كأداة لارتكاب إحدى هذه الجرائم، وبالتالي نفرق بين ثلاث حالات[1]:

[1] محمد أمين الرومي، المرجع السابق، ص19.

الحالة الأولى:

وتتحقق هذه الحالة إذا كانت المكونات المادية للحاسب من معدات وكابلات وشبكات ربط وآلات طباعة هي محل أو موضوع لهذه الجريمة وبالتالي لا تثير هذه الحالات مشكلة باعتبار أن هذه المكونات المادية محل الاعتداء تتمتع بالحماية الجنائية للنصوص التقليدية باعتبارها من الأموال المنقولة التي تخضع سرقتها وإتلافها للنصوص الجنائية التقليدية.

الحالة الثانية:

وتتحقق هذه الحالة عندما تكون مكونات الحاسب المعلوماتية غير المادية مثل البرامج المستخدمة والبيانات والمعطيات المخزنة في ذاكرة الحاسب محلا أو موضوعا للجريمة، ونظرا للطابع الخاص الذي يميز هذه المكونات، فإنها لا تخضع للنصوص التقليدية لقانون العقوبات.

الحالة الثالثة:

في هذه الحالة لا يكون الحاسب محلا أو موضوعا للجريمة، وبالتالي لا يكون محلا للحماية الجنائية، ولكن تقع الجريمة بواسطته، فما هو إلا وسيلة لارتكابها ،ومحلها يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل والذي يشكل محل الحق أو المصلحة المحمية.

وعليه فإن موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات هو"**المال المعلوماتي**" تمييزا لماليته المغايرة للمال التقليدي وسنفصل فيما يلي لتعريف المال المعلوماتي وعناصره، ومفهوم برامج الحاسب الآلي وأنواعها.

أولا: تعريف المال المعلوماتي وعناصره

المقصود بالمال أو الشيء المعلوماتي الحاسب بكل مكوناته ، والحاسب اصطلاحا لا يخرج عن كونه آلة الكترونية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة[1].

وبعبارة أخرى، الحاسب عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب، حيث أن الحاسبات تنقسم من حيث أغراض استخدامها إلى حاسبات عامة الأغراض وأخرى متخصصة الأغراض، كما تنقسم من حيث النوعية إلى حاسبات رقمية وتناظرية ومختلفة.

والحاسبات بأنواعها وتقسيماتها المختلفة تجمعها خاصية واحدة فهي تتكون من عنصرين أساسيين هما:

- الكيان المادي
- الكيان المعنوي

فيما يخص الكيان المادي فيتمثل في المكونات المادية للحاسب وهي جهاز الإدخال وجهاز الإخراج، وحدة التشغيل المركزية والتي تشمل كل من وحدة الذاكرة و وحدة

[1] أمال قارة، المرجع السابق، ص21.

الحساب والمنطق و وحدة التحكم والتي يتم من خلالها معالجة المعلومات وتخزينها وإخراجها[1].

أما الكيان المعنوي أو ما يطلق عليه بالكيان المنطقي ويشمل البرامج التي يتحقق من خلالها قيام الحاسب بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها أو التي تمت معالجتها بالفعل.

فإن الكيان المادي للحاسب لا يطرح إشكالا من حيث حمايته جزائيا لأنه يخضع بحكم طبيعته المادية لنصوص الجرائم التقليدية، أما الكيان المنطقي وبحكم طبيعته المعنوية يحد من تطبيق النصوص التجريمية التي تعالج الجرائم التي يكون موضوعها يتسم بالمادية لا المعنوية، مما أثار إشكالية حمايته جزائيا وعليه سنتعرض إلى مفهوم برامج الحاسب الآلي وأنواعه.

ثانيا: مفهوم برامج الحاسب الآلي وأنواعها

يرتكز جوهر الكيان المعنوي للحاسبات في البرامج لأنها بمثابة القلب من جسم الإنسان وبدونها لا يكون للحاسب قيمة أكثر من قيمة المواد التي يصنع منها، فهي التي يتحقق من خلالها قيام هذا الجهاز بوظائفه المتعددة، وتعد البرامج وفقا لذلك من العناصر الرئيسية [2].

[1] محمد أمين الرومي، المرجع السابق، ص15.

[2] أمال قارة، المرجع السابق، ص 22.

وللبرامج[1] مدلولان أحدهما ضيق وثانيهما واسع، فيما يخص المفهوم الضيق يقتصر على مجموعة التعليمات والأوامر الصادرة من الإنسان للآلة أي الكيان المادي للحاسب، أما مفهومها الواسع فهو يضم إلى جانب التعليمات والأوامر (المفهوم الضيق) التعليمات والأوامر الموجهة إلى العميل مثل بيانات استعمال البرنامج أو كيفية المعالجة الالكترونية للمعلومات، أي كافة البيانات الأخرى الملحقة بالبرنامج والتي تساعد على سهولة فهم تطبيقه، وهذه البيانات عبارة عن تعليمات موجهة من المبرمج إلى العميل الذي يتعامل مع الآلة والبرامج على نوعين:

برامج التشغيل.

وتسمى كذلك ببرامج الاستغلال أو التنفيذ، وهي التي تمكن الحاسب من أداء الوظيفة المحددة له، وهي لهذا السبب تعتبر جزءا من الحاسب نفسه، ويتولى الإشراف عليها برنامج مشرف أو مراقب لتنظيم أداء هذه البرامج لدورها.

برامج التطبيق.

وتسمى برامج معالجة المعلومات وهي قد تكون برامج خاصة بمعالجة الكلمات أو برامج المعطيات أو برامج صفحات القيد وتقوم البرامج التطبيقية بتوجيه أقسام الحاسب الآلي ضمن النظام الذي وضع لها وفقا لأوامر البرامج التشغيلية المثبتة بالحاسب الآلي

[1] يعرف المشرع المصري في القرار الوزاري رقم 82 لسنة 1993 بان برامج الحاسب هو "مجموعة تعليمات معبر عنها بأي لغة أو رمز ومتخدة أي شكل من الأشكال يمكن استخدامها بطريق مباشر أو غير مباشر في حاسبة لأداء وظيفة أو الوصول إلى نتيجة سواء أكانت هذه التعليمات في شكلها الأصلي أو في أي شكل آخر تتحول إليه بواسطة الحاسب" . راجع: محمد أمين الرومي، المرجع السابق، ص16 .

نفسه أو في لوحات مستقلة يجري إدخالها معها في نظام الكمبيوتر، فهي تجعل النظام الآلي للحاسب يعمل لاستخراج نتائج معينة يرغب مستعمل الحاسب باستخدامها والاستفادة منها في عمله، كاستخراج المعلومات التي يريدها مثل الحسابات أو القضايا أو الأبحاث أو القيام بطباعة هذه المعلومات على الورق.

ويلاحظ أنه لا يدخل في مفهوم البرنامج المعطيات أو المعلومات سواء قبل معالجتها أو بعد ذلك، ولكن هذه المعطيات منذ دخولها ومعالجتها آليا وتخزينها واسترجاعها لا تنفصل عن البرامج التي تنظمها في كل مرحلة من المراحل السابقة، ولذلك فإن الحماية المقررة لتلك البرامج هي في نفس الوقت حماية لهذه المعطيات أو المعلومات[1] .

الفــرع الثاني

دور الحاسوب في جريمة المساس بأنظمة المعالجة الآلية للمعطيات

يلعب الكمبيوتر ثلاثة أدوار في ميدان ارتكاب الجرائم، ودورا رئيسيا في حقل اكتشافها.

أولا: الكمبيوتر أداة لارتكاب الجريمة

كما في حالة استغلال الكمبيوتر للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، حتى أن الكمبيوتر كوسيلة قد يستخدم في جرائم القتل، كما في الدخول إلى قواعد

[1] أمال قارة، المرجع السابق، ص23.

البيانات الصحية والعلاجية وتحويل عمل الأجهزة الطبية والمخبرية عبر التلاعب ببرمجياتها، أو كما في إتباع الوسائل الالكترونية للتأثير على عمل برمجيات التحكم في الطائرة أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها.

ثانيا: قد يكون الكمبيوتر هدف للجريمة

ويكون هدفا في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم.

ومن أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية عند توجيه هجمات الكمبيوتر إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى و التكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون تحويل ودون أن يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر، أو وقف الكمبيوتر) أو المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الإجرامية تتضمن ابتداءا الدخول غير المصرح به إلى نظام الهدف (UNAUTHORIZED ACCESS) والتي توصف بشكل شائع في هذه الأيام بأنشطة الهاكرز كناية عن فعل الاختراق(HACKING)[1].

ثالثا: الكمبيوتر مسرحا للجريمة

[1] نسرين عبد الحميد نبيه، المرجع السابق، ص90-91.

ويكون الكمبيوتر بيئة للجريمة، وذلك من خلال استخدام الكمبيوتر لنشر المواد غير القانونية(ترويج المخدرات، وأنشطة الشبكات الإباحية، ..... ونحوها) بالإضافة إلى تخزين البرامج المقرصنة، أي المنسوخة واستخدام الكمبيوتر كأداة تخزين أو اتصال لصفقات ترويج المخدرات.

رابعا: دور الكمبيوتر في اكتشاف الجريمة

تعتمد جهات تنفيذ القانون على النظم التقنية في إدارة المهام من خلال بناء قواعد البيانات ضمن جهاز إدارة العدالة للتطبيق القانوني.

ومع تزايد نطاق جرائم الكمبيوتر، واعتماد مرتكبيها على الوسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاما، استخدام نفس وسائل الجريمة المتطورة للكشف عنها، ويظهر هذا الدور في حالة استخدام الكمبيوتر على نطاق واسع في التحقيق الاستدلالي لكافة الجرائم واعتماد جهات القانون على الكمبيوتر في إدارة المهام من خلال قواعد البيانات ضمن إدارة العدالة والتنفيذ القانوني ،ويلعب الكمبيوتر دورا رئيسيا في كشف جرائم الكمبيوتر وتتبع فاعليها، وكذلك دورا هاما في إبطال تأثير الهجمات التدميرية لمخترقي الكمبيوتر وتحديد هجمات الفيروسات وإنكار الخدمة وقرصنة البرمجيات[1].

المبحـــث الثاني

أركان جريمة المساس بأنظمة المعالجة الآلية للمعطيات

[1] محمد محمود المكاوي، المرجع السابق، ص38.

حتى تقوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات لا بد من توافر أركانها، مما يقتضي دراسة أركانها بالتفصيل وذلك من خلال دراسة ركنها المفترض في المطلب الأول، وأركانها الأساسية في المطلب الثاني.

المطلب الأول

الركن المفترض: نظام المعالجة الآلية للمعطيات

هناك إحصاءات تشير إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر.

ونظرا لكثرة الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، أدى إلى التدخل التشريعي سواء على المستوى الدولي أو الداخلي، فدوليا تم وضع أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي[1]، أما على المستوى الوطني فقد تفطن المشرع الجزائري للفراغ القانوني من خلال التعديل الأخير لقانون العقوبات الذي ورد النص عليها في الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 156/66[2] بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 394 مكرر إلى394 مكرر7[3].

وإن كانت تختلف الجرائم الماسة بالأنظمة المعلوماتية في أركانها وعقوباتها إلا أنها تجتمع في كونها تحقق حماية جزائية لنظم المعالجة الآلية للمعطيات، ونظام المعالجة الآلية هو القاسم المشترك بينها، ولدراسة هذه الجريمة لا بد من توضيح وبيان مفهوم نظام المعالجة الآلية للمعطيات وعناصره.

---

[1] الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوربي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، 2007، ص100

[3] عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الطبعة الثانية، 2013، ص108.

الفــرع الأول

مفهوم نظام المعالجة الآلية للمعطيات

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام ،فإن ثبت تخلف هذا الشرط الأولي لا يكون هناك مجال لهذا البحث.

ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أي جريمة من الجرائم ، إذ أن هذا الشرط يعتبر عنصرا ملازما لكل منهما، ولذلك يكون من الضروري تحديد مفهوم نظام المعالجة الآلية للمعطيات.

حيث عرف مجلس الأمة الفرنسي نظام المعالجة الآلية للمعطيات كما يلي:" هو كل مجموعة منسجمة تتكون من وحدة أو عدة وحدات معالجة، ذاكرة، وبرامج، وحدات إدخال وإخراج ، واتصال بين هذه المكونات التي تؤدي إلى إعطاء نتيجة محددة، وهذه المجموعة تكون محمية تقنيا بموجب أي وسيلة أو بطاقة ائتمان[1]" [2].

ونستنتج من هذا التعريف بأن نظام المعالجة هو كل مجموعة معلوماتية مهما كان حجمها أو أسلوب اتصالها بمكونات أو أنظمة أخرى، ومهما كان أسلوب معالجتها للمعطيات فإنها تشكل كل نظام معلوماتي، وحتى نكون بصدد نظام المعالجة الآلية

[1] هي فيزا كارد، وبموجبها يحصل المستخدم على تسهيلات ائتمانية تتم حسب الاتفاق ما بين المستخدم والبنك وتتمكن من الشراء والدفع بواسطتها. راجع: يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر، عمان، الطبعة الأولى، 2007، ص91.

[2] نسيم دردور، المرجع السابق، ص14.

للمعطيات المعلوماتية فإنه لا يشترط أن يتوافر حجم معين وتعدد أو قلة العناصر المادية المكونة له أو التي هي باتصال به.

وتجدر الإشارة إلى أن المشرع الجزائري تأخر كثيرا في وضع تعريف واضح لمحل الجرائم المنصوص عليها في المواد 394 مكرر إلى 394 مكرر7 قانون عقوبات جزائري، أي 5 سنوات بعد صدور هذه المواد العقابية، وهذا على خلاف المشرع الفرنسي الذي أخذ احتياطاته في وضع تعريف لنظام المعالجة الآلية للمعطيات قبل إصداره للقانون حول المساسات غير المشروعة بأنظمة المعالجة الآلية للمعطيات، كون أن هذا التعريف يعد لب هذا القانون وبما أن التطبيق السليم لهذا القانون يتوقف على توافر تعريف لمحل الجريمة أي نظام المعالجة الآلية للمعطيات، فإنه كان لا بد على المشرع الجزائري أن يتبع نفس المنهج الذي اتبعه المشرع الفرنسي في هذا المجال لا غير أما فيما يخص صياغة هذا التعريف فسنرى بأن المشرع الجزائري جاء في قانونه الجديد بتعريف أحسن وأشمل إلى كل أنواع الأنظمة المعلوماتية عن الذي وضعه المشرع الفرنسي في 1987.

وبالرجوع إلى المادة 2 تحت عنوان: المصطلحات، من القانون رقم 09-04 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نجدها تنص عما يلي:

يقصد في مفهوم هذا القانون بما يأتي:

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

يمكن أن نلاحظ بعد الاطلاع على كل من التعريفات في التشريع الفرنسي والجزائري، بأن هناك اختلاف واضح من حيث صياغة تعريف أنظمة المعالجة الآلية للمعطيات يتمثل في كون أن المشرع الجزائري جاء بتعريف عام وغير دقيق بالمقارنة مع تعريف مجلس الأمة الفرنسي 1987، غير أنه رغم ذلك يمكن التأكيد بأن تعريف المشرع الجزائري صحيح و ربما أحسن من التعريف الفرنسي والأوربي من خلال اتفاقية بودابست لسبب بسيط هو أن أنواع الأنظمة المعلوماتية كثيرة ولا تنحصر فقط في أجهزة الكمبيوتر كما أشار إليه مجلس الأمة الفرنسي من خلال تعريفه والذي كان لا بد عليه أن يعدله ومما يؤكد بأن المشرع الجزائري كان على أساس يتوقف التطبيق السليم للمواد 390 مكرر إلى 394 مكرر7 قانون عقوبات جزائري، من جهة أخرى أن مجلس الأمة الفرنسي اشترط في تعريفه أن يكون النظام المعلوماتي محمي تقنيا حتى تقوم الجريمة وهو عكس ما ورد في التعريف الذي جاءت به اتفاقية بودابست المادة 2 منها حيث سنرى بأن الاجتهاد القضائي الفرنسي خالف هذه القاعدة في حين أن المشرع الجزائري لم ينص بصراحة على وجوب توافر حماية تقنية للنظام حتى تقوم الجريمة[1].

فيما يخص اشتراط أو عدم اشتراط توافر حماية تقنية للنظام المعلوماتي حتى تقوم الجريمة فتجدر الإشارة إلى أن قرار صادر عن مجلس قضاء باريس، غرفة الجنح في 5

[1] نسيم دردور، المرجع السابق، ص17-18.

أفريل 1994 حدد بأنه " حتى يعاقب الدخول أو البقاء يجب أن يتم دون ترخيص ومع علم المجرم بأن دخوله أو بقائه غير مسموح به وتجدر الإشارة إلى انه لا يشترط حتى تقوم

الجريمة أن يكون النظام محمي[1] ببطاقة ائتمانDispositif de Sécurité بل يكفي أن يكون صاحب أو مالك النظام قد صرح أو وضح للجمهور بأن الدخول أو البقاء في النظام غير مسموح به باستثناء مثلا الأشخاص الذين تحصلوا على رخصة لذلك، وبالتالي بدون ترخيص تقوم الجريمة إلا إذا تم الدخول أو البقاء خطأ أو بالصدفة ودون أن يكون هدف الشخص الإضرار بالنظام.

غير أنه من الصعب استبعاد التعريف الذي جاء به المشرع الفرنسي كليا والذي يفهم منه بأن المواد العقابية حول المساسات بالأنظمة لا تحمي المكونات المعزولة(مادية وحدها أو معنوية وحدها) إنما تحمي مجموعة منسجمة Ensemble harmonieux يهدف دورها في إعطاء نتيجة معينة، وهو المنطق الذي اتبعه المشرع الجزائري من خلال ما جاء به في المادة 2 من القانون رقم 09-04 المؤرخ في 5 أوت 2009 في ما يخص إجبارية انسجام مكونات النظام بهدف تحقيق نتيجة معينة[2].

[1] اجتهاد القضاء الفرنسي، بعدما تم الدخول غير المرخص به إلى منظومة شركة TATI الفرنسية عدة مرات من طرف شركة أخرى، قامت شركةTATI بمقاضاة تلك الشركة عن طريق الدخول غير المرخص به فإحتجت تلك الشركة بأن موقع TATI لم يكن محميا، وبالتالي ليس لهذه الأخيرة (TATI) الحق في الاحتجاج على الدخول إلى موقعها، فقضى القضاء الفرنسي بأنه ليس من الضروري أن تكون الأنظمة محمية. راجع:**www.droit-dz.com/forum** ، المرجع السابق، تاريخ التصفح 1 أفريل 2014 الساعة 11h00min صباحا.

[2] نسيم دردور ، المرجع السابق، ص19.

الفــرع الثــاني

عناصر نظام المعالجة الآلية للمعطيات

بناءا على التعريفات السابقة نجد أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

أولا: مركب يتكون من عناصر مادية ومعنوية مختلطة تربط بينهما نتيجة علاقات توحدها نحو تحقيق هدف محدد[1].

فتتمثل العناصر المادية والمعنوية التي يتكون منها المركب من الذاكرة، البرامج المعطيات، أجهزة الربط....الخ، وهي واردة على سبيل المثال لا الحصر، كما تعرفه المادة رقم 14/1 من القانون العربي النموذجي الموحد نظام المعالجة الآلية للمعطيات بأنه" يقصد به كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة"[2].

مما يؤدي إلى فتح المجال أمام إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطور التقني في هذا المجال، ولا يتوافر نظام المعالجة الآلية للمعطيات، ولا تقع أي جريمة من جرائم الاعتداء عليه المنصوص عليها إذا وقع الاعتداء على عنصر بمفرده لا يشكل جزءا في النظام، كما إذا وقع الاعتداء على برامج معروضة للبيع، أو على جهاز حاسب لم يدخل الخدمة أو على عنصر مودع بالمخازن، أو على قطع الغيار،

[1] نسرين عبد الحميد نبيه، المرجع السابق، ص195.

[2] عبد المجيد جباري، المرجع السابق، ص108-109.

أو على الأجهزة التي ما زالت في حالة التجربة، أو حتى الأنظمة التي خرجت من الخدمة تماما ولكن على العكس من ذلك. تقع الجريمة إذا وقع الاعتداء على النظام خارج ساعات تشغيله العادية، أو إذا كانت أحد عناصره في حالة عطل أو حتى لو كان النظام كله في حالة عطل تام، وكان يمكن إصلاحه.

وتقع الجريمة أيضا إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة فإذا تصورنا عدة أنظمة ترتبط فيما بينها بأجهزة اتصال ووقع اعتداء على جهاز حاسب آلي في نظام من تلك الأنظمة المرتبطة، فإن الجريمة تقع في هذه الحالة وإذا كان الدخول إلى هذا الجهاز مشروع، فإن البحث في توافر الجريمة يتوقف على ما إذا كانت توجد علاقة سببية بين هذا الدخول المشروع والاعتداء المفروض على الأنظمة ككل، ومدى حسن أو سوء نية المتدخل، كما تقع الجريمة إذا وقع الاعتداء على شبكة الاتصال التي تربط بين أكثر من نظام، لأن تلك الشبكة تعتبر عنصرا في كل نظام من الأنظمة التي تربط بينها.

وإذا كان تعريف مجلس الشيوخ الفرنسي لنظام المعالجة الآلية للمعطيات غير ملزم لأنه حذف من النص النهائي، إلا أنه يمكن للقضاء أن يستهدي به فيما يعرض عليه من منازعات في هذا الخصوص باعتبار أن هذا التعريف يعتبر من الأعمال التحضيرية التي يمكن الاستعانة بها في تفسير غموض النص أو غموض بعض عباراته، وهذا هو ما

يستفاد فعلا من أحكام القضاء الفرنسي، وإن كانت أغلب الأنظمة التي عرضت على القضاء كانت في مجال المشروعات الخاصة، وفي مجال الاتصالات[1].

ثانيا: ضرورة خضوع النظام لحماية فنية.

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات خاصة شبكة الإنترنت حاليا لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بأعمال التجارة الرقمية، ويمثل التشفير[2] أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية، وهناك شكلين أساسيين للتشفير:

أ- الشكل الأول:La Cryptologie Symétrique.

وجود نفس المفتاح التشفيري للتشفير وفك الشيفرة في آن واحد المشكل الذي تطرحه هذه الجريمة أنه يجب إيجاد وسيلة لإرسال المفتاح بطريقة آمنة للمرسل إليه.

ب- الشكل الثاني:La Cryptologie asymétrique.

عكس الشكل الأول كونه ليس نفس المفتاح هو الذي يشفر ويفك الشيفرة المستعمل يملك مفتاحا خاصا ومفتاحا عاما.

---

[1] أمال قارة، الجريمة المعلوماتية، المرجع السابق، ص34.

[2] فيما يخص تعريف التشفير فقد عرفها المشرع التونسي بأنه " استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها"، أما المشرع المصري فقد عرفه بأنه" تغير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها أو تغييرها. راجع : يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات،عمان، الطبعة الأولى،2007، ص99.

ويثير التساؤل حول ضرورة وجود أو عدم وجود حماية فنية للنظام كشرط للتمتع بالحماية الفنية الجنائية؟ حيث تنقسم الأنظمة إلى ثلاثة أنظمة.

- أنظمة مفتوحة للجمهور
- أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- أنظمة قاصرة على أصحاب الحق وتتمتع بحماية فنية.

ومقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول والثاني فلا يتمتعان بتلك الحماية، وتبرير ذلك أن الحماية الجنائية يجب أن تقتصر على الأنظمة المحمية فنيا لأنه من الطبيعي أن من يقوم باستغلالها يضع الوسائل الفنية اللازمة لمنع الغش وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله، كما أن في ضرورة تطلب حماية فنية ما يدفع مستغلي تلك الأنظمة إلى استخدام الحماية الفنية، ويكون دور القانون الجنائي في هذه الحالة وقائي وهذا ما يتفق وسياسة المشرع الجنائي التشريعية.

وما نلاحظه من المفهوم العام للحماية الجنائية للملكية ومهما كانت وجهات الإسناد السابقة إلا أن المسألة واضحة لا تحتاج إلى تفسير فالنصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات لا تتضمن شرط الحماية الفنية وخرجت تلك النصوص خالية منه تماما، ومن المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص (العام) المطلق، أو تخصيص النص العام إلا إذا وجد

نص يجيز ذلك، ولا يوجد في حالتنا نص خاص يقيد إطلاقا النص أو يخصص عمومه، ولذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أنه أراد استبعاده[1].

هذا بالإضافة إلى أن الحماية الجنائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا، وتطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية ولكن إذا نظرنا للواقع، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة وبصفة خاصة الركن المعنوي[2].

المطلـــب الثـــــاني

الأركان الأساسية لجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

يعتبر نظام المعالجة الآلية للمعطيات الشرط الأولي لقيام جريمة المساس بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الأركان التي تقوم عليها كل جريمة.

الـــفـــــــــــرع الأول

الركـــن الشرعـــــــــي

إن الجريمة تتحقق بالفعل الصادر عن الإنسان فيتخذ صورة مادية معينة، تختلف الأفعال المادية باختلاف نشاطات الإنسان وهذا ما يجعل المشرع يتدخل لتحديد فئة من

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص104-105.

[2] المرجع نفسه، ص106.

الأفعال الضارة أو الخطرة على سلامة أفراد المجتمع فينهى عنها بموجب نص قانوني جزائي يجرم هذه الأفعال ويحدد العقوبة لمن يأتي على ارتكابها[1].

فالنص القانوني هو مصدر التجريم وهو المعيار الفاصل بين ما هو مباح وما هو منهي عنه تحت طائلة الجزاء، وتبعا لذلك فلا جريمة ولا عقوبة أو تدابير أمن بغير نص قانوني[2]، هذا ما يعرف بمبدأ الشرعية الذي ينتج عنه قاعدة أساسية وهي عدم رجعية القانون الجنائي أي عدم العقاب على فعل ليس له نص ويتميز لهذا المبدأ أن القاضي الجنائي عند تفسيره لنصوص القانون أن يفسره تفسيرا ضيقا، بالإضافة إلى منع اللجوء إلى القياس أي عدم لجوء القاضي الجنائي بقياس فعل لم يرد نص بتجريمه على فعل ورد نص يجرمه فيقرر للأول عقوبة الثاني للتشابه بين الفعلين[3].

ونظرا للتطور الحاصل في الإجرام ومع ظهور شبكة الإنترنت التي ساهمت بشكل خطير في تفشي جريمة المساس بأنظمة المعالجة الآلية للمعطيات ازداد الوضع خطورة حيث أصدر المجلس الأوربي سنة 1989 توصية لتشجيع الدول الأعضاء على تبني نصوص عقابية خاصة بجريمة المساس بأنظمة المعالجة الآلية للمعطيات وقد ترددت العديد من الدول في اختيار التقنية التشريعية المناسبة، فمنها من قام بإدماج نصوص

[1] أحسن بوسقيعة، المرجع السابق، ص 58.

[2] المادة 1 من قانون العقوبات. للتوسع أكثر راجع: أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، د. ط ، 1972، ص42.

[3] أحمد خليفة الملط، المرجع السابق، ص160.

خاصة بالإجرام المعلوماتي في قانون العقوبات التقليدي، ومنها من وضع قانون جنائي مستقل للمعلوماتية يدخل في إطار القانون الجنائي التقني.[1]

حيث أن المشرع الجزائري أفرد قسما خاصا لمساس بأنظمة المعالجة الآلية للمعطيات وهو القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر7 بمقتضى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ولم يكتف المشرع الجزائري بذلك بل فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون 06-23 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 وإقراره المادة 303 مكرر إلى 303 مكرر 03، وهذا تحسبا للاستخدام السيء للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال وما يرتبط بها من تقنيات مثل ما يسمى بالبلوتوث[2].

الـــفـــــرع الـــثـــانـــي

الركـــــن المـــــــــادي

لقد تدارك المشرع الجزائري ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04[3] المتضمن تعديل قانون العقوبات، لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي، وحتى لا تكون هذه

[1] أمال قارة، الجريمة المعلوماتية، المرجع السابق، ص37.

[2] زيدان زيبخة ، المرجع السابق، ص48.

[3] القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات.

الدراسة ناقصة كان لابد من التعرض للاعتداءات الماسة بالأنظمة المعلوماتية أولا، والاعتداءات الماسة بمنتوجات الإعلام الآلي ثانيا.

أولا: الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات:

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات كالآتي:

أ- الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات[1].

نصت عليه المادة 394 مكرر من قانون العقوبات" يعاقب بالحبس من ثلاثة(03) أشهر إلى سنة وبغرامة من 50000 دج إلى 1000000دج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات، أو يحاول ذلك.

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى150000 دج[2].

ولهذه الجريمة صورتين صورة بسيطة وصورة مشددة، فتتمثل الصورة البسيطة للجريمة في مجرد الدخول أو البقاء غير المشروع بينما الصورة المشددة، تتحقق بتوافر

[1] يعاقب القانون الفرنسي في نص المادة 1/323 قانون العقوبات الفرنسي على فعل الدخول والبقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات بالحبس لمدة سنة (1) وغرامة 100000فرنك وإذا نتج عنها محو أو تغيير في المعطيات المخزنة أو إتلاف التشغيل تكون العقوبة الحبس لمدة سنتين (2) وغرامة (200.000) فرنك (القانون الفرنسي الجديد 1994). راجع : محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، الأردن، الطبعة الأولى، 2007، ص224.

[2] المادة 394 مكرر قانون عقوبات جزائري.

الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب نظام أشغال المنظومة[1]

1- الصورة البسيطة.

- **فعل الدخول:** لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع بأية وسيلة أو طريقة، ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر، وتقع هذه الجريمة من أي إنسان أيا كانت صفته.

- **فعل البقاء:**

يقصد به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظم، وقد يجتمعان ويكون البقاء معاقبا عليه مستقلا حين يكون الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، وكان عليه قطع وجوده أو انسحابه فورا، وفي حالة تجاوزه المدة المسموح له البقاء فيها بداخل النظام، أو في حالة طبع نسخة من المعلومات في حين سمح له الرؤية فقط، فإنه يعاقب على جريمة البقاء غير المشروع متى توافرت أركانها لاسيما منها الركن المعنوي، هذه الجريمة تعد جريمة سلوك مجرد أي أنها تقع وتكتمل بمجرد الانتهاء من السلوك المكون لها وهو الدخول أو البقاء دون أن يطلب المشرع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية[2].

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص106-107.

[2] ليلى لفويلي، المرجع السابق، ص85.

2- الصورة المشددة:

نصت المادة 394 مكرر فقرة 2 و3 من قانون العقوبات " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى150000 دج".

حيث نصت المادة 394 مكرر2 فقرة3 قانون عقوبات على ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، ويتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو أو تعديل المعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائفه ويكفي لتوافر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشرع وتلك النتيجة الضارة، ولا يشترط أن تكون تلك النتيجة الضارة مقصودة لأن تطلب مثل هذا الشرط يكون غير معقول، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة.

كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير العمدي فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه وبين الجريمة العمدية الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتقاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

ب- الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت عليه المادتين 5 و8 من الاتفاقية الدولية للإجرام المعلوماتي، غير أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة بداخل النظام والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء غاية فإن الفعل يشكل جريمة الاعتداء العمدي على المعطيات[1].

وتتمثل صور الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات في:

1- التعطيل(العرقلة)

تفترض وجود عمل ايجابي دون أن يشترط المشرع أن يتم التعطيل بوسيلة معينة، قد تكون تلك الوسيلة مادية أو معنوية، وتكون وسيلة التعطيل مادية سواء اقترنت بعنف أم لا ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة، وتكون وسيلة التعطيل معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات وذلك بإتباع التقنيات التالية:

-كإدخال برنامج فيروسي[2].

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص113- 114.

[2] ماهية الفيروس: هو برنامج حاسب مثل أي برنامج تطبيقي آخر يتم تصميمه بواسطة أحد المخربين بهدف محدد وهو إحداث أكبر ضرر ممكن بنظام الحاسب ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا وهذا ما يتيح له القدرة الكبيرة على الانتشار ببرامج الحاسب المختلفة وكذلك بين مواقع مختلفة في الذاكرة حتى يحقق أهدافه التدميرية. ومن بين خصائصه القدرة على الاختفاء والانتشار

-استخدام قنابل منطقية[1] تجعل النظام يتباطأ في أدائه لوظائفه إلى غيرها من التقنيات.

2- الإفــساد

وهي كل فعل وإن كان لا يؤدي إلى التعطيل، يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها، والإفساد من هذه الزاوية يقترب من التعييب الذي يعتبر ظرف مشدد لجريمة الدخول والبقاء غير المشروع، والفارق بينهما يكمن في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون عمديا بينما يتطلب هذا الشرط لجريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات[2].

ت- الاعتداءات العمدية على المعطيات:

نصت عليها المواد 03، 04، 08 من الاتفاقية الدولية للإجرام المعلوماتي، كما نص عليها المشرع الجزائري في المادة 394 مكرر2 من قانون العقوبات " يعاقب بالحبس من شهرين(02) إلى ثلاثة(03) سنوات وبغرامة من 1000000دج إلى 5000000دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

والاختراق والتدمير وأشهر أنواع الفيروسات، فيروس القردة وفيروس مايكل أنجلو وكذلك فيروس إسرائيل وفيروس كارت عيد الميلاد. راجع: محمد أمين الرومي، المرجع السابق، ص26.

[1] تعتبر القنابل المنطقية جزء من رمز ما يتم إدخاله بشكل متعمد إلى نظام برمجي لتقوم بالبدء بأداء وظيفة مدمرة عندما تجتمع شروط معينة مثال عمل مبرمج ما على إخفاء جزء من شيفرة(مثل قاعدة بيانات تحريك المرتبات) لتبدأ بحذف الملفات تلقائيا إذا ما تم الاستغناء عن خدماته ورفع اسمه من قائمة المرتبات. راجع: عادل عزام سقف الحيط، المرجع السابق، ص133.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص115-118-119.

– 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 الجرائم المنصوص عليها في هذا القسم.

– حيازة أو إفشاء أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم وعليه فإن لهذه الجريمة صورتين:

الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة داخل النظام.

ويتجسد ذلك في إحدى الصور الثلاثة الآتية:

– الإدخال:L'intrusion

– المحو:L'effacement

– التعديل:Modification

لا يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي بأفعال الإدخال والمحو والتعديل 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[1].

– فعل الإدخال:

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، 120.

يتحقق ذلك بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي، أو من غيره في حالات السرقة أو الفقد أو التزوير، أو في حالة إدخال برامج غريبة(فيروس حصان طروادة[1]– قنبلة معلوماتية زمنية) تضيف معطيات جديدة .

– فعل المحو:

يقصد به إزالة جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من تلك المعطيات إلى المنطقة الخاصة بالذاكرة.

– فعل التعديل :

يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وقد يتم عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أوجزئيا عن طريق التلاعب في البرامج[2].

الصورة الثانية: المساس العمدي بالمعطيات خارج النظام.

[1] يقصد بحصان طروادة: هو برنامج يتم تشغيله داخل جهاز حاسوب الضحية ليقوم بأغراض التجسس على أعماله حيث يقوم البرنامج منذ بداية التشغيل حتى إغلاق النظام بتسجيل كل طرقة على لوحة المفاتيح قام بها المعتدى عليه، كذلك قد يعمل حصان طروادة على تغيير البرامج والبيانات والمعلومات داخل الحاسوب، وكذلك قد يعمل على تبديلها أو حذفها وأحصنة طروادة يمكن أن تكون خطيرة وصعبة الاكتشاف. راجع: عادل عزام سقف الحيط، المرجع السابق، ص135.

[2] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص121–122

لقد كرس المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها خلال تجريمه السلوكات التالية:

1- المادة 394 مكرر2 تستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تخزن على" أشرطة أو أقراص" أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية مادامت تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

2- نص المادة 394 مكرر2 فقرة 2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بهدف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق.....الخ[1].

ثانيا: الاعتداءات على منتوجات الإعلام الآلي- التزوير المعلوماتي-.

هذه الصورة الثانية للركن المادي للجريمة المعلوماتية تتمثل في المساس بمنتجات الإعلام الآلي ويتجسد هذا المساس في فعل التزوير المعلوماتي.

وقد احتلت الدعامات المادية للحاسب الآلي مكانة المحررات والصكوك ونظرا لأهمية وخطورة ما تحتويه من بيانات والتي قد تكون محلا للاعتداء بتغيير حقيقتها بقصد

[1] المادة 934 مكرر2 قانون عقوبات.

الغش في مضمونها، والذي من شأنه إحداث أضرار مادية أو معنوية كتزوير المستخرجات الالكترونية كالأوراق المالية أو السحب على الجوائز.

إن جريمة التزوير في المجال المعلوماتي من أخطر صور غش المعلوماتية نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات وأصبحت تجري من خلاله كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف" المكتوب" في القانونين المدني والتجاري، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة.

وتجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، ربما اقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا، و الفرق أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير المعلوماتي تجعل التزوير يرد على محرر وعليه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير كما هو عليه الحال في التشريع الفرنسي مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي.

1- مفهوم منتجات الإعلام الآلي:

لا بد من التفرقة بين مفهومين هما المستند المعالج آليا والمستند المعلوماتي[1].

يقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، والمستند المعالج آليا هو كل دعامة مادية مهيأة لاستقبال المعلومات والتي تسجل المعطيات عليها من خلال تطبيق إجراءات المعالجة الآلية للمعلوماتية، أي هو الدعامة المادية التي تم تحويل المعطيات المسجلة عليها لغة الآلة.

ويقصد بالمستند المعالج آليا في الاصطلاح القانوني كل دعامة مادية تصلح لأن تدون عليها المعلومات أو الآراء والتي هي غير المادية، وهي الشيء المادي الذي يدون عليه شيء معنوي.

أما المستند المعلوماتي هو ذلك المستند غير المعالج آليا، وتعتبر مستندات معلوماتية الأوراق المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شيء بعد، والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرنامج، وكذلك أيضا البطاقات البنكية التي لم تدخل الخدمة بعد، وهذه وإن كان مسجل عليها معلومات مكتوبة بخط اليد أو مطبوعة أو محفورة،إلا انه لم يتم معالجتها بعد،إذ أنها مازالت في مرحلة الإعداد فقط.

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص133-134.

2- مدى خضوع منتوجات الإعلام الآلي لنصوص التزوير

الاعتداء على منتوجات الإعلام الآلي يتجسد في فعل التزوير المعلوماتي الذي نصت عليه المادة 7 من الاتفاقية الدولية للإجرام المعلوماتي إذ أن التلاعب في المعطيات الذي ينتج عنه معطيات غير أصلية يعد تزويرا[1].

ويقتضي الركن المادي لجريمة التزوير أن يكون تغيير الحقيقة حاصلا في محرر يشكل مستند، هذا ما يستفاد من نصوص المواد 214 إلى 229 قانون عقوبات التي تشير إلى حصول التزوير في المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية والشهادات. ومن هذا المنطلق، لا تقوم جريمة التزوير إذا كان تغيير الحقيقة قد تم الاستناد إليها لممارسة حق أو عمل.

ويشترط في المحرر أن يكون في شكل " كتابة" أو عبارات خطية، ولا يعد محررا كل ما هو غير مكتوب كالعداد الحاسب لاستهلاك الكهرباء أو المياه أو الغاز أو الأختام المنسوبة إلى فرد أوجهة، ولنفس السبب لا تعد محررات الأفلام والأسطوانة وأشرطة التسجيل والأقراص الممغنطة أيا كانت أهميتها القانونية، مما أدى بالمشرع الفرنسي نظرا للتطورات التقنية التي شهدها العالم في هذا المجال وللمكانة التي تحتلها هذه الوسائل في الحياة اليومية، إلى إضافة " كل سند آخر لتغيير الفكر" إلى المحرز ولا يتحقق الركن المادي للتزوير وبمجرد تغيير الحقيقة بأية طريقة من الطرق وإنما يجب أن يكون هذا التغيير قد حدث بإحدى الطرق التي حددها القانون على سبيل الحصر، وتختلف الطرق

[1] أمال قارة، المرجع نفسه، ص135.

من جريمة إلى أخرى، حيث حددت المواد 214 إلى 216 قانون عقوبات طرق التزوير الذي يقع في المحررات الرسمية أو العمومية في ثمانية تدخل ثلاث منها في طرق التزوير المادي بينما خمس منها تقع في طرق التزوير المعنوي.

والتزوير نوعين، مادي تتغير به الحقيقة بإحدى طرق التزوير المادية، ومعنوي تتغير به الحقيقة بإحدى طرق التزوير المعنوية، وقد استقر الفقه على أن التزوير المادي هو كل تغيير للحقيقة في محرر بطريقة تترك فيه أثرا يدركه الحس وتقع عليه العين سواء بزيادة أو حذف أم بتعديل أو باستثناء محرر لا وجود له في الأصل، أما التزوير المعنوي فهو كل تغيير للحقيقة في مضمون المحرر ومعناه وظروفه وملابساته تغيرا لا يدرك البصر أثره، بالإضافة إلى عنصر الضرر الفعلي المباشر الذي يتمثل في إهدار حق أو مصلحة يحميها القانون[1].

والإشكال المطروح هو هل يمكن تطبيق نصوص التزوير الواردة في قانون العقوبات الجزائري على الاعتداءات الماسة بمنتوجات الإعلام الآلي؟

وللإجابة على هذا التساؤل لا بد من التطرق إلى مدى انطباق وصف المحرر على البيانات المعالجة آليا ومدى خضوعها لفعل تغيير الحقيقة.

أ- مدى انطباق وصف المحرر على منتوجات الإعلام الآلي:

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، جرائم الفساد، جرائم المال والأعمال، جرائم التزوير، دار هومة، الجزائر، الطبعة الثالثة عشر منقحة ومتممة، 2013، ص403-408-418.

إن المحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة تمكن القراءة البصرية لمحتواه، وهو ما تفرضه نصوص التزوير التقليدية، وعليه يمكن إجمال خصائص المحرر في ثلاث نقاط:

- أن يتخذ المحرر شكلا كتابيا ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحالت قراءته فلا يصلح وسيلة للإثبات ولا عقاب على ما احتواه من تعبير.
- أن تكون الكتابة منسوبة لشخص معين.
- أن يحدث المحرر آثارا قانونية.

وبإسقاط المفهوم التقليدي للمحرر على مجال المعالجة الآلية للبيانات، نجد أن تغيير الحقيقة الذي يكون محله الأشرطة الممغنطة لا تقع به جريمة التزوير في المحررات وذلك لعدم وجود عنصر الكتابة، فجريمة التزوير تشترط الكتابة فأي تغيير في الوعاء المعلوماتي لا يعتبر تزويرا لانتفاء هذا الشرط.

وقد ذهبت بعض التشريعات الحديثة لمواجهة القصور في النصوص التقليدية إلى استحداث نصوص تجريمية جديدة أو إدخال تعديلات على التشريعات التقليدية من أجل المعاقبة على جريمة التزوير الواقعة على المستندات المعلوماتية، حفاظا على الثقة الواجب توافرها في المستندات المعلوماتية، ومن أمثلة هذه التشريعات التشريع الفرنسي الذي استحدث نصا خاصا بالتزوير المعلوماتي وهو المادة 21462 من قانون العقوبات ذلك بموجب تعديل سنة 1988 غير انه وبموجب تعديل سنة 1994، تراجع المشرع الفرنسي عن موقفه وألغى النص الخاص بالتزوير المعلوماتي، وأخضعه لنصوص

التزوير التقليدية، أما بالنسبة للتشريع الجزائري فيعد من التشريعات التقليدية حيث أدرج النصوص الخاصة بتزوير المحررات في المواد من 214 إلى 229 من قانون العقوبات التي تشترط المحرر لتطبيق جريمة التزوير، وكان من الأفضل على المشرع الجزائري إضافة نص إلى باب التزوير في المحررات يعرف فيه التزوير، كاقتراح أنه كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر[1].

وهذا النص قد يكون أشمل كونه تندرج في كل المستندات المعلوماتية حتى وإن كانت غير معالجة آليا، وهو ما يتضمن حماية جزائية فعالة لكافة المنتجات المعلوماتية.

ب- مدى خضوع منتوجات الإعلام الآلي للنشاط الإجرامي لجريمة التزوير:

يتمثل النشاط الإجرامي المكون لجريمة التزوير في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير، والمقصود هو تغيير الحقيقة القانونية النسبية وليس تغيير الحقيقة الواقعية المطلقة، إذ يكفي لتغيير الحقيقة الذي تتطلبه جريمة التزوير أن يكون هناك مساس بحقوق الغير أو مراكزهم القانونية الثابتة في تلك المحررات وعليه يمكن تصور تغيير الحقيقة في نطاق المعالجة المعلوماتية بالتلاعب في المعطيات مما يؤثر على أصالتها وتجدر الإشارة إلى أن تحويل البرنامج أو قواعد البيانات لا يعد تزويرا وإنما يقع تحت طائلة نصوص التقليد الواردة في قانون حق المؤلف والحقوق المجاورة ولا يتصور وقوع فعل تغيير الحقيقة من خلال طرق التزوير

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص136-137-138.

المعنوية والتي كما هو معروف لا تتحقق إلا أثناء تكوين المستند بالنسبة للجريمة محل البحث.

بينما من المتصور وقوع فعل تغيير الحقيقة بالنسبة لهذه الجريمة من خلال طرق التزوير المادية، ولكن بشرط أن يكون التزوير لاحقا على نشأة المستند الأصلي والحقيقي المعالج آليا فلا تتحقق تلك الجريمة من خلال فعل تغيير الحقيقة باستخدام طريقة تزوير مادية أثناء نشأة المستند على خلاف جريمة التزوير العادية.

نستخلص إلى أن المشرع الجزائري رغم تداركه من خلال القانون15/04 المتضمن قانون العقوبات الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا أنه أغفل تجريم الاعتداءات على منتوجات الإعلام الآلي، فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات التي عمدت إلى توسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث[1].

الـفـــرع الـــثـالـــث

الركــن المعنـــــوي

إن الركن المعنوي في مختلف الاعتداءات الماسة بأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش.

أولا: الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

[1] أمال قارة، المرجع نفسه، ص139–140.

إن الولوج والتجول والبقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا إذا تم عمدا فمن خلال المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله وتعتبر جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم والإرادة.

أي اتجاه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء وأن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي، إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر الدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصرية العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة والانتصار على النظام [1].

وبالنسبة لنية الغش تبدو من خلال الغش الذي تم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام، وفي الحقيقة أن الدخول والبقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، وإنما

[1] المرجع نفسه، ص124.

يظهر من خلال الولوج دون وجه حق إلى النظام إلا أن الجهاز الرقابي ما هو إلا وسيلة لإثبات أن الدخول للنظام غير مرخص به.

ثانيا: الاعتداءات على سير نظام المعالجة الآلية للمعطيات.

تعتبر جريمة عمدية، إذ أن من المفروض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن ذلك الاعتداء غير العمدي لسير النظام الذي يشكل ظرف مشددا لجريمة الدخول والبقاء غير المشروع داخل النظام، وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة.

ثالثا: الاعتداءات العمدية على المعطيات.

تعتبر جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.

رابعا: استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية.

وذلك إما بالتصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، فإن هذا الاستخدام يجب أن يكون عمديا وبطريق الغش أي توافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش[1].

[1] أمال قارة، المرجع نفسه، ص125–126.

الفصل الثاني

قمع جريمة المساس بأنظمة المعالجة الآلية للمعطيات

إن أنشطة مكافحة جرائم المعلوماتية أظهرت تحديات ومشاكل كثيرة تختلف في جوانب كثيرة عن التحديات والمشاكل التي ترتبط بالجرائم التقليدية الأخرى، كونها لا تترك أثرا ماديا وراءها بمسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية، كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة جدا مما يخلف تحديات كبيرة في مجال ضبط مثل هذه الجرائم وجمع الأدلة عنها والتعرف على مرتكبيها[1]، وهذا ما يطرح أمام رجال القانون وبإلحاح على كيفية ملاحقة المجرمين الكفيلة بضبط الأدلة والتفتيش عنها وكيفية الحصول على المعلومات وسماع الشهود أو إجراء خبرات؟ وكيف يمكن للمحققين الخوض في أعماق الكمبيوتر لمراقبة المعلومات وحجزها؟ ومن هم هؤلاء المحققون الذين يخولهم القانون هذه الصلاحية؟ والجزاءات المقررة لهؤلاء المجرمين[2].

وارتأينا تقسيم الفصل الثاني من البحث إلى مبحثين نخصص المبحث الأول إلى دراسة القواعد الإجرامية لمكافحة جرائم المعلوماتية ، أما المبحث الثاني نخصصه إلى إثبات الجرائم المعلوماتية والجزاءات المقررة لمرتكبيها.

[1] www.droit.dz.com/forom، المرجع السابق، تاريخ التصفح 20 أفريل 2014 الساعة18:10

[2] زيدان زيبخة، المرجع السابق، ص107.

المبحث الأول

القواعد الإجرائية لمكافحة جريمة المساس بأنظمة المعالجة الآلية للمعطيات

إن محاربة الجرائم المعلوماتية بشتى أنواعها أدى بالمشرع الجزائري إلى تدارك هذا النقص من خلال تدخله سنة 2009 أين سن القانون رقم09-04 المؤرخ في 2009/08/05 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث جاء هذا القانون بتقنيات جديدة ومعالم أخرى توضح القواعد الإجرائية لمكافحة هذا النوع من الإجرام، ومن أجل الوصول إلى ذلك كان لا بد من تقسيم هذا المبحث إلى مطلبين نخصص المطلب الأول إلى الاختصاص المحلي للجهات القضائية أما المطلب الثاني نتطرق فيه إلى أساليب التحري والتحقيق في الجرائم المعلوماتية.

المطلب الأول

الاختصاص المحلي للجهات القضائية

تقتضي دراسة الاختصاص المحلي للجهات القضائية تقسيم هذا المطلب إلى أربعة فروع، نخصص الفرع الأول منه إلى الصلاحيات المكانية للضبطية القضائية في جرائم المعلوماتية، أما الفرع الثاني فنخصصه لدراسة الاختصاص المحلي لقاضي التحقيق

ونخصص الفرع الثالث إلى التطرق إلى المركز العالمي للشكاوى الخاصة بجرائم الإنترنت أما الفرع الرابع نعرض فيه توضيح الاختصاص القضائي لجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

الفـرع الأول

الصلاحيات المكانية للضبطية القضائية في جريمة المساس بأنظمة المعالجة الآلية للمعطيات

لقد سارع المشرع الجزائري إلى تدارك النقص وسد الفراغ القائم بخصوص مجالات التحقيق الابتدائي إثر التطور الذي عرفته الجريمة سيما بأشكالها الحديثة كما هو الحال في الجرائم المعلوماتية لذلك جاءت تعديلات قانون الإجراءات الجزائية متعاقبة سيما التعديل الذي جاء به القانون 06-22 المؤرخ في 2006/12/20 والذي مدد من صلاحيات الضبطية القضائية ووسع دائرة اختصاصها، ودعمه القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أولا: الاختصاص المحلي للضبطية القضائية

منح القانون الجزائري للضبطية القضائية تماشيا مع المبدأ الدستوري المتعارف عليه "لا جريمة ولا عقوبة أو تدابير أمن إلا بنص" مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي ويتضح من نص المادة 12 من قانون الإجراءات الجزائية بالنسبة للضبطية القضائية أن مناط البحث عن الجرائم ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم

ويتقلص دورها عند ابتداء التحقيق القضائي لينحصر في تنفيذ طلبات جهات التحقيق القضائي وإنجاز ما توجه إليهم من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي بما في ذلك تنقيط ضباط الشرطة القضائية والذي يؤخذ في الحسبان عند الترقية[1].

كما تنص المادة 18 مكرر من قانون الإجراءات الجزائية في إطار الصلاحيات المحددة بنص المادة 36 من قانون الإجراءات الجزائية وهذا تحت إشراف النائب العام وتحت رقابة غرفة الاتهام بدائرة اختصاص المجلس التابعين له وفقا لأحكام المادة 206 من قانون الإجراءات الجزائية[2] نفسه ماعدا ضباط الشرطة التابعين للأمن العسكري يؤول الاختصاص بشأنهم إلى غرفة الاتهام بالجزائر العاصمة وفقا لنص المادة 207 من قانون الإجراءات الجزائية.

ومعلوم أن ضباط الشرطة القضائية نوعان:

النوع الأول: وهم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشأن الجرائم المنصوص عليها في قانون العقوبات.

النوع الثاني: يتمتعون بالاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر وهؤلاء هم المشار لهم بنص المادة 21 من قانون

[1] المادة 18 مكرر قانون الإجراءات الجزائية

[2] تنص المادة 206 من قانون الاجراءات الجزائية: " تراقب غرفة الاتهام أعمال ضباط الشرطة القضائية والموظفين والأعوان المنوطة بهم بعض مهام الضبط القضائي الذين يمارسونها حسب الشروط المحددة في المواد 21 والتي تليها من هذا القانون".

الإجراءات الجزائية وسلطتهم كذلك محدودة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني أو الأفنية أو الأماكن المحاطة بأسوار إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي وتعد محاضرهم ذات حجية وقوة إثبات كما استقر عليها القضاء الوطني[1].

أما فيما يخص الاختصاص المحلي لضباط الشرطة القضائية والذي يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في التحري والبحث عن الجريمة ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة، إلا أنه في حالة الاستعجال يجوز لهم أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به ويجوز لهم أيضا في حالة الاستعجال أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا ويجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفهم في المجموعة السكنية المعنية[2]، وأن يخبروا مسبقا وكيل الجمهورية الذين يباشرون مهمتهم في دائرة اختصاصه[3].

وفي المدن المقسمة إلى عدة دوائر للشرطة يمتد اختصاص محافظي وضباط الشرطة القضائية إلى كافة المجموعة السكنية للمدينة، أما ضباط الشرطة القضائية التابعين لمصالح الأمن العسكري، فإن اختصاصهم وطني، أي يمتد لكافة الإقليم الوطني

[1] زيدان زيبخة، المرجع السابق، ص106–107.

[2] المادة 116 فقرة 1 و2 من قانون الإجراءات الجزائية.

[3] محمد خزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، الطبعة الثامنة متممة ومنقحة، 2013، ص90.

ولا تطبق عليهم شروط تمديد الاختصاص وضوابطه المنصوص عليها في المادة 16 من قانون الإجراءات الجزائية.

وإذا تعلقت الأبحاث والمعاينات بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإن قانون الإجراءات الجزائية في المادة 16 فقرة 7 منه قد وسع مجال الاختصاص المحلي لضباط الشرطة القضائية وجعله وطنيا مهما كانت الجهة التي ينتمي إليها ضابط الشرطة القضائية من فئة الدرك الوطني أو الأمن الوطني وهذا تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات[1]، وهذا التعديل جاء به القانون رقم 06-22 المؤرخ في 2006/12/20 ويعد ضروريا بالرغم من أنه تأخر بعض الشيء عن صدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 والذي عدل قانون العقوبات والذي أدرج فيه الفصل السابع مكرر وخصصه للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات.

ويلتصق بمهام الضبط القضائي أعمال المعاونة والمساعدة المنوطة بأعوان الضبط القضائي الذين تعرفهم المادة 19 من قانون الإجراءات الجزائية ويلحق بذلك أيضا سلطات الولاة في مجال الضبط القضائي والمحددة في حالة وقوع جناية أو جنحة ضد أمن الدولة

[1] المادة 16 فقرة 4،5،6،7 و8 قانون إجراءات جزائية.

وعندما تكون الحالة مستعجلة فقط ولم يصل إلى علم السلطات القضائية بالواقع ومما تعين تأكيده كنقطة هامة هو أن اختصاص الضبطية القضائية يتصل بالنظام العام تطبيقا للقواعد العامة في الإجراءات.

ويفرق المشرع الجزائري بين مراحل التحقق في الجريمة، فالمرحلة الأولى تسمى بجمع الاستدلالات يجمع رجال القانون على تسميتها بالتحقيق الابتدائي وهي التي أوكلت إلى ضباط الشرطة القضائية فبالإضافة إلى مهمة البحث والتحري وجمع الأدلة في الجرائم والبحث عن مرتكبيها وكذا تنفيذ طلبات الجهات القضائية[1]، فيما تنص المادة 17 فقرة 1 و2 من قانون الإجراءات الجزائية على ضباط الشرطة القضائية مهمة تلقي الشكاوي والبلاغات وإجراء التحقيقات الابتدائية وعند مباشرة التحقيقات وتنفيذ الإنابة القضائية لا يجوز لهم طلب أو تلقي أوامر أو تعليمات إلا من الجهة القضائية التي يتبعونها وذلك مع مراعاة أحكام المادة 28[2]، أن يبادروا وبغير تمهل بإخطار وكيل الجمهورية التي يعلمون بها وأن يوافوه بأصول المحاضر التي يحررونها مصحوبة بنسخة منها وكذا جميع المستندات والوثائق المتعلقة بها والأشياء المضبوطة[3]، ومهلة إرسال هذه المحاضر إلى النيابة حددها القانون بمهلة خمسة أيام الموالية لتاريخ معاينة المخالفة على الأكثر إذا ما تمت هذه المعاينة من طرف ذو الرتب في الشرطة البلدية وذلك عن طريق

[1] زيدان زيبخة، المرجع السابق، ص119.

[2] محمد حزيط، المرجع السابق، ص94.

[3] المرجع نفسه، ص95.

ضباط الشرطة القضائية وهو ما أشارت إليه المادة 26 بعد تعديلها بموجب المرسوم التشريعي رقم 93-14 المؤرخ في 04 ديسمبر 1993 ومما يجب تأكيده أن محاضر الضبطية القضائية وان اعتبرها المشرع في نص المادة 215 من قانون الإجراءات الجزائية سوى مجرد استدلالات فإنه في الحالات الأخرى والتي يجول بموجبها ضباط الشرطة وأعوانهم سلطة إثبات بعض الجرائم وتعد محاضرهم ذات حجية مالم يوجد دليل عكسي بالكتابة أو بشهادة الشهود كما أكدت ذلك المادة 216 من قانون الإجراءات الجزائية وكمثال على ذلك المحاضر التي يحددها ضباط الشرطة القضائية أو عونين محلفين على الأقل من الذين أشير إليهم، ومن أمثلة المحاضر المشار له على سبيل الحصر ما أوردته المادة 32 من الأمر رقم 05-06 المؤرخ في: 2005/08/23 المتعلق بمكافحة التهريب[1].

الفرع الثاني

الاختصاص المحلي لقاضي التحقيق في جريمة المساس بأنظمة المعالجة الآلية للمعطيات

سار المشرع الجزائري بوتيرة متسارعة على خطي التشريعات العالمية في إطار مواكبة التطور الحاصل في مضمار القانون لمجابهة التطور الحاصل في مجال الإجرام

[1] زيدان زيبخة ، المرجع نفسه، ص119- 120 .

بصوره الحديثة سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1]، وتحدد قواعد الاختصاص المحلي لقاضي التحقيق لكل جهة قضائية مجالا جغرافيا معينا لا يجوز الخروج عليه، والنطاق الجغرافي المنصوص عليه بالمادة 40 من قانون الإجراءات الجزائية عدة تعديلات بداية بالأمر 69-73 المؤرخ في 1969/09/16 والتعديل الأخير الصادر في 2004/11/10.

وجاء في المادة 40 ق إ ج[2] " يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر"[3].

يجوز تمديد الاختصاص المحلي لقاضي التحقيق 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، وتقابله المادة 329 قانون إجراءات جزائية المتعلقة بالمحاكمة[4].

[1] المرجع نفسه، ص144.

[2] المادة 40 قانون إجراءات جزائية.

[3] وائل بندق أنور، موسوعة القانون الإلكتروني وتكنولوجيات الاتصالات، دار المطبوعات الجامعية، الاسكندرية، الطبعة الأولى، 2007، ص1090.

[4] فضيل العايش، شرح قانون الإجراءات الجزائية، بين النظري والتطبيقي، دار البدر، الجزائر، د. ط ، ص149.

ومن الملاحظ أن تمديد الاختصاص المحلي لقاضي التحقيق مشمولا كذلك بتمديد الاختصاص للمحاكم القضائية ووكلاء الجمهورية إلى النطاق المحدد وذلك من خلال المرسوم التنفيذي رقم 06-348 المؤرخ في5 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[1].

أولا: محكمة سيدي محمد الجزائر العاصمة

تشمل جميع محاكم المجلس القضائية التالية: الجزائر، البليدة، الجلفة، بومرداس، الشلف، البويرة، تيبازة، الأغواط، تيزي وزو، المسيلة، عين الدفلى.

ثانيا: محكمة قسنطينة

يمتد اختصاصها المحلي ولوكيل الجمهورية وقاضي التحقيق بها إلى المجالس التالية: قسنطينة، بجاية، جيجل، عنابة، الطارف، سوق أهراس، أم البواقي، بسكرة، سطيف، قالمة، الوادي، ميلة، باتنة، تبسة، سكيكدة، برج بوعريريج، خنشلة.

ثالثا: محكمة ورقلة

يمتد اختصاصها المحلي كذلك وكذا كل من وكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس التالية: ورقلة، ايليزي، أدرار، تيندوف، تمنراست، غرداية.

رابعا: محكمة وهران

[1] زيدان زيبخة، المرجع السابق، ص111.

تشمل المجالس التالية : وهران، تيارت، مستغانم، تيسمسيلت، غيليزان، بشار، سعيدة، معسكر، النعامة، تلمسان، سيدي بلعباس، البيض، عين تيموشنت.

ولقد تم تحويل الاختصاص حسب نص المادة 06 من المرسوم للبث فيها لرئيس المجلس القضائي الذي تقع في دائرة اختصاصه المحكمة التي تم تمديد اختصاصها، بمعنى رئيس مجلس قضاء الجزائر وقسنطينة وورقلة ووهران حيث اصطلح على تسميتها في التشريع الجزائري بالأقطاب أو محكمة القطب، فبالإضافة إلى توسيع الاختصاص المحلي في مجال تتبع الجرائم المعلوماتية فإن القانون يجبرها بأن تباشر إجراءات المتابعة تلقائيا في الحالات المتعلقة بالجرائم المنصوص عليها في المواد 144 مكررو 144 مكرر1 و 144 مكرر2 ومن ضمنها جرائم القذف المرتكبة عن طريق الوسيلة الإلكترونية أو المعلوماتية ضد رئيس الجمهورية أو الرسول "ص" أو بقية الأنبياء وكذا المعلوم من الدين بالضرورة[1].

الفرع الثالث

المركز العالمي للشكاوى الخاصة بجرائم الإنترنت

يعتبر من أهم المؤسسات في مجال محاربة جرائم الإنترنت، تأسيس سنة 1999 في الولايات المتحدة الأمريكية، وتمت هيكلته بشكل رسمي سنة 2002 بولاية وست

[1] زيدان زيبخة، المرجع نفسه، ص112– 113.

فرجينيا بالولايات المتحدة الأمريكية، ودوره يكمل في تلقي الشكاوى من الشاكين في إطار جرائم الإنترنت عبر العالم وعن طريق الشبكة المعلوماتية وموقعه هو (http://www.ic3.gov) ويتلقى الشكاوى من أي شخص في أية بقعة من العالم ويعمل هذا المركز على التعاون مع مختلف المنظمات الدولية المتخصصة والوكالات الدولية المنخرطة في محاربة جرائم الإنترنت لما في ذلك الوكالات والجهات الخاصة بتطبيق القانون[1].

الفرع الرابع

الاختصاص القضائي لجريمة المساس بأنظمة المعالجة الآلية للمعطيات

لقد تخطى القانون الجزائري مشكلة امتداد التفتيش خارج الإقليم الوطني بموجب ما رسمه القانون 09-04 من معالم لكن لا تزال مشكلة الاختصاص القضائي وملائمة القانون الواجب التطبيق قائمة في مجال جرائم الإنترنت وإذا كان المشرع الجزائري بادر بتعديل قانون الإجراءات الجزائية بموجب القانون 04-14 المؤرخ في 10نوفمبر 2004 حيث عدل المادة 329 من قانون الإجراءات الجزائية وذلك بجواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات...) وقد جاء عقب ذلك المرسوم التنفيذي رقم06-348 المؤرخ في 2006/10/5 المتضمن تمديد

[1] المرجع نفسه، ص110.

الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ليشيد فعليا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.....)[1].

ويتم تمديد الاختصاص عند ما يرى ضابط الشرطة القضائية أن الملف المكون من طرفه في مرحلة البحث والتحري يشكل جريمة المساس بأنظمة المعالجة الآلية للمعلوماتية أن يخبر فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويقدم له أصل ملف الإجراءات مرفق بنسختين ثم يقوم وكيل الجمهورية فورا بإرسال النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة ذات الاختصاص الموسع وفقا للسلم الإداري وبعد اطلاع النائب العام على الملف واعتباره يدخل ضمن اختصاص المحكمة ذات الاختصاص الموسع أي ضمن الجرائم السالف ذكرها يحيله إلى وكيل الجمهورية لدى المحكمة ذات الاختصاص الموسع أي محكمة قسنطينة بالنسبة لمجلس قضاء قالمة وبعد تمسك هذه الجهة باختصاصها فإن ضباط الشرطة القضائية المنجزة للملف تتلقى تعليمات مباشرة من وكيل الجمهورية للمحكمة ذات الاختصاص الموسع.

يجوز للنائب لدى المجلس القضائي التابعة له المحكمة ذات الاختصاص الموسع أن يطالب بالإجراءات في جميع مراحل الدعوى وحتى إذا ما تم فتح تحقيق قضائي أمام قاضي التحقيق لدى محكمة مكان ارتكاب الجريمة وتبين بعد ذلك أن الجريمة تدخل ضمن

[1] زيدان زيبخة، المرجع نفسه، ص174.

اختصاص المحكمة ذات الاختصاص الموسع فإنه يتعين على قاضي التحقيق الأول أن يصدر أمرا بالتخلي لفائدة قاضي تحقيق لدى المحكمة ذات الاختصاص الموسع وفي هذه الحالة أيضا يتلقى ضباط الشرطة التعليمات والإنابات مباشرة من قاضي التحقيق لدى المحكمة ذات الاختصاص الموسع، غير أنه إذا ما سبق لقاضي التحقيق لدى محكمة مكان ارتكاب الجريمة إصدار أمرا بالقبض أو أمرا بالحبس المؤقت ثم أحيل الملف على قاضي التحقيق لدى المحكمة ذات الاختصاص الموسع فإن هذه الأوامر تحفظ بقوتها التنفيذية إلى أن تفصل فيها المحكمة ذات الاختصاص الموسع[1]، غير أن الاختصاص لا يثير أي إشكال عندما يتعلق الأمر بهذه الجريمة يرتكبها شخص داخل إقليم الوطن، و إنما تنجم الصعوبة عندما تمتد مجريات التحقيق والتحري خارج أرض الوطن أو عندما ترتكب الجريمة من خارج الوطن أو يكون لها امتداد إذ أن الوضع هنا بصدد عولمة الجريمة.

فجريمة المساس بأنظمة المعالجة الآلية للمعطيات وفي ظل انفتاح الأسواق العالمية وارتباطها دوليا أصبحت ليس لها حدود معينة، وبات التعامل التجاري والمالي عبر الإنترنت هو السيمة الرئيسية في مجال ما بات يعرف بالتجارة الإلكترونية وانتشار أنظمة الدفع الإلكترونية المالية مما قد ينجر عن هذه العمليات من أنشطة غسل الأموال وإخفاء لمصادرها غير المشروعة، وقد حاول المشرع الجزائري إيجاد حل لهذه النقطة على غرار التدابير التي أوردها القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من

[1] عبد المجيد جباري، المرجع السابق، ص119- 120.

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذ نص في المادة 15 منه على" أنه وفضلا عن الاختصاص المنصوص عليه في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجانب وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

يستخلص من هذه المادة بأن المحاكم الجزائرية ينعقد لها الاختصاص في الفصل في الجرائم التي لها صلة بتكنولوجيات الإعلام والاتصال والتي يرتكبها شخص أجنبي وخارج الوطن عند ما يكون غرضها مستهدفا ما يلي:

-مؤسسات الدولة الجزائرية

-هيئات الدفاع الوطني

-المصالح الإستراتيجية للاقتصاد الوطني.

فالملاحظ أنه بإمكان العدالة الجزائرية مباشرة الدعوى الجزائية ضد شخص أجنبي مشتبه به أو قام بارتكاب جريمة من الجرائم التي لها صلة بتكنولوجيات الإعلام والاتصال ومعلوم أن المشرع الجزائري أورد قسما خاصا بهذه الجرائم وهو القسم السابع مكرر في قانون العقوبات والمستحدث بموجب التعديل الذي جاء به القانون رقم 04-15 المؤرخ في 10 نوفمبر2004 ونص عليها في المواد 394 مكرر إلى 394مكرر7 وعندما

يثبت بأن هذه الجريمة تستهدف الأغراض المشار لها وتتم إحالته إلى المحاكم الجزائية التي تعتبر مختصة بموجب المادة 15 من القانون 09-04 المشار لها ويلاحظ أنه وبالإضافة إلى المساعدة القضائية الدولية المتبادلة المنصوص عليها في المادة 16 من نفس القانون فإن المشرع أوكل مهمة تبادل المعلومات التي من شأنها جمع المعطيات التي تفيد في التعرف على مرتكب الجريمة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1].

أما فيما يخص جمع الأدلة الخاصة بالجريمة الإلكترونية يعد من إجراءات التحقيق القضائي ويمكن أن يكون بواسطة الدخول إلى المنظومة المعلوماتية المشكوك في تخزينها للمعلومات المبحوث عنها، ونظرا للطابع الخاص لهذا النوع من الجرائم وما يتطلب تعقبها من سرعة فإن المشرع أجاز في حالة الاستعجال قبول طلبات المساعدة القضائية الدولية حتى وإن ورد عن طريق وسائل الاتصال السريعة مثل: الفاكس أو البريد الإلكتروني شريطة التأكد من صحتها وبهذا الصدد أوجبت المادة 36 من القانون رقم 05-06 الصادر في 2005/08/23 والمتعلق بمكافحة التهريب المعدل بالأمر 06-09 المؤرخ في 2006/07/15 على أنه " وفي حالة توجيه الطلب إلكترونيا من طرف السلطات الأجنبية يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا".

[1] زيدان زيبخة، المرجع السابق، ص174- 175- 176.

أولا: القيود الواردة على المساعدة القضائية الدولية

اللجوء إلى الإنابة أو المساعدة القضائية ليست مطلقة في نظر المشرع الجزائري بل أنها مقيدة بشروط منها ما يلي:

1- أنها تتم وفقا للاتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات واتخاذ الإجراءات التحفظية أو تسليم المجرمين فيما هو مرتبط بجريمة المساس بأنظمة المعالجة الآلية للمعطيات.

2- تخضع لمبدأ المعاملة بالمثل وهو المبدأ الذي أكدته م 29 من القانون رقم 05-01 الصادر في 2005/02/06 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحته.

أما القيود الواردة عليها فقد حصرتها المادة 18 من القانون 09-04 فيما يلي:

أ - أنها لا تنفد ولا يمكن الاستجابة لها في الحالات التالية:

- إذا كان فيها مساس بالسيادة الوطنية

- إذا كانت ماسة بالنظام العام.

ب- ويمكن الاستجابة لها بشروط منها:

- شرط المحافظة على سرية المعلومة المبلغة لتلك الدولة.

– شرط عدم استعمالها في غير الحالة المحددة والموضحة حصريا في طلب المساعدة القضائية وقد ألزمت الاتفاقية الدولية الموضوعة للتوقيع بمقر الأمم المتحدة في نيويورك في 2005/09/14 والخاصة بقمع أعمال الإرهاب النووي ألزمت الدول الأطراف باتخاذ التدابير لحماية سرية المعلومات التي تحصل عليها سرا بموجب الاتفاقية من دولة أخرى[1].

المطلب الثاني

أساليب التحري والتحقيق في جريمة المساس بأنظمة المعالجة الآلية للمعطيات

لم يكتفي المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل جريمة المساس بأنظمة المعالجة الآلية للمعطيات كظاهرة حديثة وبهذا الصدد جاء القانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ومنا ما

[1] زيدان زيبخة، المرجع نفسه، ص145.

نصت عليه المادة 3 منه[1] مما تتطلبه مستلزمات التحريات أو التحقيقات القضائية وهي وضع ترتيبات تقنية هدفها مراقبة الاتصالات الإلكترونية وتجميعها وتسجيلها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية وشروط صحة هذه الإجراءات ومهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الأول

الإجراءات الخاصة المنصوص عليها في القانون 04/09.

نتناول بالدراسة ضمن هذا الفرع، كيفية مراقبة الاتصالات الإلكترونية أولا، وتجميعها وتسجيلها ثانيا، والقيام بإجراءات التفتيش ثالثا وإجراءات الحجز رابعا.

أولا: مراقبة الاتصالات الإلكترونية[2]

نصت عليها المادة 4 من القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حالات اللجوء إلى المراقبة الإلكترونية وهي محددة على سبيل الاستثناء وهي:

[1] المادة 3 من القانون 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها راجع الجريدة الرسمية 47 المؤرخة في 16 نوفمبر 2009، ص6.

[2] يقصد بالاتصالات الإلكترونية هي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية. راجع: المادة 02 من القانون 09-04، الجريدة الرسمية 47 المؤرخة في 16 أوت 2009، ص5.

– الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

– حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– مقتضيات التحريات والتحقيقات القضائية عند ما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

– ويتم هذا الإجراء أي في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة بإذن مكتوب من السلطة القضائية المختصة، إلا أن النائب العام لدى مجلس قضاء الجزائر يختص بمنح الإذن لمدة ستة أشهر قابلة للتجديد لضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[1]، كون هذا الإجراء ربطه بإذن مكتوب من السلطة القضائية المختصة لعدم المساس بحرمة الحياة الخاصة وخصوصيتها وهي مقدسة ومحمية دستوريا وذلك من خلال المادة 39 من الدستور (أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة[2]، ويبدو أن المشرع الجزائري نص صراحة في المادة (65 مكرر 5 على نوع الجرائم التي يجوز فيها اعتراض المراسلات العادية كونه لم يستثنيها والتي تتم عن طريق وسائل الاتصال

[1] www.droit.dz.com/forom، المرجع السابق، تاريخ التصفح 22 أفريل 2014 الساعة11:10 ،

[2] فضيل العايش، المرجع السابق، ص128.

السلكية واللاسلكية ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك لعدم كفاية الوسائل التقليدية لجمع الدليل الإلكتروني نظرا لما تتميز به هذه الجريمة المستحدثة من خصوصية وذلك بإذن من وكيل الجمهورية[1]، ونتيجة لذلك حرصت أغلب التشريعات على توفير الحماية الجنائية على سرية الاتصالات الخاصة للأفراد، حيث عاقب المشرع الجزائري لأول مرة اعتراض الاتصالات السلكية واللاسلكية بدون إذن بموجب القانون رقم (06-23 المؤرخ في 20 ديسمبر 2006) المعدل لقانون العقوبات الجزائري، حيث تنص المادة 303 مكرر من قانون العقوبات على أنه :" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث(3) سنوات وبغرامة من 50000دج إلى 300000دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية بغير إذن صاحبها أو رضاه.

[1] تنص المادة(65 مكرر5) من قانون الإجراءات الجزائية على انه:" إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:
- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

2- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

ويعاقب على الشروع في هذه الجرائم بنفس عقوبات الجريمة التامة ويضع صفح الضحية حدا للمتابعة الجزائية.

وهذه الحماية لم تقتصر عند تجريم الأفعال الخاصة بالاعتراض بل شملتها أيضا إلى عقاب كل من احتفظ أو وضع أو سمح بأية وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

أما بالنسبة للمشرع المصري فقد عاقب بالحبس مدة لا تقل عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك في حالة ارتكاب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضا المجني عليه:

1 - استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التلفون.

2 - التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص، نص المادة(309 مكرر قانون عقوبات مصري).

وباستقراء نص المادة (303 مكرر) قانون العقوبات الجزائري والمادة (309 مكرر) قانون عقوبات مصري، يلاحظ أنهما يخصان المحادثات الخاصة التي تتم في مكان خاص، وأيضا التي تتم عن طريق التلفون، دون المحادثات التي تتم عن طريق

الكمبيوتر، والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية[1].

ثانيا: تجميع الاتصالات الإلكترونية وتسجيل محتواها

تتميز الرسالة الإلكترونية بالطابع الخاص لكنها لا تختلف عن الرسالة الورقية من حيث حفظها أو الاستغناء عنها وإهمالها لكن ما يميز الرسالة الإلكترونية سواء المهملة أو المحفوظة يمكن الوصول إليها عن طريق صناديق البريد الخاصة أو الملفات المحفوظة أو الرجوع إلى سلة المهملات فالتحقيق الذي يجري بغرض ضبط المراسلات الإلكترونية يكون أمام ثلاث خيارات بعد الولوج إلى البريد الإلكتروني (E.MAIL)

فبعد تحديد صندوق البريد للمتهم المشكو منه يتمحور العمل حول ثلاث عناصر وهي: الوارد(IN) الصادر (OUT) الحفظ وسلة المهملات (TRASH) فبذلك يمكن مراجعة قائمة الرسائل التي وصلت إلى المشكو منه في الوارد والعكس بالنسبة للمرسلة منه على قائمة الصادر وكذا الشأن بالنسبة للرسائل المحفوظة أو المهملة غير أن ما يجب تأكيده هنا هو أن المشرع ونظرا لحساسية الموضوع والذي يعد مرتبطا بقدر كبير بذاتية الأشخاص فقد جعل تدابير إجراءات التحقيق تحت طائلة المسؤولية الجزائية عندما نص في المادة 4 من القانون 09-04 فقرة (د) والأخيرة على أن الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) من نفس المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها

[1] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات في القانون الجزائري والقانون المقارن الجنائي، دار الجامعة الجديدة، د.ط ، 2010، ص169- 170.

وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير[1].

ثالثا: تفتيش المنظومة المعلوماتية

أوردها القانون رقم 09-04 المشاركة سابقا في المادة الخامسة منه" إذ أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية الدخول إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ولو عن بعد بغرض التفتيش"، كما أن القانون حدد في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كما أن القانون أجاز تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية[2].

ويتضح من خلال نص المادة الخامسة من القانون 09-04 والتي أوردناها أعلاه بأن التفتيش في مجال المنظومة المعلوماتية يختلف عما هو متعارف عليه في القواعد العامة نظرا لطبيعته ومجاله، ولم يورد المشرع الجزائري تعريفا خاصا دقيقا للتفتيش بقدر ما

[1] زيدان زيبخة، المرجع السابق، ص 128- 129.

[2] المادة 5 من القانون رقم 09-04 المؤرخ في 05/أوت/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. راجع: الجريدة الرسمية 47 المؤرخة في 16 أغسطس2009، ص5 .

اعتبره إجراء من إجراءات التحقيق[1] غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شأنها، وإذا كان التفتيش المتعارف عليه في الواعد الإجرائية العامة هو نوعان، تفتيش المساكن وتفتيش الأشخاص من خلال المواد 44 و64 من قانون الإجراءات الجزائية فإن التفتيش المنصب على المنظومة المعلوماتية يختلف عنه كليا من حيث شروطه وموضوع التفتيش.

ويلاحظ بأن التفتيش يأخذ منحنين، فهو إما أن يكون من أعمال التحقيق تقوم به السلطات القضائية المختصة، وإما أن يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناءا على أمر تصدره السلطة المختصة وفي كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر (الحاسوب) بمكوناته المادية والمعنوية، فتتمثل المكونات المادية في مجموعة وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها استقبال البيانات المعلوماتية غير المعالجة وأيضا لها في داخل جهاز الحاسوب وحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما يحتويه من ذاكرة رئيسية وعشوائية وذاكرة القراءة ثم وحدة الحساب والمنطق وتتكون من مجموعة دوائر حسابية ومنطقية وسجلات لتنفيذ العمليات وتنقسم إلى وحدة المعالجة المركزية ووحدة الذاكرة ثم وحدة التحكم ووحدة الذاكرة المساعدة ووحدة الإخراج والتي تحتوي

[1] فضيل العايش، المرجع السابق، ص113.

على أجهزة الشاشة والطابعة ومشغلات الأقراص وهي التي تشغل المعلومات المعالجة وتمريرها وإخراجها للمستخدم.

أما المكونات المعنوية لجهاز الكمبيوتر وتسمى أيضا بالكيانات المنطقية وهي عبارة عن مجموعة من البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات، ولا يشكل التفتيش أي عائق عندما يستهدف الكيانات المادية للحاسوب إذ من السهولة ضبط الأجهزة وحجزها أو إتلافها وإنما الإشكال يثور عندما ينصب التفتيش على المكونات المعنوية للكمبيوتر كالبرامج وقواعد البيانات كون ذلك يتطلب الكشف عن الرقم السري الكود(code) للمرور إلى الملفات وكذا كلمات السر أو الشفرات أو ترميز البيانات[1].

ويستخلص من نص المادة 05 من القانون 09-04 المشار له سابقا بأن المشرع الجزائري يدرج التفتيش في مجال جرائم المعلوماتية في إطار قانون الإجراءات الجزائية لكن موضوع التفتيش في مجال المعلوماتية يختلف عن التفتيش العادي، يتوقف أساسا على طبيعة المكان الذي يحتوي على أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أم عاما هذا فضلا عن تحديد الإقليم فيما إذا كان وطنيا أم أجنبيا وذلك من خلال ما صرحته المادة 05 المشار لها بالقول بأنه " يجوز للسلطة القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد"، فإنه يتبين بوضوح بأن التفتيش يكون في الأصل بصفة مباشرة بالانتقال إلى مسكن المتهم أو المكان الذي تتواجد فيه الأجهزة

[1] زيدان زيبخة، المرجع السابق، ص131- 132.

المقصودة أو في الأماكن العامة حال حيازة شخص لجهاز الحاسوب الآلي أو أحد مكوناته المادية كوسائط التخزين مثل الأقراص المرنة والصلبة والمضغوطة والأشرطة الممغنطة فواضح بأن القانون أحال هذه الإجراءات على القواعد العامة في قانون الإجراءات الجزائية.

ومن بين أهم عناصر التفتيش وفقا لأحكام المادة 44 من قانون الإجراءات الجزائية سيما بعد التعديل الذي حصل بموجب القانون 06-22 المؤرخ في 20 سبتمبر 2006 وهي:

-وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.

-الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.

-أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

-حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

-في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته.

أما التفتيش في الأماكن العامة وهي التي يرتديها العامة في كل وقت ولا تتمتع بحرمة المنزل ومن الضروري التمييز بين نوعين من الأماكن العامة (الأماكن العامة بطبيعتها والأماكن العامة بالتخصيص أو المصادفة)

فالأولى لها صفة العامة على وجه دائم مثل الشوارع والحدائق العامة أما الثانية فيرتادها الجمهور في أوقات محددة كالمقاهي والمطاعم، ويمكن دخولها خلاف للأماكن الخاصة وتفتيشها إذا ما تم غلقها لانتهاء فترة العمل وانصراف العامة فتأخذ الخصوصية كذلك الشأن فيما يحتويه من مكاتب أو غرف خاصة لصاحبها ومن الواضح أن التفتيش الذي ينصب على مكونات الحاسوب المادية تبدو عادية نظرا لإمكانية ضبط وحجز تلك المكونات وإتلافها جزئيا أو كليا[1] ولا يتم التفتيش والضبط للأشياء إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة لرضاه.

وتطبق فضلا عن ذلك أحكام المواد من 44 إلى47 من هذا القانون[2].

إلا أن القانون الجزائري قد خالف نص المادة 64 من قانون الإجراءات الجزائية وأورد عليها استثناءات بموجب القانون(06-22) المعدل والمتمم للأمر رقم (66-156) والمتضمن قانون الإجراءات الجزائية، حيث استثنى المشرع تطبيق هذه الضمانات على طائفة من

[1] زيدان زيبخة، المرجع نفسه، ص133-134.

[2] المادة 64 من قانون الإجراءات الجزائية.

الجرائم المذكورة في المادة 47 فقرة3[1] من القانون رقم (06-22) ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2].حيث نص في المادة 64 الفقرة الثالثة "غير أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47 فقرة 3 من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة47 مكرر حيث أجاز إجراء التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص.

والملاحظ أن المشرع الجزائري غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لا سيما حرمة المسكن باعتبارها مستودع أسرارهم، فظاهر النص يشير إلى التعدي (المشروع) على حرمة الحياة الخاصة للشخص، إلا أن ما يبرره ويقل من خطورته الطبيعة الخاصة للجريمة فهي جريمة قابلة للمحو والتعديل في أقل من ثانية، ومرتكبها ذو دراية بالأمور التقنية، وقد تكون الصعوبة أكثر إذا كان هذا الدليل الإلكتروني الوحيد في الدعوى

[1] تنص المادة (3/47) " عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة الحاسب والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم تبييض الأموال فإنه يجوز إجراء التفتيش والمعاينة و الحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص" .

[2] يلاحظ أن المشرع الجزائري عندما استثنى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا، يكون قد أدرك فعلا ميزة هذه الجرائم، من حيث قابلية الدليل الإلكتروني فيها للمحو والتدمير في أقل من ثانية، لذلك أن إرجاء التفتيش في الموعد القانوني قد يعرقل السير الطبيعي لمجريات التحقيق وهذا ما يؤدي إلى الإضرار بمصلحة العدالة.

الجنائية، لذلك أجاز المشرع إجراء تفتيش منزل المتهم في حالة واحدة وهي حالة صدور إذن من وكيل الجمهورية المختص.

أما بالنسبة للأماكن العامة، فإذا وجد الشخص فيها وهو يحمل مكونات الحاسب سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في القانون.

أ - تفتيش المنظومة المعلوماتية عن بعد

لقد أجاز القانون الجزائري تفتيش المنظومة المعلوماتية عن بعد من خلال القانون 09-04، ويكون الدخول إليها بدون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب فالتفتيش هنا يستهدف أشياء معنوية وفنية وليست مادية لأن هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومة بشأنها سيما إذا كانت هذه المعلومات غير مرتبطة بعد بأية دعامة مادية وقد أجاز المشرع الجزائري إفراغ أو نسخ تلك المعلومات المشكوك فيها أو التي من شأنها الإفادة في الكشف عن الجريمة أو مرتكبيها نسخها على دعامة تخزين إلكترونية تكون قابلة للحجز، كما أوردت ذلك المادة 6 من القانون 09-04 بخصوص حجز المعطيات والتي سوف نتطرق لها.

وللتوضيح فإن دعائم تخزين المعلومات مختلفة منها الأشرطة المغناطيسية، الأقراص الصلبة، الأقراص اللينة، ومنها كذلك المنتجات البصرية، أما إذا كانت تلك البرامج مندمجة مع كيان مادي كالقرص الصلب أو المرن...الخ، فإنه من السهل الوصول

إليها وضبطها كدليل إثبات ضد المتهم يقدم أمام المحكمة ولأن برنامج الحاسوب وقاعدة البيانات تتمتع بالحماية القانونية في القانون الداخلي وفي الاتفاقيات الدولية كما هو شأن التشريع الجزائري إذا اعتبر برنامج الحاسوب وقاعدة البيانات مصنفات فكرية محمية بموجب القانون 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة[1].

ففي فرنسا مثلا يرى بعض الفقهاء أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة، وبالتالي لا تعد من قبيل الأشياء المحسوسة المادية[2]، غير أن بعض الآراء الفقهية تعتبر بأن برنامج الحاسوب يمكن أن تنطبق عليه مواصفات " المادة" ويدخل في مجال الأشياء المادية سواء كان برنامج نظام أو برنامج تطبيقات ومعلوم أن برنامج الحاسوب وقواعد البيانات تتمتع بالحماية القانونية في التشريع الجزائري وكذلك في الاتفاقيات الدولية[3] ومنها اتفاقية برن في التاسع من سبتمبر 1887 والمكملة في باريس 1897.

فالتفتيش عن بعد للمنظومة المعلوماتية سواء عن قرب أي بطريقة مباشرة أو عن طريق الولوج عن بعد يأخذ طريقين:

[1] زيدان زيبخة، المرجع السابق، ص135.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص91.

[3] وقد علق المشرع الجزائري التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على شرط احترام الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل ومن ثمة نستخلص أنه لا غنى عن الاتفاقيات الدولية في مجال مكافحة هذه الجريمة.

-إما الدخول إلى المنظومة المعلوماتية أو جزء منها وكذا المعطيات أو البيانات المعلوماتية المخزنة فيها.

-أو الدخول إلى منظومة تخزين معلوماتية[1].

فإنه وانطلاقا مما سبق شرحه يمكن القول بأن أسباب ودواعي التفتيش ووفقا للقواعد العامة هي[2]:

- وقوع الجريمة سواء كانت جناية أو جنحة وهذا ما يستخلص من أحكام المادة 44 من قانون الإجراءات الجزائية.

- توجيه الاتهام لشخص أو لمجموعة أشخاص ممن يظهر أنهم ساهموا في الجريمة كما أشير إليه في المادة 44 المذكور غير أنه وخلافا لذلك كله فإن التشريع الجزائري وكما أسلفنا خرج عن هذه القواعد العامة بخصوص جريمة المساس بأنظمة المعالجة الآلية للمعطيات وجعل من التفتيش المنصب على المنظومة المعلوماتية إجراء وقائي في مواجهة ما قد يقدم عليه المجرم المعلوماتي واستعمال الرقابة التقنية لوسائل الاتصالات الإلكترونية قد تكون مسبقة لارتكاب أي جرم ودون توجيه الاتهام لأي شخص وقد وضحت ذلك المادة 5 من القانون 09-04 حين أشارت بالقول بأن تفتيش المنظومة

[1] زيدان زيبخة ، المرجع السابق، ص136.

[2] تعتبر شروط موضوعية للقيام بإجراء التفتيش.

المعلوماتية جائز في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 05 من نفس القانون 09-04[1].

ب- تمديد التفتيش إلى منظومة معلوماتية أخرى أو جزء منها(داخل الدولة):

تفطن المشرع الجزائري إلى تقنية ذات أهمية بالغة في عالم المعلوماتية ويتعلق الأمر بارتباط شبكة الحواسب ببعضها البعض وبالتالي وجود ترابط بين الأنظمة المعلوماتية فمن المعلوم أن شبكة الانترنت هي نفسها شبكة ممتدة من خلال اتصال أجهزة الحواسب الآلية اتصالا سلكيا أو لا سلكيا فتكون مرتبطة ببعضها في مكان واحد وهو ما يطلق عليه الشبكة المحلية أو موزعة ومرتبطة بواسطة خطوط الهاتف أو بواسطة الأقمار الصناعية، ويطلق عليها بالشبكة الممتدة وهي شبكة الإنترنت[2].

ومما يستخلص أن القانون 09-04 وفي المادة الخامسة 05 منه وتحسبا لما قد يقبل عليه المجرم الإلكتروني أو الجاني مستعمل أجهزة الحاسوب بغرض ارتكاب الجريمة من محاولات تهريب المعلومات وتسريبها من جهاز لآخر أو لتخزينها أو إخفائها فإن الوضع هنا يستدعي وفق ما تصوره المشرع طابع السرعة والدقة في تعقب آثار وخطوات هذه الأفعال وعليه فقد نصت المادة(05) المشار لها على ما يلي:

" في الحالة المنصوص عليها في الفقرة-أ- من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه

[1] زيدان زيبخة ، المرجع نفسه، ص139.

[2] زيدان زيبخة ، المرجع نفسه، ص139.

المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة سبقا بذلك والملاحظ أن تمديد التفتيش إلى منظومة معلوماتية أخرى مشكوك فيها يكتسي طابعا خاصا فهو يجري عن بعد وثانيا يتم بشكل سريع تماشيا مع طابع السرعة الفائقة الذي يجري عليه نقل المعلومة أو نقل المعلومات وواضح أيضا أن الولوج إلى منظومة المعلومات يتم هنا بمجرد الشك أو الاعتقاد بتواجد المعلومات محل البحث داخل المنظومة لكن ولكي تكسي هذه الإجراءات طابعها الرسمي وتقع تحت طائلة القانون أوجب المشرع أن يكون الدخول إلى النظام المعلوماتي المقصود قانونيا وذلك يندرج دون شك في إطار حماية الحياة الخاصة للأفراد تفرض إبلاغ الجهات القضائية المختصة مسبقا[1].

ت- الإنابة القضائية[2] في مجال تفتيش المنظومة المعلوماتية خارج الإقليم الوطني:

لقد أقر المشرع الجزائري إجراءات صارمة في مجال ملاحقة هذا النوع الجديد من الجريمة، ومن ذلك أنه وسع من نطاق التفتيش ولو عن بعد حين رخص في المادة 05 من القانون 09-04 للسلطة القضائية المختصة وكذا ضباط الشرطة القضائية الدخول إلى المنظومة المعلوماتية وحتى وأن تبين لهذه السلطات أو وجد لديها اعتقاد بأن المعطيات محل البحث مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن ذلك لا يمنع من

[1] المرجع نفسه، ص140.

[2] هو الإجراء الذي بواسطته يكلف قاضي التحقيق سلطات معينة بالقيام ببعض إجراءات التحقيق التي لا يريد أو لا يستطيع القيام بها بنفسه. راجع:أحسن بوسقيعة، التحقيق القضائي، دارهومة، الجزائر، الطبعة العاشرة، 2012، ص103.

تتبعها والوصول إليها لكن في إطار المساعدة الأجنبية بسلطاتها المختصة ويتم ذلك في نطاق الاتفاقيات الدولية التي تم إبرامها في مجال ملاحقة هذا النوع من الجريمة ويلاحظ أن المشرع الجزائري أورد هنا عبارة " وفقا لمبدأ المعاملة بالمثل" مما يفيد بأن المساعدة القضائية لها شروط وضوابط[1].

وفي نفس الاتجاه تجيز توصيات صدرت عن المجلس الأوربي بتمديد تفتيش الكمبيوتر إلى الشبكة المتصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة فتنص التوصية رقم(13 لسنة 1995) المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه " لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها ما دام أنه من الضروري التدخل الفوري للقيام بذلك"[2].

رابعا: حجز المعطيات المعلوماتية[3]:

تعتبر عملية التفتيش للمنظومة المعلوماتية الهدف الأساسي لوضع اليد على الأدلة المادية التي تساعد على كشف الحقيقة لكن من البديهي القول بأن حجز الأشياء المادية

[1] زيدان زيبخة، المرجع نفسه، ص144.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص97.

[3] تم حجز 200 قرص مضغوط يحتوي لقطات مختلفة لطالبات بعد مداهمة نوعية قامت بها الفرقة المتنقلة للشرطة القضائية التابعة لأمن دائرة منصورة في تلمسان، وسط الإقامة الجامعية مليحة حميدو للبنات، فضيحة أخلاقية من العيار الثقيل للأفلام الجنسية لطالبات إقامة مليحة حميدو في وضعيات مخلة بالحياء. راجع جريدة النهار، العدد 1954 بتاريخ 04 مارس 2014.

كالمعدات والأوراق والمستندات يعد شيئا سهلا وغير مثير لأية إشكالات في نظر القانون غير أنه ليس من السهل أبدا توقيع الحجز على منظومة معلوماتية ذلك أن المعلومات هي في الأصل شيء معنوي[1].

إذ يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، ويجوز استعمال الوسائل التقنية الضرورية لتشكيل وإعادة تشكيل المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات تحت طائلة العقوبات، إذا استعملت في غير الحدود الضرورية للتحريات أو التحقيقات القضائية كما أن القانون 09-04 نص على إمكانية الحجز عن طريق منع الوصول إلى المعطيات وذلك بأمر من السلطة التي تباشر التفتيش عن طريق تكليف أي شخص مؤهل باستعمال وسائل تقنية مناسبة لذلك.

وللوصول إلى الأدلة رأى المشرع من الضروري إلزام الأطراف المتدخلة في خدمات الإنترنت بتقديم المساعدات الضرورية للجهات المكلفة بالتفتيش والسلطات القضائية المتخصصة وقد خص القانون 09-04 الفصل الرابع منه لهذه النقطة بالذات وسوف فتطرق إليها فيما يلي:

أ- مساعدة السلطات (التزامات مقدمي الخدمات)

[1] زيدان زيبخة، المرجع السابق، ص148.

وبالإضافة إلى مقتضيات المرسوم التنفيذي رقم 98-257 المؤرخ في1998/08/25 والذي يحدد شروط وكيفيات استعمال خدمة الإنترنت والذي بموجبه فسح المجال لظهور مزودي الخدمة آخرين إلى جانب مركز البحث في الإعلام العلمي والتقني بالجزائر.

فإن المادة 10 من القانون 09-04 ألزمت مقدمي الخدمات بتقديم المساعدات للسلطات المكلفة بالتحريات القضائية والتفتيش كما ألزمتهم أيضا بكتمان السر بخصوص العمليات التي ينجزونها بطلب من المحققين وما تحصل عن ذلك من معلومات وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحقيق[1].

ويطلق على مقدمي الخدمات أحيانا الوسطاء في خدمة الإنترنت من الدخول إلى الشبكة والإطلاع عما يبحث عنه أو ما يريد معرفته ومنهم: **مزود الخدمة** وهو إما أن يكون شخصا طبيعيا أو معنويا يقوم بنقل الخدمة بتمكين أو تسهيل دخول المستخدم لشبكة الإنترنت وبهذا فإن مقدم الخدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها هذا المستخدم إذ بإمكانه معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها.

ومن هنا فإن مزود الخدمة بإمكانه مساعدة جهات التحقيق بكل المعلومات والتي يبحث عنها بل إنه ملزم بذلك وفقا لنص المادة 10 المشار لها ثم يوجد أيضا **متعهد**

[1] زيدان زيبخة، المرجع نفسه، ص153.

توصيل المعلومات ودوره تقني يتجسد في إيصال المستخدم إلى شبكة الإنترنت وذلك بربطه بالمواقع التي يريدها وليس له علاقة بالمعلومات أو بمحتواها.

بالإضافة أيضا إلى **متعهد الإيواء** هو إما أن يكون أيضا شخصا طبيعيا أو معنويا يقوم بعمل محدد وهو عرض الأمكنة على الشبكة أو بمعنى آخر إيواء صفحات (WEB) على حاسوبه الخادم مقابل أجر لصالح المستخدم الذي يعمل على نشر ما يريد من صور أو معلومات أو يقوم بربط علاقات مع مواقع أخرى، وقد عرفت المادة الأولى الفقرة الثالثة من الاتفاقية الأوربية لمكافحة جرائم المعلوماتية التي تم إقرارها في بودابست لسنة 2001 عرفت مزودي الخدمات بأنهم (كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الاتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة المعطيات المخزنة نيابة عن مزود الخدمة)[1]، ومعلوم أن المرسوم التنفيذي 98-257 المشار له رتب على عاتق مقدمي خدمات الإنترنت التزامات خلال ممارستهم لنشاطهم من خلال المادة 14 منه[2].

ب- حفظ المعلومات أو المعطيات المتعلقة بحركة السير

إلى جانب الالتزام المترتب على عاتق مقدمي الخدمات في مجال الإنترنت والمتعلق بمساعدة السلطات المكلفة بالتحريات والتحقيقات القضائية فإن القانون 09-04 رتب على عاتقهم كذلك التزاما آخر وهو المنصوص عليه في المادة 11 منه وهي حفظ المعلومات

[1] زيدان زيبخة ، المرجع نفسه، ص154.

[2] المرجع نفسه، ص155.

التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة وحدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب القانون على هؤلاء التزامات خاصة منصوص عليها في المادة 12 وهي:

1 - واجب التدخل فورا لسحب المعطيات أو المحتويات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل تقنية تحول دون الدخول إليها.

2 - وضع الترتيبات التقنية التي بموجبها يتمك حصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها وقد نصت المادة 11 المشار لها على ما يلي:

مع مراعاة طبيعة ونوعية الخدمات يلتزم مقدموا الخدمة بحفظ :

1 -المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

2 -المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال

3 - الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

4 - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

5 - المعطيات التي تسمح بالتعرف على المرسل إليه أو الاتصال وكذا عناوين المواقع المطلع عليها بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة –أ– من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

وفضلا عن العقوبات التي سلطها المشرع الجزائري على مقدمي الخدمة من أصحاب المحلات ومقاهي الإنترنت فيلاحظ أنه وفقا لما نصت عليه المادة 394 مكرر 6 من قانون العقوبات من مصادرة للأجهزة والوسائل وإغلاق المحلات فقد نص القانون 09-04 بمعاقبتهم بـــ 06 أشهر إلى 05 سنوات حبس وبغرامة من 50000 دج إلى 500000دج ومعاقبة الشخص المعنوي وفقا للقواعد المقررة في قانون العقوبات ويستخلص من نص المادة 11 أنه وحتى في حالة استعمال الهاتف فإن المتعاملين في هذا الشأن ملزمون كذلك بما هو محدد في الفقرة –أ– من المادة 11 أي القيام بحفظ المعطيات التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه ويلاحظ أن المشرع ربط بين مراقبة الشبكة الإلكترونية و شبكة الهاتف مع اختلاف وسائل المراقبة[1].

[1] زيدان زيبخة، المرجع نفسه، ص155– 156.

الفرع الثاني

شروط صحة هذه الإجراءات

نتناول ضمن هذا الفرع شروط صحة الإجراءات السابقة من خلال ذكر السلطة المخولة بتسليم الإذن أولا، وطبيعة الإذن ثانيا، وثالثا وأخيرا تسخير ذوي الاختصاص في إطار المساعدات التقنية.

أولا: السلطة المخولة بتسليم الإذن

فيما يتعلق بتسليم الإذن ميز المشرع بين مرحلتين، ففي مرحلة التحقيق الابتدائي فإن الجهة المخولة بمتابعة العملية المأذون بها هي النيابة العامة وقد جسدتها المادة 65 المذكورة في وكيل الجمهورية بالقول بأن العمليات تجري تحت مراقبته المباشرة ومما لا شك أن القانون 09-04 باعتباره قانونا خاصا يمكن اعتبار الإطار الإجرائي الذي رسمه مرجعا لكل هذه الإجراءات وهو يكون قد حول النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته والمنصوص عليها في المادة 13 من القانون 09-04 لمنحهم الإذن بمراقبة الاتصالات الإلكترونية والقيام بالتفتيش داخل المنظومة لمعلوماته والمحدد مدته بستة (06) أشهر قابل للتجديد غير أنه وفي مرحلة التحقيق القضائي فإن الجهة المختصة بمنح الإذن بوضع الترتيبات التقنية يمنحه قاضي التحقيق والذي يتولى بنفسه مراقبة العمليات المذكرة أما عن طبيعة التقنيات فإنه وأمام عدم

تعريفها في قانون الإجراءات الجزائية فإن القانون 09-04 أناط بضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأن يقدموا للنائب العام المختص بمنحهم الإذن تقريرا مفصلا يبينون فيه طبيعة تلك الترتيبات التقنية المراد استعمالها وتحديد الأغراض الموجهة لها والمستهدفة باستعمالها[1].

[1] زيدان زيبخة ، المرجع نفسه، ص162.

ثانيا: طبيعة الإذن ومدته:

أ- **الشروط الشكلية والزمنية:**

إذا كان القانون 09-04 قد حدد طبيعة الإذن بالمراقبة وشروطه الشكلية والزمنية كما أوردته المادة 3 منه ومنها:

1- أن يكون الإذن مكتوبا.

2- أن يصدر من السلطة القضائية المختصة.

3- أن يكون على أساس تقرير يبين الترتيبات التقنية المستعملة والأغراض الموجهة لها.

فإن هذا القانون لم يترك المجال مفتوحا أو مبهما بخصوص هذه الأغراض حتى لا تستغل تلك التقنيات للمساس بالحياة الخاصة للأفراد فحددها المشرع حصريا في الفقرة الأخيرة من المادة 03 المشار لها كما يلي:

" تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) من المادة (03)[1] موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها"، أما في قانون الإجراءات الجزائية وفي المادة 65 مكرر 07 وبموجب تعديل القانون 06-22 المؤرخ في 2006/12/20 قيد الإذن بالشروط التالية:

1- أن يكون مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد.

[1] المادة(03) من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. راجع: الجريدة الرسمية 47 المؤرخة في 16 أغسطس2009، ص6.

2- أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غير سكنية ونوع الجريمة التي تبرر اللجوء إلى هذه التدابير[1].

ثالثا: المساعدات التقنية في إطار البحث عن الجرائم المعلوماتية

أ- تسخير ذوي الاختصاص

أدرك المشرع من خلال القانون 09-04 مدى الصعوبة التي تواجه المحققين والقضاة على حد سواء في البحث عن الدليل الإلكتروني وفي رصده وحجز المعطيات المبحوث عنها وفي الدخول عن بعد في المنظومة المعلوماتية فإن نص المادة 05 من القانون 09-04 فقرة أخيرة تنص " يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

فكل من السلطات القضائية أو الضبطية القضائية وجهات التحقيق مخولة قانونا أن تصدر تسخيرة بموجبها تسخير أي شخص من ذوي الاختصاص والخبرة في مجال الإعلام الآلي يعهد إليهم بالجانب التقني أثناء التفتيش وبعده فهم المؤهلون والعارفون بكيفيات نسخ المعطيات على دعامات التخزين الإلكترونية وحجزها ووضع الحواجز التي تحول دون الوصول إليها إذا كان محتواها يشكل جريمة ذلك ما تؤكده المادة 08 من نفس

[1] فضيل العايش، المرجع السابق، ص126.

القانون، غير أنه ومما يلاحظ أنه لم يرد توضيحا بخصوص ممارسة المهام المنوطة بهؤلاء المسخرين وفيما إذا كانوا ملزمين بأداء اليمين وبكتمان السر المهني وفقا لمقتضيات المادة 45 من قانون الإجراءات الجزائية وما بعدها وأن انتدابهم يجري وفقا لأحكام المادة 143 وما بعد من قانون الإجراءات الجزائية.

ومن الواضح أن اعتماد التسخيرة يعين في نظر المشرع بخصوص هذه النقطة أمرا يضع هؤلاء الأشخاص تحت سيطرة مسخرهم[1].

ب- في إجراءات التسرب

استحدث المشرع الجزائري في مجال مكافحته لجرائم المساس بأنظمة المعالجة الآلية للمعطيات إجراء للكشف عن الجريمة ومرتكبيها وتقديمهم للعدالة لينالوا جزاء ما اقترفوه من جرم في حق المجتمع، وترجع العلة في استحداث مثل هذه الإجراء إلى عجز أساليب البحث والتحري التقليدية والتي لم تعد كافية وفعالة للكشف عن الجرائم المستحدثة من بينها جريمة المساس بأنظمة المعالجة الآلية للمعطيات، ويتمثل هذا الإجراء في عملية التسرب.

أدرج المشرع الجزائري عملية التسرب بموجب القانون رقم (06-22) المؤرخ في (20 ديسمبر 2006) المعدل والمتمم للأمر رقم(66-155) المتضمن قانون الإجراءات

[1] زيدان زيبخة ، المرجع السابق، ص168.

الجزائية، والذي أفرد الفصل الخامس منه تحت عنوان" في الشرب" والذي تضمن ثمانية مواد (من المواد 65 مكرر 11 إلى المادة 65 مكرر18)[1].

حيث تعرف المادة 65 مكرر12 من قانون الإجراءات الجزائية التسرب بما يلي:

" يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف .

يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض، هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب جرائم"[2].

ويتم هذا الإجراء في إطار الإذن المسبق وفقا لمقتضيات المادة 65 مكرر 11 من قانون الإجراءات والتي أجازت لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يصدر إذن بمباشرة عملية التسرب وذلك لضباط الشرطة القضائية أو أحد أعوانها وتحت مسؤولية ضابط الشرطة القضائية، والأفعال المنصوص عليها في المادة 65 مكرر 14 من قانون الإجراءات الجزائية هي:

– إفشاء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو المستعملة في ارتكابها.

[1] عائشة بن قارة مصطفى، المرجع السابق، ص119.

[2] المادة 65 مكرر 12 من قانون الإجراءات الجزائية.

– استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال، ويلاحظ أن المشرع شدد على حماية الضابط أو العون المتسرب ونص على معاقبة كل من يكشف هويته خلال مراحل التحقيق بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000دج إلى 200000دج.

أما إذا تسبب الكشف عن هويتة أعمال عنف أو ضرب أو جرح على أحدهم أو أفراد عائلتهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمسة سنوات إلى عشر سنوات والغرامة من 200000دج إلى 500000دج وإذا تسبب في الوفاة لأحد هؤلاء الأشخاص تكون العقوبة الحبس من 10 سنوات إلى 20 سنة والغرامة من 500000دج إلى 1000000دج[1].

1– مواصفات الإذن بالتسرب وطبيعته

أوجبت المادة 65 مكرر 15 من قانون الإجراءات الجزائية أن تتوفر فيه المواصفات التالية[2].

–أن يسلم فقط لضرورة التحري أو التحقيق القضائي.

–أن يكون مكتوبا

–أن يكون مسببا

[1] زيدان زيبخة، المرجع السابق، ص169– 170.

[2] المرجع نفسه، ص170.

وكل ذلك تحت طائلة البطلان فإغفال أي من هذه الشروط يؤدي إلى بطلان الإذن

-أن يذكر في الإذن طبيعة الجريمة التي ينصب عليها الإذن.

-يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته

-يحدد فيه المدة المقررة للعملية والمحددة بأربعة أشهر وهي قابلة للتجديد لمدة أربعة أشهر أخرى كل ما دعت الضرورة لذلك.

-أن تودع الرخصة أي الإذن في ملف الإجراءات بعد الانتهاء من عملية التسرب[1].

وقد أجاز قانون الإجراءات الجزائية في المادة 65 مكرر18[2] سماع ضابط الشرطة القضائية الذي جرت العملية تحت مسؤوليته كشاهد على العملية ومن نص المادة يتبين من خلال إشارتها بالقول سماعه بصفته شاهد دون سواه عدم جواز سماع الضابط أو العون الذي باشر عملية التسرب[3].

[1] المادة 65 مكرر15 من قانون الإجراءات الجزائية.

[2] المادة 65 مكرر18 من قانون الإجراءات الجزائية، تنص على أنه (يجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية).

[3] زيدان زيبخة، المرجع السابق، ص171.

الفرع الثالث

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

من خلال نص المادة 13 تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم، وتتولى الهيئة المذكورة في المادة 13 أعلاه من خلال المادة 14 المهام التالية:

أولا: تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

ثانيا: مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

ثالثا: تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم[1].

[1] المادة 13 و14 من قانون 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته. راجع: الجريدة الرسمية، العدد47، المؤرخة في 16 نوفمبر 2009، ص8.

المبحث الثاني

إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطـيات والجـزاءات المقـــررة لها

سنتناول في هذا المبحث إثبات الجرائم المعلوماتية في المطلب الأول، أما المطلب الثاني فنخصصه إلى الجزاءات المقررة للجرائم المعلوماتية.

المطلب الأول

إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات

تعتبر جريمة المساس بأنظمة المعالجة الآلية للمعطيات كغيرها من الجرائم لها أركانها وعناصرها، وتمر بذات المراحل التي تمر بها الدعوى الجنائية في شأن الجرائم العادية كالسرقة والقتل وهذه المراحل هي التفكير في الجريمة والتحضير لها، ثم تنفيذ الجريمة ومحاولة التخلص من آثارها، ولذلك تثور هنا مسألة استخلاص الدليل الذي تثبت به هذه الجريمة[1].

ولاستخلاص الدليل المعلوماتي فلا بد من معرفة طبيعة هذا الدليل الذي سوف نتطرق إليه في الفرع الأول، ومدى حجيته في الإثبات الجنائي في الفرع الثاني.

الفرع الأول

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، بهجات للطباعة والتخليد، مصر، طبعة خاصة، 2009، ص91.

طبيعة الدليل الإلكتروني

يختلف الدليل[1] الجنائي لإثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات تماما عن الدليل الجنائي في الجريمة التقليدية، حيث يعرف الدليل المعلوماتي بأنه ذلك الدليل المستمد من وسائط ترتبط بتقنية المعلومات، وكلها تدور حول استخدامات الحاسب الآلي وتطبيقاته وشبكة الإنترنت وغيرها من التقنيات الحديثة، ويتعلق بالطبع بجريمة معلوماتية، إذن فالدليل المعلوماتي يتعلق بجريمة معلوماتية وهي جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية[2]، وكونه يختلف مفهومه عنه في الجريمة التقليدية.

فإن أدلة الإثبات في مثل هذا النوع من الجرائم هي ذات نوعية مختلفة، فهي معنوية الطبيعة كمعلومات الدخول والبرامج مما أثار مشاكل كثيرة أمام القضاء من حيث مدى قبولها وحجيتها ومن حيث أيضا تحديد المعايير الواجب توافرها في تلك الأدلة حتى تكون لها حجية الإثبات، مثل قواعد الإثبات التقليدية[3].

أولا: طبيعة دليل الإثبات الإلكتروني أمام القضاء المدني

فإذا انطلقنا من مثال بسيط وهو إبرام عقد بين طرفين فإن ذلك المعقد إذا كتب على الورق وتم إمضاؤه من الجانبين فإن تلك الورقة هي دليل إثباته، وأما إذا كتب العقد

[1] يعتبر الدليل الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه. راجع : مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الثاني(أدلة الإثبات الجنائي)، دارهومة، الجزائر، الطبعة الرابعة، 2010، ص9.

[2] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة، الإسكندرية، الطبعة الأولى، 2009، ص709.

[3] **www.droit-dz.com/forum** ، المرجع السابق، تاريخ التصفح 2014/05/25 الساعة 11:00.

بالحاسوب فمعناه أن البيانات قد تم تخزينها في القرص الصلب أو القرص اللين أو القرص المضغوط أو الفلاش ديسك على شكل رقمي، والإمضاء الذي يضعه الأطراف بدوره يتم بطريقة مشفرة خاصية تضمن مصداقيته، ثم في حال النزاع يمكن للأطراف تقديم الدعائم التي تم تخزين العقد عليها إلى الجهة القضائية (المدنية أو الجزائية) وعندئذ تبرز الأسئلة القانونية الجوهرية المتعلقة بمدى حجية تلك الدعائم في الإثبات لأن النصوص القانونية التقليدية لم تكن ستتطرق إليها.

وبداية الطريق تكون لامحالة من الاعتراف رسميا بأن الكتابة الإلكترونية والإمضاء الإلكتروني هي مثل الإثبات بالكتابة تماما، وإن مصداقية الإثبات الإلكتروني هي أقوى من مصداقية الكتابة التي تزعزعت الثقة حيالها بفعل تطور أساليب التزوير كما هو مشاهد في الحياة اليومية، أين أصبحت كل المحررات الرسمية والخاصة قابلة للتزوير بطرق يصعب اكتشافها (أو يستحيل) بالنسبة للفرد العادي، وأمام تطور وتعدد المعاملات التجارية أساسا بالطرق الإلكترونية مثل:

- الشيكات الإلكترونية.
- المحفظة الإلكترونية.
- الرفع بواسطة التحويل المصرفي
- السحب النقدي والتحويل عبر الإنترنت
- الدفع بواسطة استعمال بطاقات الائتمان الإلكترونية والممغنطة

– المعاملات التي تتم بواسطة الكمبيوتر مثل عرض السلع والخدمات وشرائها والتعاقد عبر الإنترنت.

– عقود التجارة الإلكترونية التي تتم عن بعد.

فقد أصبحت معالجة هذا الموضوع يغلب عليها طابع العولمة أكثر من طابع المعالجة المحلية بالنسبة لكل دولة، لأن المصالح الاقتصادية المفروض لها أن تمر عبر الشبكة الرقمية العالمية أوسع مجالا وأكثر أهمية أضعافا مضاعفة إذا ما قورنت بالمصالح الاقتصادية الوطنية، وكما لا يخفى أن المصلحة في الوقت الراهن هي المحرك الرئيسي لمعالجة أي موضوع والاهتمام به، وحيث لا مصلحة فإن أي موضوع مصيره أن يبقى حبيس أدراج المكاتب، والمسألتان اللتان تتطلبان المعالجة القانونية هما:

– الكتابة الإلكترونية.

– الإمضاء الإلكتروني

تمت معالجة الأمر في فرنسا بموجب القانون رقم 2000–230 المؤرخ في 13–03–2000 المتضمن مطابقة قانون الإثبات مع تكنولوجيا الإعلام وبالإمضاء الإلكتروني، وكان ذلك في إطار توجيهات صادرة عن منظمات دولية نمثل لجنة الأمم المتحدة للقانون التجاري الدولي[1]، وهذا القانون أدرج في القانون المدني المواد 1316–1316–4

– حيث أن المادة 1316 تعرف الدليل بالكتابة بأنه ذلك الدليل المشكل من مجموعة حروف أو أرقام أو أية علامات أو رموز لها معنى مفهوم مهما كانت الدعامة التي تسجل

[1] جمال نجيمي ، إثبات الجريمة على ضوء الاجتهاد القضائي، دار هومة، الجزائر، د. ط ، 2012، ص255– 256.

عليها وكيفيات تحويلها، وبذلك لم يعد الإثبات بالكتابة يقتصر على الورقة المكتوبة فقط بل أصبحت البيانات المحفوظة في الحاسوب أو على قرص مضغوط تعتبر وسائل إثبات كتابية.

– أما المادة 1316–1 نصت بأن الكتابة في الشكل الإلكتروني مقبولة كدليل إثبات تماما مثل الكتابة على الورقة شريطة التأكد من الشخص الذي أصدرها، وأن تكون قد أنجزت وحفظت في ظروف من طبيعتها أن تضمن نزاهتها.

– والمادة 1316–2 نصت بأنه في حالة ما إذا لم يحدد القانون مبادئ أخرى وعدم وجود اتفاق بين الأطراف فإن القاضي يفصل في المنازعات المتعلقة بالإثبات بالكتابة بأن يحدد بكل الطرق السند الأكثر مصداقية مهما كانت الدعامة المسجل عليها.

– المادة 1316–3 نصت بأن الكتابة على الدعامة الإلكترونية لها نفس القيمة الإثباتية كالكتابة على الورق.

– المادة 1316–4 تتعلق بالإمضاء، ونصت الفقرة الأولى على الإمضاء العادي الذي يكمل التصرفات القانونية وعرفته بأنه هو الذي يجدد شخصية واضعة، ويعبر على رضا الأطراف بالالتزامات الناجمة عن تلك التصرفات، وعندما يكون الإمضاء من طرف ضابط عمومي فإنه يصبغ الصفة الرسمية على ذلك التصرف.

وأما الفقرة الثانية تتعلق بالإمضاء الإلكتروني ونصت بأنه يتمثل في استعمال طريقة موثوق بها تضمن الصلة بين الإمضاء والتصرف القانوني المرتبط به، ومصداقية هذه

الطريقة تكون مفترضة إلى غاية إثبات العكس عندما يوضح الإمضاء وتحدد هوية الممضي ويتم ضمان نزاهة التصرف وفقا لشروط يحددها المرسوم بعد استشارة مجلس الدولة وهو المرسوم الذي صدر بتاريخ 30-03-2001 تحت رقم 2001-272، واهم ما جاء فيه أن الإمضاء الإلكتروني المؤمن هو كذلك الإمضاء الإلكتروني الذي يستجيب إلى الشروط التالية[1].

-أن يكون خاصا بالممضي.

-أن ينشأ وفقا لوسائل يمكن للممضي أن يحتفظ بها تحت مراقبته الخاصة.

-أن يضمن وجود رباط بين الإمضاء والوثيقة الذي يتصل به بحيث أن كل تعديل لاحق للوثيقة يمكن اكتشافه.

وقد سلك المشرع الجزائري نفس المسلك من خلال تعديل القانون المدني بموجب القانون رقم 05-10 المؤرخ في 20-06-2005 والذي أضاف المواد 323 مكرر و324 مكرر1 إلى الباب السادس المتعلق بإثبات الالتزام في فصله الأول المتعلق بالإثبات بالكتابة، وهذين النصين يتضمنان نفس أحكام المواد 1316و 1316-1 من القانون المدني الفرنسي المشار إليهما أعلاه.

-المادة 323 مكرر:" ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تضمنتها وكذا طرق إرسالها".

[1] جمال نجيمي، المرجع نفسه، ص260.

-المادة 223 مكرر1" يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

-الفقرة الأخيرة من المادة 327:" ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1 أعلاه".

ولكن لم يتعرض القانون الجزائري لكيفية التأكد من صحة التوقيع الإلكتروني عكس ما فعله المشرع الفرنسي الذي أصدر مرسوما يتناول المسألة بالتفصيل، ومن المؤكد أنه من الناحية العملية لا يمكن الخروج عن الطريقة التي رسمها القانون الفرنسي، وعندما يطرح الأمر بجدة على المحاكم فسوف يضطر المشرع إلى التدخل، ولكن إلى أن يحدث ذلك على الاجتهاد القضائي أن يغطى هذه الثغرة[1].

والبريد الإلكتروني هو عبارة عن المراسلة التي تتم عبر الشبكة الإلكترونية من حاسوب إلى آخر لنقل الرسائل والملفات والصور والبرامج، ويكون لكل طرف علبة بريد شخصية لدى الموقع الإلكتروني محمي برقم دخول سري يفترض ألا يدخلها إلا صاحبها وكل رسالة تحمل اسم المستعمل (صاحب صندوق البريد) متبوعا برمز @ (آروباز = آت) ويلفظ هذا الرمز باللغة الإنجليزية على الشكل (at) متبوعا باسم الموقع، ولكن نظرا للثغرات التي لا تزال قائمة حول إمكانية اختراق المواقع فإنه لا يمكن الجزم بأن رسالة إلكترونية ما قد صدرت فعلا عن شخص معين، وبالتالي فقوتها في الإثبات مقارنة

[1] جمال نجيمي، المرجع نفسه، ص259.

بالورقة المكتوبة ناقصة، وذلك ما دفع إلى ابتكار الإمضاء الإلكتروني الذي أصبح يسمح بضمان أن الوثيقة صادرة عن صاحب الإمضاء وبذلك تساوت قوة الإثبات بين الرسالة الإلكترونية والرسالة الورقية الممضاة.

ويتمثل التوقيع الإلكتروني في وجود سلطة مختصة تتولى حفظ التوقيع الذي يضعه صاحبه على شكل حروف أو أرقام أو رموز تكون كلها مشفرة بحيث يستحيل استعمالها من طرف الغير، ويتم التوقيع على الوثيقة باستعمال مفتاحين أحدهما عام والثاني خاص يكونان تحت حفظ سلطة المصادقة، ويستعمل المفتاح الأول لتشفير الوثيقة والثاني يستعمل لفك الشيفرة.

فمصداقية الإمضاء الإلكتروني تأتي من وجود جهة محايدة هي سلطة مختصة ومعتمدة بصفة رسمية تضمن مصداقية التوقيع والسند الذي يشمله بحيث لا يمكن تغييره ولا يمكن إنكار الإمضاء ممن نسب إليه.

ثانيا: طبيعة دليل الإثبات الإلكتروني أمام القاضي الجزائي

يعتبر الوضع شديد الارتباط عندما يطرح تساؤل ما علاقة هذا الإثبات الوارد في القانون المدني بموضوع الدراسة وهو الدليل الجنائي[1]، لأنه مثلما أن الورقة المكتوبة كما سبقت الإشارة إليها في باب الإثبات بالكتابة قد تكون هي موضوع الجريمة أو قد تكون هي وسيلة إثباتها، فكذلك السندات الإلكترونية قد تكون هي موضوع الجريمة فتكون هي وسيلة إثبات العديد من الجرائم من أبسطها تزوير في محرر إلى حركة رؤوس الأموال

[1] جمال نجيمي، المرجع نفسه، ص260.

عبر الشبكة العنكبوتية العالمية، وقد يكون إثبات الركن المادي للجريمة العادية يتطلب الإثبات وفقا لأحكام القانون المدني مثل حالة إثبات عقد من عقود الائتمان أبرم وأمضي إلكترونيا، إلى جانب أن بعض الجرائم المعلوماتية تنصب على مشتملات الحاسوب فلا مفر للقاضي الجزائي من دراسة هذا الباب ومعرفة أحكامه حتى يتمكن من القيام بعمله على الوجه المطلوب.

وإن الكتابة على الورق تمتاز بوضوح العبارة فيشاهدها الشخص مباشرة ويعلم محتواها، كما تبرز بوضوح إمضاء الموقعين عليها للدلالة على إرادتهم بقبول ما تضمنته ويمكن للمعنيين حفظهما بأمان واستظهارها عند الحاجة بكل بساطة ودون الحاجة إلى معدات وأجهزة لقراءتها، فهي تحسم الجدل وتزيل الشك بمجرد طرحها للمناقشة وهذه الميزات ليست بهذا الوضوح في السند الإلكتروني، فالمعني بالأمر إذا كان يشاهد على الشاشة ما هو مكتوب فإنه لا يعرف حقيقة ما هو مسجل في القرص الصلب وهو الأصل كما أنه لا يؤمن على ما يحدث من تغييرات على البيانات المسجلة على الدعامة (الوسائط) التي تحتوي البيانات سواء بفعل الأطراف أو بفعل البرامج المسماة بالفيروسات، ناهيك عما يعرف بالاختراقات التي يقوم بها البعض (الهاكرز) ويدخلون إلى المواقع فيأخذون المعلومات ويحرفون المعطيات بل ويتلاعبون بأرقام الحسابات من خلال برامج فك الأرقام السرية وليس ببعيد ما تناولته[1] الأخبار من اختراق أكبر المواقع تحصينا في العالم وهي مواقع البيت الأبيض الأمريكي وغيرها، ثم أيضا عند الاستظهار

[1] جمال نجيمي، المرجع نفسه، ص261.

بها يجب إحضار الأجهزة والبرامج الكفيلة بفك رموزها وقراءتها، فكيف يحدث الاقتناع للقاضي الجزائي في ظل هذا الاضطراب، وهو القاضي الذي ليس من السهل إقناعه بالأدلة المباشرة الواضحة فما بالك بالأدلة المعقدة وغير المباشرة، علما بأن جريمة المساس بأنظمة المعالجة الآلية للمعطيات تمتاز بسرعة تنفيذها إذ يتطلب الأمر في بعض الأحيان ثواني معدودة لارتكاب الجرم وتتبعها ثواني أقل منها عددا لمحو وإزالة أثر الفعل، فالأمر لا يتعدى النقر على زر الفأرة أو الضغط على احد مفاتيح اللوح إلى جانب أن البيانات قد تسجل أحيانا في الذاكرة الحية فقط للحاسوب بحيث يزول كل شيء بمجرد قطع التيار الكهربائي، ناهيك على أن بعض البرامج المعدة مسبقا لارتكاب الجرائم المعلوماتية تكون مبرمجة ذاتيا لتدمير نفسها بمجرد أن يحاول غير صاحبها أن يشغلها مما يبرز صعوبة الحصول على الدليل في عالم المعلوماتية.

وفي الميدان العملي قد تقدم جهة المتابعة من بين أدلة الإثبات رسالة إلكترونية (أيميل) أو صفحة ويب تتضمن مثلا تهديدا أو قذفا ..فإذا اعترف المتهم بصدورها منه فلا إشكال ولكنه قد ينكر ما هو منسوب إليه وينكر صدور الرسالة أو الصفحة من جانبه خصوصا وأنها لا تحمل إمضاءه الإلكتروني فكيف تثبت جهة المتابعة مزاعمها وتثبت أن مضمون السند المقدم صادر عن المتهم.

إن ذلك هو ما يدرس تحت عنوان التحليل الجنائي لمعلومات الحاسوب، ويعرفه المختصون بأنه جمع وحفظ وتحليل الأدلة الرقمية من أية دعامة للتخزين تعمل بواسطة

الإعلام الآلي لعرضها أمام القضاء قصد إثبات التهمة أو نفيها عن شخص ما، فبداية الطريق تنطلق إذن من جهاز الحاسوب، فعندما نتحدث عن جريمة المساس بأنظمة المعالجة الآلية للمعطيات معناه أننا نتحدث عن الحاسوب، وهذا الجهاز إما أن يكون هو محل الجريمة أو هو وسيلة إثباتها، ولا داعي للحديث عن المكونات المادية للحاسوب إذا تعرضت لفعل غير مشروع كالسرقة أو التخريب ولكن المهم هو البيانات المخزنة داخله أو المارة عبره، وهي تشمل المعطيات المحفوظة المتعلقة بكتابات أو حسابات أو صور كما تشمل برامج تستعمل في تسيير مختلف الأنشطة الخاصة والعامة في كل فروع المعرفة وبالتالي فإنها في بعض الأحيان لا تقدر بثمن كتلك الخاصة بالشركات الدولية أو ببعض الدوائر الحكومية.

ومسايرة من قانون العقوبات للتطورات الحديثة في باب جريمة المساس بأنظمة المعالجة الآلية للمعطيات فإنه قد تصدى لتجريم مجموعة من التصرفات الماسة بسلامة المعالجة الآلية للمعطيات، فاستحدث قانون العقوبات إثر التعديل التالي المتضمن تجريم وعقاب الأفعال التي تشكل بمختلف صورها جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وكان ذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 الذي استحدث القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات المواد من394 مكرر إلى 394 مكرر7[1].

الفـرع الثاني

[1] جمال نجيمي، المرجع نفسه، ص262-263.

مدى حجية المستخرجات الالكترونية كدليل إلكتروني في إطار نظرية الإثبات الجنائي

الحجة هي الاستدلال على صدق الدعوى أو كذبها وهي مرادفة للدليل، والحجة أيضا البينة والبينة على من ادعى، وحجية المخرجات الكمبيوترية هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبة.

والمقصود بحجية المخرجات الكمبيوترية هو " قيمة ما يتمتع به المخرج الكمبيوتري بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية من قوة استدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه[1].

أولا: موقف النظم القانونية من حجية المخرجات الكمبيوترية:

سنتعرض في هذا العنصر إلى موقف كل من القوانين الأنجلوسكسونية والقوانين اللاتينية والقوانين ذات الصياغة المختلطة.

1- حجية المستخرجات الكمبيوترية في القوانين الأنجلوسكسونية:

إن الفكرة السائدة التي تقوم بها هذه القوانين أن المشرع هو الذي يحدد أدلة الإثبات ويقدر قيمتها الإقناعية، ومقتضى ذلك أن يتقيد القاضي في حكمه بالإدانة أو بالبراءة بأنواع معينة من الأدلة، أو بعدد منها لممارسة التشريع المطبق، دون أن يأبه في ذلك بمدى اقتناع القاضي بصحة ثبوت الواقعة أو عدم ثبوتها، إذ يقوم اقتناع المشرع بصحة

[1] نصر الدين مروك، المرجع السابق، ص461.

الاستناد أو عدم صحته مقام اقتناع القاضي، وهكذا فإن اليقين القانوني يقوم أساسا على افتراض صحة الدليل، بغض النظر عن حقيقة الواقع أو اختلاف ظروف الدعاوي، أما دور القاضي فلا يتعدى مراعاة تطبيق القانون من حيث توافر الدليل أو شروطه بحيث إذ لم تتوافر هذه الشروط وتلك الشكليات فإن القاضي لا يستطيع أن يحكم بالإدانة بصرف النظر عن اقتناعه الشخصي، أي ولو اقتنع يقينا بأن المتهم مدان في الجريمة المسندة إليه.

وعليه فإن حجية المخرجات الكمبيوترية في القوانين ذات الصياغة الأنجلوسكسونية تجد بعض الصعوبات، خاصة مع وجود قاعدة الدليل الأفضل أو الأحسن وقاعدة الدليل السماعي، وإذا رجعنا للواقع العملي والتطبيقي نجد مثلا إنجلترا كدولة ذات النظام الأنجلوسكسوني على قمة الدول التي أصدرت قانونا خاصا بالحاسب الآلي[1] وهو قانون إساءة استخدام الحاسب الصادر في 29 جوان 1990، والذي طبق اعتبارا من 29 أوت 1990، وهذا القانون رغم أن محله الحاسب الآلي إلا أنه إحدى المسائل الهامة التي لم يتناولها تتعلق بقواعد قبول الأدلة الناتجة عن الحاسب، ويعزى ذلك إلى أن قانون البوليس والإثبات الجنائي الصادر سنة 1984 والمعمول به 1986، والذي حل محل قانون الإثبات الجنائي لعام 1965 قد حوا تنظيما محددا لمسألة قبول مخرجات الحاسب كأدلة إثبات في المواد الجنائية، والمستند الناتج عن الحاسب الآلي لا يقبل كدليل إذا لم يستكمل باختبارات الثقة المنصوص عليها في القسم 69 من هذا القانون.

[1] المرجع نفسه، ص462.

و تشير الأحكام الصادرة عن المحاكم البريطانية إلى أن شرائط القسم رقم 69 لا تنطبق إذا كانت مطبوعات الحاسب دليلا حقيقيا أو أصليا وليس مجرد نقل عن الغير، وقد أشار بعض المتخصصين في مجال الحاسب الآلي إلى استحالة إثبات دقة هذا الحاسب بالطريقة الموضحة في القانون ويقترح بعض الفقهاء الانجليز أنه في حالة ما إذا كان الحاسب موضوع للاستخدام غير المصرح به، فإن أي أدلة ناتجة عن الحاسب بخصوص أصل ومدة الاستعمال لن يكون مقبولا ، لأن سوء استخدام الحاسب في حد ذاته أدى إلى أن الجهاز لا يعمل كما ينبغي[1].

وفي الولايات المتحدة الأمريكية تناولت بعض القوانين حجية المخرجات الكمبيوترية ومن ذلك على سبيل المثال ما نص عليه قانون الحاسب الآلي لسنة 1984 الصادر في ولاية أيوا–Towa من أن مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزونة فيه المادة 716أ 16.

كما يتضح أيضا من قانون الإثبات الصادر في 1983 في ولاية كاليفورنيا من أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات، وهذا ما ترجمه القضاء الأمريكي في أحكامه المختلفة من أن المخرجات الكمبيوترية يجب أن تكون مقبولة كأداة إثبات، طالما كان الحاسب المتولدة عنه يؤدي وظائفه بصورة سليمة، وكان القائم عليه تتوافر فيه الثقة والطمأنينة.

[1] نصر الدين مروك ، المرجع نفسه، ص463.

ويرى جانبا من الفقه الأمريكي ادوارد واير أن الوضع بالنسبة لمدى قبول الأدلة الناتجة عن الحاسب بقوله إن الصعوبات الحقيقية في الولايات المتحدة الأمريكية نابعة من عدم الألفة مع تكنولوجيا الحاسب الآلي أكثر من كونها صعوبات قانونية، ولذا فمن غير المعتقد على وجه العموم أن تكون هناك حاجة ماسة إلى سن تشريعات بخصوص التعامل مع مدى قبولية السجلات المعالجة بواسطة الحاسب.

وفي كندا فإن قبول السجلات الناجمة عن الحاسب الآلي تخضع لشروط مسبقة يجب توافرها، فالمادة 29 من قانون الإثبات الكندي والخاص بسجلات المؤسسات المالية تقرر عددا من الشروط التي يجب توافرها قبل عمل صورة Copy [1] من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي.

وتطبيقا لما تقدم أعلاه فقد قضت محكمة استئناف أونتاريوا الكندية في قضية "مكملان" بأنه يشترط لكي تكون سجلات الحاسب الآلي مقبولة بوصفها نسخا حقيقية من السجلات الإلكترونية، أن تكون مستكملة بوصف كامل لنظام حفظ السجلات السائدة في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفا للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها حتى يتبين أن المخرج الكمبيوتري موثق به بشكل كاف[2].

2- حجية المخرجات الكمبيوترية في القوانين الذاتية:

[1] نصر الدين مروك، المرجع نفسه، ص464.

[2] المرجع نفسه، ص466.

حيث تشمل القوانين اللاتينية كل من القانون الفرنسي والقانون الإيطالي والإسباني، والقانون المصري.

فهذه القوانين تتشابه في الصياغة ومصادر القانون فيها واحد وتقسيماتها متماثلة والاصطلاحات القانونية فيها متشابهة، والقوانين اللاتينية يسود فيها مبدأ حرية الإثبات والاقتناع، ومن ثم فإن حجية المخرجات الكمبيوترية لا تثير صعوبة بالنسبة لمدى حرية القاضي الجنائي في تقدير المخرجات الكمبيوترية باعتبارها أدلة إثبات في المواد الجنائية.

ففي فرنسا مثلا فالفقه الفرنسي تعددت دراساته المتعلقة بتطور قانون الإثبات في المواد المدنية والتجارية والتي انصبت حول معرفة ما إذا كانت المحررات الموضوعية على دعامة مغناطيسية لها نفس القيمة الدافعة المعطاة للمحررات المكتوبة، تطبيقا لمبدأ هيمنة الكتابة والذي تحقق بصدور قانون 12 جوان سنة 1980 والذي سمح بعمل أرشيف للنسخ الموثوق بها والدائمةdurables et copies fidèles المادة 1348 من القانون المدني الفرنسي والتي يمكن اللجوء إليها كأدلة إثبات غير مادية في المواد المدنية والتجارية، فإن مشكلة حجية المخرجات الكمبيوترية على المستوى الجنائي لا تبدو ملحة في نظر الفقهاء فالأساس عندهم هو حرية الأدلة وحرية القاضي في تقدير هذه الأدلة[1].

وما تجدر الإشارة إليه في هذا المقام هو أن الفقه الفرنسي يدرس حجية المخرجات الكمبيوترية في المواد الجنائية ضمن مسألة أوسع وأهم من مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل الرادارات، الأجهزة السينمائية، أجهزة التصوير، أشرطة

[1] نصر الدين مروك، المرجع نفسه، ص467.

التسجيل، أجهزة التصنت، هذه الأدلة أخذ بها المشرع وقبلها القضاء في إطار مجموعة من الشروط من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة وأن يتم مناقشتها حضوريا عن طريق الأطراف.

وتطبيقا لهذا قضت محكمة النقض الفرنسية أن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي هذا ولا يختلف الأمر بالنسبة لقبول مخرجات الحاسب الآلي، حيث لم يتضمن قانون 05 جانفي 1988 الخاص بالتعديلات التي تقع على نظم المعالجة الآلية للبيانات.

وفي لكسمبورغ يعتبر مبدأ الاقتناع الذاتي للقاضي هو حجر الزاوية في الأحكام الجنائية وعليه فإن ظهور المعلوماتية بكل خصائصها لم تغير شيئا من هذا المبدأ فالاقتناع يجب أن يكون بناء على أثر الدليل المتولد في نفس القاضي والذي لا يترك مجالا للشك، حيث أن القانون لم يقدم للمجال الجنائي نموذجا خاصا للإثبات ، فإن قاضي الموضوع تكون له حرية تقدير الأدلة المقدمة إليه ومنها المخرجات الكمبيوترية والتي يكون للأطراف حرية الاعتراض عليها في كافة مراحل الدعوة[1].

3- حجية المخرجات الكمبيوترية في القوانين ذات الصياغة المختلطة:

القوانين ذات الصياغة المختلطة هي تلك التي جمعت ما بين النظامين اللاتيني والأنجلوسكسوني، فجاءت نظاما وسطا بين النظامين ومن القوانين التي تأخذ بالنظام المختلط القانون الإجرائي الياباني، حيث حدد وسائل الإثبات مثل القانون الأنجلوسكسوني

[1] المرجع نفسه، ص468-469.

وأخذ بقاعدة الاقتناع الشخصي للقاضي مثل القانون اللاتيني، ويظهر أخذ المشرع الياباني بنظام الاقتناع الشخصي في المادة 318، وقد حصر المشرع الياباني طرق الإثبات فيما يلي:

- أقوال المتهم.
- أقوال الشهود.
- القرائن.
- الخبرة.

ومن هنا السؤال الذي يطرح نفسه في هذا المقام هو ما مدى قبول الأدلة الناتجة عن الحاسب الآلي؟

في هذا الخصوص يقرر الفقه الياباني أن السجلات الإلكترومغناطيسية تكون مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسب سواء كانت هي الأصل أم كانت نسخة من هذا الأصل.

ولكن ما هو السند القانوني لقبول هذه المخرجات الكمبيوترية؟ قانون الإجراءات الجنائية الياباني يستبعد الشهادة السماعية كقاعدة عامة بمقتضى المادة 32 أ ج ، إلا أنه يرد على هذه القاعدة بعض الاستثناءات التشريعية المنصوص عليها في المواد 321،

328 أ ج، ويدخل في هذه الاستثناءات الأدلة المتولدة عن الحاسب الآلي والمادة 323 أ. ج التي تقرر قبول ثلاث أنواع من السجلات كأدلة إثبات في المواد الجنائية وهي[1]:

– نسخة من السجل العائلي للفرد، أو نسخة من صك من السجل موثق أو أي مستندات رسمية تشهد على الوقائع التي يكون من واجب الموظف العام (بما في ذلك موظفي الحكومات الأجنبية) التصديق عليها.

– دفتر الحساب، سجل السفر، المستندات الأخرى التي تعد لتنظيم السير المعتاد للأعمال التجارية.

– أية مستندات أخرى غير مذكورة في البندين السابقين، إذا تم إعدادها تحت ظروف تضفي مصداقية خاصة على توكيد الحقيقة المتضمنة في مسألة معينة.

وبالإضافة إلى هذا الاستثناء المنصوص عليه في المادة 323 أج فإنه يمكن طباعة المخرجات الكمبيوترية وقبولها أثناء فترة المحاكمة من خلال شهادات الخبراء[2].

المطلب الثاني

الجزاءات المقررة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات

سنتاول الجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث وذلك طبقا لنص المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي، فلا بد أن تكون

[1] نصر الدين مروك، المرجع نفسه، ص469– 470.

[2] نصر الدين مروك، المرجع نفسه، ص470–471.

العقوبات المقررة للجريمة رادعة وتتضمن عقوبات سالبة للحرية، والمتمثلة في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، كما توجد عقوبات تطبق على الشخص المعنوي بناء على تبني مساءلة الشخص المعنوي الواردة في المادة 12 من الاتفاقية[1].

الفرع الأول

العقوبات المطبقة على الشخص الطبيعي

نتناول ضمن هذا الفرع العقوبات الأصلية لكل جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات و العقوبات التكميلية.

أولا: العقوبات الأصلية

أ- الدخول والبقاء بالغش (الجريمة البسيطة)

حسب نص المادة 394 مكرر من قانون العقوبات الجزائري فإن العقوبة المقررة هي الحبس من 03 ثلاثة أشهر إلى سنة وغرامة من 50000 دج إلى 100000دج[2].

ب- الدخول والبقاء بالغش (الجريمة المشددة)

فحسب نص المادة 394 مكرر فقرة 2 و3 قانون عقوبات تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة وتكون العقوبة من (06) ستة أشهر

[1] عبد المجيد جباري ، المرجع السابق، ص120.

[2] المادة 394 مكرر قانون عقوبات. راجع: أحمد لعور، نبيل صقر، موسوعة الفكر القانوني قانون العقوبات نصا وتطبيقا، دار الهدى، عين مليلة، د.ط ، ص270.

إلى سنتين (02) والغرامة من 50000 دج إلى 150000 دج، إذا ترتب عن الدخول أو البقاء غير المشروع تخريب نظام اشتغال المنظومة، وهذا ما أخذ به المشرع الجزائري عن المشرع الفرنسي من خلال نص المادة 323 من قانون العقوبات الفرنسي في فقرتها الثانية.

ت- الاعتداء العمدي على المعطيات:

طبقا لنص المادة 394 مكرر 1 فالعقوبة المقررة على جريمة التلاعب في بيانات تظم المعالجة للمعطيات هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000دج إلى 2000000دج ، أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وذلك بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أو عن طريق حيازة أو إفشاء أو نشر أو استعمار لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها، فعقوبتها هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000دج إلى 5000000دج[1].

ث- الظروف المشددة

اعتبر المشرع الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي من المؤسسات الرسمية بمثابة ظرف مشدد وذلك من خلال نص المادة 394 مكرر 3 أن

[1] عبد المجيد جباري، المرجع نفسه، ص121. راجع: أحمد لعور ونبيل صقر، المرجع السابق، ص272.

العقوبة المشددة تتصرف على جميع الجرائم المنصوص عليها في المادة 394 مكرر والمادة 394 مكرر 1 ومكرر2.

فتضاعف العقوبة المقررة للجرائم الماسة بالأنظمة المعلوماتية إذ استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام تكتسي طابعا خاصا بما تحتويه كمبيوتراتها من معلومات ومعطيات ذات طابع خاص وقد تكون مرتبطة بأسرار عسكرية أو اقتصادية أو غيرها[1].

ج- الجزاء المقرر للاتفاق الجنائي

يعاقب المشرع الجزائري على الاتفاق الجنائي بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية وذلك من خلال نص المادة 394 مكرر5 ، ولم يخضعها للمادة 176 قانون العقوبات لجمعية الأشرار حيث نصت المادة 394 مكرر 5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة".

والحكمة من توسيع نطاق العقوبة بإخضاع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا ما تمت في إطار اتفاق جنائي بمعنى الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالعقاب، وذلك كون الإعداد للجرائم المعلوماتية تتم

[1] زيدان زيبخة، المرجع السابق، ص99- 100.

عادة في إطار جماعات خاصة منها القرصنة، وعقوبة الاشتراك في الاتفاق الجنائي نفس عقوبة الجريمة ذاتها وشروط العقاب على الاتفاق الجنائي يمكن تلخيصها فيما يلي:

-اشتراط المشاركة في مجموعة أو اتفاق.

-الغرض من المشاركة، الإعداد لجريمة أو أكثر من الجرائم الماسة بالأنظمة المعلوماتية.

-تجسيد هذا التحضير بفعل أو عدة أفعال مادية.

-القصد الجنائي

كذلك نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي، والمادة 04/323 قانون عقوبات فرنسي

ح- الجزء المقرر للشروع

نصت عليها المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي، والمادة 7/323 من قانون العقوبات الفرنسي، وبالرجوع إلى قانون العقوبات الجزائري حيث نصت عليها المادة

394 مكرر7" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم الخاص بالمساس بالمعالجة الآلية للمعطيات بالعقوبات ذاتها المقررة للجنحة[1].

ثانيا: العقوبات التكميلية

[1] عبد المجيد جباري، المرجع السابق، ص124- 125.

من خلال نص المادة 394 مكرر6 استثنت الغير حسن النية بحفظ حقوقه[1]، ونصت على العقوبات التكميلية التي يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في:

- **المصادرة:** وتشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية.

- **إغلاق المواقع:** يتعلق الأمر بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

- **إغلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب فيه مثل هذه الجرائم بشرط توافر عنصر العلم لدى مالكها.

الفرع الثاني

العقوبات المقررة للشخص المعنوي

لقد نص المشرع الجزائري على مسؤولية الشخص المعنوي في نص المادة 18 مكرر من قانون العقوبات في القانون 15/04، وسواء كان فاعلا أصليا أو شريكا، كما يسأل عن الجريمة التامة أو الشروع فيها، كل هذا شرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد ممثليه أو أعضائه مع ملاحظة أن المسؤولية

[1] المادة 394 مكرر 6 قانون عقوبات.

الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة[1].

والعقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

-حل الشخص المعنوي

-غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس(05) سنوات

-الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس(05) سنوات

-المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز 5 سنوات

-مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها

-نشر وتعليق حكم الإدانة

-الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

-تساوي الغرامة من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة مع إمكانية الحكم بمصادرة الشيء الذي استعمل في ارتكاب الجريمة أو ما نتج عنها[2].

[1] عبد المجيد جباري، المرجع السابق، ص122.

[2] زيدان زيبخة، المرجع السابق، ص102.

خـــاتمـــــة

في نهاية هذا العمل نخلص إلى القول أنه ونظرا للتطور التكنولوجي الواقع في العالم نتج عنه ظهور جرائم جديدة لم يتوقعها المجتمع ولا رجال القانون، ومن بينها جريمة المساس بأنظمة المعالجة الآلية للمعطيات، التي بدأت بالظهور والانتشار في معظم المجتمعات، وهي في تطور مستمر نظرا لارتباطها بتقنية متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وخصائصها وأنواع مرتكبيها ودوافعهم ودور الحاسوب في ارتكاب الجريمة وصولا إلى الأفعال التي تدخل ضمن دائرتها وأساليب قمعها وطبيعة الدليل المعلوماتي فيها ولمواجهة هذا النوع من الإجرام تدخل المشرع الجزائري بسن كل من القانون 15/04 المعدل والمتمم لقانون العقوبات والقانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كان لهما أهمية في تدارك الفراغ التشريعي الذي كان يعتري القانون الجزائري وذلك من خلال حسم المشرع الجدل الفقهي القائم حول تسميات الجرائم المعلوماتية وقد اصطلح عليها المشرع بمصلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وحسم الجدل كذلك حول تعريفها بموجب أحكام المادة 2 من قانون 04/09 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

بالإضافة كذلك إلى حسم الجدل حول طبيعة المعلوماتية باعتبارها مالا من نوع خاص باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في

الفصل الثالث من الباب الثاني من الكتاب الثالث من المواد 394 مكرر إلى 394 مكرر7 من قانون العقوبات كون أن القسم السابع ورد تحت الكتاب الثالث المتعلق بالجنايات والجنح ضد الأموال.

كما أن هذا التعديل يعد خطوة في مجال التشريع كونه واكب التشريعات المقارنة بتجسيده معظم أحكام الاتفاقية الدولية للإجرام المعلوماتي لسنة 2001، من خلال التجريم أفعال الدخول والبقاء غير المشروع داخل النظام المعلوماتي وتجديد العقوبة إذا ترتب عن ذلك المساس بالمعطيات أو نظام التشغيل للمنظومة المعلوماتية، المساس بالمعطيات أو تغيرها، استخدام المعطيات كوسيلة لارتكاب الجرائم المعلوماتية حيازة أو إفشاء أو نشر أو استعمال المعطيات المحصلة من هذه الجرائم لأي غرض، تجريم المساس بنظام التشغيل على أساس اعتبار المطيات المعلوماتية من خلال الفقرة ج من المادة الثانية من قانون 09-04 تشمل برامج التشغيل.

كما أن المشرع الجزائري بالإضافة إلى مسؤولية الشخص الطبيعي تبنى مبدأ مسؤولية الشخص المعنوي ووسع نطاق العقوبة بتجريم الشروع في هذه الجرائم بتجريمه حتى الأعمال التحضيرية في إطار الاتفاق الجنائي مما يدل على رغبة المشرع في القضاء على هذه الجريمة حتى في مرحلة التحضير.

ومن جهة أخرى فإنه بالرغم من مزايا هذين القانونين إلا أنهما لا يخلوان من بعض العيوب والنقائص والانتقادات خاصة بمقارنتهما مع قوانين الدول المتقدمة.

ومن خلال هذا البحث يمكننا استعراض أهم ما توصلنا إليه من نتائج:

-فنظرا لحداثة جريمة المساس بأنظمة المعالجة الآلية للمعطيات فإنه لا يوجد لحد الآن إجماع فقهي على تعريف موحد لها فهي متفاوتة فيما بينها ضيقا واتساعا، وقد عرفها المشرع الجزائري بموجب أحكام المادة 02 من قانون 09-04 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية".

-عدم وجود مصطلح موحد للدلالة عليها وذلك خشية حصرها في مجال ضيق يمكن أن يضر بها ولكن بات من الضروري وضع تعريف لها يشمل العناصر الأساسية التي تسمح بتحديدها، وقد اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

-من خلال التعريف الذي وضعه المشرع الجزائري في المادة 02 من قانون 09-04 فقد تبنى المفهوم الموسع للجرائم المعلوماتية وتميز بالقصور لعدم تحديد صور السلوك الإجرامي، كون أن مبدأ الشرعية يحكم المجال الجزائي فلا بد من تحديد الأفعال المجرمة بدقة.

-موضوع الجريمة المعلوماتية هو المال المعلوماتي تمييز المالية المغايرة للمال التقليدي بمعنى أن المال المعلوماتي هو الحاسب بكل مكوناته المادية (جهاز الإدخال والإخراج ووحدة التشغيل المركزية)، ومكوناته المعنوية (البرامج والمعلومات).

-يستهدف الركن الشرعي للجريمة كل أشكال الاعتداءات على النظام المعلوماتي كونها تدخل في نطاق الجريمة المعلوماتية.

-يشمل الركن المادي لجريمة المساس بأنظمة المعالجة الآلية للمعطيات صورتين، الاعتداء على نظام المعالجة الآلية للمعطيات، والاعتداء على منتوجات الإعلام الآلي.

-بالنسبة للركن المعنوي للجريمة المساس بأنظمة المعالجة الآلية للمعطيات يتخذ صورة القصد الجنائي إضافة إلى نية الغش، وعليه فإن الدخول والبقاء بالغش والاعتداء على المعطيات الموجودة داخل النظام يستلزمان قصدا جنائيا عاما وقصدا خاصا متمثلا في نية الغش، أما الاعتداء على سير نظام المعالجة الآلية للمعطيات فالقصد الجنائي فيه مفترض، يستنتج من طبيعة الآلية للمعطيات فالقصد الجنائي فيه مفترض، يستنتج من طبيعة الأفعال المجرمة المتمثلة في العرقلة والتعطيل، أما الاعتداء غير العمدي على سير النظام ما هو إلا ظرف مشدد لجريمة الدخول و البقاء غير المشروع.

-كما أهمل المشرع الجزائري تقرير نصوص خاصة بالتزوير المعلوماتي فالركن المعنوي فيه يخضع لأحكام جريمة التزوير في المحررات، والمتمثل في القصد الجنائي العام المتمثل في العلم وإرادة تغيير الحقيقة في مستند معلوماتي، ويمكن أن يكون هناك قصد احتمالي عند العلم بإمكانية إحداث ضرر وما يميز الركن المعنوي للجريمة المعلوماتية هو صعوبة إثباته.

-اختلاف أدلة الإثبات في الجريمة المعلوماتية عنها في الجريمة التقليدية يتمحور حول الكتابة الإلكترونية والإمضاء الإلكتروني التي تخزن في القرص الصلب أو الليـــــــن أو المضغوط أو الفلاش ديسك على شكل رقمي والإمضاء يتم بطريقة مشفرة، بالإضافة إلى البريد الإلكتروني، التي ترسل من خلاله مختلف البيانات والوثائق.

-المعاقبة على الشروع في الجريمة المعلوماتية من قبل المشرع الجزائري، كذلك يعاقب على الاتفاق الجنائي بهدف التحضير للجريمة مما يبين رغبته في تغطية أكبر قدر ممكن من الإجرام المعلوماتي.

-أما بالنسبة لمواجهة هذا الشكل الجديد من الإجرام المتمثل في جريمة المساس بأنظمة المعالجة الآلية للمعطيات فإن القانون الجنائي التقليدي لا يكفي لمواجهته ولم يكن في ذهنه وقت وضع النصوص هذا النوع من الاستثمار الجديد وهو "البرامج" وهنا تظهر المخاطر كون القانون الجنائي له مبادئه وأصوله وعلى رأسها مبدأ الشرعية " لا جريمة ولا عقوبة أو تدابير أمن إلا بنص" الذي ينتج عنه مبدأ التفسير الضيق للنصوص ومبدأ حظر القياس في مجال التجريم، لذلك تم التدخل تشريعيا عن طريق تعديل النصوص القانونية.

-إخضاع برامج الحاسوب إلى قوانين الملكية الفكرية والفنية.

-عدم وجود تشريع جنائي عربي موحد يجرم صور الجرائم المعلوماتية بأنواعها بحيث يضع لكل صورة منها العقوبة التي تتناسب مع خطورتها.

-كما أهمل المشرع الجزائري تقرير نصوص خاصة للأفعال التي يكون النظام المعلوماتي وسيلة مسهلة لارتكابها كالجرائم الأخلاقية والإرهابية المرتكبة عبر النظم المعلوماتية، فلا بد للمشرع بالتدخل من خلال تشديد العقوبات على الأفعال التي تكون فيها المعلوماتية وسيلة لارتكاب جرائم أخرى خاصة جرائم التحرش الجنسي.

واعتمادا على النتائج التي توصلنا إليها من خلال دراستنا ارتأينا إعطاء مجموعة من الاقتراحات في ظل دخول المجتمع الجزائري نفق الإدمان والاعتماد الرهيب على شبكة الإنترنت وما يصاحبها من آليات وخدمات إلكترونية.

- استحداث قانون جنائي للمعلوماتية مستقل يحدد ويجرم كل أنواع جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتحديد الجهات المسؤولة والمختصة بمراقبة هذه الجرائم.

- استحداث نصوص خاصة بالتزوير المعلوماتي وإخضاعها للنظرية العامة للتزوير باعتبار أن المصلحة المحمية في تجريم الاعتداءات على نظام المعالجة الآلية للمعطيات هي مصلحة صاحب النظام، بينما المصلحة التي يحميها القانون بصدد جريمة التزوير هي الثقة العامة في المستندات.

- كون هذه الجريمة تتميز بطابعها العابر للحدود مما ينتج عنه صعوبة كشفها وكشف مرتكبيها والقانون الواجب التطبيق فكان لا بد من زيادة التعاون الدولي والتكاثف فيما بين الدول للقضاء على هذه الظاهرة وإخضاع إجراءات البحث والتحري إلى السرعة قبل طمس أدلة الإثبات.

- العمل على تكوين فرق من الشرطة المختصة تكلف بالبحث والتحري على هذا النوع من الجرائم والاهتمام بالطرق الفنية للتحقيق في جرائم الحاسب الآلي وذلك من خلال دورات تدريبية للقائمين على ذلك.

- ضرورة استحداث قواعد مناسبة في مجال الإجراءات الجزائية لعدم ملائمة الإجراءات الجزائية الحالية في مجال التحقيق في جريمة المساس بأنظمة المعالجة الآلية للمعطيات.

– سن مراسيم تنفيذية لأنه لا جدوى من سن قانون إن لم ترافقه مراسيم تطبيقية تفعله.

– ضرورة تكوين القضاة في مجال هذا النوع من الإجرام خاصة وأن القاضي الجزائري وفي غياب النصوص التجريمية ونظرا لمستلزمات مبدأ شرعية الجرائم والعقوبات وحظر القياس في المجال الجنائي يجد نفسه مقيدا اتجاه هذا الشكل المستحدث من الإجرام.

– ضرورة التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية، وهذا ما أوحت به الاتفاقية الدولية للإجرام المعلوماتي وذلك بتشجيع الدول على إدراج الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قوانينها العقابية كما أن المنظمة الدولية للملكة الفكرية أصدرت نموذجا للنصوص أدرجت من خلالها الحاسب الآلي في إطار المصنفات المحمية ووضعت أحكاما تتماشى وطبيعة هذا المصنف.

– خلق تواصل دائم بين القضاة والمتخصصين في الاتصالات لتجنب تذبذب وغموض العقوبات الدقيقة في مثل هذه الجرائم.

– العمل على تكوين متخصصين وخبراء قادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها.

– ضرورة استحداث استراتيجيات عقابية وتقنية لحماية ضحايا هذه الجريمة، خاصة فئة الأطفال ورجال المال كونهم الأكثر عرضة لها.

– عدم احتفاظ المستخدمين على بياناتهم أو أموالهم على أجهزتهم لتقليل المخاطر التي يمكن الاختراق عن طريقها، كون البيانات الشخصية هي العملة الرائجة اليوم في الأسواق الرقمية.

- لابد من تشديد العقوبات المالية.

- تجسيد القوانين على أرض الواقع بقوة، كون تجسيده ضعيف إلى حد الساعة بعدما أهملت الجوانب التقنية الكفيلة وتحديد العقوبة المناسبة في حق مرتكبيها.

قائمة المراجع المعتمدة

أولا: المراجع باللغة العربية

أ- الكـــتب:

1- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، الطبعة العاشرة، 2011.

2- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الثاني، جرائم الفساد، المال والأعمال، التزوير، دارهومة، الجزائر، الطبعة الثالثة عشر منقحة ومتممة، 2013.

3- أحسن بوسقيعة، التحقيق الجنائي، دار هومة، الجزائر، الطبعة العاشرة منقحة ومتممة، 2012.

4- أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر،الطبعة الثانية، 2007.

5- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط2،2006.

6- أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، مصر، د. ط، 1972.

7- جباري عبد المجيد، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة، الطبعة الثانية، 2013.

8- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، د. ط، 2010.

9- زيبخة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، د. ط، 2011.

10- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، د. ط، 2007.

11- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، دار

الثقافة، عمان، الطبعة الأولى، 2011.

12- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات في القانون الجزائري والقانون المقارن الجنائي، دار الجامعة الجديدة، القاهرة، د. ط، 2010.

13-عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، مصر، د. ط، 2009.

14- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، بهجات للطباعة والتخليد، مصر، د. ط، 2009.

15- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2007.

16- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة، الإسكندرية، مصر، الطبعة الأولى، 2009.

17- عفيفي كامل عفيفي، جرائم الكمبيوتر، منشأة المعارف، الإسكندرية، مصر، د.ط، د.ت.ن.

18- عمر عيسى الفقى، الجرائم المعلوماتية ، المكتب الجامعي الحديث، الأزاريطة، الإسكندرية، مصر، د . ط، 2006.

19- فضيل العايش، شرح قانون الإجراءات الجزائية بين النظري والتطبيقي، دار البدر، الجزائر، د. ط، د. ت. ن.

20- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، د. ط، 2004.

21-محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، الأردن، الطبعة الأولى، 2007.

22- محمد محمود المكاوي، الجوانب الأخلاقية والمهنية للحماية من الجرائم

المعلوماتية، المكتبة العصرية ، مصر، الطبعة الأولى، 2010.

23- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دارهومة، الجزائر، الطبعة الثامنة، 2013.

24- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى،2009.

25- منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم، عنابة، د. ط، 2006.

26- نجيمي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي(دراسة مقارنة)، دار هومة، الجزائر، د. ط، 2012.

27- نصر الدين مروك ، محاضرات في الإثبات الجنائي، الجزء الثاني(أدلة الإثبات الجنائي)، دار هومة، الطبعة الرابعة، 2010.

28- نسرين عبد الحميد بنية، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، مصر، د. ط، 2008

29- نهلا عبد القادر المومنى، الجرائم المعلوماتية، دار الثقافة ، عمان، د. ط، 2008.

30- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل، عمان، الطبعة الأولى، 2007.

ب- الدوريات والمجلات:

1 - الجريدة الرسمية رقم 47 المؤرخة في 16 نوفمبر 2009.

2 - جريدة الخبر، الصادرة بتاريخ 03 مارس 2014 عدد 7361.

3 - جريدة النهار، الصادرة بتاريخ 04 مارس 2014 عدد 1954.

ت- الموسوعات:

1 -أحمد لعور، نبيل صقر، موسوعة الفكر القانوني(قانون العقوبات نصا وتطبيقا)، دار الهدى، عين مليلة، الجزائر، د. ط، د.ت.ن.

2 -وائل بندق أنور، موسوعة القانون الإلكتروني وتكنولوجيات الاتصالات، دار المطبوعات الجامعية، الإسكندرية، مصر، الطبعة الأولى، 2007.

ث- الرسائل الجامعية:

1 -أمال قارة، الجريمة المعلوماتية، مذكرة تخرج لنيل شهادة الماجستير، جامعة بن عكنون الجزائر العاصمة، 2002.

1 -دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير شعبة القانون الجنائي، جامعة قسنطينة، سنة2013.

2 -سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة تلمسان، سنة 2011.

3 -لفويلي ليلى، الجريمة الالكترونية، مذكرة لنيل شهادة ماستر في القانون، اختصاص قانون العقوبات والعلوم الجنائية، جامعة قسنطينة، سنة 2013.

جـ- النصوص القانونية:

جـ.1- المواثيق الدولية:

1- الاتفاقية الدولية حول الإجرام المعلوماتي الصادرة في 08-11-2001 عن هيئة الأمم المتحدة

جـ.2- القوانين:

1 -الأمر 66-155 المؤرخ في 1966/06/08 يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

2 -الأمر 66–156 المؤرخ في 1966/06/08 يتضمن قانون العقوبات المعدل والمتمم.

3 -القانون 04 /15 المؤرخ في 10 نوفمبر2004 يتضمن قانون العقوبات المعدل والمتمم.

4 -القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: المراجع باللغة الفرنسية:

01- g-Stéfani,g . Le Vasseur, b. bauloc : droit général Dalloz, 17eme édition.

02- Pierre catala« la propriété de l'information» cité parf. toubal, le logiciel-analyse

juridique fudul, L.G. D. J. 1986.

03- Rose Philippe la criminalité informatique que saiege ? 1er édition, puf, 1988.

ثالثا: الموقع الإلكتروني:

01- http://www.droit-dz.com/forum.

02- https://sites.google.com/site/foycelcyber.paycel.bendaas@gmail.com

فهـــــرس المحتويات

المحتويات	الصفحة
مقــدمة.....	أ
الفصل الأول: ماهية جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	01
المبحث الأول: مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	01
المطلب الأول: مفهوم جريمة المساس بأنظمة المعالجة الآلية للمعطيات وخصائصها.....	02
الفرع الأول: تعريف جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	02
أولا: تعريف المعلوماتية	02
ثانيا: التعريفات المختلفة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات	05
الفرع الثاني: خصائص جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	11
أولا: جريمة عابرة للحـــدود.....	12
ثانيا: صعوبة اكتشاف الجريمة.....	12
ثالثا: صعوبة إثبات الجريمة.....	12
رابعا: أسلوب ارتكاب الجريمة.....	12
خامسا: تتم الجريمة بتعاون أكثر من شخص	13
سادسا: خصوصية مجرمي المعلوماتية وضحاياها ونوعية جرائمهم.....	13
المطلب الثاني: موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات ودور الحاسوب في الجريمة.....	20
الفرع الأول: موضوع جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	20
أولا: تعريف المال المعلوماتي وعناصره	21
ثانيا: مفهوم برامج الحاسب الآلي وأنواعها.....	22
الفرع الثاني: دور الحاسوب في جريمة المساس بأنظمة المعالجة الآلية للمعطيات.....	24
أولا: الكمبيوتر أداة لارتكاب الجريمة	24

ثانيا: الكمبيوتر هدف للجريمة 24
ثالثا: الكمبيوتر مسرحا للجريمة 25
رابعا: دور الكمبيوتر في اكتشاف الجريمة 25
المبحث الثاني: أركان جريمة المساس بأنظمة المعالجة الآلية للمعطيات..... 25
المطلب الأول: الركن المفترض (نظام المعالجة الآلية للمعطيات) 26
الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات..... 26
الفرع الثاني: عناصر نظام المعالجة الآلية للمعطيات..... 29
أولا: مركب يتكون من عناصر مادية ومعنوية مختلطة تربط بينهما نتيجة علاقات توحدها نحو تحقيق هدف محدد 29
ثانيا: ضرورة خضوع النظام لحماية فنية 31
المطلب الثاني: الأركان الأساسية لجريمة المساس بأنظمة المعالجة الآلية للمعطيات..... 32
الفرع الأول: الركن الشرعي 32
الفرع الثاني: الركن المادي 34
أولا: الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات..... 34
ثانيا: الاعتداءات على منتوجات الإعلام الآلي (التزوير المعلوماتي)..... 39
الفرع الثالث: الركن المعنوي..... 44
أولا: الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات.... 44
ثانيا: الاعتداءات على سير نظام المعالجة الآلية للمعطيات..... 45
ثالثا: الاعتداءات العمدية على المعطيات..... 45
رابعا: استخدام المعطيات كوسيلة في ارتكاب الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات..... 45
الفصل الثاني: قمع جريمة المساس بأنظمة المعالجة الآلية للمعطيات..... 46
المبحث الأول: القواعد الإجرامية لمكافحة جريمة المساس بأنظمة المعالجة الآلية للمعطيات..... 47

المطلب الأول: الاختصاص المحلي للجهات القضائية..... 47
الفرع الأول: الصلاحيات المكانية للضبطية القضائية..... 48
أولا: الضبطية القضائية..... 48
الفرع الثاني: الاختصاص المحلي لقاضي التحقيق..... 52
أولا: محكمة سيدي محمد الجزائر العاصمة..... 53
ثانيا: محكمة قسنطينة..... 53
ثانيا: محكمة ورقلة..... 53
رابعا: محكمةوهران..... 53
الفرع الثالث: المركز العالميللشكاوي الخاصة بجرائم الانترنت 54
الفرع الرابع : الاختصاص القضائي لجريمة المساس بأنظمة المعالجة الآلية للمعطيات..... 54
المطلب الثاني: أساليب التحري والتحقيق في لجريمة المساس بأنظمة المعالجة الآلية للمعطيات 59
الفرع الأول: الإجراءات الخاصة المنصوص عليها في قانون 04/09..... 59
أولا: مراقبة الاتصالات الالكترونية..... 59
ثانيا: تجميع الاتصالات الالكترونية وتسجيل محتواها 62
ثالثا: تفتيش المنظومة المعلوماتية 62
رابعا: حجز المعطيات المعلوماتية 70
الفرع الثاني: شروط صحة هذه الإجراءات 74
أولا: السلطة المخولة بتسليم الإذن 74
ثانيا: طبيعة الإذن ومدته 75
ثالثا: المساعدات التقنية في إطار البحث عن الجريمة 75
الفرع الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 79

المبحث الثاني: إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات والجزاءات المقررة لها 80
المطلب الأول: إثبات جريمة المساس بأنظمة المعالجة الآلية للمعطيات 80
الفرع الأول: طبيعة الدليل الالكتروني 80
أولا: طبيعة الدليل الالكتروني أمام القضاء المدني 81
ثانيا: طبيعة الدليل الالكتروني أمام القضاء الجزائي 85
الفرع الثاني: مدى حجية المستخرجات الالكترونية كدليل الكتروني في إطار نظرية الإثبات الجنائي 87
أولا: موقف النظم القانونية من حجية المخرجات الكمبيوترية..... 88
المطلب الثاني: الجزاءات المقررة للجريمة 93
الفرع الأول: العقوبات المطبقة على الشخص الطبيعي 93
أولا: العقوبات الأصلية 93
ثانيا: العقوبات التكميلية 95
الفرع الثاني: العقوبات المطبقة على الشخص المعنوي 96
الخاتمة: 98
قائمة المراجع: 103
الفهرس: 107