جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية

قسم القانون العام

خصوصية جرائم المعالجة الآلية للمعطيات

مذكرة لنيل شهادة الماستر في الحقوق
تخصص: قانون جنائي

إعداد الطالبة:
– هني لندة

إشراف الأستاذ:
– صغير يوسف

لجنة المناقشة

الأستاذ(ة): حمودي ناصر.....رئيسا
الأستاذ(ة): صغير يوسف.....مشرفا ومقررا
الأستاذ(ة):.....ممتحنا

السنة الجامعية: 2021/2020

شكر وتقدير

نشكر الله عز وجل ونحمده حمدا كثيرا على توفيقه لنا وتذليله لصعوبات في انجاز هذا العمل

وعن الرسول صلى الله عليه وسلم: "من لم يشكر الناس لم يشكر الله، ومن اسدى إليكم معروفا فكافؤوه فإن لم تستطيعوا فادعوا له".

وعليه أتقدم بجزيل الشكر للأستاذ المشرف الفاضل " الأستاذ صغير يوسف "على تعبه معي ومساعدته لي، والذي لم يبخل بتوجيهاته ونصائحه القيمة التي كانت عونا في إتمام هذا العمل زاده الله رفعة وارتقاء في الدرجات العلمية.

إلى كل من ساهم في إنجاز هذا العمل المتواضع سواء من قريب أو بعيد وبالامتنان على ما قدموه لي من المعونة والمساعدة والنصح والمشورة مما كان له في الواقع الحسن على قلبي والحرارة الكبيرة التي غذت إرادتي للخروج بهذا العمل المتواضع والبسيط، فلهم جميعا أقدم كلمة شكر وتقدير.

الإهداء

أهدي ثمرة جهدي

إلى الرجل العظيم صاحب الصبر الجميل إلى الذي افنى حياته من أجل تعليمي

إلى من جرع الكأس فارغا ليسقيني قطرة الحب،

إلى من كلت أناملة ليقدم لنا لحظة سعادة

إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم إلى أعز إنسان

أبي العزيز

إلى من أرضعني الحب والحنان إلى رمز الحب و بلسم الشفاء

إلى قرة العين، إلى من جعلت الجنة تحت قدميها إلى التي وهبتني كل شيء

إلى أغلى إنسان أمي الغالية حفظها الله

إلى من هم دعمي وسندي في هذه الدنيا إلى من لولا وجودهم لا طعم للحياة إخوتي

عبد الله، خالد، ريماس

إلى أسرتي الثانية إلى القلوب الطاهرة الرفيقة والنفوس الصافية إلى أعز

صديقاتي نادية وابنتها الكتكوتة ميرال، كنزة،

وبالأخص الى رفيقة دربي و أعز صديقاتي وأختي الغالية التي لم تلدها أمي

لونيي أمينة

وإهدائي الخاص إلى أستاذي المشرف الذي سهر على نجاح هذا العمل

"الأستاذ صغير يوسف"

وإهداء إلى كل من نسيناه ولم يذكره قلمي إلى كل من لم تحمل أسمائهم مذكرتي

ولم تنساهم ذاكرتي

مع تحيات: هنيي لندة

مقدمة

إن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول.

فبات يطلق على هذا العصر عصر المعلومات، فمنذ وقت ليس ببعيد كان كم المعلومات المتولدة عن التفاعلات البشرية محدودا إلى حد كبير ولم يشكل حجمها أي مشكلة أمام لمواجهة هذه الطفرة، فكان أن ظهرت الحاسبات الإلكترونية، بالإضافة إلى ظهور مستحدثات تقنية كأقراص الفيديو الرقمية وأقراص الليزر، ووسائط الاتصال... وذلك من أجل تسهيل التحكم في المعلومات ومعالجتها واسترجاعها.

وهو ما دعا بالكثير من رجال الاقتصاد والاجتماع إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في القرنين التاسع عشر والعشرين، ففي حين كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان.

فإن هدف الثورة الثانية هو إحلال الآلة محل النشاط الذهني للإنسان. عمليات تجميعها وتخزينها وإعادة استرجاعها، إلا أنه ومع تقدم البشرية وتزايد معارف الإنسان وعلومه بدأ كم المعلومات يتزايد ويتكاثر وصارت الطرق التقليدية لتجميع وتنظيم هذه المعلومات عاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفعالية، وأصبح من الضروري اللجوء إلى استخدام أساليب علمية وتقنية متطورة.

إن القوانين هي مرآة المجتمع ومقياس لحضارة ورقي الدولة، ويعيش عصرنا الحاضر تسارعا مذهلا في مجال التكنولوجيا والعولمة وعلى الرغم من الإيجابيات التي أحرزتها الوسائل التقنية فإنها لا تخلوا من السلبيات ولعل من أبرزها ظهور الجرائم المعالجة

الآلية للمعطيات التي تختلف باختلاف مجلات ارتكابها كالتصنت وإتلاف المعلومات والسرقة المعلوماتية وإجراء التحويلات المصرفية بطرق غير مشروعة وذلك باستخدام الحاسب آلي والإنترنت إضافة إلى ارتكاب الجرائم المخلة بآداب و الأخلاق العامة التي تتخذ عدة صور منها إشاعة الفاحشة عن طريق إنشاء موقع أو نشر ونطرا لخصوصية هذا النوع من الجرائم فقد أقدمت كل من التشريعات الداخلية والعالمية إلى إضفاء حماية تشريعية جنائية ملائمة لجرائم المعالجة الآلية للمعطيات.

من بين الآثار السلبية للثورة المعلوماتية هي ظهور الجرائم جرائم المعالجة الآلية للمعطيات، لذلك المشرع الجزائري على غرار باقي التشريعات بالعالم حاول التصدي لها حيث عرفها بجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وكما أنها تحوز هاته الجريمة على مجموع من الخصائص التي تجعلها مختلفة عن الجريمة التقليدية، كما لها صور متعددة من جرائم يرتكبها الشخص الطبيعي والتي يرتكبها الشخص المعنوي وهي في ازدياد كلما تطورت وسائل التكنولوجيا، لكن رغم تميزها عن الجريمة التقليدية لكنها تشترك معها في الأركان التي تقوم بهم وتزول بزوال إحداهما، من الركن الشرعي الذي يجرم الفعل، والركن المادي المتمثل في السلوكات الإجرامية المحددة بنص والركن المعنوي الذي يدور حول القصد الجنائي لهذه الجريمة.

أهمية البحث:

تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة وبالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات التي لم تنل حظها (من البحث والتحقيق والمحاكمة) على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها، لاسيما أن هذا الموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها، على الرغم من الصعوبات العديدة التي واجهتنا في إعداد المذكرة نظرا لصعوبة الموضوع وتشعبه.

تظهر هذه الأهمية من خلال اعتبار أن موضوع الجرائم الإلكترونية حديث وكثير الانتشار حاليا، كما أنه من الموضوعات التي تثير جدلا فقهيا لدى فقهاء القانوني الجنائي، إضافة إلى تعلق الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوب ارتكاب هذا النمط من الجرائم، وهذا ما شكل عائقا أما القائمين على البحث والإثبات الجرائم الإلكترونية، حيث أن قواعد البحث والتحري وأسس الإثبات الجنائي في القوانين التقليدية لا تكفي، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلاءم مع طبيعتها الفنية.

اختيار موضوع المتابعة الجزائية في الجريمة المعلوماتية يرجع في حقيقة الأمر إلى العديد من الاسباب بعضها شخصي والآخر موضوعي

فالأسباب الشخصية: تمكن في اهتمامي بمجال الجريمة المعلوماتية وما يلقاها من جرائم وكذا من إجراءات خاصة وإن إجراءات المتابعة فيها تختلف كل الاختلاف عن إجراءات المتابعة في الجرائم التقليدية بالإضافة إلى أنه موضوع جديد، ورغبتي الشديدة في الغوص في مجال إجراءاتها وكذا مكافحتها والوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

أما الأسباب الموضوعية: فتكمن فيما يطرحه موضوع الحماية الإجرائية للجريمة المعلوماتية من إشكاليات قانونية التي لا بد من الوقوف نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الافعال او الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، والقواعد الإجرائية

الحديثة التي جاء بها تعديل الإجراءات الجزائية الجزائري وكذا قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

فإن بحثنا هذا يسعى لتحقيق جملة من الأهداف التي من خلالها يمكن الإحاطة بجوانب الموضوع المختلفة، فنظرا للتطورات التكنولوجية و المعلوماتية الحديثة، و كذا ظهور المعاملات الإلكترونية و انتشارها على نطاق واسع وغير محدود، أصبحت الدول أمام مشاكل قانونية متعددة، خصوصا فيما يتعلق بالاعتداءات الواقعة على الأنظمة المعلوماتية، فأصبحت مواجهة هذه الجرائم واقعا مفروضا على مختلف التشريعات، و بالتالي فإننا نهدف الى تبيان الاتي:

– تقديم دراسات قانونية و موضوعية، تكشف الملامح و الجوانب المختلفة لهاته الظاهرة الإجرامية.

المنهج المتبع:

أما بخصوص المنهجية المتبعة في هذا البحث، فقد اعتمدت كل من المناهج التالية، التي أرى أنها تتماشى مع طبيعة الموضوع المطروح:

المنهج التحليلي:

لأن دراستنا ستعتمد على تحليل أهم النصوص القانونية المنظمة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في مختلف التشريعات و كذا وصف هاته الجرائم وفقا لما نص عليه التشريع الجزائري و الاتفاقيات الدولية.

الإشكالية:

الفصل الأول

طبيعة جرائم المعالجة الآلية للمعطيات

الفصل الأول

طبيعة جرائم المعالجة الآلية للمعطيات

موضوع جرائم المعالجة الآلية للمعطيات من الجرائم التي باتت الحاجة إلى دراستها دراسة جيدة ومتأنية من طرف الباحثين ودارسي القانون من الأمور الضرورية والملحة في الوقت الراهن، وهو الأمر الذي دفعنا إلى إجراء دراستنا في هذا المجال القانوني.

حيث نهدف من خلال هذه الدراسة إلى تغطية الفراغ القانوني الملحوظ في هذا المجال، باعتبارها من أخطر الجرائم في العصر الحديث فآثارها لا تقتصر على الفرد أو مؤسسة أو على الدولة الواحدة بل أنها تتجاوز الحدود الإقليمية لها[1].

جرائم المعالجة الآلية للمعطيات جرائم حديثة نسبيا وذلك لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات، ونتيجة لحداثة الجريمة فقد كانت هناك اتجاهات مختلفة في تعريفها كما انها اتسمت بمجموعة من الخصائص و السمات التي ميزتها عن غيرها من الجرائم الأخرى كما أن هذه الجريمة جلبت معها طائفة جديدة من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية[2].

لذا قمنا بتقسيم الفصل الأول إلى مبحثين نستعرض من خلال المبحث الأول ماهية جرائم المعالجة الآلية للمعطيات والمبحث الثاني صور جرائم المعالجة الآلية للمعطيات.

---

[1]– أحمد، هلالي عبد اللاه، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003، ص12.

[2]– نهلا عبد القادر المومني، الجرائم المعلوماتية، الجرائم المعلوماتية ، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 45.

المبحث الأول:

ماهية جرائم المعالجة الآلية للمعطيات

عصر الإنترنت أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة. ويبدو بالفعل أن التكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وأن المعلومات في حد ذاتها هي الخام الأساسية للإنتاج التي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها.

وفي الواقع إن الوجه المشرق لتقنية المعلومات يخل من الجانب المظلم الذي تمثل في الإجرام المعلوماتي والذي كان موجودا ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب تتنوع وتتعدد[1].

وتعد جرائم المعالجة الآلية للمعطيات من الظواهر الإجرامية الحديثة، وتحديد مفهومها يعد الخطوة الأولى للتعرف على هذه الظاهرة الجرمية من جميع جوانبها القانونية، خاصة إذا علمنا أنه لا يوجد قانوني موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة الكومبيوتر بسبب ذاتيتها وتميزها عن غيرها من الجرائم التقليدية، سواء في محلها أو خصائصها، ومما لاشك فيه أن أي محاولة من أجل اختيار وتحديد المصطلح الملائم لهذه الظاهرة ينبغي أن يكون مبنيا ومؤسسا على عدة ضوابط تقنية وقانونية أولها إدماج البعدين التقني والقانوني، ذلك أن تقنية المعلومات في أصلها هي نتيجة إدماج الحوسبة والاتصال، فالحوسبة تقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة المعطيات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق وأما الاتصال فهو قائم على وسائل لنقل المعلومات والضابط الثاني أن يكون اختيار المصطلح شاملا لما يعبر عنه ملما بحدود محله،

[1]– نهلا عبد القادر المومني، مرجع سابق، ص 46.

فلا ينبغي أن يقتصر على جزء ليعني الكل ولا ينصرف إلى ما لا يجب أن ينطوي تحت نطاقه.

لذلك فقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة جرائم المعالجة الآلية للمعطيات، ذلك أن عدم الاتفاق على تعريف هذه الظاهرة الإجرامية إنما يؤدي إثارة من المشكلات العلمية يتمثل أهمها في صعوبة تقدير حجم هذه الظاهرة وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذا تحقيق التعاون الدولي لمكافحته إلا أن المتفق عليه أن فكرة المعلوماتية هي الفكرة الجوهرية والمركزية في دراسة هذه الظاهرة الإجرامية ذلك أن المعلوماتية هي شرط مفترض لقيام هذا النوع من الجرائم[1].

ومن هذا المنطلق آثرنا تخصيص المبحث الأول إلى مفهوم جرائم المعالجة الآلية للمعطيات كمطلب أول ثم سأعرض في المطلب الثاني أهم صور جرائم المعالجة الآلية للمعطيات.

المطلب الأول

مفهوم جرائم المعالجة الآلية للمعطيات

تعتبر جرائم المعالجة الآلية للمعطيات الشرط الأولي للبحث في توافر أو عدم توافر اي جريمة من الجرائم الاعتداء على الجرائم المعالجة فإذا تخلف هدا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم (الماسة بنظام المعالجة الآلية للمعطيات) إذا أن هذا الشرط يعتبر عنصرا لازما لكل منها.

ولذلك يكون من اللازم تحديد مفهوم شرط الجرائم المعالجة الآلية للمعطيات حيث ذكر مجلس الشيوخ الفرنسي في اقتراح لتعريف هذا النظام بأنه «كل مركب يتكون من وحدة

[1]– نائلة عادل محمد فريد قورة، جرائم الحساب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي، سوريا، 2005، ص 28.

أو مجموعة وحدات المعالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات والتي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات على ان يكون هذا المركب خاضع لنضام الحماية الفنية".

وانطلاقا من هذا التعريف المقترح المجلس الشيوخ الفرنسي نجد انه قد ركز في مفهوم هذا النظام على عنصرين أساسيين هما: تعريف نظام المعالجة الآلية للمعطيات وكذا ضرورة وجود حماية فنية لهذا النظام

وسوف نتناول كل من عنصرين في الفرعين المواليين تعريف نظام المعالجة الآلية للمعطيات (فرع أول). وأهم الخصائص التي تميزها عن غيرها من الأنماط الأخرى للجرائم (فرع ثاني)[1].

الفرع الأول: تعريف جرائم المعالجة الآلية للمعطيات

إن الجرائم الناشئة في البيئة الرقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطوراتها المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل إلكتروني، وكذا بتكنولوجيا وسائل الاتصال وشبكات الربط. لذلك فإنه من الضروري أن يكون أي تعريف لهذا النمط من الجرائم متسما بالمرونة بما يسمح باستيعابه ومتواكبه مع سائر التقنيات المبتكرة والراهنة والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات.[2]

لكن مع التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم جرائم المعالجة الآلية للمعطيات حشية من حصر نطاقها داخل إطار تجريمي محدد قد يضر بها خاصة في ظل التطور المستمر للتقنية

[1]– خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات، طبعة 2010، دار الهدى للطباعة و النشر و التوزيع، عين مليلة الجزائر، 2010، ص ص 108 – 109.

[2]– خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009، ص 73.

المعلوماتية، فيما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى تطهر نتيجة استخدام تقنيات جديدة.

وإذا كان التطور المتجدد والمستمر للمعلوماتية يمنع صور التجريم الحالية عن مواكبة ما يطرأن صور إجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، وهذا ما يقع على عاتق الفقه بداية بوضع تعريف لهذه الظاهرة الإجرامية، والذي قد يسهم المشرع للنصوص القانونية ويساعد القضاء في تفسير هذه النصوص وتكييف الوقائع.

وقد ذهب الفقهاء في تعريف جرائم المعالجة الآلية للمعطيات مذاهب شتى ووصفوا تعريفات مختلفة تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته فاختلف بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن تقنية المعلوماتية، وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية، وحتى من الوجهة القانونية تعددت التعريفات واختلفت بحسب الدراسة القانونية التي تناولتها

وفي سبيل ذلك فإن الفقه الجنائي قد بذل محاولات عديدة لتعريف جرائم المعالجة الآلية للمعطيات، ولعل جميع المحاولات التي بذلت من أجل تعريف جرائم المعالجة الآلية للمعطيات لا تخرج عن اتجاهين أولهما يضيق في مفهومها و الثاني يوسعه[1].

[1]– ذلك أن الجريمة المرتكبة بواسطة تقنية المعلومات تدخل في نطاق دراسات القانون الجنائي الوطني، والتي تقع في صميم القسم الخاص لقانون العقوبات، و أنها من الجرائم التي تتخطى حدود الدولة الواحدة فهي تدخل أيضا في نطاق دراسات القانون الجنائي الدولي و نظرا لنمو و تزايد التجارة الالكترونية من خلال التبادلات و المراسلات التجارية الالكترونية فإن الجرائم المرتكبة بواسطة تقنية المعلومات لصيقة الصلة بالقانون التجاري و بحركة التجارة العالمية الحديثة، كما أن الاستعمال الواسع لتقنية المعلومات في المجتمع مكنت من تخزين و استرجاع و تحليل كميات هائلة من البيانات الشخصية فخلقت بذلك سلسلة من التحديات الجديدة و التهديدات الخاصة بالحياة الشخصية و أدى ذلك إلى تزايد انتهاك الحقوق الأساسية و الحريات الفردية التي كفلتها القوانين الدستورية مما يدل على ارتباط الموضوع أيضا بالقانون الدستوري، و ارتباطه في نفس الوقت بالقانون الإداري خاصة في ضل ظهور و بروز الحكومات الالكترونية.

أولا: الاتجاه الذي يضيق مفهوم جرائم المعالجة الآلية للمعطيات

يذهب أنصار هذا الاتجاه إلى حصر جرائم المعالجة الآلية للمعطيات في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وأن الجرائم التي تفتقر إلى هذه المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية وذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة.

فهي التي فقط تكون بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية[1].

ومن التعريفات التي وضعها أنصار هذا الاتجاه أن جرائم المعالجة الآلية للمعطيات هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى.

وفي هذا الاتجاه عرفها **DAVID THOMSON** دافيدتومسون: "بأنها أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".

وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة على درجة كبيرة من العلم بتكنولوجيا الحاسبات وهذا المفهوم قد أخذت به وزارة العدل الأمريكية في تقريرها الصادر عام 1989بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاث حينما عرف جرائم المعالجة الآلية للمعطيات بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها [2].

[1]– نائلة محمد فريد قورة، مرجع سابق، ص 30.

[2]– المرجع نفسه، ص ص 28– 30 .

وفي هذا الاتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذ **MASS** أن المقصود بجرائم المعالجة الآلية للمعطيات "هي تلك الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح.".

كما عرف الأستاذ **PAEKER** جرائم المعالجة الآلية للمعطيات بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل [1].

والملاحظة أن التعريفات المتقدمة تضيق على نحو كبير من جرائم المعالجة الآلية للمعطيات، حتى أن البعض يرى أن جرائم المعالجة الآلية في ظل هذا الاتجاه تصبح أشبه بالخرافة فحصرها مثلا في الحالات التي تتطلب أن يكون مقترف هذه الجريمة متمتعا بقدر كبير من المعرفة التقنية لارتكابها وهو إن تحقق في بعض الأحوال فقد لا يتوفر في كثير منها، إذ قد يرتكب الفعل الغير مشروع في البيئة الرقمية دون أن يكون فاعله بحاجة إلى هذا القدر من المعرفة.

ورغم ذلك فإنه لا يمكن إنكار أن هذه الأفعال تدخل في عداد جرائم المعالجة الآلية للمعطيات لذلك فإنه يأخذ على هذه التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه الإجرام المعلوماتي فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة والبعض الآخر ركز على وسيلة ارتكابها والبعض الآخر ركز على معيار النتيجة[2].

ثانيا: الاتجاه الذي يوسع مفهوم جرائم المعالجة الالية للمعطيات

إزاء الانتقادات التي وجهت للاتجاه الأول حاول بعض الفقه عريف جرائم المعالجة الآلية للمعطيات على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي.

---

[1]– رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، سوريا 2012، ص 40.

[2]– أحمد أمين شوابكة، جرائم الحاسوب و الانترنت، الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر و التوزيع 2009، ص 08.

فعلى عكس الاتجاه السابق فإن أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم جرائم المعالجة الآلية للمعطيات باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصبغ عليه وصف جرائم المعالجة الآلية للمعطيات.

وقد تباينت مواقف أنصار خذا الاتجاه في تعريف هذه الجريمة بحسب المعايير التي اعتمد عليها كل فريق في تعريف جرائم المعالجة الآلية للمعطيات وتتباين مواقف أنصار هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة، فيذهب فريق من الفقهاء إلى تعريف جرائم المعالجة الآلية للمعطيات بأنها سلوك إجرامي يتم بمساعدة الحاسب الآلي وفريق آخر يعتبرها أنها كل جريمة تتم في محيط الحاسبات الآلية، ومن هذه التعريفات ما جاء به الفقيه **(MERWE)** الذي يرى أن جرائم المعالجة الآلية للمعطيات تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي[1].

كما ذهب البعض إلى القول بأن جرائم المعالجة الآلية للمعطيات هي كل عمل أو الامتناع يأتيه إضرار بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها[2].

وفي ذات الاتجاه يرى كل من **MICHEL et CREDO** أن جرائم المعالجة الآلية للمعطيات تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب.

المجني عليه أو بياناته كما تمتد لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به[3].

---

[1]– أحمد هلالي عبد الاله، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة ، ة الطبعة الأولى، دار النهضة العربية، 2000، ص 04.

[2]– خالد عبد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة، 2001، ص 30.

[3]– و ضع هذا التعريف من طرف مجموعة من خبراء منظمة التعاون الاقتصادي و التنمية في اجتماعها المنعقد في باريس عام 1983 ضمن حلقة الاجرام المرتبط بتقنية المعلومات.

وهناك اتجاه آخر عرفها بالقول أن جرائم المعالجة الآلية للمعطيات هي كل سلوك غير مشروع وغير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[1].

ولا شك أن الاتجاه المتقدم ينطوي توسع كبير لمفهوم جرائم المعالجة الآلية للمعطيات، إذ يأخذ عليه هذا التوسع الذي من شأنه أن يصبغ وصف الجريمة على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسب الآلي في النشاط الإجرامي.

ولم يسلم هذا الاتجاه من سهام النقد أيضا حين وسع من نطاق هذه الجريمة إلى درجة التسوية بين السلوك غير المشروع قانونا والسلوك الذي يستحق اللوم أخلاقيا واستهجان الكافة له.

كما في التعريف الذي أورده خبراء منظمة التعاون الاقتصادي والتنمية **OECD**، ذلك أنه ليس بالضرورة أن يكون الانحراف عن الأخلاق والسلوك المآثم معاقب عليه قانونا[2].

الفرع الثاني: خصائص جرائم المعالجة الآلية للمعطيات

ارتباط جرائم المعالجة الآلية للمعطيات بجهاز الحاسوب وشبكة الإنترنت أضفى عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية هي:

أولا: جرائم المعالجة الآلية للمعطيات متعدية الحدود (جريمة عابرة الدول)

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود

فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدر التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في الدول مختلفة قد تتأثر بجرائم

[1]– محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص 60.

[2]– نائلة محمد فريد قورة، المرجع السابق، ص 31.

المعالجة الآلية للمعطيات. فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[1].

هذه الطبيعة التي تتميز بها هذه الجريمة كونها جريمة عابرة للحدود حلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام[2].

كانت القضية المعروفة باسم مرض نقس المناعة المكتسبة (الايدز) من القضايا التي لفت النضر الى البعد الدولي للجرائم المعلوماتية، وتتخلص وقائع هذه القضية التي حدث عام 1989 في قيام احد الاشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره الى اعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة.

إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، اذا كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من حصول على مضاد للفيروس؛ وفي الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتقدم الملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث إن أرسل هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه أحدا عشرة تهمة ابتزاز أليه وقعت معظمها في دول مختلفة الا ان إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. ومهما كان الامر فإن لهذه القضية اهميتها من ناحيتين:

[1]– نهلة عبد القادر المومني، مرجع سابق ص ص 50 – 51.

[2]– نائلة محمد فريد قورة، مرجع سابق، ص 48.

الأولى: انها المرة الاولى التي يتم فيها تسليم متهم في جرائم المعالجة الآلية للمعطيات.

الثانية: انها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة اعداد برنامج خبيث (فيروس)[1].

ونتيجة لهذه الطبيعة الخاصة لجرائم المعالجة الآلية للمعطيات ونضرا للخطورة التي تشكلها على مستوى الدولي والخسائر التي قد تتسبب بها ؛تعالت الاصوات الداعية الى التعاون الدولي المكثف من اجل التصدي لهذه الجرائم[2]، والتعاون الدولي يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديم للقضاء العادل.

تكمن اهم المشاكل المتعلقة بالتعاون الدولي حول جرائم المعالجة الآلية للمعطيات في انه لا يوجد هناك مفهوم عام مشترك بين دول حول صور النشاط المكون لهذه الجريمة بالإضافة الى نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص

[1]– نائلة محمد فريد قورة، مرجع سابق، ص 48.

[2]– تجدر الاشارة في هذا المجال إلى مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاقبة المجرمين الذي عقد في هافانا عام 1990، وفي قراره المتعلق بالجرائم ذات الصفة في الحاسوب، ناشد المؤتمر الدول الأعضاء، أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات اساءة استعمال الحاسوب و التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في تحديث القوانين و الاجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن الجزاءات و القوانين الراهنة بشأن سلطات التحقيق و قبول الأدلة في الإجراءات القضائية تنطبق على جرائم المعالجة الآلية للمعطيات و ادخال تغييرات مناسبة عليها إذا دعت الضرورة، كما حثّ مؤتمر دول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدة في المسائل المرتبطة في الجرائم ذات الصلة بالحاسوب، انظر محمود عبد الله، سرقة المعلومات في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002، ص ص 361–362.

عناصر الجريمة ان وجدة جمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك امام التعاون في مجال مكافحة هذا النوع من الجرائم[1].

وبالتالي من اجل تصدي للإجرام المعلوماتي لابد ان تعمل الدول في اتجاهين:

الاول: داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم

الثاني: دولي عن طريق عقد اتفاق دولية، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم [2].

ثانيا: صعوبة اكتشاف جرائم المعالجة الآلية للمعطيات

تتميز الجريمة جرائم المعالجة الآلية للمعطيات بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة[3]. حيث يبدو من الواضح أن عدد الحالات التي تتم فيها اكتشاف هذه الجرائم قليلة إذ قورنت بما يتم اكتشافه من الجرائم التقليدية.

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجرائم المعالجة الآلية للمعطيات إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية كما أن الجاني يمكنه ارتكاب هذه الجريمة في دول وقارات أخرى، إذ أن جرائم المعالجة الآلية كما سبق وأشرنا جريمة عابرة للدول(دولية). وكذلك أن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

---

[1]– عوض محمد محي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكومبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص ص 361 – 362.

[2]– أحمد هلالي عبد الاله، مرجع سابق، ص ص 29 – 32.

[3]– الصغير جميل عبد الباقي، القانون الجنائي و التكنولوجيا الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992، ص 17.

فجرائم المعالجة الآلية للمعطيات في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير مرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها [1].

كما أن المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بموظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها[2].

ويرى البعض أن للمجني عليه دورا مثيرا للريبة في بعض الأحيان فهو قد يشارك بطريق غير مباشر في ارتكاب الفعل وذلك بسبب وجوده في ظروف تجعل تعرضه لجرائم المعالجة الآلية للمعطيات أمرا مرتفعا بشكل كبير ويرجع ذلك بشكل أساسي القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي ويترتب على ذلك أخرى تميز جرائم المعالجة الآلية للمعطيات هي أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم إذ يعتمد ذلك أساسا على تطوير نظم الأمنا لخاصة بأنظمة الحاسبات وشبكاتها[3].

---

[1]– رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، 1994، ص 16.

[2]– وتشير بعض التقديرات إلى أن ما يتراوح بين 20 و 25 بالمائة من جرائم الحاسبات لا يتم الابلاغ عنها مطلقا حشية الإساءة إلى السمعة وفي دراسة – وصفت بأنها تثير الذهول – أجريت على ألف شركة من الشركات المنتجة لجهاز (FORTUNE 500) أظهرت نتائجها أن 2بالمائة فقط من كل جرائم الحاسب هي التي يتم الإبلاغ عنها للشرطة أو مكتب التحقيقات الفيدرالي. أنظر رسم هشام محمد فريد، مرجع سابق ص25 – 26 .

[3]– نائلة محمد فريد قورة، مرجع سابق، ص 46.

وفي الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع جرائم المعالجة الآلية للمعطيات يبدو أكثر وضوحا في المؤسسات المالية البنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية

حيالها إلى تضائل الثقة فيها من جانب المتعاملين معها. حيث أن التجنب الأكبر من جرائم المعالجة الآلية للمعطيات لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحتها وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي[1].

وإلى جانب ذلك فإن المجني عليه يتردد أحيانا غي الإبلاغ عن هذه الجرائم خوفا من أن الكشف عن أسلوب ارتكاب هذه الجرائم قد يؤدى إلى تكرار وقوعها بناء على تقليدها من الآخرين كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه [2].

ثالثا: صعوبة إثبات جرائم المعالجة الآلية للمعطيات

اكتشاف جرائم المعالجة الآلية للمعطيات أمر كما سبقنا وأشرنا ليس بالسهل ولكن حتى في حال اكتشاف وقوع الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب.

---

[1]– من الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الامريكية مطالبة البعض بان تفرض النصوص المتعلقة بجرائم الحاسبات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل الى علمهم من جرائم في هذا المجال مع تقرير جزاء الاخلال بهذا الالتزام. وعرض ذات الاقتراح على لجنة خبراء مجلس أوربا ل و لاقت الفكرة رفضا باعتبار انه ليس مقبولا تحويا المجني عليه الى مرتكب الجريمة. انظر، رستم هشام محمد فريد، مرجع سابق، ص ص 25– 27 .

[2]– الهيتي محمد حماد، تكنولوجيا الحديثة و القانون الجنائي، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2004، ص 166.

فجرائم المعالجة الآلية للمعطيات تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحو كليا من قبل الفاعل أمرا في غاية السهولة.

ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير[1].

وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث حيث تخلف آثارا مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على آثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في جرائم المعالجة الآلية للمعطيات يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين[2]:

الأول: جرائم المعالجة الآلية لا تخلف أثارا مادية.

ثانيا: إن كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها في فترة طويلة نسبيا، الأمر الذي يعطي مجالا

[1]– رستم هشام محمد فريد، مرجع سابق، ص 23.

[2]– المعاينة يقصد بها إثبات حالة الأماكن والأشخاص والأشياء وكل ما يعتبر في كشف الحقيقة، والمعاينة بهذا المعنى يستلزم الانتقال إلى محل الواقعة او أي محل آخر توجد به أشياء أو آثار يرى المحقق ان لها صلة بالجريمة ,أنظر حجازي عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، 2002، ص 59.

للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت الأمر الذي يورث الشك في دلالة الأدلة المساقاة من المعاينة في جرائم المعالجة الآلية للمعطيات[1].

بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائقا أساسيا أمام إثبات جرائم المعالجة الآلية للمعطيات ذلك إن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت. ونتيجة لنقص الخبرة والتدريب كثيرا ما تخفق اجهزة الشرطة في تقدير اهمية جرائم المعالجة الآلية للمعطيات فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية. بل ان المحقق قد يدمر الدليل بمحوه محتويات الاسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة[2].

رابعا: أسلوب ارتكاب جرائم المعالجة الآلية للمعطيات

ذاتية جرائم المعالجة الآلية للمعطيات تبرز بصورة اكثر وضوحا في اسلوب ارتكابها وطريقتها. فإذا كانت جرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو جريمة السرقة... فإن جرائم المعالجة الآلية للمعطيات هي جرائم هادئة بطبيعتها **soft crime** لا تحتاج إلى العنف، بل كل ما تحتاج إليه ,هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير مشروعة. تحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك دون الحاجة لسفك الدماء.

[1]– حجازي عبد الفتاح بيومي، مرجع سابق، ص ص 28 – 29.

[2]– المرجع نفسه، ص 28 – 29.

خامسا: جرائم المعالجة الآلية للمعطيات تتم عادة بتعاون أكثر من شخص

تتميز جرائم المعالجة الآلية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرار بجهة المجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه[1].

والاشتراك في إخراج جرائم المعالجة الآلية للمعطيات إلى حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا وهو غالبا كذلك يتمثل في مساعدة فنية أو مادية[2].

سادسا: خصوصية مجرمي المعلوماتية

المجرم الذي يقترف جرائم المعالجة الآلية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي).

فإذا كانت الجرائم التقليدية لا اثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكبها باعتبارها قاعدة عامة فإن الأمر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية في الغالب الأعم ومن يرتكبها عادة يكون من ذوي الاختصاص في المجال تقنية المعلومات، او على الأقل شخص لديه حد ادني من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

[1]– عفيفي كامل، جرائم الكومبيوتر وجرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى، بدون ناشر، ص 32.

[2]– سامي الشوا، مرجع سابق، ص 46.

فعلى سبيل المثال فإن جرائم المعالجة الآلية للمعطيات ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبها.

كذلك فإن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي[1].

المطلب الثاني

صور جرائم المعالجة الآلية للمعطيات

نص المشرع الجزائري على مجموعة من الأفعال المجرمة من خلال المواد 394 مكرر إلى 394 مكرر 7[2] والتي يمكن تلخيصها فيما يلي:

1- الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش أو جزء منها.

2- إتلاف أو حذف لمعطيات المنظومة أو تخريب اشتغال المنظومة.

3- إدخال بطريق الغش معطيات في نظم المعالجة الآلية للمعطيات وإزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

4- كل من يقوم عمدا بطريق الغش بما يأتي:

أ- تصميم أو بحث أو تجميع أو توفير نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم[3].

---

[1]- نهلة عبد القادر المومني، مرجع سابق، ص ص 58- 59.

[2]- أمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.

[3]- خثير مسعود، مرجع سابق، ص 113.

ب- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم.

وانطلاقا من هذا التقسيم سأتعرض من خلال الفروع الموالية لأهم هاته الجرائم التي قد تمس مباشرة بنظام المعالجة الآلية للمعطيات بصفة عامة أو بالبرامج بصفة خاصة وذلك على النحو التالي:[1]

الفرع الأول: الصور البسيطة لجرائم المعالجة الآلية للمعطيات

بالبحث في المواد التجريمية المتصلة بجرائم المساس بنظام المعالجة الآلية للمعطيات، نصل إلى قائمة حد أدنى لأهم السلوكيات المقصودة بالتجريم المتمثلة أساسا في جريمة الدخول و/أو البقاء غير مشروع في المنظومة المعلوماتية، في صورتيها الشكلية والمادية.

أولا: جريمة الدخول أو/و البقاء غير مشروع داخل نظام المعالجة الآلية للمعطيات

عمد المشرع الجزائري إلى تجريم سلوك الدخول و/أو البقاء في أنظمة المعلومات، وفق صورتيه المادي والشكلي، [2] الأمر الذي نطرحه وفق ما يلي:

1- الدخول و /أو البقاء في نظام المعالجة الآلية للمعطيات كجريمة شكلية جرم المشرع الجزائري السلوك القصود في 394 مكرر من قانون العقوبات الجزائري.[3] المقابلة لنص المادة 313-1 من قانون العقوبات الفرنسي. والمادة 2 من اتفاقية بودابيست.[4]وسنحاول تفصيل هذه الجريمة من خلال مما يلي

1-1- تعريف الجريمة: يصعب الوصول إلى تعريف جامع للجريمة المطروحة، لكن من خلال النصوص المذكورة أعلاه يمكن القول:" هي من أهم الظواهر الإجرامية التي أسفرت

[1]- خثير مسعود، مرجع سابق، ص 114.

[2]- يرى جانب من الفقه أنه لا ضرورة لتجريم مجرد الدخول و/أو البقاء كجريمة شكلية، على أساس أنه سلوك غير ضار ومن خلاله يعرض الفاعل قدراته الفنية، نهلا عبد القادر المومني، مرجع سابق، ص 156.

[3]- الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[4]- المعنونة بالدخول غير القانوني.

عنها التطورات التكنولوجية وهي إن كانت جريمة شكلية، غير أنه في الغالب ما يرتبط بالدخول ارتكاب جرائم أخرى مادية. لذا عاقب المشرع على مجرد الدخول لنظم المعالجة الآلية للمعطيات تفاديا للتمادي في الاعتداءات على النظم[1].

وما تحتويه من معلومات وشدد العقوبات في حال ما إذا ترتب على فعل الاختراق نتيجة مادية ما، تتمثل في الاضرار بالمعلومات أو نظم معالجتها ".[2]

كما يمكن القول أنها :" قيام شخص بالدخول /أو البقاء في منظومة معلوماتية بمفهومها الواسع، دون وجه حق ودون أهداف حاصة، باستعماله لآليات معينة ".[3]

1-2 أركان الجريمة:

يمتاز الركن المادي والمعنوي للجريمة محل الدراسة بما يلي:

أ- الركن المادي: من خلال استقراء نص المادة 394 من قانون العقوبات الجزائري[4]، أن الجريمة المطروحة هي من الجرائم الشكلية – جرائم الخطر أو جرائم السلوك المحض.

التي لا تتطلب لقيامها النتيجة الإجرامية.[5] فيتضح لنا بأن الركن المادي لهذه الجريمة يتحقق بإتيان سلوك يتمثل في صورة الدخول لنظم الم أن تكون مؤمنة بإجراءات فنية [6]. عكس البعض الآخر الذي لا يرى ضرورة لذلك – وهو الرأي الغالب –.[7] غير أننا وبدون

---

[1]- رشيدة بوك، مرجع سابق، ص 116.

[2]- رشيد بوكر، مرجع سابق، ص 116.

[3]- بطرح التعريف، نكون قد تطرقنا للركن الشرعي للجريمة.

[4]- الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[5]- مصطلح الدحول، اعتمده المشرع الجزائري في المواد ذات الصلة، أما نظيره الفرنسي فاعتمد مصطلح (accès) الذي بترجمته قد يقودنا إلى الى مفهوم " التجاوز أو الولوج "، هذا الاخير يعد أكثر دقة ومقبولية من الأول، الذي يدل على الدخول المادي ، كدخول المنازل، أما الجريمة محل الدراسة فتتطلب التجاوز والولوج المعنوي لا المادي.

إلا أنه يرى الفقه أن الدخول المقصود في جريمة الحال هو الشبيه بالدخول المعنوي الذهني في ذاكرة الإنسان، ايمن عبد الله فكري، جرائم نظم المعلومات –دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 231.

[6]- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية ، مصر، 2008، ص 267.

[7]- أيمن عبد الله الفكري، مرجع سابق، ص 233-234.

الخوض في هذا الجدل، نرى أن المشرع الجزائري لم يتطلب ذلك. لذلك سوف نقتصر على السلوك الإجرامي فقط الذي يقوم على ما يلي:

أ-1 – فعل الدخول: لنحدد المفهوم الدقيق لفعل الدخول، وجب الإجابة على: [1]

المشرعان الفرنسي والجزائري، يشترطان أن يكون الدخول "موصوفا بالغش frauduleusement" وفي هذا الصدد يرى أغلب الفقهاء أن المقصود يتمثل في " عدم حصول الجاني على ترخيص محدد ومن الجهة المختصة التي لها السلطة والمسؤولية على المنظومة الرقمية ومعطياتها، و بالتالي ليس من صلاحياته وحقه القيام بذلك[2].

إلى أين يدخل ؟ يكمن محل الدخول حسب المشرعان الفرنسي و الجزائري، في كل أو جزء من منظومة المعالجة الآلية للمعطيات. حيث يؤخذ على المشرعين الفرنسي و الجزائري أنهما لم يعرفا منظومة المعالجة الآلية للمعطيات من جهة، [3] ولم يحددا من جهة أخرى مضمونها الدقيق، هل يضم شبكة الاتصال الدولية أيضا على جهاز الإعلام الآلي فقط[4].

الدخول غير مصرح به يستمد عدم مشروعيته من كونه غير مصرح به وتم دون رضاء من صاحب هذا النظام أو رغما عنه. سواء كان الدخول لكل النظام أو جزء منه فقط، وفي كلتا الحالتين نكون بصدد دخول معنوي لا يتم بالطرق التقليدية.[5]

---

[1]– حيث تقوم المسؤولية الجنائية للشخص المعنوي بخصوص جريمة الخول وحتى البقاء وباقي الجرائم المدروسة إذا ما توافرت شروط معينة، خاصة شرط نص حاص يقر ذلك، الأمر الذي أكد عليه المشرع الفرنسي في المادة 323 –6 من قانون العقوبات، و في المادة 394 مكرر 4 من قانون العقوبات.

[2]– نسيم دردور، (جرائم المعلوماتية على ضوء القانون الجزائري والمقارن)، مذكرة لنيل شهادة الماجيستير في القانون الجنائي، كلية الحقوق، جامعة متنوري – قسنطينة، الجزائر، 2013، 27.

[3]– المرجع نفسه، ص 16.

[4]– المرجع نفسه، ص 18.

[5]– أسامة أحمد الناعسة، جلال الزعبي، صايل فاضل الهواوشة جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، الأردن، ص 231.

ونجد أن المشرع الجزائري أسوة بالمشرع الفرنسي، قد صاغ النص بطريقة تشمل جميع طرق الدخول الممكنة، دون تحديد طريقة أو وسيلة بعينها. مما يمكن من مواجهة جميع إشكال الاختراق غير المشروع للنظم المعلوماتية.

عدم التصريح بالدخول: التصريح بالدخول يثير مسألتين هامتين، هما: من المسئول عن التصريح، وما هي حدود هذا التصريح وحالاته ؟بخصوص الأولى، فإن التصريح يجب أن يمنحه الشخص المسئول أو المسيطر أو المالك لتنظيم النظام المعلوماتي. وإن كان للنظام أكثر من مسئول واحد، فهنا يكون لكل منهم الحق في منح التصريح. لذا فالجريمة التي نحن بصدد دراستها، تقوم في الحالة التي لا يكون هناك فيها تصريح بالدخول، أو أن يوجد تصريح بالدخول ولكن المصرح له يقوم بتجاوز الحدود التي له في هذا التصريح. سواء من حيث الوقت المخصص له أو من حيث تجاوز الغرض الذي لأجله منح الترخيص[1].

ما هي طبيعة فعل الدخول؟ هو سلوك وقتي شكلي لا يتطلب النتيجة إيجابي حيث يقوم الجاني بعمل وقد يكون بالاتصال المباشر أو غير مباشر[2].

أ-2- فعل البقاء: "البقاء هو التواجد داخل المنظومة المعلوماتية ضد إرادة من له الحق في السيطرة عليه "[3].

أو يقصد بفعل البقاء غير المشروع داخل النظام المعلوماتي هو التواجد داخل هذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له السيطرة عليه.[4]

---

[1]- حمودي ناصر، ، ص

[2]- يتحقق المباشر بوجود الجاني أمام جهاز الإعلام الآلي، أما غير المباشر فيكون عبر شبكة الاتصال الدولية عن بعد.

[3]- هيام حاجب، (الجريمة المعلوماتية)، مذكرة التحرج لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر، 2008، ص 50.

[4]- حجازي عبد الفتاح، مرجع سابق، ص 235.

ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء داخل النظام وعدم قطع الاتصال به.

فالركن المادي في هذه الحالة لا يتمثل في إقامة الاتصال مع النظام، فالفرض هنا أن هذا الاتصال لم يقصده ولم يرده الجاني[1]. ويمكن تصور ذلك في الحالة التي يكون فيها الشخص في سبيله للدخول إلى نظام معلوماتي له الحق في الدخول إليه. إلا أنه يجد نفسه ولسبب ما مثل استخدام الشيفرة خاطئة مثلا- داخل نظام آخر اعتبر جريمة البقاء غير المشروع داخل النظام المعلوماتي بشكل عام من التي يصعب تقديم دليل على إثباتها، حيث يزعم المتهم في حالة القبض عليه أنه كان على وشك الانفصال عن النظام المعتدى عليه[2].

ومما لاشك فيه أن البقاء داخل نظام الكومبيوتر بعد دخوله عن طريق الخطأ، لا يختلف عن الدخول غير مصرح به من حيث وجوب التجريم. فاتحاه إرادة الفاعل إلى البقاء داحل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف لا يختلف في جوهره عن الدخول غير مصرح به إلى نظام الكومبيوتر.

فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى نظام غير مصرح للدخول إليه، فالمصلة التي يحميها القانون هي حماية نظام الكومبيوتر في الحالتين[3].

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى نظام معلوماتي ويدخل إليه فعلا ضد إرادة من له

---

[1]- الحسيني، عمر الفاروق، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1995، ص 105.

[2]- الشوا سامي، مرجع سابق، ص 210.

[3]- نائلة عادل محمد فريد قورة، مرجع سابق، ص 346.

حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق هذا الفرد بالاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[1].

والإشكالية التي تثور في هذا الصدد: متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء ؟

ذهب رأي من الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، ويبقى مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي بانتهاء حالة البقاء.

ويذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه أن بقاءه داخل النظام غير مشروع.

بينما يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة الي يبدأ فيها الجاني التجول داحل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول إلى النظام أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[2].

صور فعل البقاء: لفعل البقاء العديد من الصور، حيث فد يرتكب الجاني جريمة الدخول غير الشرعي ومن ثمة يبقى ولا يغادر النظام فنكون أمام جريمة الدخول والبقاء معا، وقد يدخل سهوا، ودون قصد ثم يتفطن أنه في منظومة معلوماتية دون ترخيص إلا أنه يبقى ولا يغادر، فنكون أمام

[1]– علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكومبيوتر، المكتبة القانونية، القاهرة 1999، ص 123.

[2]– خثير مسعود، مرجع سابق، ص 117.

جريمة بقاء فقط دون دخول، يدخل الشخص بالخطأ ويبقى بالخطأ مما ينفي الجريمة تماما، كما قد يكون له الحق في الدخول والبقاء لمدة معينة إلا أنه يتجاوزها.[1]

الطبيعة القانونية لفعل البقاء: تعد هذه الجريمة من الجرائم الشكلية التي لا يشترط فيها حدوث نتيجة جرمية معينة، فيكفي البقاء غير المصرح به داخل النظام المعلوماتي ليقوم الركن المادي لهذه الجريمة[2].

جريمة البقاء غير المشروع داخل النظام المعلوماتي من الجرائم المستمرة.[3] وذلك نظرا لاستمرار الاعتداء على المصلحة التي يحميها القانون طالما استمر البقاء غير مصرح به داخل النظام.

يجدر الإشارة إلى أن جريمة البقاء غير المصرح به داخل نظام المعلوماتي جريمة عمدية لا يتطلب النتيجة –حيث يمتنع الجاني عن فعل –، وقد يكون بالاتصال المباشر أو غير مباشر – كما سبق بيانه.

ونشير في هذا المجال إلى ما نصت عليه اتفاقية بودابست لمكافحة الاجرام المعلوماتي في المادة الثانية منها. حيث جاء فيها (يجب على كل طرف في الاتفاقية ان يتبنى الاجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبار جريمة جنائية الولوج العمدي لكل أو جزء من جهاز الحاسوب دون حق، كما يمكن أن تشترط التشريعات أن ترتكب الجريمة من خلال انتهاك اجراءات الأمن). [4]

ب– الركن المعنوي: تتطلب جريمة الدخول و/أو البقاء الشكلي توفر القصد الجنائي العام، حيث اكتفى المشرع الجزائري والفرنسي بلفظة "الغش" التي تدل بطريقة مباشرة على توفره

[1]– هيام، حاجب ، مرجع سابق، ص ص 50 – 51.

[2]– نهلا عبد القادر المومني، مرجع سابق، ص 161.

[3]– الجريمة المستمرة هي "الجرمية التي يتكون ركنها المادي من تصرف أو حالة تحتمل بطبيعتها الاستمرار لفترة زمنية غير محددة من الوقت. صالح، نائل عبد الرحمان، محاضرات في قانون العقوبات الأردني، (القسم العام)، الطبعة الأولى، دار الفكر للطباعة والنشر، عمان، 1995، ص 46.

[4]– أحمد هلالي عبد اللاه، مرجع سابق، ص 68.

– القصد الجنائي –لكون الغش يتطلب القصد. إلا أن القصد العام في حد ذاته يختلف من صورة لأخرى، ففي جريمة الدخول يجب أن يعلم الجاني أنه بصدد الدخول بطريقة غير شرعية في نظام معلوماتي ومع ذلك يريد القيام بالفعل، دون الرغبة في تحقيق نتيجة معينة، وأما في حالة جريمة الدخول والبقاء، فتضاف رغبة البقاء والعلم بعدم مشروعية ذلك، وأخيرا في حالة جريمة البقاء فقط فيعلم الجاني أنه بصدد التواجد في نظام معلوماتي بصورة غير شرعية ومع ذلك يتواصل بالبقاء فيه.[1]

1-3- الصورة المشددة لجريمة الدخول إلى النظام أو البقاء فيه (العقوبة الجنائية)

نص المادة 394 مكرر قانون العقوبات[2]: "يعاقب بالحبس من ثلاثة أشهر (3) إلى سنة (1) وبغرامة مالية من (50.000 دج إلى 100.000 دج) كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.[3]

2- الدخول و/أو البقاء في منظومة معلوماتية كجريمة مادية

قد تتحول طبيعة الدحول و/أو البقاء غير مشروع، من جريمة شكلية إلى مادية تتطلب تحقيق النتيجة، الأمر المعتمد في القانون العقوبات الفرنسي في المادة 323-2/1 والمادة 394 مكرر 3/2 قانون العقوبات الجزائري.[4]

1- تعريف الجريمة: انطلاقا من التعريف المذكور سابقا، المتصل بالدخول و/ أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات كجريمة شكلية، وما جاء في المواد المذكورة أعلاه، يمكن أن نصل إلى تعريف بخصوص الجريمة المقصودة ونقول أنها: "قيام شخص

[1]- بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة)، رسالة لنيل الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2013، ص ص 33-34.

[2]- الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[3]- المشرع الجزائري أخذ بالحل الأوسط، فلم يشدد ولم يتساهل، مع إعماله لمبدأ مرونة العقوبة دون الخيار بينهما.

70- أمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق.

بالدخول و/ أو البقاء في منظومة معلوماتية بالمفهوم الواسع، باستعماله لآليات وهذا دون وجه حق.

2- أركان الجريمة: تتفق الجريمة المعلوماتية المقصودة مع سابقتها، من حيث الأركان المذكورة سابقا، إلا تزيد عنها من حيث النتيجة الإجرامية والركن المعنوي في بعض أحكامه.

أ-النتيجة الإجرامية: عمل المشرع على حماية المعلومات بمفهومها الواسع عن طرق تجريم النتائج التالية:

أ/1-المساس بالمعطيات المعلوماتية: تنطوي النتيجة الإجرامية في هذه الحالة، على المساس بالمعطيات المعلوماتية الموجودة في النظام المعلوماتي، الذي قام بمعالجتها.

باستقراء المواد المذكورة أعلاه نجد أن المشرع الفرنسي اقتصر على حماية المعطيات دون البيانات، التي حماها من الحذف والتعديل، الأمر الذي تبعه نظيره الجزائري إلا أنه عبر عنها "بمعطيات المنظومة " التي قد تدل على معطيات تشغيل المنظومة أو المعطيات التي تحتويها كما قد تقيدهما معا[1].

أ-2- المساس بالمنظومة المعلوماتية: تنطوي النتيجة الإجرامية في هذه الحالة، على المساس بالمنظومة المعلوماتية بمفهومها الواسع.

حيث باستقراء المواد المذكورة أعلاه نجد أن المشرع قد قرر حماية المنظومة المعلوماتية من " التوقيف والتعطيل "كنتيجة للدخول / أو البقاء، وعبر عنه بمصطلح:" Altération" المنطوي على " الاضطراب أو الضعف "، الذي يؤدي بالضرورة إلى التوقيف أو التعطيل. أما المشرع الجزائري فعبر عن ذلك:

[1]- راجع المادة 394 مكرر 2 من الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

بمصطلح المتمثل في " التخريب " الأمر الذي يدفع للقول، أن تعطيل المنظومة نسبيا دون تحريبها لا يعد جريمة وفق التفسير الحرفي لمصطلح التخريب[1].

ب- الركن المعنوي: الدخول /أو البقاء في المنظومة المعلوماتية كجريمة مادية ، يتطلب القصد العام بعنصريه العلم والإرادة، حيث اكد المشرع الفرنسي والجزائري بتعبير غامض على تحقيق نتيجة لكن لم يبينا هل يريدها الجاني أم لا، إلا أنه تطلب الدخول والبقاء الشكلي القصد الجنائي، نقول أن تحولها إلى جريمة مادية يقود بالضرورة إلى تطلبه القصد الجنائي.[2]

3- العقوبة الجنائية: اعمل المشرع على تشديد العقوبة الأصلية، فرفع العقوبة المشرع الفرنسي الحبس إلى 3 سنوات والغرامة إلى 45.000 أورو، أما نظيره الجزائري فقرر مضاعفة العقوبة في حالة المساس بالمعطيات، لتصبح من 6 أشهر إلي 2 سنة وغرامة مالية من 100.000 دج إلى 200.00 دج، وعقوبة الحبس المضاعفة نفسها عند المساس بأنظمة المعلومات وغرامة من 50.000 إلى 150.000دج [3].

---

[1]- راجع المادة 394 مكرر 3 من الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[2]- إلا أنه يرى جانب من الفقه، أن جريمة الدخول و / أو البقاء المادي تقدم سواء بتوفر القصد الجنائي أو بتخلفه، فالمهم تحقق النتيجة الجرمية المحددة سواء أرادها الجاني أم لا، - عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، ليبيا، اكتوبر، 2009، ص 27.

[3]- يلاحظ، أن المشرع الفرنسي، شدد العقوبة مع حفاظه على نهج عدم إعمال مبدأ مرونة العقوبة، أما نظيره الجزائري، فمن جهة واصل إعماله لمبدأ المرونة وعدم الخيار بين الحبس والغرامة، ومن جهة أخرى عقد الأمور، حيث فرق بين المساس بالمعطيات والمساس بالأنظمة، إلا أنه أقر لهما نفس العقوبة السالبة للحرية وتكاد تكون نفسها بخصوص الغرامة، ما يدفع للتساؤل عن جدوى معالجتها في فقرتين بدل فقرة واحدة.

الفرع الثاني: الصور المشددة لجرائم المعالجة الآلية للمعطيات

سأتعرض في هذا الفرع إلى جريمة الاعتداء القصدي على النظام وجريمة الاعتداء القصدي للمعطيات لبيان أهم الطرق وصور الاعتداء على هذا النظام والمعطيات والتي من شأنها تعطيل وعرقلة سير هذا النظام والمعطيات وإفسادهما.

أولا: جريمة الاعتداء القصدي على النظام

لم يتعرض المشرع الجزائري لهذه الجريمة، بل اكتفى بالنص على جريمة الاعتداء على المعطيات فقط بخلاف المشرع الفرنسي حيث نص عليها بموجب نص المادة 2/323 القانون الفرنسي: " يعاقب كل من عطل أو أفسد نشاط أو وظائف المعالجة الآلية للمعطيات بالحبس حتى ثلاث سنوات وبالغرامة حتى ثلاثمائة ألف فرنك ".

من خلال استقراء نص المادة نجد أنها قد نصت على السلوك الاجرامي لهذه الجريمة، والذي يتحذ إحدى الصورتين إما "التعطيل أو الإفساد "وبذلك فالهدف الأساسي من هذا النص هو التعرض لكل محاولة لإعاقة أو تحريف قد تلحق بهذا النظام.

ولذلك فإنه لتحقيق هذه الجريمة يجب توافر الركن المادي والركن المعنوي.

أ – الركن المادي: يتمثل الركن المادي إما في فعل التوقيف أو تعطيل نظام المعالجة الآلية للمعطيات عن أداء نشاطه، وإما في فعل إفساد نشاط أو وظائف هذا النظام.[1]

ولا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية (جهاز الكومبيوتر نفسه، شبكات الاتصال، أجهزة النقل، ...) أم المعنوية (البرامج والمعطيات، ...).

أ–1– التعطيل أو التوقيف: تعتبر عملية إعاقة سير عمل نظام المعالجة الآلية للمعطيات بأنها "فعل يتسبب في تباطء أو ارتكاب عمل نظام المعالجة، ومن ثم ينتج عن ذلك تغيير في حالة

[1]– علي عبد القادر قهوجي، مرجع سابق، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص 139.

عمل النظام. وهذا الارتباك الناجم عن الإعاقة تتأثر به أجهزة الكمبيوتر والبرامج على سواء"[1].

ويحصل فعل التعطيل أو التوقيف بأي وسيلة كانت، فالمشرع لم يشترط وسيلة معينة، وبالتالي فيستوي أن يكون وسيلة مادية أو معنوية. ومن أمثلة وسائل التعطيل المادية استعمال العنف لمنع الوصول إلى الأجهزة "ككسرها، او تحطيمها او تحطيم أسطوانة..... " أما التعطيل بوسيلة معنوية، فقد تتحقق بإدخال فيروس على البرنامج، أو تعديل كلمة السر، أو كيفية أداء النظام لوظيفته، بوسيلة تؤدي إلى أن يباطئ في أدائه لوظيفته المعلوماتية داخل النظام المعلوماتي. [2]

أ-2- الإفساد أو التعييب: ويقصد بالتعييب أو الإفساد كل فعل وإن كان لا يعطل نظام معالجة البيانات لكنه يجعل هذا النظام غير قادر على الاستعمال السليم، وذلك بأن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها.

ويذهب جانب من الفقه إلى أن الإفساد من هذه الزاوية يقترب من التعييب الذي صادفناه عند دراسة الظرف المشدد لجريمة الدخول و / أو البقاء غير المشروع، ولعل الفارق بينهما يكمن فقط في أن الإفساد في حال الظرف المشدد لا يشترط فيه أن يكون قصديا، بينما يتطلب فيه هذا الشرط بالنسبة لجريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات.

وتتنوع وسائل التعييب والإفساد كاستخدام القنبلة المعلوماتية، بحيث يدخل من خلالها مجموعة من المعطيات تتكاثر داخل النظام بحيث غير صالح للاستعمال[3].

---

[1]- يونس عرب، جرائم الكومبيوتر و الأنترنت، ورقة عمل مقدمة إلى الأمن العربي، 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية.

[2]- علي عبد القادر قهوجي، مرجع سابق، ص 139

[3]- يونس عرب، مرجع سابق، ص 20.

ب-الركن المعنوي: جريمة الاعتداء القصدي على نظام المعالجة الآلية للمعطيات جريمة عمدية بحيث يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة. على اعتبار أن تتجه إرادة الجاني إلى فعل الإفساد مع علمه بأن نشاطه الجرمي من شأنه أن يوصله إلى تلك النتيجة.

فإذا قام شخص يتعامل مع النظام بصورة مشروعة بإعاقة أو إفساد النظام نتيجة لخطأ في التشغيل أو التعامل مع البيانات ينتفي القصد الجنائي لديه، ولا يسأل عن هذه الجريمة.[1]

ثانيا: جريمة الاعتداء القصدي على المعطيات

نص المشروع الجزائري في المادة 394 مكرر2 ق ع[2]: "يعاقب بالحبس مدة ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000دج الى 2.000.000دج، كل من ادخل بطريقة الغش معطيات نضام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

يتضح من خلال النص أعلاه أنه حتى تقوم الجريمة لابد من توافر ركنيها المادي و المعنوي.

1-الركن المادي.

النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل، ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها، ومن ثما يقام الركن المادي في الجريمة، لكن القاسم المشترك في هذه الأفعال جميعا هو انطوائها على تلاعب في المعطيات التي يتضمنها نضام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر قائمة[3].

[1]- عبد الفتاح بيومي، نظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، ص 43.

[2]- الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[3]- علي عبد القادر قهوجي، مرجع سابق، المكتبة القانونية، 1999، ص 143.

ومن هنا يمكن القول ان النشاط الإجرامي لهذه الجريمة انما ينصب على المعطيات أي المعلومات المعالجة آليا والتي أصبحت رموزا وإشارات وليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام والتي تشكل جزءا منه، وبناء عليه

فالجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها، أم ا المعلومات غير المعالجة التي لم تدخل إلى النظام فهي خارج نطاق الحماية الشمولية بهذا النص كان يجوز حمايتها وفقا لنصوص جنائية أخرى[1].

ونبين فيما يلي المقصود بالأفعال المكونة لهذه الجريمة والتي أشرنا لها سابقا مع العلم أنه لا يشترط لقيامها توافر كل هذه الأفعال، بل يكفي لقيامها توافر واحد منها.

أ-فعل الإدخال: ويقصد بذلك إدخال بيانات في نظام المعالجة لم تكن موجودة من قبل، وقد يتم إدخال هذه البيانات بقصد التشويش على صحة البيانات القائمة، ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولا سيما في المنشآت ذات الأموال، حيث يعد المسؤول في القسم المعلوماتي في أفضل وضع يؤهله لارتكاب هذا النمط غير المشروع من التلاعب. [2]

ب-فعل المحو: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة، والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

ج-فعل التعديل: ويقصد بهذا الفعل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويتحقق هذا الفعل عن طرق برامج غريبة تتلاعب في المعطيات سواء

[1]- عبد الفتاح بيومي حجازي، مرجع سابق، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، ص 43.

[2]- نبيل صقر جرائم الإلكتروني والأنترنت، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الجزائر، 2005، ص141.

بمحوها كليا او جزئيا أو بتعديلها. وذلك كاستخدام القنابل المعلوماتية الخاصة بالمعطيات، برنامج الممحاة، أو برنامج الفيروسات بصفة عامة[1].

2-الركن المعنوي:

تتحقق هذه الجريمة بمجرد توافر النية الجرمية بكافة عناصرها (العلم و الإرادة) وبالتالي يكفي أن يعلم الجاني أنه يقوم بأحد الأفعال السابقة " الإدخال، التعديل، المحو "أو فعل منها مع إرادته للقيام بهذا الفعل تقوم الجريمة، وبالتالي لا يشترط لقيامها توافر نية الإضرار بالشخص مالك البرنامج او صاحب النظام، وإن كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا أنه ليس عنصر في الجريمة[2].

[1]- عبد الفتاح بيومي حجازي، مرجع سابق، ص 49.

[2]- نبيل صقر، مرجع سابق، ص ص 65 – 66.

المبحث الثاني

الجزاءات والعقوبات المقررة لجرائم المعالجة الآلية للمعطيات

إن الجزاءات والعقوبات المقررة لجرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات. لقد نصت المادة 03 من الاتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبات المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية، كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ له مساءلة الشخص المعنوي الوارد في المادة 07 من نفس الاتفاقية .وباستمرار نصوص المواد الخاصة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات الجزائري، من المادة 394 مكرر إلى غاية المادة 394 مكرر 2 من قانون العقوبات نجد أن المشرع الجزائري قد تبنى هذا المبدأ في تقريره للجزاءات الواجبة على هذا

النوع من الجرائم فسن عقوبات تطبق على الشخص الطبيعي عقوبات التي تطبق على الشخص المعنوي وذلك ما سنتناوله فيما يلي[1].

المطلب الأول

العقوبات المطبقة على الشخص الطبيعي

الفرع الأول :العقوبات الأصلية المطبق على جريمة من جرائم المعالجة الآلية للمعطيات

من خلال استقراء هذه النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذا نجد سلم خطورة يتضمن ثالثة درجات، جريمة الدخول أو

[1]– الدزيري هيبة، جريمة الدخول غير المشروع لنظام المعالجة الالية للمعطيات، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، قسم القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم 20–06–2020، ص 65.

البقاء بالغش في الدرجة الأولى، وبعدها الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات[1].

أولا: جريمة الدخول والبقاء

تعتبر هذه الجريمة من أهم الجرائم الالكترونية وأخرطها على المؤسسات والأفراد لكونها تشكل انتهاكا صارخا ومباشرة للحقوق والحريات ويختلف الفقه في طبيعة هذه الجريمة بين من يقسمها الى يعتبرها جريمة واحدة تؤدي نفس النتيجة وبين من يقسمها إلى جريمتين بحيث يفضل رواد هذا المذهب بين الدخول إلى النظام المعلوماتي كجريمة أولى البقاء غير المشروع في النظام كجريمة ثانية.

ويقصد بجريمة الدخول إلى الأنظمة المعالجة الآلية للمعطيات تحقيق فعل الدخول إلى النظام وتشير الكلمة إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والسيطرة على المعطيات أو المعلومات التي يتكون منها، كما يقصد به الدخول إلى محتويات جهاز الكمبيوتر والقيام بأي عملية اتصال بالنظام محل الحماية بدون أي ترخيص أو وجه حق"[2].

أما جريمة البقاء غير مشروع داخل النظام المعلوماتي فتعتبر من الجرائم المستمرة وتبقا القائمة مستوفية اركانها مدام الجاني لا يزال على اتصال بنظام المعلومات التي تم الدخول إليه بطريقة غير مشروعة ودون ترخيص.

ويقصد بالبقاء **كفعل" التواجد داخل نظام المعالجة الألية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام والتصرف فيه"**[3] وستقر أغلب الفقه على أن الجريمة البقاء غير المشروع داخل النظام المعلوماتي تعتبر بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها وكثيرا ما تقترن الجريمتان (أي الدخول غير المشروع والبقاء غير مشروع) ببعضهما

[1]– أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر، سنة 2007،

[2]– لتفاصيل حول هذه الجزئية راجع نهلا عبد القادر المومني، مرجع سابق، ص 158.

[3]– أمال قارة، مرجع سابق، ص 110.

البعض وهو الأمر الذي جعل الكثير من الفقه المقارن وأغلب التشريعات الجنائية تجمع الصورتين في جريمة واحدة تحت مسمى

الدخول والبقاء غير المشروع في النظام المعلوماتي، وقد قرر المشرع في إطار قانون العقوبات وبموجب المادة 394مكرر عقوبتين اصليتين لجريمة الدخول أو البقاء غير المشروع:

1-العقوبة المقررة للجريمة في صورتها البسيطة: يعاقب القانون على هذه الجريمة في صورتها البسيطة بحبس من ثلاثة اشهر إلى سنة وبغرامة مالية من خمسين ألف دينار (50.000) إلى مائة

ألف دينار (100.000) وفتح هذا المجال للقاضي السلطة التقديرية بأن جعل له حدا أقصى في تقدير العقوبة بالعودة إلى الحيثيات والوقائع، وبالنضر للباعث الذي دفع الشخص لارتكاب الجريمة

2-العقوبة للجريمة في صورتها المشددة: تضاعف عقوبة الجريمة إذا ترتب عنها حذف أو تغيير في المعطيات، بحد أدنى يقدر بستة أشهر بعدما كان ثلاثة اشهر، وحد أقصى يقدر بسنتين بعدما كان سنة واحدة، ويعاقب على هذه الصورة بغرامة مالية تقدر مئة ألف (100.000) دينار إلى مئتين ألف (200.000) دينار وفي حال ما تم القيام بتخريب نظام المعالجة الألية فيعاقب عليها بالحبس من ستة أشهر إلى سنتين وبغرامة من خمسين ألف (50.00) دينار إلى مئة وخمسون ألف (150.000) دينار[1].

[1]- دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 13 جانفي 2020، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين سطيف 2020، ص 146.

ثانيا: جريمة التلاعب بالمعطيات

نصت عليها المادة 394 مكرر 1، قانون العقوبات الجزائري. بالحبس من 06 اشهر الى 03 سنوات وعقوبة الغرامة التي تتراوح من 500.000 دج إلى 2.000.000 دج.

والملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لأن في صورتها البسيطة لا تؤدي إلى أضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلي نفس النتائج التي تؤدي إليها جريمة التلاعب بالمعطيات وهي ازالة المعطيات أو تعديلها، فإن العقوبة المقررة لجريمة التلاعب تبقى أكبر لأنها جريمة عمدية يتوافر لدى مرتكبها القصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة [1].

ثالثا: جريمة التعامل في معطيات غير مشروعة

تعاقب المادة 394 مكرر 7 من ق. ع. ج. على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من شهرين إلى 3 سنوات وبغرامة مالية من 1000000 دج إلى 5000000 دج.

بهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات (غير أن حدها الأدنى يقل عن كلتا الجريمتين).

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول او البقاء في صورتيها (سنة أو سنتين) وستساوى مع الحد الأقصى لجريمة التلاعب بالمعطيات (03 سنوات).

[1]– نايلة عادل محمد فريد قورة، مرجع سابق، ص 228.

غير أن حدها الأدنى يقل عن الجريمتين معا، ألنه في جريمة الدخول أو البقاء البسيطة 03 أشهر وفي هذه الجريمة في صورتيها المشددة وفي جريمة التلاعب هو 06 أشهر[1].

الفرع الثاني: العقوبات التكميلية

نصت المادة 394 مكررة من قانون العقوبات الجزائري[2] على العقوبات التكميلية، التي يمكن الحكم بها إلى جانب العقوبات الأصلية وجاء فيها مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محال لجريمة من الجرائم المعاقب عليها في هذا القسم، علاوة على إغلاق المحل أو مكان الاستعمال إذا كانت الجريمة قد ارتكبت بعلم مالكها ويستخلص من نص هذه المادة العقوبات التكميلية التالية:

أولا: مصادرة الأجهزة والوسائل والبرامج المستخدمة

وذلك مع الاحتفاظ بحقو ق الغير حسن النية، وتجدر الإشارة إلى أن المشرع نص فقط على مصادرة الأجهزة والبرامج والوسائل المستخدمة فقط، وأغفل مصادرة الوسائل الموجهة لارتكاب الجريمة من المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في الفقرة الأولى من المادة 394 مكرر 2 قانون عقوبات جزائري، حيث أن عبارة المستخدمة الواردة في نص المادة 394 مكرر 6 الخاصة بالعقوبات التكميلية تفيد صيغة الماضي وهذا ما نصت عليه المادة 394 مكرر6 من قانون عقوبات جزائري التي تنص على العقوبات التكميلية، وفي فقرتها الثالثة على المصادرة فنجد أنها تناولت مصادرة الشيء الذي كان موجها للقيام

[1]– الدزيري هبة، مرجع سابق، ص 67.

[2]– أمر 66–156، المتضمن قانون العقوبات، مرجع سابق.

ثانيا: اغلاق المواقع التي تكون محال للجريمة من جرائم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات[1].

ثالثا: اغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها واضاف المشرع شرط علم المالك إذا كان على سبيل المثال الجاني مستأجرا للمحل المالك مؤجر له، ويعلم خطورة الأفعال التي يقوم بها الجاني، كغلق نادي الأنترنت الذي ترتكب فيه هذه الجرائم مع علم مالك أو مسير النادي بالأفعال الخطيرة التي يقوم بها زبونه، ولكن المشرع لم يحدد المدة القصوى لغلق المحل أو مكان الاستغلال، مما يطرح مشكلا في تنفيذ هذه العقوبة فمن جهة يعتبر إغلاق المحل أو أماكن كعقوبة تكميلية للشخص الطبيعي المسؤول جزائيا، ومن جهة أخرى لا يمكننا الرجوع الى القواعد العامة للمسؤولية الجزائية للشخص المعنوي لتحديد المدى المدة، لأنه في هذه الحالة تقع المسؤولية الجزائية على عاتق الشخص الطبيعي فيوجد حسب راينا في توقيع الجزاء، حيث تم توقيع جزاء خاص بالشخص المعنوي غلق المحل على الشخص الطبيعي.

– إن العقوبة التكميلية الواردة في المادة 394 مكرر 01، ق. ع. ج.[2] غير كافية في مواجهة الحالات العديدة التي يمكن أن يرتكبها الشخص الطبيعي فمثلا تنص المادة على العقوبة التكميلية الخاصة بالموظف العمومي المصرح له بالدخول على نظام الآلية المعطيات لكنه يبتعد ذلك إلى ارتكاب جرائم اخرى متعلقة بالمنظومة المعالجة أليا، وكذلك الشيء بالنسبة للوظيفة المهنية فيما يخص المحامين أو الأطباء مثلا، وكذلك الوظيفة الاجتماعية إذا ارتكبت الجريمة عند تأدية الوظيفة أو بمناسبتها وهذا ما جاءت به احكام المادة23 3– 05 من قانون العقوبات الفرنسي والتي نصت على تكميلية أخرى، تدعوا المشرع الجزائري الى الأخذ بها وهي كما يلي:

– المنع لمدة أقصاها 5 سنوات من الحقوق المدنية والسياسية

[1]– اذلدزيري هبة، مرجع سابق، ص 68.

[2]– أمر 66–156، المتضمن قانون العقوبات، مرجع سابق..

– المنع لمدة أقصاها 5 سنوات من ممارسة الوظيفة العمومية أو النشاط المهني أو الاجتماعي إذا ارتكبت الجريمة اثناء تأدية الوظيفة او بمناسبتها.

– مصادرة الشيء الذي استخدم أو الموجه الارتكاب الجريمة او الشيء محل الجريمة الغلق لمدة أقصاها 5 سنوات للمؤسسات، أو لحد أو عدة مؤسسات المقاولة التي استعملت في ارتكابها الأفعال المجرمة.

– الحرمان لمدة أقصاها 2 سنوات من الصفقات العمومية.

– المنع لمدة اقصاها خمس سنوات في اصدار الشيكات، بما فيها التي تسمح سحب الأموال من طرف الساحب لدى المسحوب له أو المرخص أو المرخص لهم بذلك. تقليل أو نشر الحكم أو القرار الصادر[1].

الفرع الثالث: العقوبات المشددة

نصت المادة 394 مكرر2 و مكرر3 [2] على ظرف التشديد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما واما تخريب نظام اشتغال المنظومة.

حذف أو تغيير المعطيات التي يحتويها النظام في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر[3] وفي الحالة الثانية تكون العقوبة بالحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 200.000 دج.

هذا الظرف المشدد هو طرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافر. نصت المادة 394 مكرر

[1]–الدزيري هبة، مرجع سابق، ص 70.

[2]–أنظر نص المادة 394 مكرر 2 ومكرر 3 من الأمر 66–156 المتضمن قانون العقوبات.

[3]–أنظر المادة المادة 394 مكرر من الأمر 66–156 المتضمن قانون العقوبات، مرجع سابق.

3 [1]، على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام[2].

المطلب الثاني

العقوبات المطبقة على الشخص المعنوي

لقد كانت العقوبة إحدى أهم الحجج التي استند إليها المعارضون لمبدأ إقرار مسؤولية الشخص المعنوي حيث رأوا أنه لا يمكن تطبيقها على هذا الأخير خاصة تلك العقوبات السالبة والمقيدة للحرية، لكن وبعد اتساع تطبيق عقوبة الغرامة وابتكار عقوبات جديدة تتلاءم وطبيعة الشخص المعنوي لم لهذا الاعتراض محل، ولقد تضمنت المادة 18 مكرر من قانون العقوبات الجزائري بعد تعدليه سنة2004، انواع العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح، وأول هذه العقوبات في الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى المقررة على الشخص الطبيعي، لكن المادة 394 مكرر 4، فهي غرامة ذات حد واحد أو الأخذ بالحد الأقصى لهذه العقوبات، وهو خمس مرات فيما يتعلق بجرائم المعطيات[3].

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنوية بموجب القانون 04-15 في نص المادة 18 مكرر ليعزز ذلك بالقانون رقم 23 لسنة 2006 بنص المادة 51 مكرر وفي مضمون هذا النص استثنى المشرع الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة، ومن خلال استقراء المادة م 18 كرر فالعقوبات التي تطبق على الشخص المعنوي في الجنايات والجنح كالتالي:

---

[1]-ن المادة 394 مكرر 3 من الأمر 66-156 المتضمن قانون العقوبات، مرجع سابق.

[2]-جدي نسيمة، جرائم المساس بالأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر 2016-2017، ص ص 127-128.

[3]- الدزيري هبة، مرجع سابق، ص 71.

1- الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص 1 الطبيعي في القانون الذي يعاقب على الجريمة[1].

2- واحدة أو أكثر من العقوبات التكميلية الآتية: حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات، الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات ال، منع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس سنوات، مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها، نشر وتعليق حكم الإدانة، الوضع تحت التصرف لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى جريمة أو الذي ارتكبت الجريمة بمناسبته .ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد من 394 مكرر وما بعدها فإن الغرامة المطابقة على هذا الأخير هي 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك تطبيقا للمادة 394 مكرر 4 من قانون العقوبات الجزائري [2].

حيث أن المشرع الجزائري شدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية وهي الطائفة التي تنتمي إليها جل جرائم الدراسة، إذ نصت المادة 394 مكرر 4 بمضاعفة قيمة الغرامة 5 أضعاف ما قررته للشخص الطبيعي ونصت على الآتي: ..." بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. "أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في

[1]- نص المشرع الجزائري على نوعين من العقوبات المطبقة على الشخص المعنوي هي الغرامة كعقوبة أصلية والعقوبات التكميلية.

[2]- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية أطروحة مقدمة لنيل شهادة الدكتوراه في علوم القانون، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان 2017-2018، ص ص 284-249.

التشريع الجزائري مرتين، إذ تضاعف إلى خمس 5 مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشر 10 أضعاف عما هو مقرر على الشخص العادي[1].

الفرع الثاني: عقوبة جريمة الاتفاق و الشروع الجنائي

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي[2] بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار، حيث تنص المادة 394 مكرر 5 من قانون العقوبات:" كل من شارك في مجموعة أوفي اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة بالجريمة ذاتها .

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أوفي اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص .ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلاصها من نص المادة 394 مكرر 5 من قانون العقوبات والتي هي، مجموعة أو اتفاق، بهدف تحضير جريمة من الجرائم الماسة

[1]– رابحي عزيزة، مرجع سابق، ص 249.

[2]– نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي.

بالأنظمة المعلوماتية، تجسيد هذا التحضير بفعل مادي، مع فعل المشاركة في هذا الاتفاق، إضافة إلى القصد الجنائي، وبالنسبة للمجموعة أو الاتفاق، يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي كما يستوي. أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الأخر من قبل ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي، المهم أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر .

وتكاثف الجهود لا يكفي بل يجب أن يكون بهذه تحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه فإنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات فالجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

والتحضير لا يكفي بل يتم تجسيده بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور أو رمز الدخول وغيرها ففعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر 5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي ل ب يجب توافر فعل إيجابي للمشاركة، توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة كل عضو أي تحقيق نشاط إجرامي معين وهو العمل التحضير بينما عن عقوبة الشروع في الجريمة

فالشروع يراد به في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة كانت لتقع بالفعل لولا تدخل عامل خارج عن إرادة الفاعل في اللحظة الأخيرة دون وقوعها.

تبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، حيث أنه نصت المادة 394 مكرر 7 قانون العقوبات:" يعاقب على الشروع في ارتكاب الجنح 2 المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"[1].

ويبدو من خلال هذا النص أن رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في أحد الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات أيضا مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي أيضا[2].

[1]– إتفاقية بودابست اتفاقية بودابست (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 08-11-2001 المتعلقة بالجريمة المعلوماتية تبنت الشروع أيضا في المادة 11 في الفقرة الثانية من الفصل الخامس منها والمعنون بأشكال أخرى للمسؤولية والجزاءات.

[2]– رابحي عزيزة، مرجع سابق، ص 250.

الفصل الثاني

خصوصية جرائم المعالجة الآلية

للمعطيات من حيث المتابعة

الفصل الثاني

خصوصية جرائم المعالجة الآلية للمعطيات من حيث المتابعة

إن التطور المذهل والمتسارع والمتلاحق تكنولوجيا المعلوماتية وشبكات المعلومات أدى إلى ظهور نمط جديد وهو جريمة المعلوماتية وفرت لها الوسائل التقنية، حيث ساهمت شبكات الاتصال المتعددة في عولمة الجريمة المعلوماتية، وتنوعت الأنشطة الإجرامية فيها مما حتم تنوعا في ملاحقتها ومتابعتها ابتداء من تجريمها وبيان إجراءات ملاحقتها وكذا الأجهزة المختصة في الوقاية منها أي على مستوى الجزائر أو في التشريعات المقارنة.

تختلف جرائم المعالجة الآلية للمعطيات (عن بعضها البعض في مجال الاختصاص ففي حالة ما إذا ارتكبت الجريمة المعلوماتية بواسطة المكونات المادية للحاسب الآلي فهذه الجريمة تعود اختصاصها إلى المحاكم الجزائية العادية، أما في حالة ارتكاب جريمة على نظام المعالجة الآلية (على المكونات المعنوية) ففي هذه الحالة فإن القطب الجزائي هو المختص في هذه الجريمة نظرا لصعوبة اثباتها، أثناء مرحلة جمع الاستدلالات والتحقيق ونظرا لخطورة الفعل المرتكب، ونقص الخبرات للقضاة في المجال المعلوماتي أمام المحاكم العادية، هذا في مجال مكافحة الجريمة المعلوماتية على المستوى الداخلي مرحلة المحاكمة.

لذا سنحاول من خلال هذا الفصل التطرق إلى خصوصية متابعة جرائم المعالجة الآلية للمعطيات (مبحث أول)، وخصوصية متابعة جرائم المعالجة الآلية للمعطيات من حيث إجراءات المتابعة (مبحث ثان).

المبحث الأول

خصوصية متابعة جرائم المعالجة الآلية للمعطيات من حيث الوسائل والأجهزة

وضع المشروع الجزائري كغيره من التشريعات بعض القواعد والضوابط التي تستهدف متابعة مرتكبي الجرم المعلوماتي حماية لمعطيات الحاسب الآلي خاصة في مرحلة جمع الاستدلالات، حيث إن أجهزة الشرطة تقوم بدور فعال ورئيسي حال وقوع الجريمة لمعاينة مكانها وضبط أدلتها والقبض على مرتكبيها والقيام بكل ما يفيد في كشف الحقيقة وذلك بعد مساعدة أجهزة التحقيق للتوصل إلى حقيقة الواقعة ومعرفة مرتكبيها، وهو ما سنتناوله بالتفصيل.

المطلب الأول

خصوصية من حيث أجهزة المتابعة

إن الدعوة العمومية باعتبارها الوسيلة القانونية لاستفتاء حق الدولة في العقاب نبدأ إجراءاتها بمرحلة البحث والتحري أي مرحلة جمع الاستدلالات التي تهدف الى البحث عن الجريمة والكشف عن مرتكبيها، وان الإجراءات الجزائية المتخذة خلال هذه المرحلة تتولاها أجهزة الشرطة القضائية وقد حددها قانون الإجراءات الجزائية[1].

الفرع الأول: تشكيل الضبطية القضائية

إن أعضاء الضبطية موظفون منحهم القانون صفة الضبطية القضائية مكلفون خلال مرحلة التحقيق التمهيدي بالكشف عن وقوع الجريمة وجمع الاستدلالات عنها، وعن المساهمين فيها باعتبارهم فاعلين اصليين وشركاء فيها ليتم تحرير محاضر بشأنها وتقديمها

[1]– أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء 2، طبعة 05، ديوان المطبوعات الجامعية الجزائر، دون سنة النشر، ص 159.

أمام الأجهزة المختصة وقد حدد لنا قانون الإجراءات الجزائية أهداف الضبطية القضائية تتمثل فيما يلي:

- ضباط الشرطة القضائية

- الموظفون والأعوان المنوط بهم قانون بعض مهام ضباط القضائي[1].

أولا: ضباط الشرطة القضائية

- يتمتع بصفة ضابط الشرطة القضائية حسب قانون الإجراءات الجزائية الجزائري –رؤساء المجالس الشعبية البلدية

- ضباط الدرك الوطني

- الموظفون التابعين للأسلاك الخاصة للمراقبين ومحافظي وضباط الشرطة للأمن الوطني

- ذو الرتب في الدرك، ورجال الدرك الذين امضوا في سلك الدرك 3 سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني بعد موافقة لجنة خاصة.

- مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة 3سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية بعد موافقة لجنة خاصة ويتبين من خلال نصوص المواد أن هناك 3 فئات ممن يتمتعون بصفة ضابط الشرطة القضائية وهي:

[1]– أنظر المادة 15 من الأمر 66–156 المتضمن قانون العقوبات التي تنص على أنه: "يتمتع بصفة ضابط شرطة قضائية:
- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- محافظو الشرطة.
- ضباط الشرطة....."

الفئة الأولى: هي الفئة التي تتمتع بصفة ضابط الشرطة القضائية بحكم القانون وهم رؤساء المجالس الشعبية البلدية وضباط الدرك الوطني ومحافظو وضباط الشرطة القضائية.

الفئة الثانية: هي الفئة التي يجب لكي تتمتع بصفة ضابط الشرطة القضائية تعيينهم بقرار مشترك من وزير الدفاع ووزير العدل لمصالح الأمن العسكري في الملفات.

الفئة الثالثة: وهي الفئة التي لا تخول لها صفة الضبطية إلا بعد تجاوز امتحان وموافقة لجنة خاصة وتعيينهم بقرار مشترك أما وزير الدفاع ووزير العدل (ذوي الرتب في الدرك والدركيين الذين قضوا في الخدمة 3 سنوات على الأقل) أو وزير الداخلية ووزير العدل (مفتشي الأمن الوطني) والضباط التابعين للقطاع العسكري الذين تم تعيينهم بموجب قرار مشترك بين وزير العدل[1].

ثانيا: أعوان الضبط القضائي

وقد حددهم قانون الإجراءات الجزائية في: (المادة 19 قانون إ ج)

– موظفي مصالح الشرطة، وذوو الرتب في الدرك الوطني والدركيين ومستخدمو مصالح الأمن العسكري (الملفات) الذين بيس لهم ضابط شرطة قضائية ولموظفون والأعوان المكلفون ببعض مهام الضبط القضائي وقد حددتهم المادة 21/ 27 وهم: المهندسون، الأعوان، الفنيون، التقنيون المختصون في الغابات وحماية الأراضي واستصلاحها

– رؤساء الأقسام والأعوان التقنيون في الغابات وحماية الأراضي الذين حددتهم المادة 23 يجوز أثناء ممارسة مهامهم ام يطلبوا مساعدة القوة العمومية.

وأعوان الإدارات والمصالح العمومية الذين يباشرون بعض مهام الضبط –موظفون القضائي.

[1]– محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، طبعة 4، دار هومة للنشر والتوزيع، الجزائر، 2009، ص ص47–49.

– الولاة (المادة 28 من قانون الإجراءات الجزائية).

الفرع الثاني: اختصاص الضبطية القضائية

إن أعضاء الضبطية القضائية وهم يمارسون صلاحياتهم في اجراء التحريات اللازمة بشأن الجريمة لمعرفة مرتكبيها مقيدين في ذلك بنطاق إقليمي محدد يسمى بالاختصاص المحلي وبنوع معين من الجرائم ويسمى الاختصاص النوعي.

أولا: الاختصاص المحلي

يقصد به المجال الإقليمي الذي يباشر فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة، ويتحدد عادة بحدود الدائرة التي يباشر فيها وظائفه المعتادة.

ولذلك يتعين ان يكون مكان وقوع الجريمة او محل إقامة المتهم او محل القبض عليه[1].

أ– امتداد الاختصاص المحلي

يجيز القانون تمديد الاختصاص المحلي لضابط الشرطة القضائية في حالة الاستعجال أو بناء على طلب من السلطة القضائية، وهو ما نصت عليه المادة 2/16 ق. إ. ج (دائرة المجلس) وكذا تحديد الاختصاص المحلي لضباط الشرطة القضائية في الجرائم الستة الخطيرة إلى كافة التراب الوطني[2].

ثانيا: الاختصاص النوعي

يقصد به اختصاص عضو الضبطية القضائية بنوع معين من الجرائم دون غيرها من الجرائم. وقد ميز المشروع بين الاختصاص العام، لبعض الفئات أعضاء الضبطية القضائية أي الاختصاص بالبحث والتحري بشأن جميع الجرائم دون تحديد نوع معين من الأنواع الأخرى من الجرائم، وهي الفئات المنصوص عليها في المادة 15 ق.إ.ج، فلهم الاختصاص

[1]– أحمد شوقي الشلقاني، مرجع سابق، ص 59.

[2]– أنظر المادة 16 من الأمر 66–155 المؤرخ في 18 صفر 1386 الموافق ل 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

العام بالبحث والتحري في جميع الجرائم أما الفئات الأخرى من الضباط المحددين في الفقرة 7 من المادة 15 والمواد و 21 و 27 و 28 ق. إ. ج فإنهم ذوو اختصاص خاص وليس عام يتحدد بنطاق جرائم معينة[1].

المطلب الثاني

الوسائل المستعملة في المتابعة

يمكن تقسيم الوسائل الى وسائل مادية تتمثل في المعاينة التقنية وضبط الدليل الرقمي، وأخرى وسائل شخصية تتمثل في التسرب، وشهادة شاهد الكتروني والخبرة، وهو ما سنتناوله فيما يلي:

الفرع الأول: الإجراءات المادية

وتتمثل الإجراءات المادية كما عددناها سابقا في المعاينة التقنية من جهة والتفتيش في بيئة الكترونية و كذا ضبط الدليل الرقمي وبيانها كما يلي:

أولا: المعاينة التقنية

المعاينة التقنية هي المكان الذي ارتكبت فيه الجريمة، الوعاء الأساسي الذي يحتوي على اخطر الأدلة الجنائية التي يخلفها الجاني وراءه في أعقاب اقترافه الجريمة، وفي لحظة يكون فيها اضطرابه العصبي والذهني قد بلغ قمة الانفعال بصورة لا تتيح المراجعة الدقيقة لأعماله وإزالة الآثار التي يخلفها في مكان الحادث المجرم مهما كانت دقته سوف يترك وراءه ما قد يشير إلى شخصيته ولذلك كان من الواجب على ضباط الشرطة القضائية الانتقال إلى ذلك المكان لمعاينة واثبات الآثار المادية للجريمة والمحافظة عليها واثبات حالة

[1]– ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون – تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي ، ام البواقي، 2015 / 2016، ص 06.

الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وكذا إخطار النيابة فورا بانتقاله، لكي تنتقل بدورها إلى محل الجريمة في حالة الجناية الملتبس بها.

ويقصد بالمعاينة رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وهي تقتضي في ذلك سرعة الانتقال إلى محل تلك الواقعة حيث يقوم ضابط الشرطة القضائية بجمع الدلائل والقرائن التي يستدل بها عن الجريمة والتثبيت المباشر لحالة الأشخاص والأشياء والأماكن ذات الصلة بالحادث، وهي المرحلة الأولى للاستدلال حول ملابسات أية جريمة ونظرا لاختلاف الجريمة المعلوماتية كثيرا عن الجرائم التقليدية نظرا لكون مسرحها الاجرامي قد يتعدى حدود الدولة فان المعاينة التقنية تتم بإتباع مجموعة من الإجراءات الخاصة التي سنوردها فيما بعد.

وتظهر أهمية المعاينة في أنها تنقل لجهات التحقيق والمحاكمة صورة مجملة لموقع الجريمة بكل ما يحتويه هذا الموقع من تفصيلات سواء تعلقت هذه التفصيلات بمكانه أو وصفه من الداخل أو الآثار الموجودة به، والتي تنقلها بالجريمة وإجمالا كل ما يمكن جهات الشرطة والقضاء من وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة من المادة التي تم جمعها وحتى تحقق المعاينة ثمارها وتفي بأغراضها المشهودة، نجد إن بعض التشريعات قد قررت جزاءات جنائية على كل من يقوم بإجراء أي تغيير على حالة الأماكن التي فيها الجريمة أو ينزع أي شيء منها أو يحدث تعديلا في مكان وقوع الجريمة قبل قيام سلطة التحقيق أو الاستدلالات بإجراء المعاينة الأولى أيا كان مرتكبها.

وقد نصت المادة 42 من قانون الإجراءات الجزائية الجزائري[1] على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو مخول لجهاز الضبطية القضائية سواء في الحالة 3العادية أو حالات التلبس، ويترتب على تغيير أو تعديل يطرأ على مكان وقوع الجريمة الجزاءات المنصوص عليها في المادة 43 قانون إ.ج. ج. وحتى يكون التفتيش في

[1]– أنظر المادة 42 فقرة 3 من الأمر 66–155 المتضمن قانون الإجراءات الجزائية، مرجع سابق.

بيئة الكترونية لابد أن يتم علي مستويين تتمثل في تفتيش المكونات المادية للحاسب الآلي والتي تمثل مسرح الجريمة التقليدي وأيضا تفتيش المكونات المعنوية للحاسوب والتي تمثل مسرح الجريمة الافتراضي.

1- مدى صلاحية مسرح الجريمة المعلوماتية للمعاينة:

إذا كانت المعاينة في الجرائم التقليدية تتم في مسرح الجريمة العادي فان الجريمة المعلوماتية تتم المعاينة فيها على مستويين[1]:

أ- المسرح التقليدي الجرائم الواقعة على المكونات المادية:

المسرح التقليدي هو المسرح الذي يقع عادة خارج بيئة الحاسوب ويتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو قريب من مسرح الجريمة التقليدية، ومن أمثلة هذه الجرائم تلك الواقعة على أشرطة الحاسب والكابلات الخاصة به وشاشة العرض الملحق به ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسب الآلي ذات الطابع المادي المحسوس (الملموس).

وليس هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل ضباط الشرطة القضائية والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل الأدوات والوسائل التي استخدمت في ارتكاب الجريمة مع أخطار النيابة العامة بذلك.

وفي هذه الحالة تتميز المعاينة بالسهولة. باعتبار أنها تتم على عناصر ملموسة كانت محلا للجريمة أو تخلفت عنها.

[1]- ابتسام بغو، مرجع سابق، ص 08.

ب- المسرح الافتراضي (الجرائم الواقعة على المكونات الغير مادية أو بواسطتها):

و المسرح الافتراضي يقع عادة داخل البيئة الالكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله وفي مقدمة هذه الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم بطريق الانترنت ومنها جرائم التزوير المعلوماتي والتخريب وتتميز المعاينة في العالم الافتراضي بالصعوبة تتمثل في:

- ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات.
- الأعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة زمنية وحتى يمكن لضابط الشرطة القضائية القيام بالمعاينة في العالم الافتراضي لابد عليه أن ينتقل الى العالم الافتراضي لمعاينة من مكتبه أو اللجوء إلى مقهى الإنترنت أو إلى الخبراء وغيرها من الأماكن التي تساعده في إظهار الحقيقة.

وللمعاينة في جرائم الانترنت والحاسوب (المعلوماتية) إشكال مختلفة تختلف بحسب نوعية الجريمة المرتكبة على ان هناك طرقا عامة تتوافق مع طبيعة الاتصال بالإنترنت أو الوسيلة التي تستخدم مثلا: وسيلة تصوير شاشة الحاسوب والتي تكون بواسطة آلة تصوير تقليدية أو عن طريق استخدام برمجة حاسوب متخصصة في اخذ صورة لما يظهر على الشاشة وهذا ما يصطلح عليه تجميد مخرجات الشاشة وغيرها[1].

2- إجراءات المعاينة التقنية

لابد على الضابط الشرطة القضائية إتباع بعض القواعد والإرشادات الفنية عند معاينة مسرحا لجريمة المعلوماتية، تتمثل هذه الإجراءات في:

[1]-ابتسام بغو، مرجع سابق، ص 09.

العثور على حاسبات آلية أو أجهزة أخرى داخل مسرح الجريمة يجب عدم العبث بها، تدوين الحالة التي هي عليها إذا كانت منطفئة أو في حالة تشغيل موصولة بالكهرباء أو بجهاز لاحق أخر، كما ينبغي ترقيم لواحقها بشكل متسلسل.

– يجب تحرير الأوراق المطبوعة على الحاسب الآلي والتي عثر عليها في مسرح الجريمة ووضعها في أكياس حسب حالتها، ويمكن إعادة الطباعة إذا كان الجهاز في حالة تشغيل وتحرير الأوراق التي تمت طباعتها. بالإضافة إلى تفقد الجهاز وتسجيل ما إذا كانت هناك برامج تم استخدامها لحظة دخول مسرح الجريمة[1].

– عند العثور على دعائم التخزين (أسطوانات، أقراص، حوامل مغناطيسية) يجب ترقيمها وتسجيل الحالة التي هي عليها والمكان الذي وجدت فيها (داخل الحاسب الآلي أو خارجه).

– عند الانتهاء من الترقيم يجب تصوير ودمج الأجهزة وملحقاتها في الحالة التي هي عليها.

– يجب تحرير جميع العينات التي عثر عليها من أجهزة ودعائم داخل أكياس خاصة (بلاستيكية او ورقية) كما ينبغي حمايتها من الكسر وتأثير العوامل الجوية وإبعادها عن أي مجال مغناطيسي لتفادي فقدان المعلومات وإرسالها إلى المخبر لإجراء الخبرة.

– تقتضي القاعدة العامة بأن تكون هناك استعانة بالخبراء في المسائل العلمية والتقنية التي تحتاج إلى خبرة خاصة كخبرة الطبيب الشرعي لمعرفة سبب الوفاة فالخبرة في الجريمة المعلوماتية لها أهمية بالغة للتطور السريع والمتلاحق في مجال صناعة الحاسبات والبرمجيات شبكات الاتصال ما قد يصعب على المحقق لا تتبعها واستيعابها.

يحتاج خبراء الأدلة الجنائية الرقمية لتأدية أعمالهم التقنية إلى الأدلة الرقمية واكتشاف المعلومات التي يحتويها كل دليل ومن هذه الأجهزة والأنظمة والبرمجيات ما يلي:

– أجهزة بقدرة عالية على التحليل وتخزين المعطيات.

[1]– محمد أمين شوابكة، مرجع سابق، ص 122.

- نسخ من مختلف أنظمة التشغيل المستعملة أدى الإفراد والمؤسسات.
- نسخ من برامج حذف وكسر كلمات المرور لمختلف الحاسبات، برامج نسخ الأقراص المدمجة والمحمولة، برامج الضغط وفك الضغط، برامج التشفير وفك التشفير، برامج حماية الأنظمة والشبكات من الاختراق، برامج كشف الأجهزة المخفية من الأقراص الصلبة، برامج استعادة الملفات المحذوفة وبرامج البحث عن الانترنت[1]

ثانيا: التفتيش المعلوماتي (التفتيش في بيئة تقنية)

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها بمكان يتمتع بالحرمة او تفتيش شخص، وان لإجراء التفتيش أهمية بالغة وخطورة معتبرة على الحياة الخاصة، ولهذا نص عليه المشرع بمقتضى قواعد دستوري[2] حيث تضمن الدولة عدم انتهاك حرمة منزل (مسكن) فلا تفتش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة. هذا بالإضافة إلى نصوص قانون الإجراءات الجزائية وأيضا القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3].

غير انه في الجريمة المعلوماتية يثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب والانترنت

لكن من المعروف إن نظم المعالجة الإلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات اتصال بعدية[4].

---

[1]- ابتسام بغو، مرجع سابق، ص 13.

[2]- التعديل الدستوري الجزائري لسنة 1996 الصادر بالمرسوم الرئاسي رقم 96/ 483 بتاريخ 12/07/ 1996 الجريدة الرسمية رقم 76 بتاريخ 1996/12/08.

[3]- قانون 09-04مؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4]- ابتسام بغو، المرجع نفسه، ص 13.

1- محل التفتيش:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص أو السيارة أو الرسائل... وبالتالي فقد يكون محل ذلك التفتيش إما مسكنا، أو شخصا، وبالتالي فقد يكون محل ذلك التفتيش إما مسكنا، أو شخصا، أو سيارة...مع مراعاة الإجراءات القانونية المقررة.

ومحل التفتيش في جرائم الحاسب الآلي يعتبر النافذة التي تطل بها الانترنت على العالم، والشبكة التي تشمل في مكوناتها الخادم[1] السيارة أو الرسائل... وبالتالي فقد يكون محل ذلك التفتيش إما مسكنا، أو شخصا، أو سيارة... مع مراعاة الإجراءات القانونية المقرر ومحل التفتيش في جرائم الحاسب الآلي يعتبر النافذة التي تطل بها الانترنت على العالم، والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي[2] وغيرها.

وتجدر الإشارة هنا إلى إن مثل هذا المحل لا يكون قائما بذاته، وإنما يشمله مكان أو عقار ما أو يكون بصحبة مالكه او حائزه ولذلك وجب على ضابط الشرطة القضائية عند استصداره لأذن التفتيش إن يحدد محل ذلك الإجراء تحديدا دقيقا وكذلك الغرض منه و إلا كان باطلا.

إن إجراء التفتيش في الجريمة المعلوماتية تحتاج إلى تقنيات خاصة تختلف عن حالات التفتيش العادية (التقليدية) لان تفتيش نظم المعلومات ليست سهلة وتتطلب دراية ومعرفة بملفات أجهزة الإعلام الآلي وأماكن إخفاء المعلومات فيها لأنه يسهل إتلافها كليا أو جزئيا، كما يصعب تحديد مكان الدليل.

---

[1]- الخادم هو الجهاز الرئيسي أو المسئول في الشبكة وباقي الأجهزة المتصلة بالشبكة هي عبارة عن عملاء لأنها تطلب في خدمات معينة منه.

[2]- المزود الآلي هو المزود الذي يوفر لعملائه إمكانية الوصول إلي الانترنت.

وبالتالي ففي إطار جرائم الانترنت يقع التفتيش على موضوعين اثنين هم:

- تفتيش المكونات الحاسب الآلي، (المادية والمعنوية).

- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب التفتيش عن بعد وهو ما سنتناوله.

أ- تفتيش مكونات الحاسب الآلي:

قبل الغوص في إجراءات التفتيش لابد من تعريف الحاسب الالي" وهو كل جهاز الكتروني يستطيع ترجمة أواصر مكتوبة بتسلسل منطقي لتنفيذ عمليات ادخال او اخراج معلومات."

1- تفتيش المكونات المادية للحاسب الآلي:

تخضع المكونات المادية لنظام المعالجة الالية للمعطيات لإجراءات التفتيش المنصوص عليها في المادة 44 قانون الاجراءات الجزائية[1] أي انه يجب مراعاة مكان وجود ذلك الحاسوب اثناء مباشرة ذلك الاجراء، فيما اذا كان مكانا عاما او خاصا، ذلك لان لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كان موجود في مكان خاص كمسكن المتهم فلا يجوز تفتيشه الا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات المقررة قانونا وكذا المادة 64 من نفس القانون[2]، فلا يجوز القيام بإجراء التفتيش الا بأذن مكتوب صادر عن وكيل الجمهورية او قاضي التحقيق وبعد الحصول على رضا صريح من صاحب المسكن، ويجب كتابته بخط يد صاحب الشأن وتوقيعه، وفي حالة العكس يثبت ان صاحب الشأن لا يعرف الكتابة في المحضر مع التنويه عن رضائه اما اذا تعذر على صاحب الشأن الحضور وقت اجراء التفتيش، فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، واذا امتنع عن ذلك او كان هاربا استدعى الضابط لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته كما يجب ان يتم ذلك الاجراء في المواعيد المحددة قانون وهي

[1]- أنظر المادة 44 من الأمر 66-155 المتضمن ق.إ. ج، مرجع سابق.

[2]- أنظر المادة 64 من الأمر 66-155 المتضمن ق. إ. ج، مرجع سابق.

من الساعة الخامسة صباحا الى الساعة الثامنة مساء الا في الحالات الخاصة خاصة فيما يتعلق بالجرائم الستة الخطيرة ومن بينها الجريمة المعلوماتية التي لا تشترط المواعيد وانما في كل وقت من الليل والنهار(24 ساعة)[1].

إلا أن المشرع الجزائري بمناسبة التعديل الذي الحقه على قانون الإجراءات بالقانون 22/06 المؤرخ في 20 ديسمبر 2006 استثني بموجب الفقرة الثالثة من المادة 45 وكذا الفقرة الثانية من المادة 47 والفقرة 03 من المادة 64 تطبيق هذه الضمانات عند اجراء التفتيش بمناسبة تحقيق مفتوح بخصوص الجريمة المعلوماتية.

ويفهم من استقراء هذه المواد ان المشرع لا يشترط حضور الشخص الذي يشتبه في انه ساهم في ارتكاب الجريمة عند تفتيش مسكنه وغيرها من الضمانات التي استثناها المشرع في بعض الجرائم ومن ينتهك الجريمة المعلوماتية (جرائم أنظمة المعالجة الالية للمعطيات بموجب الفقرة 3 من المادة 47 من ق. إ.ج[2].

2- تفتيش المكونات المعنوية لنظام المعالجة الالية:

يتعلق الامر بالتفتيش عن الجريمة التي وقعت على المكونات المعنوية للحاسوب ويقصد بها أنظمة الكمبيوتر والبيانات المخزنة فيه التي جرى التلاعب فيها أو تغييرها 1 وغيرها من الوسائط التي تساعد على تخزين المعلومات.

كذلك وان الامر يتعلق بمدى صلاحية نظم الحاسوب للتفتيش وبالأجهزة المختصة بالتفتيش نظام الحاسوب والانترنت.

[1]- أنظر المادة 44 من المر 66-155 المتضمن ق. إ. ج، مرجع سابق.

[2]- أنظر المادة 47 من الأمر 66-155 المتضمن ق. إ. ج، مرجع سابق.

أما مدى صلاحية معطيات الحاسوب فهو امر تفرضه طبيعة الجريمة المرتكبة، والرأي المستقر عليه: أن معطيات الحاسوب تصلح للتفتيش عن الأدلة الجرمية وضبطها لان الغاية من التفتيش هو الحصول على دليل خاص بالجريمة وكشف الغموض الذي أحاط بها[1].

إن الطابع المعنوي للبيانات والمعلومات المخزنة علي الحاسوب والتي يمكن القيام بتفتيشها اذا كانت مخزنة علي حاسوب المتهم ؛فان الاشكال هنا في حالة ما اذا كان حاسوب المتهم مرتبطا بحاسوب اخر داخل الدولة او خارجها؛ فهل يجوز اجراء التفتيش في هذه الحالة؟ وهل يجوز تفتيش حاسوب الاخرين والكشف عن الوسائط الالكترونية؟

وبالتالي يرى البعض ان التفتيش يمتد الى سجلات البيانات الموجودة في موقع اخر، بشرط ان تكون البيانات الخاصة ضرورية بإظهار الحقيقة.

وهو ما تبناه القانون المقارن حول تفتيش الأنظمة المعلوماتية، فقد منحت المادة 251 من قانون الإجراءات اليوناني سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع 2 والانجليزي 1 الدليل، وكذلك المادة 487 من القانون الكندي والفرنسي وفي الولايات المتحدة الامريكية، وبالتالي فإن النصوص القانونية التي ارست القواعد التي تحكم التفتيش تم سنها قبل ان يعرف القانون الأشياء غير المادية، وبالتالي فالنصوص التقليدية لا يمكن اعمالها مباشرة على النظم المعلوماتية لان قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائي.

وهو ما أقرته اتفاقية بودابست[2] في المادة 01/19 من القسم الرابع على انه "يمكن لكل دولة طرف الحق في ان تسن القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش او الدخول الى نظام الكمبيوتر او جزء منه او المعلومات المخزنة فيها الوسائط التي يتم تخزين معلومات الكمبيوتر بها مادامت مخزنة في اقليمها.

[1]– ابتسام بغو، مرجع سابق، ص 16.

[2]– اتفاقية بودابست، مرجع سابق.

ويتضح موقف المشروع الجزائري من خلال القانون 09 /04المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، حيث اجازت المادة 05 منه السلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها بغرض التفتيش ولو كان عن بعد الى كل من منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها او أي منظومة تخزين معلوماتية.

وطبقا للمادة 05/2 من القانون 04/09[1] أجاز المشرع تمديد التفتيش الى هذه المنظومة بعد اعلام السلطة القضائية المختصة مسبقا بذلك متى دعت الضرورة الى الاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه الأخيرة يمكن الدخول اليها من المنظومة الأولى في إطار إقليم الدولة.

أما اذا تبين ان المعطيات المبحوث عنها والتي يمكن الدخول اليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني. فإن التفتيش او الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة.

ثانيا: ضوابط التفتيش

تحرص اغلبية القوانين على احاطة التفتيش بشروط وضمانات أساسية بوصفة اجراء يمس صميم الحرية الشخصية: الغرض منها تحقيق الموازنة الضرورية بين مصلحة المجتمع وبين حقوق المتهم.

ومن الشروط والضمانات التي يجب توافرها لإجراء التفتيش ما هو موضوعي ومنها ما هو شكلي وعلى هذا الأساس نقسم دراستنا إلى:

- شروط شكلية

[1]- القانون 09-04، مرجع سابق.

– وشروط موضوعية

1– الشروط الشكلية: وهي شروط شكلية لصحة التفتيش وهي:

– الحضور الضروري لبعض الأشخاص اثناء اجراء التفتيش في العالم الافتراضي وهي من اهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية وذلك لضمان الاطمئنان الى سلامة الاجراء وصحة الضبط، والاصل ان الشخص الذي يستجوب الحضور هو المتهم او أحد أقاربه وهو الشرط الذي استثناه المشرع الجزائري اذ اشترط المشرع الجزائري انه لا يجوز تفتيش مسكن المتهم الا بالضوابط والضمانات المقررة في نص المادة 45 و 64 ق ا ج ج. وهو ما استثناه المشرع لتطبيق هذه الضمانات بالنسبة لبعض الجرائم ومنها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات بموجب الفقرة 03 من المادة 47 ق ا ج ج.

– أن يتم التفتيش بأسلوب آلي. أي ان يكون التفتيش علي دعامة الكترونية وهو بالضرورة الحاسب الالي

– أن يتم التفتيش من طرف فريق يتكون من خبراء

– إذن التفتيش لابد ان يكون مسببا

– الميعاد الزمني لإجراء التفتيش حيث اختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش وهناك حالات استثنائية خرج فيها عن هذه القاعدة الاصل ان يكون التفتيش من الساعة الخامسة صباحا الي الساعة الثامنة مساء وإلا كان التفتيش باطلا؛ غير انه في بعض الجرائم خرج المشرع الجزائري عن القاعدة العامة لميعاد التفتيش وأجاز التفتيش في جميع الاوقات 24 ساعة في بعض الجرائم المذكورة على سبيل الحصر ومن بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[1].

[1]– أحمد شوقي الشلقاني، مرجع سابق، ص 45.

2- الشروط الموضوعية: يقصد بها الشروط اللازمة لإجراء التفتيش الصحيح، وتتمثل في:

أ- سبب التفتيش: حتى يكون التفتيش صحيحا لابد أن تكون هناك جريمة معلوماتية وهو ما أكدته المادة 5 من القانون 04/09.

ب- الغاية من التفتيش: لا يكون التفتيش بقصد ضبط أشياء تتعلق بالجريمة او في كشف الحقيقة والكشف عن أشياء تتعلق بالجريمة او تفيد في إظهار الحقيقة طبقا للنص المادة 44 ق.إ. ج. ج ولذلك يكون باطلا التفتيش الذي يجري لغاية أخرى.

ج- محل التفتيش: هو المستودع الذي يحفظ فيه المرء بالأشياء المادية التي التي تضمن سره، ومحل التفتيش، في جرائم الانترنت هو الحاسب الالي الذي يعتبر النافذة التي تطل بها الانترنت فقد يكون محل الحاسب الآلي مكان او عقار ما أو يكون بصحبة مالكه او حائزة او المكونات المادية أو المعنوية للحاسب الالي.

د- ويقصد به هو المكان الذي يحتفظ فيه الجاني او المجرم بجميع الوسائل التي ارتكب بها الجريمة ؛ويتمثل في المعلومات والآثار الموجودة والمخزنة علي الحاسوب الموجود اما في عقار(مكان اقامة المشتبه فيه مثلا)او المكونات المادية والمعنوية للحاسب الالي.

ه- اذن التفتيش: وطبقا للتشريع الجزائري فإن الاذن لابد ان يكون مكتوب من طرف اما وكيل الجمهورية او قاضي التحقيق المختص.

الفرع الثاني: الإجراءات الشخصية

وهي إجراءات تتعلق بالشخص في حد ذاته وتتمثل في الخبرة وشهادة شاهد الكتروني والتسرب وهو ما سنتناوله فيما يلي:

أولا: الخبرة الخبرة

هي اجراء يستهدف استخدام قدرات شخص الفنية او العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرنية يفيد في معرفة الحقيقة بشأن وقوع الجريمة

ونسبتها الى المتهم أو تحديد ملامح شخصيته الاجرامية[1] ولهذا فإن للخبرة التقنية في مجال جرائم المعالجة الآلية للمعطيات أهمية بالغة حيث أنه لا يستطيع التعامل مع هذه الجريمة الا شخص ذو دراية وخبرة مجال الشبكات[2].

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها[3] فإن الخبير المعلوماتي لابد أن توافر لديهم المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية من اجل كشف الغموض عن الجريمة او تجميع ادلتها والتحفظ عليها ومساعدة المحقق في ايجاد جوانب الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

ثانيا: مهام الخبير

تركيب الحاسب الالي وطرازه ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها بيئة الحاسوب او الشبكة من حيث طبيعتها تركيزها او توزيعها، نمط ووسائل الاتصال.

- المكان المحتمل لأدلة الاثبات وشكلها وهيئتها

- الاثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة المعلوماتية.

- كيفية عزل النظام المعلوماتي عند الحاجة دون اتلاف الأدلة او الأجهزة او تدميرها.

- إمكانية نقل ادلة الى اوعية دون أخرى والاوعية المادية كالأوراق على ان تكون مطابقة لما هو مسجل على الحاسب الآلي أو النظام أو الشبكة [4].

---

[1]- حمد شوقي الشلقاني، مرجع سابق، ص 259.

[2]- مرجع نفسه، ص259.

[3]- تتميز الجريمة المعلوماتية عن الجريمة التقليدية نظرا لخصوصيتها من الجانب الإجرائي من جهة وكذلك لصعوبة إثباتها لعدم وجود دليل مادي ملموس.

[4]- صغير يوسف. الجريمة المرتكبة عبر الانترنت. مذكرة لنيل شهادة الماجيستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

ثالثا: مجالات الخبرة بالنسبة للجرائم المعلوماتية

تتنوع العمليات الالكترونية بتنوع المجالات التي تستخدم شبكة الانترنت فنجد امثلة لها في الاعمال المصرفية، الإدارة الالكترونية، التجارة الالكترونية، لذلك فإن بتصور تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع العمليات الالكترونية المستخدمة في ارتكابها حيث تقتضي عمليات البحث الجنائي والتحقيق في المعلوماتية الاستعانة بخبرات عديدة ومتنوعة ومن أهم هؤلاء الخبراء في مجال مساعدة المحققين على ضبط الجريمة في الجزائر وهو المعهد الوطني للأدلة الجنائية وعلم الاجرام "بالجزائر العاصمة"

حيث عالجت دائرة الالكترونيك والإعلام الالي التابعة للمعهد ببو شاوي 325 طلب تحليل وخبرة سنة 2014، في حين تم معالجة 268 طلب سنة 2013 أي بزيادة قدرها 57 بنسبة تطور بلغت 21.26 وقد جاءت هذه القضايا كالتالي:

- 11 قضية تتعلق بانتهاك الآداب
- 04 قضايا تتعلق بتكوين جمعية أشرار
- 03 قضايا تتعلق بالاعتداء على الامن والنظام المعلوماتي العمومي
- 02 قضيتان تتعلقان بتبييض الأموال
- 04 قضايا تتعلق بالتشهير
- 04 قضايا تتعلق بالتهريب
- 01 قضية تتعلق بالرشوة
- 03 قضايا تتعلق بالقرصنة المعلوماتية
- 34 قضية تتعلق بمعلومات قضائية

حيث تقوم دائرة الاعلام والإلكترونيك بمهمة معالجة تحليل وتقديم للعدالة كل دليل رقمي وتماثلي كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة:

ولإنجاز المهمة المنوط بها تنقسم الدائرة الى 3 مخابر هي:

- مخبر الإعلام الآلي
- مخبر الفيديو
- مخبر الصوت

كل مخبر مزود بفصيلة الاستقطاب المعطيات سمعية، بصرية ورقمية من حوامل المعلومات وذلك لضمان نزاهة وشرعية الدليل.

كما سجل مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية ومكافحتها للدرك الوطني ببئر مراد رايس في معالجة 102 قضية سنة 2014 مقابل 46 قضية سنة 2013 أي بزيادة قدرها 56 قضية بنسبة تطور 121 %في حين بلغت نسبة حل القضايا 95 %ومن بينها:

13 قضية تتعلق بجرائم المساس بأنظمة المعالجة الالية للمعطيات كما تمكنت من جهة أخرى الفرق المتخصصة في مكافحة الجرائم المعلوماتية للأمن الوطني سنة 2014 بناء على شكاوى من معالجة 211 قضية تتعلق بجرائم الانترنت قدم من خلالها الدليل المادي عن تورط 205 مشتبها فيه منهم 28 امرأة ومن بين هذه القضايا قضايا تتعلق بالجريمة المعلوماتية[1].

75 قضية ماسة بأنظمة المعالجة الالية للمعطيات

03 قضايا متعلقة بالنصب والاحتيال عن طريق الانترنت

06 قضايا متعلقة بالإهانة والسب عن طريق الأنترنت

[1]– ابتسام بغو، مرجع سابق، ص ص 22–23.

02 قضايا متعلقة بالاستعمال الغير للبطاقات الالكترونية

وفي هذا الإطار أكدت إدارة الإعلام والعلاقات العامة بالمديرية العامة للأمن الوطني، أنه تم إنشاء فرق متخصصة من الشرطة عبر 48 ولاية والتي تم تعزيزها بالمحققين والخبراء من ذوي القدرة والكفاءة في مجال المعلوماتية للحد من هذا النوع من الإجرام لاسيما بعد تعدد أساليب الاحتيال التي تعتمد أساسا على استغلال التقنية الحديثة والتطور الذي تعرفه تكنولوجيات الإعلام والاتصال[1].

رابعا: ضوابط الخبرة

تخضع الخبرة لمجموعة من الضوابط القانونية والفنية:

أ- الضوابط القانونية: وتنحصر في تلك الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية كاختيار الخبراء واجبات والتزامات الخبير (الحلف اليمين، وخضوعه للرقابة القضائية)

- القيام بمهامه بنفسه واستجابته لطلبات الخصوم

- ايداعه التقارير خلال المدة المحددة[2].

ب- الضوابط الفنية: تشمل خطوات اشتقاق الدليل الالكتروني والتي تتمثل في خطوات ما قبل التشغيل والفحص وخطوات التشغيل وتحديد مدن الترابط بين الدليل المادي والالكتروني ومرحلة تدوين النتائج واعداد التقارير وتتمثل هذه الضوابط:

- في جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع ومن جهاز المعتدي بعد التوصل الى تحديد.

[1]- ابتسام بغو، مرجع سابق، ص 24.

[2]- المادة 5 فقرة أخيرة من القانون 04/09، مرجع سابق.

– تحليل رقمي لمعرفة كيفية اعداد الأدلة الرقمية ونسبتها وتحديد عناصر حركتها، ثم التوصل في النهاية الى معرفة بروتوكول الانترنت للحاسوب الذي صدرت منه الرسائل والهجمات الالكترونية ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في اشتقاق وتجميع الأدلة الرقمية يتم عبر 03 مراحل:

المرحلة ا لأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الخادمة التي دخل فيها المجرم ا لمعلوماتي.

المرحلة الثانية: مرحلة المراقبة ويتم بطرق مختلفة، كبرامج مراقبة يمكن تحميلها للبحث عن المشتبه فيه وتسجيل بيانات الدخول وخروج الموقع.

المرحلة الثالثة: فحص النظام ألمعلوماتي المشتبه فيه بعد ضبطه من طرف السلطات المختصة بمكوناته المادية والمعنوية لاشتقاق الدليل وتقديمه للعدالة[1].

ثانيا شهادة الشاهد الكتروني (الشهادة في الجريمة الالكترونية)

إن سماع الشاهد بمعرفة ضباط الشرطة القضائية يدخل في عداد ما يسمى سلطته في الحصول على الإيضاحات، والهدف من ذلك أن يجمع كل ما يمكن جمعه من المعلومات عن الجريمة ومرتكبيها.

أولا: تعريف الشاهد المعلوماتي

الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الالي، والذي لديه خبرة جوهرية لازمة للدخول الى نظام المعالجة الآلية للمعطيات متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله ولذلك يطلق على الشخص اسم الشاهد المعلوماتي تمييزا عن الشاهد التقليدي.

[1]– ابتسام بغو، مرجع سابق، ص ص 24–25.

ثانيا: من هو الشاهد المعلوماتي؟

عامل تشغيل الحاسب الالي وهو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به ولابد ان يكون لديه خبرة كبيرة في استخدام الحاسب الالي ومكوناته عن طريق استخدام هذه البيانات وكيفية ادخال البيانات ثم استخراجها ونقلها ومعالجتها كما يجب ان تكون له خبرة واسعة في الكتابة السريعة عن طريق لوحة مفاتيح الحاسب الآلي.

ب- **خبراء البرمجة: أو** خطوط البرامج وهم الأشخاص المتخصصين وكتابة أوامر البرامج وهم فئتين:

الأولى: مخططو برامج التطبيقات

الثانية: مخططو برامج النظم

ج- **المحللون:** هو الشخص الذي يحلل الخطوات، ويقوم بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه الى وحدات منفصلة واستنتاج العلاقة الوظيفة بينها.

د- وهم المسؤولين عن اعمال الصيانة الخاصة بتقنيات الحاسب بمكونات وشبكات الاتصال المتعلقة بهه /مديرو النظم وهم الذين توكل لهم اعمال الإدارة في النظم المعلوماتية[1].

ثالثا: التزامات الشاهد في الجريمة المعلوماتية

يلتزم الشاهد في الجريمة المعلوماتية متى كان على معلومات جوهرية تفيد سير التحقيق بأن يعلم بها جهات التحقيق القضائي والا تعرض للعقوبات المقررة للامتناع عن الشهادة وترتكز الشهادة على ما يلي:

- طبع الملفات البيانات المخزنة في ذاكرة الحاسب الالي او حاملات البيانات الثانوية على ان يقوم بطبعها وتسليمها الى المحقق طالما ان المصلحة العامة اقتضت ذلك.

[1]-هلال عبد الاله، مرجع سابق، ص 23.

- الإفصاح عن كلمات المرور السرية.
- الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة حيث يجب على الشاهد الكشف عن مفاتيح الشفرات المدونة[1].

رابعا: شروط الشاهد بالإعلام عن الجريمة المعلوماتية

تتلخص هذه الشروط في:

- أن يكون يصد جريمة معلوماتية وقعت بالفعل سواء كانت جنحة او جناية.
- أن يكون الشاهد المعلوماتي على علم ومعرفة بالمعلومات الجوهرية المتصلة بالنظام المعلوماتي محل الواقعة.
- أن تقتضي مصلحة التحقيق الحصول على هذه المعلومات الجوهرية.
- معرفة بيئة الحاسوب من حيث طبيعتها وتركيزها ووسائل ونمط الاتصال.
- المكان المحتمل لأدلة الإثبات وشكلها[2].

ثالثا: ضبط الدليل الرقمي

يعتبر ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش، ولذلك نجد ان التشريعات الإجرائية تجمع عادة بين احكام الضبط والتفتيش في موضع واحد لكن ليس معنى ذلك ان الضبط هو التفتيش اذ قد يكون نتيجة معاينة وغيرها وهو ما سنتناوله:

أ- مفهوم ضبط الأدلة الالكترونية:

هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عنها وعن مرتكبيها وهو يرد الا على الأشياء المادية وبالتالي الصعوبة في ضبط ادلة الجريمة الواقعة على

[1]- هلال عبد الاله، المرجع نفسه، ص 24.

[2]- مرجع نفسه، ص 31.

المكونات المادية للكمبيوتر بالبصمات مثلا، وانما تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وكذا المكونات المعنوية للحاسوب وفي هذا الإطار اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية التي لا تصلح بطبيعتها محلا لوضع اليد، وانقسم ذلك الى اتجاهين وهما:

الاتجاه الاول: يرى أصحاب هذا الاتجاه أنه يمكن تصور إجراء ضبط على الكيانات المعنوية للحاسب الألي لانتقاء الكيان المادي عنها، وبالتالي عدم صلاحيتها، ومن بين التشريعات التي اخذت بهذا الاتجاه التشريع الألماني.

الاتجاه الثاني: يرى أصحاب هذا الاتجاه ان المعطيات المخزنة اليا تصلح ان تكون محلا للضبط المنصوص عليه في النصوص التقليدية[1].

غير أن المشرع الجزائري تدخل بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال[2] حيث قررها اليات خاصة منها:

– حجز المعطيات المعلوماتية عندما تكتشف السلطة التي تباشر في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل منظومة، يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز[3].

– حجز هذه المعطيات عن طريق منع الوصول اليها، ويتم ذلك عادة عن طريق الترميز او بتقييد الدخول الى تلك المنظومة، او عن طريق اية وسيلة الكترونية[4].

– حجز المعطيات ذات المحتوى الجرمي للمجرم[5].

---

[1]– ابتسام بغو، مرجع سابق، ص 28.

[2]– قانون 04/09، مرجع سابق.

[3]– نظر المادة 07 من القانون 04/09، مرجع سابق.

[4]– نظر المادة 08 من القانون 04/09، مرجع سابق.

[5]– نظر المادة 09 من القانون 04/09، مرجع سابق.

وتقع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به في قانون العقوبات وقانون الإجراءات الجزائية الجزائري؛ لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود الضرورية للتحريات والتحقيقات القضائية.

ب- أنواع الأدلة الالكترونية:

من بين الأشياء أو الأدلة التي تضبط وتحتفظ بها في الجرائم المتعلقة بالجريمة المعلوماتية والتي لها قيمة في إثبات تلك الجريمة وتنسبها إلى المتهم:

- **الورق:** على الرغم من ان الكمبيوتر قلل من استخدام أو حجم الأوراق أو الملفات التقليدية حيث يتم حفظ المعلومات لأغراض المراجعة او التأكد من الشكل العام. للمستند أو الرسالة، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها

-**ضبط جهاز الكمبيوتر وملحقاته: أي أن** وجوده وضبطه أمر مهم جد للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو أنها مرتبطة بالمكان أو الشخص الحائز على الجهاز ولأجهزة الكمبيوتر إشكال وأنواع مختلفة الأمر الذي يتطلب على ضباط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه ومواصفاته بسرعة فائقة أما بنفسه أو بواسطة خبير.

- **البرمجيات:** إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

- **وسائل التخزين المتحركة:** كالأقراص المدمجة "أقراص الليزر، والأقراص المرئية والأشرطة المغناطيسية وغيرها.

- **المودم:** وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.

– **ضبط البريد الالكتروني:** عن طريق تحديد صندوق البريد الخاص بالمتهم محل التفتيش بعد معرفة اسم المستخدم والرقم السري للدخول وفتح البريد الالكتروني عن طريق اما: الوارد او الصادر او الحفظ او المهملات او ضبط الرسائل الالكترونية عن طريق تشغيل برامج البريد الالكتروني في جهاز المتهم ومراجعة قائمة الرسائل الجديدة ليلتقط الرسالة المطلوبة[1].

ج– الصعوبات التي تواجه المحقق في ضبط الدليل:

إن عملية ضبط البيانات المعالجة اليا تواجه عدة صعوبات أهمها:

– ضخامة البيانات التي من الواجب فحصها.

– الضبط في مجال المعلوماتية قد يمثل أحيانا اعتداء على حقوق الغير او على حرمة حياتهم الخاصة مما يستوجب اتخاذ ضمانات لازمة لحماية هذه الحقوق.

– قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة اجنبية مما يستدعي تعاونها مع جهات التحقيق الوطنية[2].

ثالثا: التسرب

وهو من الإجراءات الشخصية، والجريمة المعلوماتية من بين الجرائم التي تسمح فيها التشريعات اللجوء الى مثل هذا الاجراء، ولقد حدد المشرع الجزائري نطاق هذا الاجراء بالجرائم المذكورة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد نظمه المشرع الجزائري في القسم الخامس من قانون الاجراءات الجزائية الجزائري وهو ما سنتطرق اليه فيما يلي:

[1]– نهلا عبد القادر المومني، مرجع سابق، ص ص 23–24.

[2]– ابتسام بغو، مرجع سابق، ص 31.

أ- مفهوم التسرب:

إن التسرب من الناحية الأمنية هو تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط لمعرفة او استعلام عن نشاط جرمي ومعرفة ادق التفاصيل فيه وخصوصياته اما من الناحية القانونية في المشرع الجزائري حدد مقصود هذا الإجراء بموجب المادة 65 مكرر 12 على انه "قيام ضابط الشرطة القضائية أو عون تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة اشخاص مشتبه في ارتكاب جناية او جنحة بإيهامهم انه فاعل معهم أو شريك[1].

ويلاحظ ما سبق ذكره ان التسرب عملية معقدة تتطلب ان يدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ويربط معهم علاقة من اجل تحقيق الهدف النهائي من العملية، وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الاجرامية التي تسرب اليها، وعلى هذا فإن التسرب يرتكز على مبدأين.

المبدأ العام: يستند على تقديم صورة على الوسط المراد التسرب فيه ويستوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات ونشاطاته.

المبدأ الخاص: يستند على تعميق التحري عن هذا الوسط ونشاطاته او مميزاته ووسائله وطبيعة الأشخاص المنتمين، ليتم بعد ذلك دراسة الوظيفة العمليات في هذا المجال بتوفير الوسائل البشرية والتقنية.

ب- شروط التسرب:

من أجل أن تتم عملية التسرب وانجاح العملية وتسهيل متابعة الجريمة المعلوماتية والمجرمين ومهام المتسرب، فقد أحاط المشروع جملة من الشروط يعين مراعاتها عندما

[1]- انظر المادة 65 مكرر ج. ج. إ. ق 12.

تقتضي التحريات كون هذا الاجراء من أخطر الاجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيه[1].

وتتمثل هذه الشروط في: شكلية وأخرى موضوعية سنتناولها:

الشروط الشكلية:

- إن يكون صادر بإذن قضائي اما وكيل الجمهورية او قاضي التحقيق المختص.
- أن يكون الاذن مكتوبا والا وقع تحت طائلة البطلان[2].
- ذكر اسم الضابط الذي تتم عملية التسرب تحت مسؤوليته او عون الشرطة القضائية باعتباره مساعدا له[3].
- المدة المطلوبة لعملية التسرب 4 أشهر محددة قانونا قابلة للتجديد ويمكن توقيفها حتى انتهاء المدة المحددة لها[4].

الشروط الموضوعية:

- تسبيب الإذن بالتسرب خاصة إذا اثبت إن الاعتداء على الوسائط الفعلية العادية غير كاف للتوصل إلى الحقيقة ومن ثمة لابد من وكيل الجمهورية أو قاضي التحقيق أن يقدم تبريرا أو الأساس الذي تم الاعتماد عليه من اجل السماح بالقيام بعملية التسرب.
- إن نوع الجريمة هي من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[5].

ج- التسرب الرقمي (طرق التسرب في مجال الجريمة المعلوماتية):

يمكن تصور التسرب في نطاق الجرائم المعلوماتية في دخول ضابط شرطة قضائية أو عون شرطة القضائية إلى العالم الافتراضي (شبكة الانترنت) وذلك بتسجيله على مواقع

---

[1]- مجمد حزيط، مرجع سابق، ص 65.

[2]- انظر المادة 65 مكرر 15 من القانون 66-155، مرجع سابق.

[3]- أنظر المادة 65 مكرر 16 من القانون 66-155، مرجع سابق.

[4]- انظر المادة 65 مكرر 15 فقرة 03 من القانون 66-155، مرجع سابق.

[5]- انظر المادة 65 مكرر 05 من القانون 66-155، مرجع سابق.

معينة كمواقع التواصل الاجتماعي أو اشتراكه في محادثات عبر غرف الدردشة أو حلقات الاتصال المباشر لرفع ومعاينة الجرائم أو ربط الاتصال مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أو صفات مستعارة ووهمية سعيا منه للتعرف عليهم وتحديد أماكنهم[1].

[1]–ابتسام بغو، مرجع سابق، ص 33.

المبحث الثاني

خصوصية متابعة جرائم المعالجة الآلية للمعطيات من حيث إجراءات المتابعة

تعتبر الجريمة الإلكترونية من الجرائم الحديثة النشأة، ولذلك فإن القواعد العامة لمكافحة نما استحدث قواعد وآليات جديدة خاصة فقط بالجريمة الجريمة الإلكترونية غير صالحة أو الإلكترونية نظرا لخصوصيتها من الناحية الإجرامية خاصة في مجال التحقيق، فيجب على المحقق في حالة وقوع أي جريمة لابد أن يستظهر أركانها الثلاث، الشرعي، والمادي والمعنوي للجريمة محل التحقيق.

أ- إظهار الركن المادي: يتطلب النشاط أو السلوك الإجرامي في جرائم الانترنت وجود بنية رقمية واتصال بالأنترنت، وأيضا معرفة بداية هذا النشاط والشروع فيه نتيجته.

ب- إظهار الركن المعنوي للجريمة الإلكترونية: يتمثل في الحالة النفسية التي يكون عليها الجاني التي دفعت به لارتكاب الجريمة والعلاقة التي تربط بين الشخص الجاني والفعل المرتكب أو المكون للجريمة ويتمثل أساسا في العلم و الإدارة المعروف باسم القصد الجاني العام.

ج- علانية ال تحقيق من الضمانات اللازمة للعدالة الجنائية علاقة التحقيق في الإجراءات الجنائية وهي تختلف عن التحقيق الابتدائي عنها في مرحلة المحكمة[1].

[1]- محمد بوعمرة، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، قسم القانون الخاص، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة 2019-2020، ص 40.

المطلب الأول

خصوصية إجراءات التحري والتحقيق

إن أهمية جهاز الشرطة القضائية في كشف عن الجريمة الإلكترونية والتعرف على المجرم الإلكتروني، تبعه استعداد المشرع الجزائري لأساليب التحري الخاصة المستعملة بما تناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن يتكيف دورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر، وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الإلكترونية كشكل من أشكال الجريمة المنظمة[1].

ما تجدر الإشارة إليه أن هذه الإجراءات لا يرخ ضبها إلا في بعض الجرائم المعنية من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية التي استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية، القانون رقم 06-22 والتي تتمثل في النقاط التالية:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية ولا سلكية.

- جواز التسرب أو الاختراق للكشف عن الجريمة الإلكترونية حسب المادة 65 مكرر 12 من القانون 06-22 المتضمن قانون الإجراءات الجزائية[2].

- ولأنه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطه المشرع الجزائري بجملة من الضوابط أبعادها، الإذن القضائي بالسرب من قاضي التحقيق أو وكيل الجمهورية، المادة 65 مكرر 11، وأيضا احترام المدة القانونية للتسرب[3].

---

[1]- محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 40.

[2]- القانون 06-22، مرجع سابق.

[3]- أنظر المادة 65 مكرر 11 من الأمر 66-155 المتضمن قانون الإجراءات الجزائية.

الفرع الأول: إجراءات التحري والاستدلال

المحقق أو المحتوى هو الشخص المكلف بإبراء التحري بواسطة الحاسب الإلكتروني عن المتحري عنه، سواء كان شخصا أو مكانا أو شيئا حسب طبعته، على المتحري أن يكون لديه استعداد وقدرة على إجراء مهامه وأن يميز من الحقائق والأقوال والآراء والاستنتاجات، حتى ل هذا الاستعداد لقدرات خاصة تساهم في قيام المتحري بمهامه بشكل سليم، من أهم السمات التي يجب أن تتوفر في المحقق يمكننا أن نذكر، دقة الملاحظة في تتبع للمهتمين والشهود أثناء التعامل معهم، سرعة الأداء، كتمان السر حتى لا يضر بمصالح الغير الترتيب والدقة والتأني وبذل العانية، الصبر، قوة الذاكرة.

المتحري المهني هو مأمور الضبط القضائي المسئول عن تلقي البلاغ وسماع الشهود وسؤال المتهمين، والمهارة الرئيسية التي يجب على المتحري تنميتها بالتدريب هي ترتكز في مهارات الاتصال التي أصبحت اليوم أساس أي تعامل أمني سواء على المستوى الشخصي أو العملي تنقسم هذه المهارة إلى 3 أقسام هي: الحديث إلى الغير، الإنصات، كتابة المحاضر.

وبما أن الحديث إلى الغير في مجال التحري يكون في حدود توجيه الأسئلة والاستفسارات، فيجب أن تكون مقنعة مليئة بالثقة، في حين أن كتابة المحاضر يجب أن تتميز بالوضوح والتسلسل المنطقي والإقناع لتصل إلى العدالة، كما أن الإنصات وحسن الاستعمال يساعد المتحري في اتخاذ القرارات المحبة[1].

أولا: تلقي البلاغات والشكاوي

1- تلقي البلاغات في الجريمة الإلكترونية:

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوي التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند وردها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب

[1]- محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 41.

على المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص المكاني أو النوعي بها، في حين أن الواجب اتخاذ الإجراءات المقرة بشأنها، تم إخطار جهة الاختصاص إحالة المحضر إليها.

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى إجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، كإبلاغها عن وجوه صفحات أو مواقع غير مشروعة بإرسال رسالة إلكترونية مثلا تتضمن التبليغ عنى وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال.

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ، يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ وقت تلقي البلاغ، المعلومات الخاصة، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة[1].

2- الشكوى في الجريمة الإلكترونية:

قد يترتب على الجريمة ضرر خاص قد يصيب أحد الأفراد ماديا أو معنويا، فينشأ له حق تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في قانون الإجراءات الجزائية أنه يحق لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص وقد عرفت الشكوى بأنها

[1]- محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 42.

البلاغ أو الإخطار الذي يقدمه المجني عليه أو ووكيله الخاص إلى السلطات المختصة طلبا تحريك الدعوى العمومية بشأن جريمة معينة.

ولقد خصصت العديد من المراكز لمعالجة هذه الشكاوي من بينها مركز نلقي الشكاوي عن جرائم الاحتيال عبر الإنترنت المؤسسة في فيرجينيا الغربية بالولايات المتحدة الأمريكية من طرف مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء من أجل مكافحة ظاهرة الاحتيال عبر الانترنت[1].

ثانيا: الاستجواب وسماع الشهود في الجريمة الإلكترونية

1- الاستجواب:

وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وان لم يقدر يجوز للمحقق أن يعين له محامي من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق.

2- سماع الشهود في الجريمة الإلكترونية:

سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية.

[1]- محمد بوعمرة، سيد علي بنينا، المرجع نفسه، ص 43.

الفرع الثاني: اجراءات التحقيق

عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما، فإنه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها إلا أنه تجدر الإشارة إلىأن مسرح الجريمة الإلكتروني بالإضافة إلى المسرح المادي يوجد مسرح إلكتروني متمثل في البيئة الإلكترونية التي يجد فيها المحقق صعوبة استخلاص الدليل منها، مما يدفعه بالاستعانة بالخبراء الفنيين في هذا المجال، في معاينة مسرح الجريمة أو القيام بالعمليات التفتيش والضبط وفحص آثار الجريمة، لا تشكل خللا فنيا أو قانونيا، كما هو الحال في التحقيق مع الشهو د والمتهمين، إذ أن أخذ أقوال الشهود واستجواب المتهمين يعتمد على خبرات المحققين، ويعتبر الاستجواب مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق، ومطالبته له بإدلاء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة الكشف عن الحقيقة واستظهارها بالطرق القانونية.

يمكن القول بصفة عامة أنه لا يوجد حتى الآن خبير معلوماتي لديه المعرفة المتعمقة في سائر أنواع الحسابات وشبكاتها، كما لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم، ولهذا يتمتع مأمور الضبط القضائي وكذلك المتحري بحرية كاملة حتى يتمكن من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها هو أنها مناسبة، ولذلك لأي منهما أن يندب الخبير يأنس فيه الكفاءة الفنية اللازمة لحل هذه المسألة[1].

أولا: التفتيش وضبط الأدلة

1- التفتيش: تتميز الجريمة الإلكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها و تتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم العادة الاخرى، نظرا لسرعة ارتكابها ومحو آثارها وتخطيها الحدود الوطنية.

[1]- محمد حزيط، مرجع سابق، ص 102.

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ماله علاقة بها أو بأفعالها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه يتكون من شقين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص[1].

2- ضبط الأدلة: هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط لم يكن في اغلب الأحيان هو غرض التفتيش وإن لم يكن له السبب الوحيد، فقد يتم الضبط استنادا لأسباب أخرى غير التفتيش من ذلك المعاينة وما يقدم المتهم والشهود لمأموري الضبط القضائي، لذا يرى جانب من الفقه أن الضبط ليس من إجراءات التحري بل من إجراءات الاستدلال خاصة إذا تم في مكان يجوز لسلطات الضبط دخوله مثل الأشياء التي يتم العثور عليها خارج المساكن أو في الطريق العام أو في الحقول أو غيرها.

والضبط لا يخرج من كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقارا أو منقولا الضبط حسب الأصل لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكومبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير مشروع أو إتلافه بوسائل تقليدية كالكسر، الحرق، لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وفي ضبط البيانات الكمبيوتر لعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثواني معدودات ولعدم معرفة كلمة السر أو ثغرات المرور أو ترميز البيانات[2]

[1]- محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 45.

[2]- مرجع نفسه، ص 45.

ثانيا: المعاينة وندب الخبراء في الجريمة الإلكترونية

1- المعاينة:

المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يري المحقق أن لها صلة بالجريمة، والأصل أن إجراء المعاينة متروك لتقدير المحقق، لا يقوم بها إلا إذا كمان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية ملتبس بها، يجب على القائمين بالمعاينة تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة و إخطاره مسبقا حتى يستعد من ناحية الفنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية[1].

2- ندب الخبراء:

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتثبيت عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.

الخبير هو كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء أو على مستوى المحاكم أم لا، وهو كل شخص له دراية بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستشير فيها خبراء كما هو الحال في تقرير الصفة التشريعية ف ي جرائم القتل أو تحليل المادة المطعمة في جريمة تسمم، أو فحص لخطوط الكتابة المدعي بتزويرها، ولما كان قاضي التحقيق هو المختص بالتحقيق، قد يتعرض في عمله

[1]- محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 46.

لمسائل فنية يصعب عليه كرجل قانون البت فيها، حينئذ يجوز له ندب أهل الخبرة، حتى يخرج التحقيق في صورة موضوعية صادقة[1].

المطلب الثاني

خصوصية إجراءات المحاكمة

تستهل المحكمة جلستها بالإعلان أولا عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسئول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها. وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة، وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر 6 مستحدثة بموجب الأمر 15 02 المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية تتخذ المحكمة إحدى الإجراءات التالية:

- ترك المتهم حرا

- إخضاع المتهم لتدابير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر 1 قانون الإجراءات الجزائية

- وضع المتهم في الحبس المؤقت

- مع الإشارة وأن هذه التدابير لا تقبل الاستئناف.

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفردي فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في اختيار محام الدفاع عنه فإن طلب ذلك أمهاه القاضي مهلة لا تقل عن ثلاثة أيام لتحضي دفاعه. ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده ويتم

[1]– محمد بوعمرة، سيد علي بنينال، المرجع نفسه، ص 47.

مناقشتها بالتفصيل من طرف القاضي و بعدها يقوم القاضي بسماع الشهود. وبعد الانتهاء من تحقيق تعطى الكلمة للطرف المدني فقط دون المطالبة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساها في الشق الجزائي فقط وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم التماساها، ويكون بعدها لنيابة العامة والمدعى حق الرد على مرافقة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميهم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق منطق بالحكم.[1]

الفرع الأول: القواعد العامة للمحاكمة

تنفيذ المحاكمة بمجموعة من المبادئ تنطبق على محكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية سنحاول شرحها على توضيح الاتي بيانه:

أولا: علانية الجلسة

جل التشريعات تقر بمبدأ علانية الجلسة، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الاطمئنان والشعور بالعدالة وهذا على التحقيق الأولي الذي تقوم به ضباط الشرطة القضائية وكذا التحقيق الابتدائي الذي تقوم به الجهات التحقيق، فكلاهم يتم في سرية، إلا أن العلانية ليست في جميع الجلسات بل القاضي سلطة تقديرية في إخراج القصر من الجلسة، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على نظام العام والآداب العامة، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية، ويحكم هذا المبدأ نص المادة 285 من قانون الإجراءات الجزائية الجزائري[2].

[1]– محمد بوعمرة، سيد علي بنينال، مرجع سابق، ص 48.

[2]– أنظر المادة 285 من الأمر 66–155، مرجع سابق.

ثانيا: شفوية المرافعات

فأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولا يتم الاكتفاء بالتحقيقات الأولية والابتدائية التي سبقت المحاكمة[1].

ثالثا: حضور أطراف الخصومة

لا يجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة لنيابة فهي جزء من التشكيلة.

رابعا: تدوين التحقيق النهائي

لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دورها يتجسد في تدوين كل ما يدور بالجلسة وفي الأخير نستنتج أن الجريمة الإلكترونية لم يخص لها إجراءات المتابعة خاصة بها وإنما تخضع نفس إجراء الجريمة التقليدية[2].

الفرع الثاني: تنظيم الأقطاب الجزائية المتخصصة

أصبحت الأقطاب الجزائية المتخصصة أمرا مهما لابد منه بعد الفترة العسيرة التي مرت بها، وذلك ما حدث في سنة 2008 من خلال قيام وزير العدل حافظ الأختام بتنصيب 4 أقطاب ممثلة في سيدي محمد وهذا بتاريخ 26 فيفري 2008، قطب جزائي بقسنطينة المنصب بتاريخ /03/ 03 2008، وتنصيب القطب الجزائي بوهران بتاريخ /05/ 03 2008.وأخيرا القطب الجزائي المتخصص بورقلة بتاريخ /19/ 03 2008، والتطرق أيضا إلى الجانب البشري المكون في إطار هيكلته وكذا التطرق إلى قواعد الاختصاص الذي خوله القانون لهذه الأقطاب المتخصصة.

[1]– محمد بوعمرة، سيد علي بنينال، مرجع يابق، ص 52.

[2]– مرجع نفسه، ص 52.

أولا: هيكلة الأقطاب الجزائية المتخصصة

في إطار دراستنا هيكلة الأقطاب الجزائية المتخصصة سنتطرق إلى الجانب البشري وهو الجانب الذي يمثلها ويقوم بتسيير أعمالها وكذا الجانب التقني، والهياكل القاعدية.

1- الجانب البشري:

ويعني هذا ابراز دور العنصر البشري الذي يتكون منه القطب، وبالتالي فالحديث يكمن هذا عن القضاة وكذا أمناء الضبط، فنجد أن جميع المعالم الجزائية موجودة في النظام القضائي الجزائي حيث تتكون من:

- قضاة التحقيق
- قضاة الحكم
- أمناء الضبط.

وباعتبار أن الأقطاب الجزائية هي أقطاب أو أجهزة تنتمي إلى القضاء الجزائي فهو يتكون من:

- وكيل الجمهورية.
- وكيل جمهورية مساعد.
- قاضيان للتحقيق على الأقل يشرفان على غرفة التحقيق.
- قاضي حكم يشرف على قسم تابع للقضاء الجزائي المتخصص.
- أمناء ضبط مكلفون بأعمال تنظيم الملفات ومساعدة القضاة[1].

[1]- ابتسام بغو، مرجع سابق، ص 73.

2- التكوين التقني:

ويقصد به خضوع القضاة والأمناء العاملين في القطب الجزائي إلى تأهيل خاص بهم من أجل التخصص والتعمق أكثر في مجال البحث والتحقيق في الجرائم والقضايا المعروضة عليها خاصة وأنها جرائم محددة على سبيل الحصر نظرا لخطورتها، ولذلك فهي تتطلب تكوين خاص.

فمنذ إنشاء وتأسيس هذه الأقطاب والنص عليها في القانون الجزائري فهي تعاني من عدم وجود تخصص فعلي في القضاة، يعني لا وجود لقضاة متخصصين في هذا المجال، لذلك نجد أن الدولة تسعى دائما إلى جعل القضاة متخصصين من خلال الدورات التكوينية في إطار سياسية التكوين المستمر للقضاة في مجال الأقطاب الجزائية المتخصصة قامت وزارة العدل بتنظيم دورات تكوينية لفائدة القضاة العاملين بالمحاكم الجزائية المتخصصة بالمدرسة العليا للقضاء من 03 إلي 07 ماي 2008.

3- التكوين القاعدي:

ويقصد به توفر جميع المرافق والأجهزة التي تستكمل بها الأقطاب الجزائية عملها من اجل تفعيلها، وتتمثل في مدى توافر المقرات وجاهزيتها، ولابد أن تكون مستقلة.

ثانيا: اختصاص الأقطاب الجزائية المتخصصة

تم النص في قانون الإجراءات الجزائية المعدل. في المواد 37، 40، 329 منه على توسيع الاختصاص المحلي لكل من وكيل الجمهورية، قاضي التحقيق وكذا المحكمة إلى دائرة اختصاص المحاكم الأخرى تحدد عن طريق التنظيم وذلك بخصوص 6 جرائم مذكورة على سبيل الحصر. ومن بينها الجريمة المعلوماتية (أو جرائم المساس بأنظمة المعالجة الألية للمعطيات) موضوع بحثنا هذا حيث تم انشاء محاكم أو أقطاب جزائية متخصصة ذات اختصاص إقليمي ومحلي موسع وهو ما سنعرضه من خلال ما يلي:

- الاختصاص المحلي.

- الاختصاص النوعي.

1- الاختصاص الإقليمي (المحلي):

تتميز الأقطاب الجزائية المتخصصة بأنها ذات اختصاص محلي موسع طبقا لقانون الإجراءات الجزائية، فقد تم تمديد الاختصاص المحلي لوكيل الجمهورية وقضاة التحقيق. وبصدور المرسوم التنفيذي رقم 06-348[1] والذي تم بموجب تحديد وتعيين المحاكم ذات الاختصاص الإقليمي ال1موسع وكذا الجهات القضائية لهذه المحاكم اليها. حيث تم تحديد هذه المحاكم كما يلي:

-القطب الجزائي بالجزائر (سيدي محمد) ويمتد اختصاصها الاقليمي إلى المجالس القضائية التالية :الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، أي 10 2 مجالس قضائية [2].

- القطب الجزئي بقسنطينة يمتد اختصاصه المحلي له ليشمل المجالس القضائية التالية: قسنطينة، أم 3 البواقي، بجاية، سكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، وبرج بوعريريج، أي 12 مجلس قضائي[3].

- القطب الجزائي بوهران ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية: وهران، بشار، 4 تلمسان، سعيدة، سيدي بلعباس، مستغانم، معسكر، غليزان، أي 09 مجالس قضائية[4].

---

[1]- الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم 06 -348 المؤرخ في 2006/10/05 متعلق بتمديد الاختصاص المحلي لبعض المحاكم أو وكلاء الجمهورية وقضاة التحقيق. الجريدة الرسمية العدد 63.

[2]- -أنظر المادة 02 من المرسوم التنفيذي 06-348.

[3]- أنظر المادة 03 من المرسوم التنفيذي 06-348.

[4]- أنظر المادة 05 من المرسوم التنفيذي 06-348.

-القطب الجزائي بورقلة، ويمتد اختصاصه الإقليمي ليشمل المجالس القضائية التالية، ورقلة، ادرار، تمنراست، إليزي وغرداية أي 5 مجالس قضائية ويتضح مما سبق ان الاختصاص الإقليمي الموسع للقطب الجزائي المتخصص يشمل جميع مراحل الدعوى العمومية ابتداء من جمع الاستدلالات الى المحاكمة [1].

ثانيا: الاختصاص النوعي

بمقتضى القانون 14/04 المؤرخ في 2004/11/10 المتضمن تعديل قانون الإجراءات الجزائية، وذلك في المواد 37، 40، 329 منه، والمادة 01 من المرسوم التنفيذي رقم 06-348 المتعلق بتحديد وتعيين المحاكم ذات الاختصاص الإقليمي الموسع جاءت بالجرائم التي تخضع لاختصاص تلك المحاكم، وجاءت على سبيل الحصر.

ثالثا: طرق اتصال القطب الجزائي المتخصص بالقضايا

إن المحاكم الجزائية ذات الاختصاص المحلي الموسع او الأقطاب الجزائية المتخصصة تخضع لمقتضيات ولقواعد متميزة.

وبالتالي إجراءات مختلفة عن تلك المتعلقة بالجهات القضائية الكلاسيكية، وهذا يتطلب توافر هذه الجهات القضائية المتخصصة على نوع جديد من التنظيم وقواعد جديدة للسير والاتصال بالقضايا متى اتضحت معالم الجريمة من حيث التكييف القانوني للوقائع والطابع المميز للجريمة ولذلك لابد من اللجوء الى الجهة القضائية المتخصصة وتفادي إحالة الملفات البسيطة والعادية على الجهات القضائية المتخصصة، وهو الشيء الذي تتميز به فهي تنظر فقط في الجرائم الخطيرة، ومن خلال ذلك لابد أولا من التطرق إلى كيفية إخطار واتصال القطب الجزائي بالقضايا .وإجراءات المطالبة من طرف النائب العام[2].

[1]- نظر المادة 04 من المرسوم التنفيذي 06-348

[2]- ابتسام بغو، مرجع سابق، ص ص 75-76.

1- اخطار الأقطاب الجزائية المتخصصة:

لكي يتم اتصال الأقطاب الجزائية المتخصصة بالقضية لابد من إجراءات حتى يعود لها الاختصاص للنظر فيها، وهذا لا يأتي إلا من خلال إخطارها وذلك عن طريق إجراء المطالبة بممارسة النائب العام فهذا الإجراء الذي يقوم به النائب العام له أثرين:

- ناقل للاختصاص.

- تخضع الضبطية القضائية للأجهزة القضائية المتخصصة مباشرة من حيث الإدارة لوكيل الجمهورية، الإشراف للنائب العام المراقبة لغرفة الاتهام الإنابة القضائية لقاضي التحقيق.

وقد نص قانون الإجراءات الجزائية في مواده 40 مكرر 01، 40 مكرر 02، 40 مكرر 03، 40 مكرر 04، و 40 مكرر 05 على كيفية سير هذه المحاكم ذات الاختصاص الإقليمي الموسع والكيفية التي تخطر بها بحيث لابد من إخبار وإخطار وكيل الجمهورية لدى المحكمة العادية فورا من قبل الضبطية القضائية بالواقعة حصول او حدوث جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات (جريمة معلوماتية) بهذه الجريمة في دائرة اختصاصه، ويبلغونه عن طريق نسختين من المحاضر التحقيق التي قاموا بها .

ثم يرسل وكيل الجمهورية النسخة الثانية الى النائب العام لدى المجلس القضائي التابعة له المحكمة ذات الاختصاص المحلي الموسع حسب ما جاء في المرسوم التنفيذي 06 -348 السابق ذكره. كما وجعلت جعل قانون الإجراءات الجزائية للنائب العام التابعة له المحكمة المختصة دورا محوريا وأساسيا في إخطار المحكمة المختصة بملف الجريمة المعلوماتية.

إذ للنائب العام وحده صلاحية طلب ملف القضية من الجهات القضائية الداخلة ضمن اختصاص القطب الجزائي، اذ اعتبر هذا الأخير ان الجريمة تدخل ضمن اختصاص.

2- المطالبة بالإجراء من النائب العام:

كما وسبق ذكره انه للنائب العام دور أساسي في مجال إخطار او المطالبة من القطب الجزائي الاختصاص في مجال الجريمة المعلوماتية وهو ما أكدته المادة 40 مكرر02 والمادة 40 مكرر 03 حيث انه يجوز للنائب العام لدى المجلس القضائي مطالبة الإجراءات في جميع مراحل الدعوى[1].

[1]-ابتسام بغو، مرجع سابق، ص ص 78-79

الخاتمة

لقد أضحى العالم اليوم يعيش في زمن التطور التكنولوجي أو ما يعرف بالثورة المعلوماتية، حيث أصبحت حياتنا اليومية تستدعي اللجوء إليها، فقد مكنت طرق المعالجة ا لكون التكنولوجيا عابرة للحدود الآلية المجتمعات من تجاوز فكرة الحدود الإقليمية، نظر. وأمام هذا التطور قد ارتبط به ظهور ما يعرف بالجريمة الإلكترو نية، وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب، الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات منة جهة وتمس بحرية الأفراد والمؤسسات من جهة أخرى.

يتبين لنا بعد تطرقنا لموضوع جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ان هذا النوع من الجرائم ذات الطابع المعلوماتي، تشكل خطورة على المحيط المعلوماتي، و ذلك بسبب اتخاذها لإبعاد كبيرة من حيث الاضرار التي تتسبب بها، و التي تؤثر بشكل مباشر على امن و سلامة الانظمة المعلوماتية، و التي تهدف أيضا و بشكل اساسي الى الغش و الاضرار بالمستخدمين. فبعد دراستنا لكل جريمة على حدى، توصلنا الى فكرة ان هذا النوع من الافعال غير المشروعة، نتميز بعدة خصائص، تختلف بها عن الجرائم التقليدية، و من اهم هاته الخصائص، عدم امكانية و عدم القدرة على حصرها. تطبيق احكام الجرائم التقليدية على جرائم المساس بأنظمة المعالجة الالية للمعطيات، لصعوبة تصنيفها لذا، اصبحت مختلف التشريعات تسعى للحد من هاته الانتهاكات، بالرغم من التحديات التي طرحت امامهم في الاطار القانوني، و التي من بينها طبيعة جرائم المساس بأنظمة المعالجة الالية للمعطيات الخاصة و كيان بيئتها غير المحسوس، و التي تظهر صعوبة فيما يتعلق بمهام السلطات، في اداء دورها للكشف عن الجريمة و البحث عن ادلتها، فقامت بإصدار احكام قانونية تنظم هاته الجرائم و تبين حدودها، و كذا تنفيذ اطار تشريعي قادر على تقليص ظاهرة الاجرام في مجال الانظمة المعلوماتية، و حماية المستخدمين لأجهزة الحاسب الالي من هاته الافعال، و كانت اولى تلك الاصدارات، "اتفاقية بودابست لمكافحة الاجرام المعلوماتي الصادرة في 2001، "و التي شهدت ميلادها في العاصمة المجرية *بودابست*، فهي تعد اولى التشريعات و الاتفاقيات الدولية التي تكافح جرائم الانترنت بجميع انواعها، و

التي مهدت لمختلف التشريعات الطريق لان تصدر قوانين مستحدثة، فعلى المستوى الوطني، كان اول نص تشريعي جزائري في مجال جرائم المعلوماتية في 2001، لمكافحة هاته الظاهرة الاجرامية، والمتمثل في المواد 144 مكرر 1، 144 مكرر 2 و المادة 146 من قانون العقوبات الجزائري، و الذي يليه تعديل قانون العقوبات بموجب القانون 15/04 الذي اضاف القسم السابع مكرر بعنوان الجزائري جميع جرائم المساس بأنظمة المعالجة الالية للمعطيات، بمختلف احكامها، و التي تمثلت "المساس بأنظمة المعالجة الالية للمعطيات"، و قد تضمن هذا القسم ثمانية مواد، تناول فيها المشرع في اربعة جرائم (جريمة الدخول والبقاء غير المصرح به، جريمة التلاعب بمعطيات الحاسب الآلي، جريمة التعامل في معطيات غير مشروعة)، و لم يتوقف المشرع الجزائري عند هذا الحد، بل قام بإصدار قوانين اخرى اهمها قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها و الذي الحق في وقت لاحق بالمرسوم الرئاسي رقم 15/261، الذي حدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجر ائم المتصل بتكنولوجيات الاعلام والاتصال و مكافحتها، و التي من بينها جرائم المساس بأنظمة المعالجة الالية للمعطيات.

لكن و بالرغم من كل هاته المجهودات المبذولة من طرف المشرع الجزائري، الا انه يبق بعيدا عن التطور القانوني الذي توصلت إليه باقي التشريعات الدو لية، سواء من ناحية إقرار القواعد القانونية المجرمة لهاته الجرائم او من ناحية أساليب مكافحتها.

ومن خلال دراستنا هذه توصلنا الى النتائج التالية:

- أن قانون الإجراءات الجزائية الجزائري ينص فقط على القواعد العامة التي تطبق على الجرائم التقليدية وكذا على المعلوماتية من خلال بعض الإجراءات الخاصة الممثلة في حجز المعطيات أو البيانات وكذا مراقبة الاتصالات الإلكترونية وحفظ البيانات.

- أن بعض الإجراءات تعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم الإلكترونية، كالمعاينة على المسرح الجريمة وكذا التفتيش الإلكتروني وضبط الدليل الرقمي والمستحدث هو إجراءات جديدة جاء بها تعديل قانون الإجراءات الجزائية الجزائري سنة 2006 التي تعرف بأساليب التحر ي حيث جاء بإجراءات لا تطبق إلا على الجرائم الإلكترونية كإجراءات المحاكمة التي يخص بها الأقطاب الجزائية المتخصصة وبالإضافة غلى إجراءات خاصة جاء بها قانون 09-04.
- بالرغم من وجود نصوص قانونية فإن مكافحة الجريمة الإلكترونية رهينة بالمعيقات الإجرائية في مجال المتابعات فإن أول إشكال أو عائق هو غياب القدرات التأملية والوسائل تلاف الفنية التي تتيح سرعة إدراك ما حصل، وأن غياب التأميل قد يؤدي إلى إتلاف الدليل وا مرتكبي هذه الجرائم من العقاب بالإضافة إلى مشكلات في القانون الواجب التطبيق كون الجريمة الإلكترونية عابرة للحدود.
- إن هذه الجريمة ومع تعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو بإستخدامه، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد والمجتمع وهي يضع مسؤولية كبيرة على ضباط تتسم بالغموض حيث يصعب إتباعها والتحقيق فيها مما الشرطة والقضاء.
- محدودية النصوص القانونية المتعلقة بجرائم المساس بأنظمة المعالجة الالية للمعطيات.
- قصور النصوص القانونية المتعلقة بهاته الجرائم من الناحية الاجرائية، مما يجعل من غياب جهات متخصصة في البحث و التحقيق عن هاته الجرائم.
- انعدام برامج و وسائل التوعية من مخاطر هذا النوع من الجرائم.
- عدم التشديد في العقوبات الموقعة على مرتكبي جرائم المساس بأنظمة المعالجة الالية للمعطيات.
- عدم وجود مختصين و خبراء في مجال المعلوماتية، قادرين على تشخيص الجريمة ذات الطابع المعلوماتي، سواء قضاة او شرطة قضائية او غيرهم.

- عدم توفير حماية جنائية تامة للأنظمة المعلوماتية كباقي التشريعات، و هو ما أدى الى انعدام الوضوح و الدقة في صياغة النصوص التشريعية المرتبطة بهاتة الجرائم انتشار هذا النوع من الجرائم بشكل كبير.
- اقرار عقوبات مخفضة مقارنة بالأضرار الناتجة عن هاته الجرائم.

قائمة المراجع

قائمة المراجع:

أولا: الكتب

1. أحمد أمين شوابكة، جرائم الحاسوب و الانترنت، الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر و التوزيع 2009.

2. أحمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري. طبعة، 4 دار هومة للنشر والتوزيع، الجزائر 2009.

3. أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء 2، طبعة 05، ديوان المطبوعات الجامعية الجزائر، دون سنة النشر.

4. أحمد هلالي عبد الاله، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، 2000.

5. أحمد، هلالي عبد اللاه، الجوانب الموضوعية و الإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

6. أسامة أحمد الناعسة، جلال الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، الأردن.

7. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه للطباعة والنشر والتوزيع، الجزائر، سنة 2007.

8. ايمن عبد الله فكري، جرائم نظم المعلومات –دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

9. بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، مصر، 2008.

10. الحسيني، عمر الفاروق، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية.

11. خالد عبد الحلبي، اجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة، 2001.

12. خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، 2009.

13. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب و ثغرات، طبعة 2010، دار الهدى للطباعة و النشر و التوزيع، عين مليلة الجزائر، 2010.

14. رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، 1994.

15. رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، أسيوط، 1994.

16. الصغير جميل عبد الباقي، القانون الجنائي و التكنولوجيا الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة.

17. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، الطبعة الأولى، دار الكتب القانونية، القاهرة، 2002.

18. عفيفي كامل، جرائم الكومبيوتر وجرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى، بدون ناشر.

19. علي عبد القادر قهوجي، الحماية الجنائية لبرامج الكومبيوتر، المكتبة القانونية، القاهرة 1999.

20. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.

21. محمود عبد الله، سرقة المعلومات في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002.

22. نائل عبد الرحمان، محاضرات في قانون العقوبات الأردني، (القسم العام)، الطبعة الأولى، دار الفكر للطباعة والنشر، عمان، 1995.

23. نائلة عادل محمد فريد قورة، جرائم الحساب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي، سوريا، 2005.

24. نبيل صقر جرائم الإلكتروني والأنترنت، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الجزائر، 2005.

25. نبيل صقر جرائم الإلكتروني والأنترنت، موسوعة الفكر القانوني، دار الهلال للخدمات الإعلامية، الجزائر، 2005.

26. نهلا عبد القادر المومني، الجرائم المعلوماتية، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

27. الهيتي محمد حماد، تكنولوجيا الحديثة و القانون الجنائي، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2004.

ثانيا: الرسائل والمذكرات

أ) رسائل الدكتوراه:

- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية أطروحة مقدمة لنيل شهادة الدكتوراه في علوم القانون، قسم القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان 2017-2018,

ب)مذكرة الماجيستير:

1. بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة)، رسالة لنيل الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، الأردن.

2. جدي نسيمة، جرائم المساس بالأنظمة المعالجة الآلية للمعطيات، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، الجزائر 2016-2017.

3. صغير يوسف. الجريمة المرتكبة عبر الانترنت. مذكرة لنيل شهادة الماجيستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

4. نسيم دردور، (جرائم المعلوماتية على ضوء القانون الجزائري والمقارن)، مذكرة لنيل شهادة الماجيستير في القانون الجنائي، كلية الحقوق، جامعة متنوري، قسنطينة، الجزائر.

ج) مذكرة الماستر:

1. ابتسام بغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، ام البواقي، 2016/2015.

2. الدزيري هيبة، جريمة الدخول غير المشروع لنظام المعالجة الالية للمعطيات، مذكرة لنيل شهادة الماستر، ميدان الحقوق والعلوم السياسية، قسم القانون العام، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم 20-06-2020.

3. محمد بوعمرة، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، قسم القانون الخاص، تخصص قانون

أعمال، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة 2019-2020.

ثالثا: المجلات والملتقيات العلمية

أ) المجلات:

- دمان ذبيح عماد، بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 13 جانفي 2020، جامعة عباس لغرور خنشلة، جامعة محمد لمين دباغين سطيف2020.

ب) المقالات:

1. حمودي ناصر، الحماية الجنائية لنظم المعالجة الآلية للمعطيات، قسم القانون العام، كلية الحقوق، جامعة البويرة.

2. يونس عرب، جرائم الكومبيوتر و الأنترنت، ورقة عمل مقدمة إلى الأمن العربي، 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية.

ج) الملتقيات:

- عطاء الله فشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، ليبيا، اكتوبر، 2009.

رابعا: النصوص القانونية

أ) القوانين:

- قانون 09-04مؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ب)الأوامر:

1. أمر 66-156 المؤرخ في 18 صفر عام 1386 الموافق ل 08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.

2. الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق ل 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

خامسا: الاتفاقيات الدولية

1. إتفاقية بودابست اتفاقية بودابست (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 08-11-2001 المتعلقة بالجريمة المعلوماتية تبنت الشروع أيضا في المادة 11 في الفقرة الثانية من الفصل الخامس منها والمعنون بأشكال أخرى للمسؤولية والجزاءات.

فهرس

المحتويات

فهرس المحتويات:

شكر وتقدير ..... /
إهداء..... /
مقدمة 1
الفصل الأول: طبيعة جرائم المعالجة الآلية للمعطيات.....6
المبحث الأول: ماهية جرائم المعالجة الآلية للمعطيات 7
المطلب الأول: مفهوم جرائم المعالجة الآلية للمعطيات.....8
الفرع الأول: تعريف جرائم المعالجة الآلية للمعطيات.....9
أولا: الاتجاه الذي يضيق مفهوم جرائم المعالجة الآلية للمعطيات 11
ثانيا: الاتجاه الذي يوسع مفهوم جرائم المعالجة الالية للمعطيات 12
الفرع الثاني: خصائص جرائم المعالجة الآلية للمعطيات 14
أولا: جرائم المعالجة الآلية للمعطيات متعدية الحدود (جريمة عابرة الدول) 14
ثانيا: صعوبة اكتشاف جرائم المعالجة الآلية للمعطيات 17
ثالثا: صعوبة إثبات جرائم المعالجة الآلية للمعطيات 19
رابعا: أسلوب ارتكاب جرائم المعالجة الآلية للمعطيات 21
خامسا: جرائم المعالجة الآلية للمعطيات تتم عادة بتعاون أكثر من شخص.....22
سادسا: خصوصية مجرمي المعلوماتية 22
المطلب الثاني: صور جرائم المعالجة الآلية للمعطيات.....23
الفرع الأول: الصور البسيطة لجرائم المعالجة الآلية للمعطيات 24
أولا: جريمة الدخول أو/و البقاء غير مشروع داخل نظام المعالجة الآلية للمعطيات 24
الفرع الثاني: الصور المشددة لجرائم المعالجة الآلية للمعطيات 34
أولا: جريمة الاعتداء القصدي على النظام 34
ثانيا: جريمة الاعتداء القصدي على المعطيات.....36

المبحث الثاني: الجزاءات والعقوبات المقررة لجرائم المعالجة الآلية للمعطيات 39
المطلب الأول: العقوبات المطبقة على الشخص الطبيعي 39
الفرع الأول :العقوبات الأصلية المطبق على جريمة من جرائم المعالجة الآلية للمعطيات .39
أولا: جريمة الدخول والبقاء.....40
ثانيا: جريمة التلاعب بالمعطيات.....42
ثالثا: جريمة التعامل في معطيات غير مشروعة.....42
الفرع الثاني: العقوبات التكميلية 43
أولا: مصادرة الأجهزة والوسائل والبرامج المستخدمة.....43
الفرع الثالث: العقوبات المشددة.....45
المطلب الثاني: العقوبات المطبقة على الشخص المعنوي.....46
الفرع الثاني: عقوبة جريمة الاتفاق و الشروع الجنائي 48
الفصل الثاني: خصوصية جرائم المعالجة الآلية للمعطيات من حيث المتابعة.....52
المبحث الأول: خصوصية متابعة جرائم المعالجة الآلية للمعطيات من حيث الوسائل
والأجهزة.....53
المطلب الأول: خصوصية من حيث أجهزة المتابعة.....53
الفرع الأول: تشكيل الضبطية القضائية.....53
أولا: ضباط الشرطة القضائية 54
ثانيا: أعوان الضبط القضائي.....55
الفرع الثاني: اختصاص الضبطية القضائية 56
أولا: الاختصاص المحلي.....56
ثانيا: الاختصاص النوعي 56
المطلب الثاني: الوسائل المستعملة في المتابعة.....57
الفرع الأول: الإجراءات المادية.....57

أولا: المعاينة التقنية.....57
ثانيا: التفتيش المعلوماتي (التفتيش في بيئة تقنية).....62
ثانيا: ضوابط التفتيش.....67
الفرع الثاني: الإجراءات الشخصية.....69
أولا: الخبرة الخبرة.....69
ثانيا: مهام الخبير.....70
ثالثا: مجالات الخبرة بالنسبة للجرائم المعلوماتية.....71
رابعا: ضوابط الخبرة.....73
أولا: تعريف الشاهد المعلوماتي.....74
ثانيا: من هو الشاهد المعلوماتي؟.....75
ثالثا: التزامات الشاهد في الجريمة المعلوماتية.....75
رابعا: شروط الشاهد بالإعلام عن الجريمة المعلوماتية.....76
ثالثا: ضبط الدليل الرقمي.....76
ثالثا: التسرب.....79
المبحث الثاني: خصوصية متابعة جرائم المعالجة الآلية للمعطيات من حيث إجراءات المتابعة.....83
المطلب الأول: خصوصية إجراءات التحري والتحقيق.....84
الفرع الأول: إجراءات التحري والاستدلال.....85
أولا: تلقي البلاغات والشكاوي.....85
ثانيا: الاستجواب وسماع الشهود في الجريمة الإلكترونية.....87
الفرع الثاني: اجراءات التحقيق.....88
أولا: التفتيش وضبط الأدلة.....88
ثانيا: المعاينة وندب الخبراء في الجريمة الإلكترونية.....90

المطلب الثاني: خصوصية إجراءات المحاكمة.....91
الفرع الأول: القواعد العامة للمحاكمة.....92
أولا: علانية الجلسة.....92
ثانيا: شفوية المرافعات 93
ثالثا: حضور أطراف الخصومة.....93
رابعا: تدوين التحقيق النهائي.....93
الفرع الثاني: تنظيم الأقطاب الجزائية المتخصصة.....93
أولا: هيكلة الأقطاب الجزائية المتخصصة.....94
ثانيا: اختصاص الأقطاب الجزائية المتخصصة.....95
ثانيا: الاختصاص النوعي 97
ثالثا: طرق اتصال القطب الجزائي المتخصص بالقضايا 97
الخاتمة 101
قائمة المراجع.....106
فهرس المحتويات.....113