>وزارة التعليم العالي و البحث العلمي
جامعة الشيخ العربي التبسي
كلية الحقوق و العلوم السياسية
قسم الحقوق

مذكرة تخرج لنيل شهادة ماستر جنائي
الموسومة بـ:

إجراءات جمع الأدلة في مجال الجريمة المعلوماتية

إنجاز الطالب :
سفيان زعيري

الأستاذ المشرف :
عبد الوهاب بوعزيز

السنة الجامعية 2014-2015


بسم الله الرحمن الرحيم

الإهـــداء

بسم الله الرحمان الرحيم

الحمد لله الذي بنعمته تتم الصالحات وبتوفيقه تتحقق المقاصد والغايات

يا ربي لك الحمد حتى ترضى, ولك الحمد إذا رضيت, يا ربي لك الحمد كما ينبغي لجلال وجهك وعظيم سلطانك, والصلاة والسلام على من لا نبي بعده وعلى آله وصحبه .

أهدي ثمرة مجهودي إلى من كان بالأمس حاضرًا بالجوار, واليوم أبى واختفى عن الأنظار, إلهي إنتظر هذه اللحظة بفارغ الصبر شغفًا لمقاسمتي فرحتي روح أبي الغاليقدامًا الله تعالى له بالرحمة والمغفرة وأن يسكنه فسيح جناته مع النبيين والصديقين والشهداء. آمين يا رب .

إلى الشمعة التي أضاءت حياتي, إلى من وهبت نفسها من أجل أن أصل إلى هدفي و مبتغاي وحملتني وهنًا على وهن, 'أمي الحبيبة 'أطال الله في عمرك وسدّد خطاك.

إلى اللذان اصطفاهم المولى الكريم لجواره, إلى اللذان لن أنساهم مهما طال زماني,

أخي : زهيري العربي رشيد, والصديق الذي علمني معنى الصبر والتحدي والأمل

الأستاذ الكريم : مروم بشير, طيب الله تعالى ثراهما, فهذه هي الدنيا لقاء ثم فراق

إلى كل أفراد عائلتي الكريمة كبيرًا وصغيرًا وخصوصًا إبنة أختي جيهان ...

إلى الأستاذ المشرف : بوعزيز عبد الوهاب, والأساتذة : جديدي طلال, زواي حكيم, شاكرًا إياهم مجهوداتهم الجبارة وآرائهم النيرة ومساهمتهم الفعالة في هذا البحث.

إلى من ساعدني ومهد لي الطريق : رئيس أمناء الضبط ' بعلي سليمان, خذيري رضا ' والنائب العام السابق : موهوب محمد المهدي, وكافة زملائي وأصدقائي...

إلى كل أساتذتي الأجلاء بجامعة تبسة,من نهلنا العلم على أيديهم ...

وبإسم هؤلاء كلهم أبعث بألف تحية وألف سلام

إلى روح العلامة الشيخ محمد الغزالي, طيب الله ثراه ونفع الأمة بعلمه وتقاه

إلى كل معلم , معلمة ... تؤمن بأنها رسالة, وإلى كل طالب للعلم ينتفع وينفع غيره ومنه إلى كل ضمير حي ... يتألم ... ويؤمن بأنها قضية الجميع " الأرض العربية "

إلى الأرواح التي آمنت برسالتها وأدركت سبيلها ...

شكـــــر وعرفـــــان

الحمد لله الذي وفقني وهدى خطاي لإنجاز هذا البحث الذي تم بفضله وعونه ولولاه لما وصلت إلى ما أنا فيه الآن، فالحمد لله أولاً وآخراً ...

قال تعالى ش"لَئِن شَكَرتُم لأَزِيدَنَّكُم " الآية 07

وقال سيدنا محمد عليه أفضل الصلاة والسلام : " من لا يشكر الناس لا يشكر الله "

عرفاناً بالجميل أتقدم بأسمى عبارات التشكر والتقدير لأساتذتي الأفاضل الذين كان لهم الفضل الكبير علي ولا يسعني من بعد ما بذلوه من أجلي إلاّ أن أقدم لهم شهادة تقديـر وعرفـان ...

كما لا أنسى الأستاذ جديدي طلال الذي حرص على تتمة بحثي, وسهر على الإشراف على هذا العمل إلى آخر نقطة من نقاطه ...

وأن أتقدم بالشكر الجزيل للأستاذ المشرف " بوعزيز عبد الوهاب " الذي كان لي نعم العون والسند والمرشد والموجه والذي مهما شكرته فلن أوفيه حقه ...

كما أتقدم بخالص الشكر لأساتذتي الأفاضل: الدكتور سعدي حيدرة , والأستاذ كعنيت محمد والأستاذ المشرف بوعزيز عبد الوهاب, اللذان سوف يتشرفا على مناقشتي في هذه الدراسة المتواضعة ... أدامكم الله ورعاكم

كما أتقدم بالشكر الجزيل لكلّ الأساتذة الكرام الذين ساهموا في تكويني عبر مسيرتي الدراسية... وأبعث إليهم تحية تقدير واحترام.

كما لا يفوتني أن أشكر كل من : رئيس أمناء الضبط بعلي سليمان, خذيري رضا, اللذان ساعداني ومهد لي الطريق.

إلى الأستاذ الفاضل والمحترم " زواي حكيم "

وإلى كل من قدم لي يد المساعدة من قريب أو بعيد في إعداد هذه المذكرة له خالص التقدير والاحترام... فلكم مني جزيل الشكر

مقدمـــــة

ممّا لا شك فيه أن التطورات الحديثة في مجال الثورة المعلوماتية,أدّى إلى انتشار استخدام الحاسوبومن ورائه شبكات المعلومات، ممّا انجر عنه في الكثير من الأحيان إساءة الاستعمال بوجود سلوكات غير مشروعة، بل وصل الحد لإطلاق وصف التجريم عليها طالما أن تلك السلوكات تمس بالأشخاص أو الأموال وحتى أمن الدول والمجتمعات...

ونتيجة لذلك حاولت جلّ التشريعات رصد نصوص قانونية تساير التطور المذهل لوسائل الاتصال وفي مقدمتها الإلكترونية، الأكثر من ذلك حاولت أخرى تفريد مدونات لأجلها، حتى باتت تشكل جريمة مستقلة بذاتها يطلق عليها بالجريمة المعلوماتيـة.

وعطفا على ذلك, أضحى التخصص ضرورة ملحة بالنسبة للأجهزة القائمة على متابعة الجريمة والحدّ منها، سواء تعلق الأمر بقضاة النيابة العامة والحكم أو الضبطية الإدارية والقضائية, ولعلّ الأخيرة تلعب الدور الأساس في الكشف عنها.

ومن ثم كان لازماً مسايرة قانون الإجراءات الجزائية للمهام المناطة بهم في هذا المجال، حيث طالت يد المشرع بالتعديل والتتميم العديد من المواد بموجب القانون 04-14[1] و06-22[2] وفضلاً على ذلك جاءت نصوص خاصة -بالنظر لاصطدام عمل رجال القضاء وأعوانه بحريات الأفراد وسريات المراسلات مهما كانت طبيعتها- تجسدت في القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

أهمية الدراسـة :

تتجلى لنا أهمية دراسة موضوع إجراءات جمع الأدلة في مجال الجرائم المعلوماتية, في كبر حجم هذه الجرائم منذ الوهلة الأولى لظهورها, وذلك لتنوع أساليبها وتعدد اتجاهاتها حتى صارت من مصادر التهديد البالغة لأمن الدولخصوصاً تلك التي تتركز مصالحها على المعلوماتية وتعتمد

---

[1]- القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 155/66, والمتضمن قانون الإجراءات الجزائية, الجريدة الرسمية, العدد 71 الصادرة بتاريخ 10 نوفمبر 2004.

[2]- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 155/66, والمتضمن قانون الإجراءات الجزائية, الجريدة الرسمية, العدد 84 الصادرة بتاريخ 24 ديسمبر 2006.

[3]- القانون رقم 09-04 المؤرخ 2009/08/05،والمتضمن القواعد الخاصة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47 الصادرة بتاريخ 2009/08/16، ص5.

عليها في سير شؤونها, كما أن ظهور هذه الأنواع منالجرائم المعلوماتية أدّى إلى تبلور أنماط جديدة من الإعتداءات على الحقوق والمصالح التقليدية بتفكيك معلوماتي جديد, كاختراق شبكة المعلومات وتشويه صورة الأشخاص, وتزييف العملةوا ٍتلاف البرمجيات, وتدمير وسرقة المعلوماتفكان لا بـُدّ من مواجهة هذا النوع من الجرائم بتطوير وسائل إثبات تلك الجرائم بما يواكب تلك الطفرة الهائلة التي حدثت في الجرائم المعلوماتية, وما يستلزمه من ضرورة قبول الأدلة الناتجة عن الحاسوب في الإثبات الجنائي, حيث أن القواعد التقليدية لم تعد تفي بالغرض لإثبات الجرائم المعلوماتية بالنظر لتطور هذه لجرائم وعدم مواكبة القوانين الإجرائية التقليدية لهذا التطور.

حيث يتبين لنا, أنه لا مجال للشك لمدى أهمية دراسة هذه الظاهرة الإجرامية المستحدثة, والتي أصبحت تقرع في جنباتها أجراس الخطر, وتنبه مجتمعات العصر الراهن لحجم مخاطرها وهول خسائرها الناجمة عن الإعتداءات التي تستهدف المعطيات بدلالتها التقنية الواسعة.

أسباب اختيار الموضوع :

من الأسباب التي دعتنا إلى تناول مثل هذا الموضوع :

أسباب ذاتيـة :

- الرغبة الشديدة والملحة في معرفة ما يحتويه هذا الصنف الحديث من الجرائم والتعمق أكثر في خفاياه.
- ضرورة تطوير وسائل الإثبات الجنائي بما يواكب التطور الهائل الحاصل في مجال الإجرام المعلوماتي, فأصبح من المهم للسلطات القضائية أن تتعامل مع أشكال جديدة من الأدلة في مجال الإثبات الجنائي.

أسباب موضوعية :

- حداثة الموضوع, فهذه الظاهرة (لإجراءات الوقائية من جرائم المعلوماتية) فرضت نفسها مؤخر ًا على الساحة الوطنية والدولية.
- خطورة هذا النوع من الجرائم, إذ تكمن في صعوبة إكتشاف مرتكب الجريمة المعلوماتية, كما أن آثارها تمس بالفرد والدولة على حدّ السواء.
- إنفراد الجريمة المعلوماتية بإجراءات خاصة متميزة عن تلك الإجراءات المطبقة على الجريمة التقليدية.

الإشكاليـة :

إن تضارب الحقوق في مجال الجريمة المعلوماتية بين حقوق تتعلق بالصالح العام تتمثل في حق المجتمع في توقيع العقاب على الذين يسعون إلى زعزعة الاستقرار الاجتماعي، وبين حقوق للمتهم تبتدئ بسرية استخدام وسائل نقل المعلومات وتنتهي عند الحق العام المتمثل في قرينة البراءة إلى غاية إثبات العكس، وعليه فإن التحري والتنقيب الذي تضطلع بها الضبطية القضائية في مرحلة جمع الأدلة تصطدم بلا ريب بهذه الحقوق، **فيا ترى كيف وازن المشرع الجزائري في مرحلة جمع الأدلة بين حقوق المتهم وصلاحيات الضبطية القضائية؟**

منهـج الدراسـة :

لقد لعبت طبيعة دراسة الموضوع دور ًا رئيسي ًا ومهم ًا في اختيار منهجية البحث, إذ إعتمدنا في دراستنا هذه المناهج الآتيـة :

1.المنهـج التحليلي : لأننا تعرضنا لمناقشة الإشكاليات القانونية التي تطرحها مواجهة الجريمة المعلوماتيةوا يجاد الحلول المناسبة على ضوء ما هو سائد في الفقه والتشريع والقضاء المقارن.

2.المنهـج الوصفي : لأن في دراستنا اعتمدنا على وصف الجريمة المعلوماتية وأركانها وا جراءاتها.

3.المنهـج المقارن : لأننا تطرقنا لإبراز وتحديد خصائص كلّ من الجريمة المعلوماتية والجريمة التقليدية, وتحديد الفروق بينهما.

التصريح بالمحـاور الرئيسـة :

تطرقنا إلى هذا الموضوع من خلال تقسيمه إلى فصلين, فصل أول تناولنا فيه ماهية الجريمة المعلوماتية, لأضع القارئ الكريم في الصورة ثم أتدرج به في الفصل الثاني, إلى كيفية إثبات الجريمة المعلوماتية, وعليه أكون قد راعيت التسلسل المنطقي القاضي بالانتقال من العام إلى الخاص ليس بخصوص المحاور الرئيسة بل في جميع تفاصيل دراستي وهو ما تشهد عليه المعالجة التالية:

الفصـل الأول : ماهيـة الجريمة المعلوماتيـة

انطلاقاً من كون الجريمة ظاهرة اجتماعية ظهرت بظهور الإنسان وارتبطت ارتباطاً وثيقاً به, وأصبحت بذلك الوجه السلبي الذي ينتقل عبر العصور التي يتطور فيها الإنسان, فكان من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق, لذلك اُعتبرت الجرائم المعلوماتية في الوقت الحالي أبرز تطور للجريمة، باعتبارها أثراً من الآثار السلبية التي خلّفتها التقنية العالية, كونها تطال في اعتداءاتها قيماً جوهرية تخص الأفراد والمؤسسات والدول في كافة نواحي الحياة, الاقتصادية, الثقافية, الأمنية. كما أن هذه الجرائم تركت في النفوس شعوراً بعدم الأمان, وغياب الثقة, الأمر الذي يؤدي إلى تهديد هذه التقنية على حياة الأفراد وأمنهم.

ومن ثم فإن حداثة الجريمة من جهة, ومن جهة أخرى تشعب مجالات وآليات, جعل من الفقه يقف عند صعوبات, وتباينات بشأن وضع تعريف لها جامع مانع واستخلاص أركانها وخصائصها، لذا أحاول من خلال هذا الفصل في مبحثين,تناول الإطار المفاهيمي لهذه الجريمة, من خلال تعريفها والطبيعة القانونية لها وأبرز خصائصها والأركان التي تقوم عليها الجريمة المعلوماتية, ثم في المبحث الثاني نتطرق إلى دراسة أهم أنواع الجريمة المعلوماتية.

المبحث الأول: مفهوم الجريمة المعلوماتيـة

وقد أدّى التقدم في عالم الكمبيوتر وهندسته وشيوع استعماله من فئات المجتمع كافة, العمرية منها والوظيفية,إلى تحوير الأهداف السامية المعدّة لها, الأمر الذي استنهض أفعالاً من شأنها أن تتصف بالطابع الجرمي, بل وصل الأمر إلى تشكيلها أفعالاً إرهابية وتدميرية فكرياً وأمنياً, حيث تمّ استخدام شبكة الإنترنت لأهداف سياسية للترويج للمعلومات والأفكار والأيديولوجيات التي تتلائم مع مصالحهم,ممّا يؤثر في الأفكار السياسية بحيث يؤثر طرف ضدّ الطرف الآخر ممّا يخلق جرائم سياسية قد تمس بأمن الدولة مثل تنظيم داعش الإرهابي[1] .

هذا الأمرحتّم على الباحث العلمي الحقوقي التصدي لها بالتحليل والتنقيب ولاسيما في مجال بيان كنهها ممّا يجعلنا نتتبع خطاه عبر مطلبين بداية برصد الآراء حول تعريف الجريمة المعلوماتية وتحديد طبيعتها كمسألة أولية ثم بصدد المطلب الثاني نجلي خصائصها.

المطلب الأول: تعريف الجريمة المعلوماتيـة وطبيعتها القانونية

الجريمة المعلوماتية نوع جديد من الإجرام المعاصر, تثير الكثير من المشكلات من نواحي عديدة, فهذا النوع من الإجرام يتّسم بالمكر والحيلة والدهاء والغش والإحتيال باستخدام تقنيات معلوماتية عالية الكفاءة والتي أصبحت لسهولة استخدامها وسرعة انتشارها من الوسائل لارتكاب هذه النوعية من الجرائم,فالجريمة المعلوماتية تتّم في بيئة أو إطار, لا علاقة له بالأوراق أو المستندات وإنّما عن طريق الحاسب الآلي, أو شبكة المعلومات الدولية - إنترنت -, فقبل الخوض في تحليلها لا بُدّ من تعريفها أولاً وهذا ضمن الفرع الأول,تليها الطبيعة القانونية لها وهذا كفرع ثانٍ .

---

[1] عرّف هذا التنظيم المتطرف في البدء بـ "الدولة الإسلامية في العراق والشام" المعروفة اختصاراً بـ داعش, يتبنى التنظيم الفكر السلفي الجهادي, يهدف أعضاؤه إلى إعادة "الخلافة الإسلامية وتطبيق الشريعة حسب ظنّهم", تعود جذوره إلى فرع تنظيم القاعدة "قاعدة الجهاد في بلاد الرافدين",نشر تنظيم داعش الإرهابي تهديداً على أحد المواقع الإلكترونية بقتل "جاك دورسي" أحد الذين شاركوا في تأسيس موقع (تويتر) للتواصل الإجتماعي عام 2006 ويشغل حالياً منصب رئيس المجلس التنفيذي للموقع,ويذكر أنه تمّ رصد نحو 46 ألف حساب على موقع تويتر إستخدمها متعاطفون مع تنظيم داعش خلال ثلاثة أشهر فقط, فضلاً عن الأساليب المختلفة التي تعتمدها تلك التنظيمات الإرهابية عن طريق المواقع الإلكترونية لكي تستدرج الشباب ليقاتلوا تحت رايات متطرفين,والنساء عموماً والفتيات الصغيرات أيضاً مثل (موجة جهاد النكاح) وكيف روج له هذا التنظيم,وكيف تمّ التغرير بنساء وفتيات (الموقع الرسمي لجريدة الفجر بتاريخ 2015/03/28 على الساعة 06:30 مساءً http:// www.elfagr.org).

الفرع الأول: تعريف الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات, فقد أصطلح على تسميتها بداية بإساءة استخدام الكمبيوتر, ثم احتيال الكمبيوتر, فالجريمة المعلوماتية, بعدها جرائم الكمبيوتر, والجريمة المرتبطة بالكمبيوتر, ثم جرائم التقنية العالية, إلى جرائم الهاكرز فجرائم الإنترنت وأخيراً السيبركرايم[1] .

تحتوي مصطلح الجريمة المعلوماتية على مصطلحين مختلفين من حيث المعنى والتكوين نفصل أولاً كلّ كلمة:

- **الجريمـــة** : هي كلّ عمل أو امتناع يجرّمه النظام القانوني ويقرر له جزاءاً جنائياً هو العقوبة, توقعه الدولة عن طريق الإجراءات التي رسمها المشرع[2] .
- **المعلوماتية** : يقصد بها ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات أو البيانات وتجميعها وتنظيمها واختزانها واسترجاعها ثمّ تفسيرها وإعادة بثّها واستخدامها, وهي عملية ديناميكية غاية في التعقيد تتّم بسرعة وبدقة متناهية بهدف إعادة توظيفها في مجال محدّد باستخدام رموز أو " كود " عند نقل أو بث المعلومات, هذا من ناحية التعريف اللغوي للجريمة المعلوماتية أمّا من الناحية الفقهية فقد أحاط بتعريفها الكثير من الغموض حيث تعدّدت الجهود الرامية إلى وضع تعريف محدّد جامع مانع لها, لكن الفقه لم يتفق على تعريف مُحدّد, بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلاّ جريمة تقليدية ترتكب بأسلوب إلكتروني, ويمكن بوجه عام تصنيفها إلى ثلاث فئات هي[3] :

أولاً / الفئة الأولى: تعريفات مرتكزة حول وسيلة ارتكاب الجريمة : يستند أصحاب هذا الإتجاه في تعريفهم للجريمة المعلوماتية إلى وسيلة ارتكاب الجريمة فيشترطون وجوب ارتكابها بواسطة الكمبيوتر, فالفقيه تايدمان يعرفها على أنها "كلّ أشكال السلوك غير المشروع (أو الضار بالمجتمع) الذي يرتكب باستخدام الحاسب الآلي ".

كما عرّفها توم فوريستر في مؤلفه عن قصة ثورة تقنية المعلومات تعريفاً يكاد أن يطابق

---

[1]- هلالي عبداللاه أحمد, إلتزام الشاهد والإعلام في الجرائم المعلوماتية, دراسة مقارنة, القاهرة, دون طبعة, دار النهضة العربية, 1997, ص 13.

[2]- عبد الحكيم رشيد توبة, جرائم تكنولوجيا المعلومات, , دار المستقبل, عمان, الأردن, الطبعة الأولى , 2009, ص 19.

[3]- سامي علي حامد عياد, الجريمة المعلوماتية وإجرام الإنترنت, دار الفكر الجامعي, الإسكندرية, دون طبعة، 2007، ص 38-40.

التعريف السابق بقوله "أنها فعل إجرامي تمّ باستخدام الحاسوب كأداة رئيسية ".

يُعرّفها أيضاً مكتب تقييم في الولايات المتحدة الأمريكية من خلال تعريف جريمة الحاسب الآلي بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً ", فالاعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكابها لها وليس فحسب إلى الوسائل المستخدمة لتحقيقها, وليس لمجرد أن الحاسب أستخدم في جريمة تعتبر من الجرائم المعلوماتية.

ثانياً / الفئة الثانية: التعريفات المرتكزة حول موضوع الجريمة : هناك مجموعة من التعريفات استندت إلى موضوع الجريمة وإلى أنماط السلوك محل التجريم, أي يستند أصحاب هذا الاتجاه في تعريفهم للجريمة المعلوماتية إلى وجوب أن يكون الكمبيوتر هو محل الجريمة, فيجب أن يتم الاعتداء على الحاسب الآلي أو على نظامه, ويمثل أنصار هذا الاتجاه الفقيه "روزمبلات " الذي عرف الجريمة المعلوماتيـة بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه "[1] .

كما عرفت أيضاً بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات "[2].

كما عرفها الأستاذ Artar Solerz "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات"[3].

كما عرفها مكتب المحاسبة العامة للولايات المتحدة الأمريكية GOA بأنها " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات, وإضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الكمبيوتر ", وعرفها الدكتور علي القهوجي بأنها " سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها "[4].

ثالثاً / الفئة الثالثة: التعريفات المستندة إلى وجوب إلمام الفاعل بتقنية المعلومات : ويستند

---

[1]- هشام محمد فريد رستم, قانون العقوبات ومخاطر تقنية المعلومات, مكتبة الآلات الحديثة, القاهرة, دون طبعة، 1995, ص 29-31.

[2]- هدى حامد قشقوش, جرائم الحاسب الإلكتروني في التشريع المقارن, دار النهضة العربية, الإسكندرية, القاهرة, الطبعة الأولى, 1992, ص 05.

[3]- خالد عياد الحلبي, إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت, دار الثقافة, عمان, الطبعة الأولى, 2011, ص 28.

[4]- علي القهوجي, الحماية الجنائية لبرامج الحاسوب, الدار الجامعية للنشر, الإسكندرية, دون طبعة, 1997, ص 02.

أصحاب هذا الاتجاه إلىمعيار شخصي يستوجب أن يكون الفاعل مُلمًّا بتقنية المعلومات واستخدام الحاسب الآلي, فهي تلك التي يكون لمقترفها معرفة كافية بالحاسوب ومشتملاته, وقد أورد الدكتور هشام رستم التعاريف المختلفة لأنصار هذا الإتجاه, منها تعريف"David Thompson" بأنها " أية جريمة يكونمتطلبًا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب "[1].

ومن التعريفات التي تقوم على أساس شخصية مرتكب الفعل, حيث عرفتها وزارة العدل الأمريكية بأنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تُمكنه من ارتكابها "[2], وأمام قصور التعريفات المؤسسة على معيار واحد, سواء القائمة على معيار قانوني موضوعي أو شخصي, برز عدد من التعريفات ترتكز على أكثر من معيار لبيان جريمة الحاسوب, فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف لجرائم الحاسوب على ما يلي " يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية, أو داخل نظام حاسوبي, والجريمة تلك التي تشمل من الناحية المبدئية, جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية "[3].

وهناك تعريفات أخرى تستند إلى معايير مختلفة وقد تعرضت للنقد باستثناء التعريف الذي إعتمده جانب كبير من الفقهاء والذي تبنته منظمة التعاون الإقتصادي والتنمية OCDE للجريمة المعلوماتية في إجتماع بباريس عام 1983 من أنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها "[4], وهو تعريف تبنى أكثر من معيار, حيث يتعلق الأول بوصف السلوكأمّا الثاني باتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

من خلال هذه التعريفات نقول أن تعريف الجريمة المعلوماتية يُؤسسإمّا على وسيلة ارتكابها أو على موضوعها والهدف منها وأخيرًا يُؤسس على الشخص المرتكب لها ومدى معرفته بتقنية المعلومات.

هذه أهم التعريفات التي يمكن أن تفي بغرض شرح ووضع مفهوم للجريمة المعلوماتية, لكن

1- David Thampson, Current trends in computer crime, control computer quarterly, Vol, n1, 1991, P2.

2- خالد عياد الحلبي, المرجع السابق, ص 30.

3- خالد عياد الحلبي, المرجع نفسه, ص 30.

4- سميرة معاشي, مجلة المنتدى القانوني, دورية تصدر عن قسم الكفاءة المهنية للمحاماة, جامعة محمد خيضر بسكرة, الجزائر, العدد السابع 2010, ص 279.

وباعتبار الموضوع حديث النشأة والبحوث حوله ما زالت في بدايته يمكن أن تكون هناك مستجدات حول مفهوم هذه الجرائم المتطورة بتطور وتقدم التكنولوجيا.

الفرع الثاني : الطبيعة القانونية للجريمة المعلوماتية

المعلومات, كلمة شاع استخدامها منذ الخمسينات من القرن الماضي في مجالات مختلفة وسياقات شتىممّا جعل لها في الاستعمال الدارج مفاهيم متنوعة ومتعدّدة, وهي من حيث اللغة مشتقة من كلمة "علم" ودلالتها فيها تدور بوجه عام حول المعرفة التي يمكن نقلها واكتسابها, فهي مجموع رموز يستخلص منها معنى معين في مجال محدّد وتتمتع بالتحديد والابتكار والاستئثار والسرية وعلى ذلك فهي ذات قيمة اقتصادية كسلعة تباع وتشترى وكمعطيات يمكن تبادلها بين الجهات ولها قيمة مالية , والمعلومات هي الأساس المكون للمعلوماتية, والمعلوماتية تعرف على أنها علم " معالجة الآلية للبيانات والمعلومات "[1], ومن هنا تتضح العلاقة بين الجريمة المعلوماتية والمعلوماتية والتي تدفع إلى طرح التساؤل التالي: ما هو الوضع القانوني للمعلومة؟ هل للمعلومة قيمة في حدّ ذاتها؟ أم العكس لها قيمة ما تتمثل في أنها مجموعة مستحدثة من القيم, ويرجع هذا التساؤل إلى أنه إذا كانت المعلومات لها قيمة وتعتبر من قبيل القيم القابلة للاستئثار, إذن يمكن الاعتداء عليها بأي طريقة كانت, ومن أجل ذلك, فقد انقسم الفقه إلى اتجاهين:

- **الاتجاه الأول:** يرى أن المعلومة لها طبيعة من نوع خاص.
- **الاتجاه الثاني:** يرى أن المعلومة ما هي إلاّ مجموعة مستحدثة من القيم.

لنرى ذلك بشيء من التفصيل :

أولاً / المعلومات لها طبيعة من نوع خاص : يرى الفقه التقليدي أن المعلومة لها طبيعة من نوع خاص وذلك انطلاقا من حقيقة أن وصف القيمة يضفي على الأشياء المادية وحدها, وبمعنى آخر أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الاستحواذ عليها, وبمفهوم المخالفة وبإعتبار أن المعلومات لها طبيعة معنوية فلا يمكن الاستحواذ عليها, إلاّ في ضوء حقوق الملكية الفكرية, ومهما كان الأمر فإنه مستقر يحدّد وجود خطأ عند الاستيلاء على معلومات الغير ولذلك فقد حاول هذا

[1] – أحمد خليفة الملط, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, دون طبعة، 2006, ص 103.

الاتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة,وذلك استناداً إلى حكم محكمة النقض الفرنسية " أن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استحواذي "[1].

ثانياً / المعلومات مجموعة مستحدثة من القيم[2] : يرى هذا الاتجاه الحديث أن المعلومات ما هي إلاّ مجموعة مستحدثة من القيم, ويعود الفضل في ذلك للأستاذين Catala و Vivant, حيث يذهب الأستاذ Catala إلى قابلية المعلومة المستقلة عن دعامتها المادية للاستحواذ, على سند من القول"أن المعلومة تقوم وفقاً لسعر السوق متى كانت غير محظورة تجارياً وأنها تنتج بصرف النظر عن دعامتها المادية عن عمل من قدّمها وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما "[3].

أمّا الأستاذ Vivant فيقدم لنا رأيه : "أن كلّ الأشياء المملوكة ملكية معنوية,والتي يعترف بها القانون, وترتكز على الإعتراف بأن للمعلومة قيمة, عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف "[4].

هذا ويرى الأستاذ الدكتور" محمد سامي الشوا " ويؤكد أن المعلومة, وبالنظر إلى حقيقتها الذاتية واستقلالها,فالمعلومة تُعدّ قيمة في ذاتها, ولها بالتأكيد مظهر معنوي ولكنها تملك قيمة اقتصادية مؤكدة, بحيث يمكن عن الاقتضاء أن ترفعها إلى مصاف القيم القابلة لأن تحاز حيازة مشروعة, وبذلك فهي مال قابل للتملك أو الاستغلال, على أساس قيمتها الاقتصادية وليس على أساس كيانها المادي, ولذلك فهي تستحق الحماية القانونية, ولما كانت البرامج في جوهرها معلومات معالجة بطريقة آلية ولها قيمة اقتصادية, فإنه يجب معاملتها معاملة المال.

---

[1]- محمد سامي الشوا, الجرائم المعلوماتية للتعدي على الذمة المالية للغير, بحث مقدم إلى مؤسسة الأعمال الإلكترونية بين الشريعة والقانون, كلية الشريعة والقانون وغرفة التجارة والصناعة, دبي, الإمارات العربية المتحدة, 10- 20 ماي 2003, ص 180.

[2]- محمدعلي العريان, الجرائم المعلوماتية, دار الجامعة الجديدة للنشر, الإسكندرية, مصر, دون طبعة، 2004, ص 11 - 38.

[3]- محمد سامي الشوا, المرجع نفسه, ص 182- 184.

[4]- محمد سامي الشوا, المرجع نفسه, ص 184.

المطلب الثاني: خصائص الجريمة المعلوماتيـة

عدّ تُ الجرائم المعلوماتية إفرازًا ونتاجًا لتقنية المعلومات, فهي ترتبط بها وتقوم عليها, فكلّما تطورت هذه التقنية كلّما تنوعت وازداد حجم الجرائم التي اتسع نطاقها في المجتمع, والسياسة الجنائية الحديثة استدعتمحاولة حصر خصائص الجريمة المعلوماتية والتي تتسم بلونًا وطابعاً قانونياً خاصًا يميزها عن غيرها من الجرائم - سواء التقليدية منها أو المستحدثة - بمجموعة من الخصائص قد يتطابق بعضها مع خصائص طوائف أخرى من تلك الجرائم.

تختلف الجرائم عن بعضها البعض من حيث طرق ارتكابها, كما تختلف باختلاف الوسائل المستعملة لارتكابها, فمنها ما يرتكب بواسطة السلاح, وهناك ما يرتكب بوسائل أخرى حديثة كالجرائم باستخدام الحاسوب, هذه الجرائم قد تستهدف الأشخاص وقد تستهدف الأموال.

من خلال ذلك نتناول في هذا المطلب فرعين, نعالج في الأول التمييز بين الجريمة المعلوماتية والجريمة التقليدية, وفي الفرع الثاني نذكر الفرق بين الجريمة المعلوماتية والجريمة الإلكترونية.

الفرع الأول: التمييز بين الجريمة المعلوماتيـة والجريمة التقليدية

سوف نتكلم في هذا الفرع عن الأركان التي تقوم عليها الجريمة المعلوماتية والجريمة التقليدية, والخصائص المميزة لكلّ منها وذلك كما يلي :

أولاً : أركان الجريمة المعلوماتيةو الجريمة التقليدية : إن أركان الجريمة جزء من ماهيتها وبانعدامها تنعدم الجريمة ولا يبقى مبرر للعقاب.

1/ الجريمة التقليدية :ما يهم في الجريمة التقليدية هو دراسة الأركان العامة ونوجزها كما يلي :

أ/ الركن المادي : المتمثل في العمل العضلي الذي يقوم به الجاني ويتألف من ثلاثة عناصر أساسية متمثلة في السلوك الإجرامي : " وهو الفعل الذي يأتيه الجاني ويحدث من خلاله أثر في العالم الخارجي ", النتيجة الضارة : " وهي ذلك الأثر المترتب عن السلوك الإجرامي "[1], والرابطة السببية بين السلوك والنتيجة : " أن ننسب النتيجة الضارة إلى السلوك الإجرامي ونسبة ذلك السلوك إلى شخص معين"[2].

---

[1]- منصور رحماني, الوجيز في القانون الجنائي العام, دار العلوم, عنابة, الجزائر, دون طبعة, 2006, ص 92.

[2]- سمير عالية, شرح قانون العقوبات– القسم العام–, المؤسسة الجامعية للدراسات, بيروت, لبنان, دون طبعة, دون سنة نشر, ص 206.

يرى شراح القانون بحسن تركتقدير السببية لقاضي الموضوع دائمً ا دون تقييده مقدما بافتراضات معينة لتعذر وضع قاعدة مطلقة لها[1].

ب/ الركن المعنوي : حيث يعبر الركن المعنوي على الناحية المعنوية للجريمة وبها تنسب إلى الفاعل ليتحمل المسؤولية عن تلك الأخيرة أو لا تنسب إليه, ويشمل الركن المعنوي القصد الجنائي أو العمد, والذي عرفه "أورتولان" بأنه : **"توجيه العمل أو الترك إلى إحداث النتيجة الضارة التي تتكون منها الجريمة"**.

كما يشمل الركن المعنوي كذلك الخطأ غير العمدي وهو حسب تعريف القضاء له: " **الخطأ هو كلّ فعل أو ترك إرادي تترتب عليه نتائج لم يردها الفاعل مباشرة ولا بطريق غير مباشر لكنه كان في وسعه تجنبها** "[2].

2/ الجريمة المعلوماتيـة : وأركانها هي كالآتي :

أ/ الركن المادي : يتمثل في الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

1- فعل الدخول : يقصد به الدخول الإلكتروني عن طريق الأساليب والوسائل التقنية المتاحة, كالدخول إلى مركز النظام المعلوماتي والإطلاع على المعلومات, ولم يحدد المشرع الجزائري الطريقة التي يتّم بها الدخول, وعليه فإن الجريمة تتحقق بأي وسيلة, ومن أكثر التقنيات استعمالا لتحقيق الدخول إلى النظام هي :

- ✓ استخدام البرامج المصممة أصلاً لاختراق أنظمة الحماية.
- ✓ الفخ,وهو عبارة عن منفذ يجهز به النظام مسبقً ا من قبل مصمم النظم ليسمح له لاحقً ا بإنزال برامج تعيق سير عمله.
- ✓ التخفي, ويعني انتحال صفة من له الحق في الدخول إلى النظام ثم الحصول على إمتيازاته في الإطلاع على المعلومات.
- ✓ التسلل, ومعناه التسلل وراء مستعمل مرخص له بالدخول إلى نظام معلوماتي وتَخط ِي حاجز الدخول[3].

1- رؤوف عبيد, مبادئ القسم العام من التشريع العقابي, دار الفكر العربي, القاهرة, مصر, دون طبعة, دون سنة نشر, 1979, ص 238 - 239.

2- رؤوف عبيد, المرجع نفسه, ص 346.

3- رامي حليم, "جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات", مجلة الدراسات والأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009, ص 229.

2- فعل البقاء يقصد به التواجد داخل النظام المعلوماتي ضدّ علم وإرادة من له الحق في السيطرة على هذا النظام، ومن الممكن أن تتحقق جريمة البقاء بمفردها دون جريمة الدخول وذلك في الحالة التي يكون فيها الدخول إلى نظام المعالجة بطريق الصفة أو الخطأ, أو في الحالة التي يكون فيها الدخول إلى النظام مشروعاً والبقاء فيه لمدة محدودة من الزمن يتعين عليه الخروج فوراً بانتهائها ومع ذلك يبقى الجاني داخل النظام[1].

ب/ الركن المعنوي : هو الحالة النفسية للجاني والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني, وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم, فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي,وأحياناً أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي[2].

لا يكفي لقيام الجريمة وجود الركن المادي وحده,بل لا بدّ من توافر إحدى الصورتين وهما: العلم والإرادة لدى الجاني أثناء قيامه بالفعل.

* **العلم :** أي أن يعلم الجاني أنه يعتدي على برنامج لشخص آخر[3].

* **الإرادة :** ليس بالضرورة أن يقصد المعتدي إلحاق الضرر بمؤلف البرنامج وأن تتجه إرادته إلى ذلك الفعل لقيام هذه الجريمة.

ثانياً: خصائص الجريمة المعلوماتية و الجريمة التقليدية : تتميز الجرائم المعلوماتية بطابع خاص يميزها عن نظيرتهاالجرائم التقليدية لصعوبة كشف وإثبات الجرائم الأولى دون الثانية.

1/ مميزات الجريمة المعلوماتية : تتميز الجريمة المعلوماتية بالآتي :

- ✓ تعتمد على الذكاء في ارتكابها.
- ✓ عدم ترك هذه الجرائم لأي أثر وصعوبة الاحتفاظ بها, هذا إن وجدت لها آثار أصلاً.
- ✓ قدرة الجاني على تدمير ما قد يعتبر دليلاً يمكن أن يستخدم لإدانته.
- ✓ إمكانية ارتكاب هذه الجرائم عن بعد.

1- رامي حليم, المرجع السابق, ص 230.

2- عماد مجدي عبد الملك, جرائم الكمبيوتر والإنترنت, دار المطبوعات الجامعية, مصر, دون طبعة, 2011, ص 37.

3- مسعود خثير, الحماية الجنائية لبرامج الكمبيوتر, دار الهدى, الجزائر, دون طبعة, 2010, ص 96.

- ✓ هي جرائم لا عنف فيها[1].
- ✓ هي جريمة تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.
- ✓ يلعب البعد الزمني والمكاني والقانوني دوراً هاماً في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.
- ✓ جرائم تتسم بالغموض يصعب إثباتها والتحقيق فيها[2].

2/ سمات الجريمة التقليدية : من سمات الجريمة التقليدية ما يأتي :

- ✓ الضرر, وهو المظهر الخارجي للسلوك حيث يؤدي إلى الإضرار بالمصالح الإجتماعية والإقتصادية وحتى الأمنية.
- ✓ الضرر يجب أن يكون مجرُماً قانوناً ومنصوص عليه في قانون العقوبات.
- ✓ توافر القصد الجنائي, وسبق التأكيد في ذلك على أهمية هذا الركن في الجرائم.
- ✓ وجود التوافق بين التصرف والقصد الجنائي.
- ✓ يجب توفر العلاقة بين الضرر المجرم قانوناً وسوء التصرف أو السلوك حتى يمكن تجريمه.
- ✓ النص على عقوبة الفعل المجرم قانوناً وهذا هو مبدأ الشرعيـة الذي ينص على أنه (لا جريمة ولا عقوبة إلاّ بنص).

هذه السمات تمّ إستخلاصها من خلال التعريف القانوني للجريمة التقليديـة.

الفرع الثاني: الفرق بين الجريمة المعلوماتيـة والجريمة الإلكترونيـة

نتيجة ازدياد استخدام شبكة الإنترنت في كثير من المعاملات الإلكترونية أصبحت مجالاً خصباً لكثير من الأفعال الإجرامية, والتي أطلق عليها الجريمة الإلكترونية تتميز بها عن الجريمة المعلوماتية, ولقد بدأت الجريمة الإلكترونية في الانتشار مع ظهور برامج قياس درجات الأمان في أنظمة الكمبيوتر حيث تمّ استخدام هذه البرامج لالتقاط المعلومات والتلاعب بأنظمة الكمبيوتر التي تحتوي عليها وذلك لأغراض غير مشروعة, ولا تختلف الجريمة الإلكترونية عن الجريمة المعلوماتية

---

[1] – جميل عبد الباقي الصغير, جرائم التكنولوجيا الحديثة, دار النهضة العربية, دون مكان نشر, دون طبعة, دون سنة نشر, ص 17.

[2] – حكيم سياب, " السمات المميزة لجرائم المعلوماتية عن الجرائم التقليدية ", مجلة الدراسات والأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009, ص 274- 275.

في كثير من الأحوال باستثناء أنها تتم عن طريق جهازي حاسوب أو أكثر متصلين فيما بينها عبر شبكة الإنترنت[1], ويمكن تفصيل كل منهما كما يأتي :

أولاً : الجريمة الإلكترونية : إن الجريمة الإلكترونية هي عبارة عن جريمة تقليدية تتطلب وجود الحاسب الآلي لارتكابهالأنه في حدّ ذاته موضوع للاعتداء, كإتلاف أو سرقة الجهاز نفسه أو شاشته, فهنا لا تكون أية مشكلة, لأننا أمام جريمة تقليدية ونصوص قانون العقوبات التقليدية كفيلة لردع الجاني, لأن الحاسوب هنا لا يتعدى كون من الأموال المادية المنقولةوتمرّ الجرائم الإلكترونية بثلاث مراحل أساسية هي:

1- **مرحلة إدخال البيانات** : مثال ذلك قيام المجرم الإلكتروني بتغيير أو تزوير البيانات مثل التسلل الإلكتروني إلى البيانات المتعلقة بفاتورة الهاتف قبل طبعها في شكلها النهائي حيث يتمكن من حذف بعض المكالمات من الفاتورة قبل طباعتها وا ٍرسالها.

2- **مرحلة تشغيل البيانات** : مثال ذلك قيام المجرم الإلكتروني بتغيير أو تعديل البرامج الجاهزة « software » التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة بطريق غير شرعي من قبل الجاني.

3- **مرحلة إخراج البيانات** : مثال ذلك سرقة بعض البيانات الإلكترونية أو المعلومات الآلية المتعلقة بمراقبة مخزون إحدى الشركات أو إفشاء معلومة متعلقة بإحدى الشركات أو إفشاء معلومة متعلقة بأحد العملاء[2].

ثانيًا : الجريمة المعلوماتية :

1/ الأساليب المستخدمة للاعتداء على مكونات الحاسوب : تتطلب معرفة فنية معينة يستطيع الجاني من خلالها القيام بعملية ما يسمى "بالسطو المسلح الإلكتروني" الذي يكون هدفه التقاط أو تسجيل المعلومات والبيانات المعالجة إلكترونيًا وهي في مرحلة انتقالها وبثها عن بعد, ويمكن عرض هذه الوسائل كما يأتي[3] :

---

[1]- خالد ممدوح, أمن الجريمة الإلكترونية, الدار الجامعية, الإسكندرية, مصر, دون طبعة، 2008, ص 56.

[2]- عماد مجدي عبد الملك, المرجع السابق, ص 37.

[3]- عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون, منشورات الحلبي الحقوقية, بيروت, لبنان, دون طبعة, 2003, ص 38.

أ-إلتقاط المعلومات التي توجد ما بين الحاسب والنهاية الطرفية: يحدث هذا الإلتقاط بواسطة توصيل خط تحويلة يعمل على تكبير الذبذبات الإلكترونية وا إرسالها إلى النهاية الطرفية التي تقوم بعملية التجسس وقد يحدث ذلك أيضا باستخدام جهاز مرسل صغير يمكنه نقل البيانات عن بعد.

ب- التوصيل المباشر بواسطة خط تليفوني : يمكن إحداثه بواسطة وضع مركز تصنت يجعل من تسجيل الاتصالات أمرا يسيرا كما يمكن كذلك وضع ميكروفونات صغيرة لأداء هذه المهمة.

ج- التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي : وتكمن خطورة هذه الوسيلة في أنها يمكن أن تؤدي إلى إعادة تكوين خصائص المعلومات التي تبث وتنتقل من خلال الأنظمة المعلوماتية وهذا لا يحتاج تسجيل الإشعاعات الصادرة من الحاسوب وحل شفرتها.

د- التدخل غير المشروع في نظام طرفية بعيدة : من شأن هذه الوسيلة أن يكون بالإمكان نسخ أو تدمير بعض البيانات والمعلومات أمرا يسيرا وهذا لا يحتاج إلى مجرد الحصول على حاسب آلي مايكرو ومودم مع ضرورة التعرف على كلمة السر أو مفتاح شفرة النظام[1].

2/ دور شبكة الإنترنت في الجريمة المعلوماتية : ثمة أدوار تلعبها شبكة الإنترنت في ميدان إرتكاب الجريمة المعلوماتية وهي على النحو التالي :

أ- قد تكون شبكة الإنترنت هدفاً للجريمة : كما في حالة الدخول غير المصرح به إلى أنظمة البيانات في مواقع إلكترونية معينة لتدمير المعطيات أو الاستيلاء على البيانات المخزنة.

ب- قد تكون شبكة الإنترنت أداة لارتكاب جرائم المعلوماتية : كما في حالة استغلال الإنترنت للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير.

ج- قد تكون هي البيئة التي ينمو في رحمها الإجرام المعلوماتي : كما في حالة إبرام اتفاقيات لترويج المخدرات وأنشطة الشبكات الإباحية والإرهابية وغسل الأموال[2].

من هنا نخلص للقول بأن الجريمة الإلكترونية هي نوع من أنواع جرائم المعلوماتية والتي تتمثل في برامج الحاسب الآلي ونُظمه لالتقاط بيانات ومعلومات معالجة إلكترونية والتلاعب بأنظمة

---

[1]- عفيفي كامل عفيفي, المرجع السابق, ص 39.

[2]-عبد الله عبد الكريم عبد الله, جرائم المعلوماتية والإنترنت, الجرائم الإلكترونية- دراسة مقارنة -, منشورات الحلبي, بيروت, لبنان, الطبعة الأولى, 2007, ص 20-21.

الحاسبات التي تحتوي عليها وذلك لأغراض غير مشروعة تتمثل غالباً في السرقة والإحتيال, وباستخدام هذه البرامج والتعرف على نقاط الضعف في نظام هذا الحاسب الآلي الخاص بالمجني عليه, فإن الجاني يستطيع أن يسيطر على نظام هذا الحاسب بأكمله, ثم يقوم بنشاطه غير المشروع, ويُحوَّل هذا النشاط في النهاية إلى مكاسب غير مشروعة وينتهي بمحو كل أثر يمكن أن يكشف عن أفعاله الإجرامية.

المبحث الثاني: أنـواع الجريمة المعلوماتيـة

من الصعوبة بمكان حصر وتعداد جرائم المعلوماتية,هذه الأخيرة التي تعرف تشعباً وانتشارا نظراً لتزايد استخدام الحاسبات وشبكات الإنترنت في مختلف المجالات, وبهذا المعنى يمكن القول أن الإنترنت كانت ساحة إجرام مثالية تتحدى الأجهزة الأمنية, فضلاً عن دور الحاسب الفعال في ارتكاب مثل هذه الجرائم,والتي تعدّ خطيرة مقارنة مع الجرائم التقليدية نظراً لصعوبة تحديد معالمها والحدّ من خطورتها, ومن أجل تيسير الأمور والوقوف إلى تحديد هذه التصنيفات فإننا قد ارتأينا في هذا المبحث دراسة أهم أنواع الجريمة المعلوماتية وذلك بتقسيمه إلى مطلبين, نتناول في المطلب الأول الجرائم المعلوماتية الواقعة على الأشخاص والأموال, ثم نتطرق في المطلب الثاني إلى الجرائم المعلوماتية الواقعة على أنظمة المعالجة الآلية للمعطيات.

المطلب الأول: الجرائم المعلوماتية الواقعة على الأشخاص والأموال :

إن الجرائم التي ترتكب على شبكة الإنترنت أو بواسطة استخدام الشبكة المعلوماتية متنوعة وكثيرة,وهي دائماً في ازدياد مستمر نتيجة التطور التكنولوجي المتواصل[1].

وجرائم المعلوماتية هنا يكون محل الاعتداء فيها هو الأشخاص والأموال,ويتّم هذا النوع من الجرائم بنفس سمات الجرائم العادية من حيث إلحاق الضرر بالآخرين أو الحصول على منفعة بغير وجه حق أو الخطر الذي يهدد الحقوق ذات القيمة المالية, فقد ارتأينا إلى تقسيم هذا المطلب إلى فرعين, نتناول في الفرع الأول الجريمة المعلوماتية الواقعة على الأشخاص, والجريمة المعلوماتية الواقعة على الأموال كفرعٍ ثانٍ .

---

[1]– أسامة عبد الله قايد, الحماية الجنائية للحياة الخاصة وبنوك المعلومات, دار النهضة العربية, القاهرة, مصر, دون طبعة، 1994, ص 48.

الفرع الأول: الجريمة المعلوماتية الواقعة على الأشخاص

سوف نتكلم في هذا الفرع على الجريمة المعلوماتية الواقعة على الأشخاص الطبيعية, والجريمة المعلوماتيةضدّ الأشخاص المعنوية وذلك كما يلي:

أولاً : الجريمة المعلوماتية الواقعة على الأشخاص الطبيعية :

لوحظ في الآونة الأخيرة وبعد فترة وجيزة من ظهور الحاسبات وشيوع استخدامها في كافة مجالات الحياة المختلفة إلى استخدام الحاسبات كوسيلة لتخزين بيانات متعددة تكون خاصة بالأفراد, ممّا يشكل تهديداً غير مسبوقاً لخصوصياتهم ويكون للأفراد الحق في السلامة من كلّ أذى يحيط بهم باعتبارهم مطلب أساسي ومشروع لمواجهة الإجرام التقني المستحدث, والمتمثل في شبكة الإنترنت التي يلجأ إليها المجرم المعلوماتي لتنفيذ رغباته الإجرامية في هذه البيئة[1].

1/ جرائم التهديد والقذف : من خلال تركيب العنوان نتعرض بداية للتهديد ثم القذف كالآتي:

أ/ جريمة التهديد وهو الوعيد بشرّ ويقصد به زرع الرعب والخوف في النفس بالضغط على إرادة الإنسان وتخويف من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له صلة بهم, ويجب أن يكون التهديد على قدر من الجسامة المتمثلة في الوعيد بإلحاق الأذى ضدّ نفس المجني عليه أو ماله, أو ضدّ نفس أو مال الغير الذين لهم صلة به, وقد يكون التهديد مصحوباً بالأمر أو طلب لقيام المهدد بفعل أو امتناع عن الفعل ومن كلّ ذلك إيقاع الذعر والقلق في نفس المجني عليه ممّا يؤدي بطبيعة الحال في بعض الحالات إلى التسبيب في وفاة المجني عليه نتيجة هذا الفعل المجُرّم.

ولقد أصبح الإنترنت, الوسيلة الحديثة لارتكاب جرائم التهديد بالقتل والتي في حدّ ذاتها تحتوي عدّة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة, وللأسف وجدت للجريمة وهي البريد الإلكتروني الذي بدوره سيتقبل كلّ ما يريده من رسائل سواء كتابة أو صورة المتضمنة تهديد بارتكاب جناية ضدّ نفسه أو ماله أو ضدّ الغير, أو لمجرد الانتقام أو التسلية بمشاعر الآخرين[2].

ب/ جريمة القذف والسب تعدّ جرائم السب والقذف الأكثر شيوعاً في نطاق الشبكة, فتستعمل للمساس بشرف الغير أو كرامته واعتباره,ويتّم السب والقذف عبر خطوط الاتصال المباشر أو يكون

---

[1]- عمر ممدوح خليل, حماية الحياة الخاصة في القانون الجنائي, دار النهضة العربية, القاهرة, مصر, دون طبعة، 1983, ص 207.

[2]- عمر ممدوح خليل, المرجع نفسه, ص 49.

مكتوباً أو عن طريق المطبوعات وذلك عبر المبادلات المعلوماتية, بحيث يستعمل الجاني عبارات بذيئة تمس وتخدش شرف المجني عليه, ومهما كانت الوسيلة المعتمدة مع علمه أن ما يقدم به يعدُّ مساساً بسمعة الغير, بل إن إرادته اتجهت لذلك بالذات, وبالتطور التكنولوجي أصبحت ترسل عبارات السب والقذف عبر البريد الإلكتروني, أو على صفحات الويب مما يؤدي بكل من يدخل هذا الموقع لمشاهدتها أو الإستماع إليها[1].

2/ الجرائم الجنسية وغير الجنسية : سوف نتناول كلّ واحدة في فقرة مستقلة.

أ/ جريمة التغرير والاستدراج :غالباً ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة, حيث يقوم المجرمون بإيهام ضحاياهم برغبتهم في تكوين علاقة صداقة على الإنترنت, والتي قد تتطور إلى اللقاء المادي بين الطرفين والقصد من ذلك هو ربط علاقات غير مشروعة, أو استخدام الأطفال في أغراض أخرى لا أخلاقية.

إن مجرمي التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر, وكون معظم الضحايا هم من صغار السن, فإن كثير من الحوادث لا يتمّ الإبلاغ عنها حيث لا يدرك كثير من الضحايا أنهم قد غُرّر بهم.

قد تكون جريمة الاستدراج عن طريق الإنترنت يأخذ شكل معين من خلال نشر وتسهيل واستضافة المواد الفاحشة عبر شبكة أو غرفة المحادثة أو ما يعرف بالفايسبوك بوجه عام, فيقوم المجرم بإرسال صور خليعة للضحية وإغوائه لارتكاب أنشطة جنسية غير مشروعة[2].

ب/ جريمة صناعة ونشر الإباحية : لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية وقد شجعتها بشتّى وسائل عرضها من صور وفيديو وحوارات بوضعها في متناول الجميع ولعلّ هذا يعدُّ أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا الإسلامي, وركّز المهندس حمد بن عبد العزيز مدير مركز أمن المعلومات بوحدة خدمات الإنترنت في مدينة الملك عبد العزيز للعلوم والتقنية على صناعة ونشر الإباحية عند تقسيمه لجرائم الإنترنت مما يحرض القاصرين على أنشطة جنسية غير مشروعة, وصناعة الإباحية, من أشهر

---

[1]- أسامة عبد الله قايد, المرجع السابق, ص 206.

[2]- منير محمد الجنبيهي و ممدوح محمد الجنبيهي, جرائم الإنترنت والحاسب الآلي وسبل مكافحتها, دار الفكر الجامعي, مصر, دون طبعة، 2004, ص 45.

الصناعات الحالية وأكثرها رواجا خاصة في الدول الغربية والآسيوية, كما أن هذه الجريمة مجرمة في كثير من دول العالم, خاصة تلك التي تستهدف أو تستخدم الأطفال[1].

أكثر من هذا فقد أوضحت بعض التقارير الصادرة من الولايات المتحدة الأمريكية أن هناك مشاهد جنسية يتّم عرضها عبر شبكة الإنترنت, وأن أكثر من (900,000) صورة تتعلق بالجنس تبث عبر هذه الشبكة من معلومات عن بيوت الدعارة في العديد من دول العالم, لذلك فإن بعض المؤسسات توفر عبر هذه الشبكة الأحاديث الهاتفية الحية التي تؤديها فتيات مدربات وذلك في مقابل الحصول على نسبة من عائد هذه المكالمات التليفونية.

كذلك فإن شبكة الإنترنت تتيح لمستخدميها إمكانية تخطي القيود المحلية المفروضة عليهم, وبالتالي يمكنهم الإطلاع على المواد التي فرضت الرقابة شروط معينة بالنسبة للحد الأدنى للسن المسموح له بالإطلاع عليها, ومن ذلك الأفلام التي لا يسمح بمشاهدتها سوى للكبار, وكذلك الصور التي تحذف من المطبوعات والمشاهد المعروضة لتناول موضوعات خارجة عن حدود القيم والتقاليد, وبالتالي فإن الشبكة تبطل فاعلية الرقابة المحلية على الأفلام والمصنفات, وتتيح للأفراد خاصة الأحداث منهم على مواد لا يجوز لهم الإطلاع عليها[2].

لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية عام 1998 تتعلق هذه الجر ائم بتحريض الأطفال على أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية للأطفال, وأن هذه الجرائم تشكل طائفة (Sexuolgring) تشمل ما يلي:

- ✓ لتحريض القاصرين على أنشطة جنسية غير مشروعة وا ٍفسادهم.
- ✓ تلقي ونشر معلومات عن القاصرين عبر الوسائل التقنية.
- ✓ نشر وتسهيل واستضافةالمواد الفاحشة بوجه عام عبر الإنترنت وللقاصرين تحديد ًا.
- ✓ نشر الفسق والمساس بالحياء (هتك العرض بالنظر).
- ✓ ترويج الدعارة بصورة قسرية للإغواء.

وهذه الأنشطة الجنسية الغير الأخلاقية تستهدف استغلال الضعف والانحراف لدى المستخدم

---

[1]- منير محمد الجنبيهي و ممدوح محمد الجنبيهي, المرجع نفسه, ص 46.

[2]- عبد الفتاح بيومي حجازي, الجريمة في عصر العولمة- دراسة في الظاهرة الإجرامية المعلوماتية-, دار الفكر الجامعي, الإسكندرية, الطبعة الأولى , 2007, ص 180.

والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية وبيعها.

3/ جريمة التشهير وتشويه السمعة : حيث يقوم المجرم بنشر أخبار قد تكون سرية ومضللة ومغلوطة عن ضحيته والتي قد يكون الفرد أو المجتمع أو دين أو مؤسسة تجارية أو سياسية تتعدد الوسائل المستخدمة في هذا النوع من الجرائم, لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة تحتوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين, ويضع هذه الجرائم كذلك تشويه السمعة, الشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد, قد يكون الهدف من ذلك هو الإبتزاز, نورد مثال على ذلك: ضبط المحاكم المصرية لمهندس كمبيوتر بتهمة نشر معلومات كاذبة على الإنترنت للتشهير بعائلة مسؤول مصري وتصميم موقع على الإنترنت, وقد كانت ابنة المسؤول أكثر عرضة للتشهير وتشويه سمعتها[1].

مثال ذلك أيضاً ما أكدته مصادر من فرقة الشرطة العلمية فرع محاربة الجريمة الإلكترونية بالجزائرأنها تسجل يومياً عشرات البلاغات والشكاوى من مواطنين راحوا ضحية نصب واحتيال, أبطالها منتحلو شخصيات سياسية وأخرى شعبية حوّلوا فضاء الفايسبوك لاصطياد الضحايا, كما عالجت نفس الفرقة التابعة للشرطة العلميةقضايا التشهير وإلحاق الأذى بالآخرين أخطرها ما وقع لأستاذة جامعية حين تم فتح حساب على الفايسبوك باسمها, وفبركة صورتها ووضع وجهها على جسد عار ثم وضع رقم هاتفها, وهو ما أحدث لها صدمة كادت أن تنتهي بحياتها, قضية أخرى تم معالجتها تخص فنانة تمّ تشويه صورتها ووضعها في أقبح وضعية, للمساس بشخصيتهاكذلك أيضاً تمّ خرق وكشف الحسابات المودعة في بنوك سويسرا لبعض الشخصيات السياسيـة[2].

4/ جريمة انتحال الشخصية : هيجريمة الألفية الجديدة كما سمّاها بعض المختصين في أمن المعلوماتوذلك نظراً لسرعة انتشار ارتكابها خاصة في الأوساط التجارية تتمثل في استخدام هوية شخصية أخرى بطريقة غير شرعيةوتهدف إمّا لغرض الاستفادة من مكانة تلك الهوية, أو إخفاء

---

[1] - محمد عبد الله أبو بكر سلامة, موسوعة جرائم المعلوماتية- جرائم الكمبيوتر والإنترنت-، منشأة المعارف, مصر, دون طبعة, 2006, ص 114.

[2] – أنظر: جريدة الشروق, الشروق تغوص في عالم الجريمة الإلكترونية بالجزائر, محتالون يؤسسون حكومة موازية على الفايسبوك, الخميس 02 أفريل 2015, العدد 4695, ص 16.

هوية شخص مجرم لتسهيل ارتكابه جرائم أخرى, إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل, وهذه هي أكبر سلبيات الإنترنت الأمنية والتغلب على هذه المشكلة فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت, كالتجارية في الاعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي التي تجعل من الصعب ارتكاب هذه الجريمة[1].

ثانياً: الجريمة المعلوماتية الواقعة على الأشخاص المعنوية : إن شبكة الإنترنت لم يعدّ دورها ينحصر فقط في تلقي المعلومات الهائلة التي يمكن لكلّ مستخدم أن ينتفع به بكلّ سهولة نظراً لسرعة البحث في عدّة مجالات مختلفة, فقد أصبحت شبكات الاتصال تعمل من خلال بروتوكولات مُوحدة تساهم في نقل المعلومات بين الأجهزة ممّا ساهم بشكل كبير في المساس ببعض الأمور والأسرار المتعلقة بالكيان المعنوي للشخص الطبيعي والمعنوي على حدٍّ سواء.

1/ الجرائم المعلوماتية الواقعة على أسرار الدولـة : إن الدخول على حسابات الدولة التي تتضمن أسرارها والمعلومات المتعلقة بأمنها وجيشها, هو من الجرائم التي تقع على أمن الدولة وإن إثارة الفتن الطائفية عبر البريد الإلكتروني والمواقع الإلكترونية من الجرائم التي تمس أمن الدولة,وإن اختراق الأسرار السياسية والعسكرية للدولة من الجرائم الخطيرة التي تقع على أمنها, وكذلك إثارة الفتن فجميعها من الجرائم الواقعة على أمن الدولة, وتتمثل بالدخول غير المشروع لقاعدة المعلومات والبيانات السرية, ونقلها عبر شبكات الاتصال الدولية, ولقد نص قانون حماية أسرار ووثائق الدولة الأردني لسنة 1971 في المواد 14 و15 و16 على حماية وثائق ومعلومات وأسرار الدولة ومعاقبة كلّ من خالف هذا القانون تتراوح ما بين الإعدام إلى الأشغال الشاقة المؤقتة[2].

فالمعلومة هي المادة الأولية للمعلوماتية,و المعرفة تتأتى بالضرورة من المعلومة, فهي تمثل تجميع دقيق لمعلومات مخزنة في الكمبيوتر,و المعلومة هي الجانب الحركي للمعرفة وبالعكس فإن المعرفة هي حالة أو نتيجة لفعل الإعلام, وقد عرف Catala المعلومة بقوله"أنها كلّ رسالة معدّة على نحو يمكن نقلها إلى الغير"[3], فالشيء يعرف بالحصول على معلوماته, والسر يعتبر معلومة, والإفشاء هو نقل المعلومات أي هو نوع من نقل المعلومات وإطلاع الغير بدون رضاء صاحبها التي

---

[1]- نبيل صقر, الوسيط في شرح جرائم الأموال, دار الهدى, عين مليلة, الجزائر, الطبعة الأولى, 2012, ص 203.

[2]- خالد عياد الحلبي, المرجع السابق, ص 62.

[3]- زينات طلعت شحادة, الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، مكتبة صادر ناشرون, بيروت, لبنان, دون طبعة , 2006, ص 100.

يرغب في حفظهاو الكتمان عليها, وهي الرغبة التي يحترمها المشرع, وهي علة تجريم إفشاء الأسرار, فهي صورة من صور الحماية الجنائية للإرادة.

إن استخدامالنظام المعلوماتي في الجرائم الواقعة على أسرار الدولة والتي تمثل كافة الأسرار سواء كانت إقتصادية أو مالية أو عسكرية أو سياسية تعدّ من أخطر أنواع المعلوماتية في الوقت الحاضر[1],فقد ز ادت في الوقت الحالي حوادث اختراق المراكز العسكرية والإستراتيجية, وتعرضها لقرصنة معلوماتية من أجل الحصول على البيانات والمعلومات المخزنة في ذاكرة الحاسبات الآلية المستعملة فيها,ولعلّ القاسم المشترك في هذه الحوادث أنها ترتكب في الأغلب من قبل أحداث ومراهقين وليس من قبل عصابات تعمل في الجريمة المنظمة, ومن بين هذه الحوادث سرقة معلومات عسكرية تتعلق بالسفن التي تعمل في خدمة جيوش الدولة التابعة لحلف شمال الأطلسي, وقد حدثت السرقة من نظم الحاسب الآلي الخاصة بالقوات المسلحة الفرنسية في صيف عام 1994, وهو أمر أزعج السلطات الفرنسية وأدى إلى تصميم برامج حماية جديدة[2].

أيضاً فقد تمكن قرصان أمريكي لم يتجاوز الثامنة عشر من اختراق نظام وزارة الدفاع الأمريكية - البنتاجون - غير عابئ بنظم الحماية عالية التقنية والجدران النارية التي وضعت لحماية هذه النظم, وكان يمكن له تعريض البشرية للإبادة لو تمكن الوصول إلى المخزون النووي الإستراتيجي وفك شفرته وضبطها نحو تصويب القنابل النووية[3].

ومنذ فترة قليلة تعرضت أيضاً وزارة الدفاع الأمريكية " البنتاجون " لهجوم كاسح لـ"هاكرز" حيث قام قراصنة بشن هجوم على ثلاثة عشر جهازاً مركزياً يتحكم بتدفق المعلومات على شبكة الإنترنت على مستوى العالم وتمكنوا من تعطيل ثلاثة أجهزة والسيطرة عليها بشكل كامل طوال اثني عشر ساعة, في أكبر عملية تشهدها الشبكة منذ عام 2002, وذكرت مصادر البنتاجون أن ما يقرب من 1500 مستخدم من إجمالي 3000 موظف الذين يعملون مباشرة مع مكتب وزير الدفاع, لم يتمكنوا من الدخول إلى البريد الإلكتروني بعد إختراق جهاز الكمبيوتر الرئيسي المزود بالخدمة "السيرفر", يأتي ذلك بالرغم من أكثيراً من أنظمة الحواسب للبنتاجون تشغل بواسطة "سيرفرات" سرية ومجهزة

---

[1]- أحمد خليفة الملط, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, مصر, الطبعة الثانية, 2006, ص 199.

[2]- عبد الفتاح بيومي حجازي, الجريمة في عصر العولمة, المرجع السابق, ص 221.

[3]- عبد الفتاح بيومي حجازي, المرجع نفسه, ص 221.

ببرامج حماية قوية بخلاف الأنظمة غير السرية,ووجهت كلّ من ألمانيا والولايات المتحدة وبريطانيا أصابع الإتهام إلى الصين بشن هذا الهجوم (القراصنة) على شبكاتهم الإلكترونية وأكدت الصين بالنفي و عدم صحة ما تردد من أنباء حول قيام قواتها المسلحة باختراق كمبيوترات وزارة الدفاع الأمريكية "البنتاجون"[1].

وفي إسرائيل ألقي القبض على كاتب إسرائيلي بتهمة الاعتداء على أمن الدولة لأنه نشر معلومات محظورة على شبكة الإنترنت تتعلق باختفاء غواصة في البحر المتوسط عام 1968.

2/ الجرائم المعلوماتية الواقعة على الأسرار المهنية : المعلوماتية هي المعالجة الآلية للبيانات التي توجد داخل النظام المعلوماتي يجب أن تكون سرية بطبيعتها وهو ما يفترض توافر في من توكل إليه, كما يجب أن يعلم الموظف المكلف بحمايتها أثناء مباشرته مهنته أو وظيفته قيمة هذه السرية, وقد ثار خلاف حول تحديد تلك المعلومة السرية, فذهب البعض إلى أن السر هو ما خصص لذاك, أي لا يكون العلم به إلاّ لصاحبه أو ما يؤتمن عليه بحكم الوظيفة أو المهنة لطبيعته السرية وما لا يخصص للإفشاء بعلم الغير به[2].

وذهب البعض الآخر إلى أن السر هو واقعةأو صفة ينحصر نطاق العلم بها في عدد محدّد من الأشخاص إذا لكت تعدّ مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم بها محصورًا في ذلك النطاق[3].

ولا يكتفي لوصف إحدى الوقائع بالسرية أن تكون أبلغت صراحة للغير بل يكتفي أن تكون وصلت إلى علم الأمين عليها أثناء حماية مهنة أو وظيفة سواء من خلال ما أبلغ إليه صراحة أو ما فهمه أو سمعه من الوقائع, بل يشمل السرية للمعلومة ولو كانت مجهولة لصاحبها مثل المرض, فيلتزم الطبيب بالمحافظة على الأسرار التي يقرّرها له المرض والتشخيص أو المرض الذي يكتشفه أثناء الفحوص الطبية عليه, وكذلك يلتزم المحامي بحفظ أسرار موكله في الدعاوى المودعة لديه, وهناك إستثناء على ذلك فقد سمح القانون بإعطاء تبادل المعلومات الشخصية إلى بعض الأجهزة الإدارية والقضائية مثل: " إدارة الضرائب أو الصحة أو النيابة العامة أو القضاة أو الشرطة وبعض

---

[1]- عبد المجيد بوناب, " الحرب الإلكترونية, قمة الصراع العالمي وحصاد العولمة التقنية ", مجلة العلم والإيمان, العدد 33, الجزائر, ماي 2009, ص 25.

[2]- أحمد خليفة الملط, المرجع السابق, ص 199.

[3]- أحمد خليفة الملط, المرجع نفسه, ص 199.

الأجهزة الأمنية ", بتبادل هذه المعلومات أو الإطلاع عليها دون وضع ضمانات وفي الأحوال المصرح بها قانوناً[1].

الفرع الثاني : الجرائم المعلوماتية الواقعة على الأمـوال

جرائم الإعتداء على الأموال - بوجه عام - هي الجرائم التي تنال بالاعتداءأو تهدّد بالخطر الحقوق ذات القيمة المالية,ويدخل في نطاق هذه الحقوق كلّ حق ذي قيمة إقتصادية, وتدخل بذلك في دائرة التعامل ومن ثم كان أحد عناصر الذمة المالية[2].

يقتضي الحديث في هذا الفرع عن الجرائم المعلوماتية الواقعة على الأموال التطرق إلى الجرائم المعلوماتية ضدّ الأموال الخاصةوالجرائم المعلوماتية ضدّ الأموال العامة وذلك كما يلي :

أولاً :الجرائم المعلوماتية ضدّ الأموال الخاصة : في نطاق شبكة الإنترنت, يعتبر الحاسب أداة سلبية لارتكابالجريمة ضدّ الفرد, إذ تستخدم الحواسيب المرتبطة بشبكة الإنترنت كوسيلة لتنفيذ الجرائم إلى فرض الحماية على أموال الغير والتي اتخذت صور مستحدثة, لذا برزت الدعوى إلى فرض الحماية الجنائية من مخاطر استخدام الإنترنت[3].

1/ السرقة المعلوماتية : بالنسبة للنشاط الإجرامي المكون لجريمة السرقة وهو الاختلاس وبتطبيقه على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة, نلاحظ أن الجانيوا ٕن كان يدخل في ذمته ما استولى عليه من برامج, إلاّ أنه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تصل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون انتقاص من محتواها, كما يلاحظ على أن الاستيلاء على البرامج باعتبارها معلومات لا يتصور من الوهلة الأولى إلاّ على أنه انتقال لهذه المعلومة من ذهن إلى ذهن آخر أو من ذاكرة إلى ذاكرة وهذه عقبة ثانية, ويلاحظ ثالثًا أن المعلومات التي تحتويها البرامج من طبيعة مادية على شيء معنوي وهذه عقبة ثالثة, نتيجة لهذه العقبـات, فليس من السهل بسط أحكام السرقة على برامج الحاسب الآلي وذلك في[4] :

---

[1]- أحمد خليفة الملط, المرجع السابق, ص 200.

[2]- خالد ممدوح, حجية البريد الإلكتروني في الإثبات, دار الفكر الجامعي، القاهرة, مصر, دون طبعة, 2001, ص 117.

[3]- محمد أمين الشوابكة, جوائم الحاسوب والإنترنت, دار الثقافة, عمان, الأردن, الطبعة الأولى , 2006, ص 137.

[4]- عطاء الله فشار, "مواجهة الجرائم المعلوماتية في التشريع الجزائري ", مجلة الدراسات والأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009, ص 17.

أ- سرقة المعلومات عن طريق النسخ غير المشروع للبيانات : أي عن طريق إعادة إنتاج الوثيقة أو الدعامة التي تحتويها لمحاولة بسط أحكام السرقة على حالات النسخ غير المشروع, حيث توصل الإجتهاد القضائي الفرنسي في هذا الصدد إلى إعلانه صراحة أن المعلومات التي نسخت أو أعيد إنتاجها هي التي سرقت, فلم يخرج المشرع الفرنسي عن مبدأ الشرعية الجنائية وحافظ على مبدأ مادية الإختلاس, وعلاوة على ذلك فإن إقرار الحكم باختلاس المعلومات عن طريق إعادة إنتاج المستند الذي يحويها يحمل في طياته ثورة مستمرة ولكنها عميقة, لأنها تسمح بالعقبات على إعادة الإنتاج لا يمكن أن يقع تحت طائلة جريمة التقليد, وبالاستناد إلى الحكم الصادر من محكمة « MONBELLIARD » قسم الجنح في 26 ماي 1978 والذي تتلخص وقائعه في أن أحد المبرمجين قدم إستقالته من الشركة التي يعمل بها ونقل لوظيفة في شركة أخرى أكثر دخلاً بعد أن قام بنسخ أو تسجيل برامج المعلوماتية على قرص مغناطيسي كان قد حمله معه خصيصاً لهذا الغرض فتوبع بجريمة السرقة,إستناداً إلى أنه إستحوذ على تسجيلات للمعطيات التي أصبحت ملكا للشركة الأولى, وعوقب بالحبس مع وقف التنفيذ وفقاً للمادة 379 من قانون العقوبات الفرنسي[1].

ب- سرقة وقت الآلة : إن المشرع الجزائري لا يأخذ بما يسمى سرقة الخدمة, وعليه يتطلب تدخلاً تشريعياً على غرار ما فعل المشرع الفرنسي بتجريمه البقاء غير المشروع في نظام المعالجة الآلية للمعلوماتفإذا كانت هذه الجريمة تهدف أساساً إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة, إلاّ كانت تحقق أيضا وبصورة غير مباشرة حماية المعلومات ذاتها, إذ ورد النص عليها في الباب الثالث من القسم الثاني من قانون العقوبات الفرنسي, وهي تضم المواد 01/323 إلى 07/323 بقولها :[2] « le fait d'accéder ou de se maintenir… » .

ج- الالتقاط الذهني للمعلومات : كأن يقوم شخص بالتقاط معلومات ظهرت على شاشة الحاسب الآلي وقام بحفظها واختزانها في ذاكرته, هذا المسلك يمكن أن يكون اختلاسا رغم أنه لم يرد على ذات مادة المستندوا ٍنما اقتصر الشيء المختلس على مضمون المستند مع بقائه في حيازة صاحبه لأن هذا المضمون شيء منقول مملوك للغير منحصر في منفعة المستند كجزء في حيازة من حق صاحبه في ملكيته, إلاّ أن المشرع الجزائري لا يأخذ بسرقة الاستعمال, وعليه وجب تدخل تشريعي

---

[1]- أحمد خليفة الملط, المرجع السابق, ص 255.

[2]- زينات طلعت شحادة, المرجع السابق, ص 52.

يشمل حالتي الالتقاط الذهني للبيانات وحالة سرقة المعطيات دون استنساخها ودون المساس بسلامتها أو أصالتها وأن البدء في قبول وجود جرائم تتمثل ماديتها في محض نشاط ذهني من شأنه فتح المجال أمام التسلل إلى دخائل الفرد والعقاب على ما يدور في الأذهان أو يجيش بالصدور من الأفكار والآراء وهو أمر ليس مقبول[1].

2/ التحويل الإلكتروني غير المشروع للأموال يتّم التحويل غير المشروع للأموال بعّدة وسائل يصعب حصرها لسرعة تطورها, لكن يمكن الإشارة إلى أكثرها انتشارا ومن أهمها:

أ-استخدام برامج معدّة خصيصًا لتنفيذ الاختلاس : أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر سواء كان من المصرف نفسه أو من حساب آخر في مصرف آخر,على أن يتّم ذلك في وقت معين يحدّده مصمم هذا البرنامج.

ب- التحويل المباشر للأرصدة :يتّم ذلك عن طريق اختراق أنظمة الحاسب الآلي وشفرات المرور, أشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة الأمريكية باختراق النظم المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط,ويتّم ذلك أيضًا عن طريق إدخال معلومات مزيفة وخلق حسابات ومرتبات وهمية وتحويلها إلى حساب الجاني, ويمكن أن يتّم التحويل المباشر أيضًا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلاً بشبكة تعمل عن طريق الأقمار الصناعية, فهناك بعض الأنظمة التي تستخدم طابعات سريعة تصدر أثناء تشغيلها إلكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز وإعادة بثها مرة أخرى بعد تحويرها, وهو ما نصت عليه اتفاقية بودابست في المادة 05[2].

ج- التلاعب بالبطاقات المالية : لقد ظهر هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي إلى أن ظهرت الصرافة الآلية والنقود المالية,وجرائم الاعتداء عليها تتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها,وهو ما يتّم عن طريق اختراق بعض المواقع التجارية التي يمكن أن

---

[1]- آمال قارة, الحماية الجزائية للمعلوماتية في التشريع الجزائري, دار هومة, الجزائر, الطبعة الثانية , 2007, ص 25.

[2]- رحاب عميش, الجريمة المعلوماتية, ورقة عمل مقدمة إلى المؤتمر المغاربي حول المعلوماتية والقانون, أكاديمية الدراسات العليا, طرابلس, ليبيا, 28 - 29 أكتوبر 2009, ص 11.

تسجل عليها أرقام هذه البطاقات[1].

ثانياً : الجرائم المعلوماتية ضد الأموال العامة : الأموال العامة تلك الأموال التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع العام أي تلك الحقوق التي ليست لفرد من أفراد معينين بذواتهم, فالحق المعتدى عليه هو المجتمع في مجموع أفراده, أو هو الدولة باعتبارها الشخص القانوني الذي يمثل المجتمع في حقوقه ومصالحه.

وعليه ارتأينا أن نعرض لجريمة الاختلاس المعلوماتي وجريمة تزييف العملة كما يلي :

1/ الإختلاس المعلوماتي : هو " تغيير نية المؤتمن على المال, وعزمه على السيطرة الفعلية للمال الذي في عهدته, والحلول محل صاحبه, دون أن يترتب عن ذلك خروج المال من حيازته "[2], أي اتجاه النية إلى تملك المال والتصرف فيه على اعتبار أنه مملوك له, ويكون الشيء المختلس في جريمة الاختلاس بحيازة الجاني بصفة قانونية, وتنصرف نيته إلى التصرف فيه باعتباره مملوكاً له.

وفي نطاق المعلوماتية فإن المادة 422 عقوبات أردني والمادة 341 عقوبات مصري و 314 عقوبات فرنسي تنطبق في حالة تسليم الدعامات والأشرطة الممغنطة والأقراص الممغنطة والبرامج المحتوية على البيانات والمعلومات إلى الغير, وفي هذا السياق نذكر على سبيل المثال واقعة حدثت في إحدى الجامعات المصرية تتلخص في قيام شركة تدعى "سيليكون للكمبيوتر" باختلاس الأدوات والنظم المعلوماتية والأجهزة التابعة لشبكة الجامعة, وذلك باستغلال الشركة تعاقدها مع الجامعة بعمل برمجة وصيانة للشبكة, إذ اختفت الديسكات الخاصة بتشغيل نظم الشبكة في الجامعة مما أدى إلى توقف العمل بمعظم مرافق الجامعة, وتخريب شبكة المعلومات ومسح المعلومات مما سهل للجناة إخراج الأشياء المستولى عليها[3], والاختلاس لا يخرج عن صور ثلاث تتمثل في :

الصورة الأولى : التبديد يُعرف التبديد بأنه تصرف الأمين في المال الذي أؤتمن عليه, بشرط أن يؤدي هذا التصرف إلى خروج المال من حيازته[4] ويستوي أن يكون التصرف قانونياً كالبيع أو الهبة أو الرهن أو مادياً كاستهلاك الشيء, ومغناطيسية وأسطوانات معلوماتية ومعدات كالأجهزة بما تحويه من ذاكرة تحتوي على معلومات.

---

[1] - رحاب عميش, المرجع نفسه, ص 12.

[2] - آمال قارة, المرجع السابق, ص 55.

[3] - محمد أمين الشوابكة, المرجع السابق, ص 16-17.

[4] - آمال قارة, المرجع نفسه, ص 55.

الصورة الثانية : الإتـلاف : الإتلاف يعني إفناء مادة الشيء, أو على الأقل إدخال تغييرات شاملة عليها بحيث تصبح غير صالحة للاستعمال في الغرض الذي من شأنه أن يستعمل فيه فتضيع تبعًا لذلك قيمته بالنسبة إلى مالكه, والهدف من تدمير نظم المعلومات هو إتلاف أو محو أو شطب تعليمات البرامج أو البيانات ذاتها, أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي, ولا يهدف التدمير إلى مجرد الحصول على منفعة من الحاسوب أيًا كان شكلها, ولكن يريد ببساطة إحداث ضرر بالنظام المعلوماتي وإعاقته عن أداء وظائفه وإن الأضرار الناشئة عن تدمير وتخريب البيانات والمعلومات والبرامج تفوق نظيرتها الناتجة عن إتلاف المعدات المادية للحاسوب, فالقانون الفرنسي المعدل عام 1988 فقد جرّم الاعتداء على العناصر المعنوية للحاسوب وهذا في المادة 4/462 وعاقب مقترفها بالحبس من ثلاثة أشهر إلى ثلاث سنوات وغرامة من 2000 إلى 500,000 فرنك أو بإحدى هاتين العقوبتين[1].

وتجدر الإشارة إلى أن صور الإتلاف مستحدثة في القانون المتعلق بالوقاية من الفساد ومكافحته, ولم ينص عليها المشرع الجزائري في قانون العقوبات ضمن المادة 119 الخاصة بتجريم فعل الإختلاس سابقًا.

الصورة الثالثة : الإحتجاز بدون وجه حق : يكفي في هذه الصورة أن يتحقق الركن المادي لجريمة الإختلاس في القطاع العام بمجرد إحتجاز محل الجريمة عمدًا وبدون وجه حق, إذ عمد المشرع حفاظًا على الودائع إلى توسيع مجال التجريم إلى التصرف الذي من شأنه أن يعطل المصلحة التي أعدّ المال لخدمتها[2].

2/ جريمة التزييف في المعلوماتية : تعدّ جريمة تزييف العملة من الجرائم التي تطال الإقتصاد الوطني خاصة مع تطور أساليب ارتكابها, إذ يتّم بواسطة شبكة الإنترنت, هذا ما يسمى بالتزييف الإلكتروني, وتتمثل أركان جريمة التزييف المعلوماتي في الآتي:

أ- محل جريمة التزييف في المعلوماتية: إن محل الجريمة يقع على العملة سواء كانت معدنية أو ورقية, حيث أنها هي الأداة الأولى للتعامل بين الناس لذلك تحتكر الدولة إصدارها وتجريم تزييفها.

---

[1]- خالد عياد الحلبي, المرجع السابق, ص 68-69.

[2]- محمد أمين الشوابكة, المرجع السابق, ص 216.

وتعتبر قضية تزييف العملات, من أهم مصادر القلق الإقتصادي لدى حكومات الدول القائمة على حماية إقتصادها الوطني, خاصة بعد تطور أساليب التزييف في الآونة الأخيرة, وضبط كميات ضخمة من العملات لدى العصابات التي تخصصت بتزييف العملة بالحاسوب في المنطقة العربية[1].

ب- الركن المادي لجريمة التزييف في المعلوماتية : يشكل الركن المادي لجريمة التزييف في المعلوماتية ما يتّم من أساليب وطرق في تزوير وتزييف وتقليد العملات الورقية وترويجها, ولا يوجد ما يمنع من تطبيق نصوص قانون العقوبات الواردة في القواعد العامة لجريمة التزييف على التزييف بواسطة الآلات الحديثة باستخدام النظام المعلوماتي.

ج- الركن المعنوي لجريمة التزييف : يتوافر القصد الجنائي في جرائم التقليد والتزييف والتزوير بإنصراف إرادة الجاني إلى غاية معينة هي ترويج العملة غير الصحيحة, فلا يرتكب الفاعل جناية من الجنايات إلاّ إذا ثبت أنه يهدف إلى هذه الغاية (القصد الجنائي)[2].

المطلب الثاني:الجرائم المعلوماتية الو اقعة على أنظمة المعالجـة الآليـة للمعطيـات

ما من عصر يمرّ على الإنسان إلاّ وتظهر فيه أنواع جديدة من الجرائم لم تكن موجودة فيما سبقه من العصور,إذ أن تلك الجرائم تظهر مع الجديد الذي يطرأ في حياة الإنسان, والذي تتعلق به مصالحه, ومن ثم يصبح الاعتداء عليه غير مشروع, ولا شك أن ما يطبع عصرنا الآن هو ما يسمى بالمعلوماتية, فقد غزت هذه مختلف جوانب الحياة حتى سمي هذا العصر بإسمها, فهذه المعلوماتية وا ٕن عادت على الإنسان بالخير الكثير فهي قد أوجدت معها صنوفاً من الإجرام لم تكن لتعرف لولاها, كما أنها عززت من بعض الجرائم الموجودة, عندما أصبحت وسيلة مثلى يستعين بها المجرمون في تنفيذ تلك الجرائم, ولعله من أخطر الجرائم المتعلقة بالمعلوماتية إن لم تكن أخطرها تلك الجرائم التي تقع على معطيات الحاسب الآلي.

فقد أفرزت تلك الثورة المعلوماتية كيانات جديدة لم يكن للإنسان عهد بها قبل وقت قريب, ولعلّ أهم هذه الكيانات هي المعطيات وما تقدمه من معلومات.

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية, إستدعى

---

[1]- أحمد خليفة الملط, المرجع السابق, ص 507.

[2]- أحمد خليفة الملط, المرجع نفسه, ص 513.

تدخلاً تشريعياً صريحاً, سواء على المستوى الدولي أو الداخلي,فدولياً وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي,أمّا على المستوى الوطني, فقد استدرك المشرع الجزائري الفراغ القانوني وذلك باستحداث نصوص تجريمية لقمع الإعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات الجزائري بقسم سابع مكرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات " ويشمل المواد من 394 مكرر إلى 394 مكرر 7.

الجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها إلاّ أن ما يجمعها أنها تحقق حماية جزائية لنظم المعالجة الآلية للمعطيات, أي أن القاسم المشترك بينها هو نظام المعالجة الآلية, ولذلك فإن دراسة تلك الجرائم التي تستهدف نظم المعالجة الآلية للمعطيات تقتضي منّا أولاً توضيح مفهوم نظام المعالجة الآلية للمعطيات في الفرع الأول,أمّا في الفرع الثاني فسنخص بدراسة جرائم المعطيات جرائم عابرة للحدود.

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

يمثل هذا النظام الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان كلّ جريمة من جرائم الاعتداء عليه, يعتبر عنصراً لازماً لكل منها, وبالتالي فإنه من الضروري تحديد مفهومه[1].

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة,فضلاً على أنه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية[2].

ولهذا فالمشرع الجزائري على غرار المشرع الفرنسي لم يُحدّد مفهوم هذا النظام تاركًا هذه المهمة على عاتق الفقه والقضاء وذلك نظراً لخضوعه للتطورات السريعة والمتلاحقة, على الرغم من أن مجلس الشيوخ أدرج ضمن التعديلات التي أوردها على اقتراح مشروع قانون النائب Godfrain

[1]- زينات طلعت شحادة, المرجع السابق, ص 32.

[2]- آمال قارة, المرجع السابق, ص 101.

المقصود بهذا النظام,وقد حدّده على الشكل التالي "بأنه كلّ مجموعة مركبة من وحدة أو عدّة وحدات للمعالجة وسواء كانت متمثلة في ذاكرات الحاسب وبرامجه ووحدات الإدخال والإخراج التي تساهم في نتيجة معينة "[1].

« Un ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées – sortie et de liaisons qui concourent à un résultat déterminés ».

هذا المفهوم يتضمن نظام المعالجة الآلية بمكوناته المادية كالمعدات والأجهزة, والمعنوية كالبرامج والمعطيات, وأن توجد بين هذه العناصر علاقة تربط بينها لتحقق هدف محدّد, وهو المعالجة الآلية للبيانات, وبالتالي نظام المعالجة الآلية هو "مجموعة الوحدات المترابطة التي تألفت معًا لتشكل كلاً لا يتجزأ ليعمل معًا كوحدة واحدة"[2], وتتمثل تلك الوحدات في وحدة الإدخال والمعالجة والإخراج والتخزين والرقابة التي تحوّل البيانات إلى معلومات مفيدة باستخدام الأجهزة والبرامج الجاهزة, ويعتمد نظام المعالجة الآلية للمعطيات على شرطين وهما:

1- مركب يتكون من عناصر مادية ومعنوية مختلفة مثل (الذاكرة, البرامج, المعطيات, أجهزة الربط...الخ) تربط بينها نتيجة علاقات تُوحدها نحو تحقيق هدف محدّد.

2- ضرورة خضوع النظام لحماية فنية, ولقد ثار خلاف في الفقه الفرنسي حول وجوب توفر هذا الشرط أو عدمه وسبب إثارة هذا الخلاف أن الأعمال التحضيرية للقانون أكدت على وجوب أن يكون النظام محميًا ضدّ الإعتداءات عليه بأجهزة أو وسائل أمنية, وهذا ما تمسك به مجلس الشيوخ الفرنسي وحجته في ذلك جذب انتباه أصحاب الأنظمة إلى هذه النقطة الأساسية كي يدعموا أنظمتهم بأجهزة الأمن, ذلك أن القانون يجرّم الإعتداء على نظم الأمن المتضمنة في النظام المعلوماتي.

ويستند هذا الرأي إلى أن الإعتداء على النظام الأمني شرط مفترض لقيام الجرائم التي تتعلق بنظم المعلوماتية الذي تمّ إختراقه.

وتطبيقًا لذلك,فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدًا بوجود حماية فنية ولكن إذا نظرنا للواقع, نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية

---

[1]- زينات طلعت شحادة, المرجع السابق, ص 33.

[2]- زينات طلعت شحادة, المرجع نفسه, ص 33.

3. J.PRADEL,les infractives à l'informatique, R.I.D.C,1990 - 2,P 827.

فنية, ووجود مثل هذا النظام يساعد على إثبات أركان الجريمة لا سيما الركن المعنوي.

بعد أن تطرقنا إلى مفهوم نظام المعالجة الآلية للمعطياتوتم ّ تبيان الركن المفترض في تلك الجرائم, يأتي الحديث عن الركن المادي والمعنوي من خلال الإعتداءات المتنوعة التي أعطيت وصفًا جرميًا يعاقب عليه القانون والتي تستهدف هذا النظام ومن بينها : جريمة الدخول أو البقاء غير المشروع داخل النظام, جريمة التلاعب بمعطيات الحاسب الآلي, جريمة التعامل في معطيات غير مشروعة.

أولاً : جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات :

لعلّ جريمة الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات هي من أهم جرائم المعطيات والجرائم المعلوماتية عمومًا, ذلك أن أغلب جرائم المعطيات لا يمكن ارتكابها إلاّ بعد الدخول للنظام,ولهذا كانت جريمة الدخول هي الباب والحدّ الفاصل بين الجاني وبين ارتكابه لمختلف جرائم المعطيات الأخرىلذلك أولت لها التشريعات إهتمامًا كبيرًا, وهناك من التشريعات من يجعلها الجريمة الأساسية وما باقي الجرائم إلاّ نتاج لها.

قد نصت عليها المادة 1/323 قانون العقوبات الفرنسي الجديد ونص المادة 394 مكرر قانون العقوبات الجزائري, كما نصت عليها المادة 02 من الإتفاقية الدولية للإجرام المعلوماتي.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع,فلم يحدّد المشرع الفرنسي وسيلة الدخول إلى النظام أو إختراقه, فيجوز إذاً الدخول إلى النظام بأي وسيلة تقنية ومن ذلك انتهاك كلمة السر الحقيقية « Passe Word » متى كان الجاني غير مخول في استخدامها أو عن طريق استخدام برنامج أو شفرة خاصة, كما يمكن كذلك استخدام الرقم السري لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول, ومن صور الدخول غير المشروع كذلك أن يكون مالك النظام قد وضع قيودًا على الدخول إليه ولم يحترم الجاني هذه القيود, أو كان الأمر يتطلب سداد مبلغ من النقود لم يسدّدها الجاني وتحايل وقام بالدخول غير المشروع إلى النظام.

والملاحظ أن المشرع يعاقب على مجرد الدخول إلى النظام المعلوماتي, حتى لو لم يترتب على دخوله ضرر أو حدوث نتيجة معينة كالوصول إلى المعطيات والبرامج أو التلاعب بها أو يتحقق له من وراء الدخول فائدة طالما أن الدخول غير مشروع.

ويتحقق فعل الدخول متى دخل الجاني إلى النظام كلّه أو جزء منه, كالدخول إلى طرفية الحاسب أو شبكة الإتصال أو البرنامج, كما يتحقق الدخول غير المشوع متى كان مسموحًا للجاني بالدخول إلى جزء معين من البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه.

أمّا فعل البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فقد كان الهدف من تجريمه البقاء غير المشروع داخل النظام لمن كان دخوله إلى النظام بطريق الصدفة البحتة, وانتفى لديه القصد الجنائي ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك, حيث يعاقب الجاني على الجريمة العمدية لأن إرادته انصرفت إلى البقاء داخل النظام رغم علمه بأن دخوله غير مشروع, وذلك الحكم ينصرف إلى من هو مسموح له بالدخول إلى جزء من النظام ثم يدخل إلى جزء آخر غير مصرح له بالدخول فيه, أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحًا له بالرؤية والإطلاع فقط.

وهناك جانب من الفقه يعرف البقاء غير المشروع بأنه " التواجد داخل نظام المعالجة الآلية للمعطيات ضدّ إرادة من له الحق في السيطرة على هذا النظام, أو- عدم وضع حد للتشعب داخل النظام مع الإعتقاد بأن ذلك يشكل خطأ "[1].

ومفهوم الدخول والبقاء غير المشروع في النظام يمثل مفهومًا للنشاط الإجرامي سواء في صورته البسيطة أو المشدّدة وهو ما سنبحثه حالاً :

1- الصورة البسيطة : تتحقق هذه الصورة بفعل الدخول غير المشروع أو البقاء غير المشروع في النظام الذي تمّ إختراقه, وقد عدت هذه الجريمة بمثابة الصورة البسيطة لأن المشرع الفرنسي عاقب عليها بالحبس مدة سنة وغرامة مائة ألف فرنك فرنسي وضاعف العقوبة متى أقترن بها ظرف مشدّد, أمّا المشرع الجزائري فقد حذا حذوه, إذ نص في المادة 394 مكرر فقرة 1 على الصورة البسيطة وفي الفقرة الثانية ضاعف العقوبة إذا اقترنت بظرف مشدّد, وحتى يتحقق الركن المادي لهذه الجريمة في صورتها البسيطة يجب تحقق فعل الدخول غير المشروع أو البقاء غير المشروع أو يتحققان معًا وذلك حتى يقوم الركن المادي لهذه الجريمة في صورتها البسيطة.

وجريمة الدخول على النظام أو البقاء فيه, هي من الجرائم العمدية التي تقوم على القصد

---

[1]- جباري عبد المجيد, دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة, دار هومة, الجزائر, الطبعة الثانية, 2013, ص 111.

الجنائي العام, الذي يتكون من عنصري العلم والإرادة, ذلك أنه يجب أن يعلم الجاني بأنه لا يحق له الدخول أو البقاء داخل النظام,وأن ذلك ضدّ رغبة مالك النظام أو صاحب السيطرة عليه, ومع ذلك تتصرف إرادته إلى إتيان هذا الفعل بالمُخالِفة للقانون وبالمخالفة لإرادة صاحب النظام أو صاحب الحق فيه, ولذلك فمتى توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا محل للإعتداد بالباعث على إرتكاب الجريمة, وبالتالي تقوم الجريمة ولو كان الباعث على الدخول إلى النظام أو البقاء فيه هي محاولة للفضول أو النزهة أو إثبات القدرة على الإنتصار على النظام المعلوماتي.

2-الصورة المشدّدة :تتحقق هذه الجريمة في صورتها المشدّدة, متى ترتب على الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام بأن يؤدي وظيفته, ويكفي لتوافر هذا الظرف المشدّد أن يكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت, وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات, وهذه النتيجة ذاتها هي التي إعتبرها المشرع ظرفًا مشددًا في هذه الجريمة, فهذه الجريمة أيضًا عمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم والإرادة, فإذا أثبت الجاني إنتفاء علاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية التي هي ذات الظرف المشدّد في الجريمة, كأن يثبت أن تعديل محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ, إنتفى السلوك الإجرامي و القصد الجنائي لدى الجاني وإذا توافرت أركان جريمة الدخول أو البقاء غير المشروع في صورتها المشدّدة, عوقب الجاني بالعقوبة المقررة لها.

ثانيًا : جريمة التلاعب بمعطيات الحاسب الآلي :

جريمة التلاعب بالمعطيات هي الجريمة الثانية التي ينص عليها قانون العقوبات الجزائري بعد جريمة الدخول والبقاء غير المصرح بهما أمّا قانون العقوبات الفرنسي فينص عليها بعد جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات, وقد تعذر المشرع الجزائري في عدم النص على هذه الأخيرة نظرًا للتشابه الكبير بينها وبين جريمة التلاعب بالمعطيات, بحيث يصعب في الكثير من الأحيان التمييز بينهما, وذلك لأن الأفعال التي تتضمنها جريمة التلاعب تؤدي هي الأخرى إلى إعاقة النظام وإفساده, وقد اكتفى المشرع الجزائري نتيجة إفساد النظام كظرف مشدّد فقط لجريمة الدخول واستبعدها

كجريمة قائمة بذاتها[1].

ولم تكن جريمة التلاعب بالمعطيات في قانون العقوبات الفرنسي لسنة 1988 عم ّا هي عليه الآن, فالمادة 462 من ذلك القانون تناولت بالتجريم مختلف أنواع السلوك التي تمس بسلامة المعطيات فنصت على ما يلي: "كل من يقوم عمدًا وبدون مراعاة لحقوق الغير بطريق مباشر أو غير مباشر بإدخال معطيات داخل نظام للمعالجة الآلية للمعطيات أو يمحو أو يعدل المعطيات التي يتضمنها أو طرق معالجتها ونقلها يعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 2000 فرنك فرنسي إلى خمسمائة ألف (500.000) أو بإحدى هاتين العقوبتين ", فتميزت عبارات هذه المادة بالغموض وأثارت الكثير من الجدل مم ّا جعلها محلاً لانتقاد الفقه, فكانت هذه الإنتقادات محل اعتبار لدى المشرع الفرنسي, إذ قام بتعديل المادتين 462-3 و 462-4 وأحل محلهما المادتان 323-2 و 323-3 ولقد أستبعدت هذه الأخيرة و الخاصة بجريمة التلاعب بالمعطيات - عبارة :" بدون مراعاة لحقوق الغير: وأحلت محلها عبارة " عن طريق الغش " كما إقتصرت هذه المادة على إدخال أو محو أو تعديل المعطيات ولم تتطرق لطرق معالجتها أو نقلها.

كما ساوى تعديل سنة 1994 في العقوبة بين جريمتي التلاعب بالمعطيات وإعاقة وإفساد أنظمة الحاسبات.

والوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي بعد تعديله, إذ نصت المادة 394 مكرر 1 والخاصة بجريمة التلاعب بالمعطيات على ما يلي: " يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من 500.000 دج إلى 2000.000 دج كل ّ من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

ولقد جاء النص شاملاً لكل ّ أنواع المعطيات ولم يشترط شروطًا معينة فيها كأن تكون من طبيعة ما أو تكون تابعة لجهة معينة,كما أن المادة جاءت شاملة لكل ّ وسائل التلاعب بالمعطيات ولم تقتصر على وسيلة معينة, وبالتالي يدخل في نطاق هذه المادة استخدام البرامج الخبيثة مهما كانت وسيلة إدخالها على الحاسب الآلي, وواضح من نص المادة أيضًا أنه لا يشترط لقيام جريمة

---

[1]- محمد خليفة, الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, دار الجامعة الجديدة, الأزاريطة, الإسكندرية, دون طبعة, 2007, ص 175.

التلاعب أن يكون التلاعب قد تمّ بعد عملية دخول غير مشروع إلى نظام الحاسب الآلي, إذ يستوي أن يكون الدخول مشروعاً أو غير مشروعٍ[1], بل أن كثيراً من عمليات التلاعب لا تتّم إلاّ من عاملين مرخص لهم بالدخول إلى النظام, وتنص هذه المادة على ثلاثة أنواع من السلوك, الإدخال والمحو والتعديل ولا يشترط أن تقع هذه الأفعال مجتمعة, بل يكفي أن يقع إحداها حتى تقوم الجريمة[2].

ثالثًا : جريمة التعامل في معطيات غير مشروعة :

إن جرائم المعطيات تعدُّ من أخطر الجرائم وأكثرها ضرراً, خاصة إذا كانت تلك المعطيات التي يتّم الإعتداء عليها تتعلق بأمن الدولة أو تتعلق بالحياة الخاصة أو تمثل قيماً مالية مهمة, ولهذا حرص المشرع في خطته لمكافحة هذه الجرائم بالتصدي لها قبل وقوعها,وذلك بمنع كلّ الأفعال التي تشكل مقدمة لها,فقام بتجريم مجموعة من الأفعال تصب كلّها في التعامل في معطيات صالحة لأن ترتكب بها إحدى جرائم المعطيات فإذا لم ينجح هذا في ردع الجناة عن القيام بجرائمهم فقد حرص المشرع على التقليل من الضرر الذي يمكن أن تسببه جرائم المعطيات ما أمكن, فقام بتجريم أشكال من التعاملات في المعطيات التي يتم الحصول عليها من إحدى الجرائم.

فكلّ معطيات غير مشروعة, سواء كانت صالحة لأن ترتكب بها جريمة أو كانت متحصلة من جريمة قامت المادة 394 مكرر 02 بتجريم التعامل فيها سعياً لمنع وقوع الجريمة أو للتخفيف من آثارها إن وقعت, وكذا بتجريم أفعال الحيازة, الإفشاء, النشر, الإستعمال,أياً كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بهدف المنافسة غير المشروعة لمنافسيها, الجوسسة, الإرهاب, التحريض على الفسق...إلخ.كذلك أيضاً نصت المادة 394 مكرر 3 على مضاعفة العقوبة المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام,وقد خصت تلك المادة مؤسسة الدفاع الوطني نظراً لأهمية هذه المؤسسة ودورها في الحفاظ على سلامة التراب الوطني والأمن العام, وحساسية المعطيات المتعلقة بها والخطورة البالغة للإعتداء عليها, وحكمة التشديد في الجرائم الماسة بالدفاع الوطني عموماً هو ما يتطلبه الأمر من

---

[1]- انظر: Linant de bellefonds (Xavier) et autres, pratique de droit informatique, 1998, op,cit, p,238

[2]- محمد خليفة, المرجع السابق, ص 179.

وجوب العمل على سلامة وأمن القوة العسكرية التي في حفظها وسلامتها حفظ وسلام للدولة بأكملها فضلاً عمّا يكون عليه الجاني في مثل هذه الجرائم من خسة ونذالة وإجرام في حق نفسه وفي حق وطنه مما يستدعي أخذه بمنتهى الشدة والقسوة.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات وقد تضمنت أنواع العقوبات المطبقة في مواد الجنايات والجنح, كذلك بالنسبة لعقوبة الغرامة المطبقة على الشخص المعنوي عندإرتكابه إحدى الجرائم الماسة بالأنظمة المعلوماتية فهي غرامة ذات حدّ واحد,تعادل طبقًا للمادة 394 مكرر4 من قانون العقوبات خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

كما عاقبت المادة 394 مكرر5 على الإشتراك في مجموعة أو في إتفاق يتألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم, ونصت المادة 394 مكرر6 على عقوبة مصادرة وسائل إرتكاب الجريمة وإغلاق المواقع التي تكون محلاً لهاوإغلاق المحل أو المكان الذي أرتكبت فيه الجريمةمع المعاقبة على الشروع في جرائم هذا القسم(394 مكرر7).

الفرع الثاني: جرائم المعطيات جرائم عابرة للحدود

ليس هناك في عالم اليوم حدود تقف حائلاً أمام نقل المعطيات بين الحاسبات الآلية المتوزعة في مختلف دول العالم عبر شبكات المعلومات, فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر فالجرائم لم تعدّ تقتصر على إقليم ولا تتعداه, بل أصبح بالإمكان ارتكاب الجرائم عن طريق الكمبيوتر باختراقه لكمبيوتر آخر في بلد آخر أو إتلاف معطياته, فالتعدي في بلد وأثره في بلد آخر وهكذا.

ففي عصر المعلومات وبفعل وجود تقنيات عالية للتقدم, فإن حدود الدولة أصبحت مستباحة بأقمار التجسس والبث الفضائي, ولقد تحولت جرائم التجسس من الطرق التقليدية إلى الطرق المعلوماتية خاصة مع استخدام الإنترنت وانتشارهاعالميًا, فقد وجدت بعض حالات التجسس الدولي ومنها ما أكتشفخيرًا عن مفتاح وكالة الأمن القومي الأمريكي,والتي قامت براعته في نظام التشغيل الشهير ويندوز,كما كشف النقاب عن شبكة دولية ضخمة للتجسس تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الإستخبارات, ومع توسع التجارة الإلكترونية عبر شبكة الإنترنت

تحولت الكثير من مصادر المعلومات إلى أهداف للتجسس.

فتعتبر جريمة التجسس من الجرائم الواقعة على أمن الدولة الخارجي, وتمثل نمطا من أنماط السلوك الإنساني رافق نشوء المجتمعات القديمة, وتطور بتطورها, وأصبح له في العصر الحاضر شأن كبير, وقد أولت ظاهرة الجاسوسية أهمية خاصة فرصدت لتلك الظاهرة الموارد والتكنولوجيا والخطط والأفراد, ولقد تجلت ظاهرة الجاسوسية في الحربين العالميتين الأولى والثانية, فجحافل الجيوش المتشابكة في ساحات المعارك الطاحنة تساندها جحافل خفية تخوض معارك المعلومات الطاحنة[1], ولقد اتسمت الجاسوسية قديماً بالطابع العسكري المحض, وتعلقت بتحركاتها الأفراد والأسلحة أثناء العمليات الحربية أما في الحروب الحديثة فقد اتسع نطاق الجاسوسية ليشتمل على التجسس العسكري والسياسي والإقتصادي والصناعي, كما لا نستبعد من استخدام سلاح فيروس الكمبيوتر في الأعمال العسكرية والحروب القادمة ويكون ذلك باختراق نظم الحاسبات بغرض الحصول على المعلومات والبيانات السرية ذات الأهمية الخاصة, وذلك عن طريق زرع فيروس له القدرة على سرقة كلمات الكود المستخدمة في النظم وعن طريقها يمكن الوصول إلى المعلومات الحساسة وتخزينها في أحد الملفات السرية بالحاسب حيث يمكن لزارع هذا الفيروس استخدام المعلومات عند الحاجة إليها, ويعدُّ ذلك من أخطر أنشطة التجسس في المستقبل, وربما يكون قد أستخدم هذا الأسلوب في التجسس على الأنشطة الصناعية[2], بالإضافة إلى تدمير البيانات أو إتلافها أو إظهار أخطاء خداعية في حاسبات نظم القيادة والسيطرة مما يربك القيادة خلال إدارة العمليات العسكرية وصولاً إلى تنشيط الفيروس بحيث يصبح قادراً على القيام بالعمليات المطلوبة في الوقت المناسب, ويعتبر هذا الأسلوب ذا تأثير شديد[3].

[1]– عبد المجيد بوناب, المرجع السابق, ص 27.

[2]– عبد المجيد بوناب, المرجع نفسه, ص 27.

[3]– عبد المجيد بوناب, المرجع نفسه, ص 27.

الفصـل الثاني : الإثبـات في الجريمة المعلوماتيـة

قال أحد الفقهاء منذ القديم " إن الحق المُجرد من الإثبات يصبح هو والعدم سواء ", فالدليل له دوراً مهماً في الإثبات الجنائي ويحتل مكانة هامة في السياسة الجنائية وخصوصاً على صعيد الجريمة المعلوماتية التي يتّسم فيها المجرم بالذكاء والدهاء، ومن ثم كان ولابدّ على نظرية الإثبات الجنائي, مسايرة خصوصية الجريمة والمجرم على حد سواء، بالتالي نجد أنفسنا نغوص في الدليل الجنائي من حيث شروطه و النصوص النظامية التي يجب توافرها حتى يمكن الاستناد إليه في الإثبات والحكم بالإدانة, وتوافر هذه الشروط يسمى بالشرعية الإجرائيـة أو قاعدة مشروعية الدليل الجنـائي.

لهذا فدراستي في هذا الفصل سوف تتمحور حول كيفية ضبط وجمع أدلة هذه الجرائم المعلوماتية,وآلية الإثبات الجنائي على المتهم مقترف هذه الجرائم, وأهم الطرق الفنية التي تقوم بها السلطة المختصة بالتحقيق في كشفها لهاته الجرائم وآليات مكافحتها من حيث ضبطها والتحقيق فيها ووجوب طرح ومناقشة تلك الأدلـة في الجلسة.

وقد أردت تقسيم الدراسة في هذا الفصل إلى مبحثين, مبحث أول أتطرق فيه إلى مراحل جمع الأدلـة أمّـا المبحث الثاني فخصصته إلى تقدير الأدلـة في الجريمة المعلوماتيـة.

المبحث الأول : مراحـل جمع الأدلـة

إن ما يميز الجرائم المعلوماتية أنها ذات طبيعة خاصة وأدلتها غير محسوسة, وتحتاج لخبرة فنية وتقنية عاليةتمر ّ بذات مرحلتي الاستدلال والتحقيق الجنائي المتكامل, وما يترتب على ذلك من إجراءات قانونية فنية وشكليةوا إجراءات التحقيق الجنائي العام هي الأساس في تحقيق جرائم الحاسب الآلي وذلك من سماع للشهود ومعاينة وقبض وتفتيش واستجواب, لكن إجراءات التحقيق الأخرى العملية والفنية والنفسية يتوقف استخدامهاعلى ظروف كلّ جر يمة على حدى مع مراعاة الخصوصية التي تتّسم بها الجريمة المعلوماتية, وكشف وتجميع الأدلة في الجريمة المعلوماتية تواجهه صعوبة بالغة سببها عدم رؤية الدليل أو عدم القدرة على استظهاره.

وعليه تضطلع النيابة العامة بإجراءات التحقيق والإشراف على الضبطية القضائية أثناء عملها في البحث الجنائي والتفتيش واستقصاء الجريمة, بالتنسيق مع أجهزة الشرطة التي تقوم بدور فعال ورئيسي حال وقوع الجريمة..

لهذا سوف تنصب دراستي في هذا المبحث على إجراءات ضبط وتوقيف المجرم المعلوماتي ومعاينة مسرح الجريمة وضبط أدلتها تليها مرحلة التوقيف للنظر وذلك من خلال مطلبين, أتطرق في الأول إلى مرحلة البحث والتحري, تليها مرحلة التحقيق وهذا ضمن المطلب الثاني .

المطلب الأول : مرحلة البحث والتحري

يقصد بالتحقيق التمهيدي, بمرحلة البحث والتحري وجمع وضبط أدلة الجريمة حول الوقائع مجلُر ّ مة المعهودة للضبطية القضائية,مالُ كلفون خلال مرحلة التحقيق التمهيدي بالكشف عن وقوع جريمة معلوماتية وجمع الإستدلالات عنها، لذا نجد قانون الإجراءات الجزائية الجزائري في المادة 16 فقرة 7 منه قد وسع مجال اختصاصهمالمحلي وجعله وطنيً ا مهما كانت الجهة التي ينتمي إليها ضابط الشرطة القضائية من فئة الدرك الوطني أو الأمن الوطني, بينما أعوان الأمن العسكري, فإن اختصاصهم وطني, أي يمتد لكافة الإقليم الوطني ولا تطبق عليهم شروط تمديد الاختصاص وضوابطه المنصوص عليها في المادة 16 من قانون الإجراءات الجزائية الجزائري.

و على كل يجب أن توافر بعض الأمور العامة في المحقق ليقوم بعمله على أحسن وجه أهمها:

- ✓ معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والإنترنت والتي تتعلق بالجريمة المرتكبة.

- وصول الإخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والإنترنت من الفنيين.
- تشكيل فرق تحقيق فنية وإعطاء كلّ واحد منهم مهمة معينة من خلال عملية التفتيش.
- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية وتخزينها.
- البحث عن الأدوات المستخدمة في ارتكاب الجريمة, وطرق الدخول على البرامج المخزنة, وكيفية الحصول على الأرقام السرية والشيفرات الفنية التي تمكنهم من الدخول إلى الحاسوب.
- وضع خطة عمل مع جميع أعضاء فريق التحقيق, والتشاور لمعرفة الجوانب الفنية للجريمة[1].

و هذا بالنسبة للمتطلبات العامة، أما بالنسبة لتمايز كل فئة وكلّ إجراء يستدعي بالضرورة دراسة هذا المطلب الأول, عبر فرعين اعتمدت فيهما التسلسل المرحلي, فالأول خصصته لمسألة معاينة مسرح الجريمة المعلوماتية وضبط أدلتها أمّا الفرع الثاني فأتطرق فيه إلى مرحلة التوقيف للنظر.

الفرع الأول : معاينة مسرح الجريمة المعلوماتية وضبط الأدلة

يمثل مسرح الجريمة المعلوماتية نقطة البداية المهمة بالنسبة إلى سلطات التحقيق في مجال كشف الجريمة المعلوماتية وإزالة غموضها, فهو حسب رأي المختصين يعتبر مستودع أسرار الجريمة الذي قد تنبثق منه الأدلة كافة التي تؤدي في النهاية إلى كشف الحقيقة.

سوف نتكلم في هذا الفرع عن المعاينة وأهميتها مع ذكر العوائق التي تعترضها مبرزًا بعض القواعد والإرشادات الفنية الواجب إتباعها, ثم توضيح بعض الأمور التي تدخل في نطاق ضبط أو جمع أدلة هذه الجرائم المعلوماتية وذلك كما يلي :

أولاً : معاينة مسرح الجريمة : لقد تعددت التعريفات الفقهية للمعاينة في ظلّ تجنب المشرع لتعريفها, ومن هذه التعريفات ما ذهب إليه جانب من الفقه بالقول أنها " رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كلّ ما يلزم لكشف الحقيقة "[2].

وقد عرف أيضًا بأنه " المكان الذي تنبثق منه الأدلة كافة, إمّا أن يكون مكانًا واحدًا أو أماكن عدّة متصلة أو متباعدة تكون في مجموعها مسرح الجريمة وكلّ مكان يستدل منه على أثر يرتبط

---

[1] - خالد عياد الحلبي, المرجع السابق, ص 184.

[2] - عفيفي كامل عفيفي, المرجع السابق, ص 353.

بالجريمة محل البحث يكون جزءً ا من مسرحها", كما عرفه آخرون مسرح الجريمة بأنه مكان وقوعها أو المكان الذي طرقه الجاني أو دخله ومارس فيه الخطوات التنفيذية لارتكاب جريمته "[1].

كما يصفها البعض الآخر وصفًا أكثر دقة بتعريفه إياها أنها " إثبات لحالة الأماكن والأشخاص وكلّ ما يفيد في كشف الحقيقة "[2], ومع التباين في الآراء حول التحديد الأنسب لمسرح الجريمة, إلاّ أن المقصود والهدف في مجال البحث الجنائي والتحقيق ومقتضيات العمل البحثي في مجال كشف الجريمة والوصول للحقائق يتطلب التوسع في تحديد مسرح الجريمة وعدم إهمال أي إحتمال أو مكان حتى ولو ظهر ضئيلاً أو بعيدً ا, لذلك نرى أنه عبارة علىكلّ مكان اتصل بالنشاط الإجرامي الذي ترتب عليه وقوع الجريمة أو حوى دليلاً يتصل به ويدعم في إجراءات الكشف.

إذًا فمن خلال استقراء تلك التعريفات نجد أن كلاهما يتمحور حول فكرة واحدة مؤداها أن إجراء المعاينة سيؤدي بالضرورة بجهات التحقيق إلى الانتقالالمسرح وقوع جريمة معلوماتية تمامً ا كما في الجرائم التقليدية الأخرى, وذلك بهدف إثبات وملاحظة الأشياء التي قد تكون استعملت في ارتكاب الجريمة وا ٍثبات حالتها للتوصل إلى كشف الحقيقة.

1/ أهمية معاينة مسرح الجريمة :إن أهمية المعاينة تكمن أساسً ا في أنها تنقل لجهة التحقيق والمحاكمة صورة مجملة لموقع الجريمةبكلّ ما يحتويه من تفصيلات سواء تعلقت هذه التفصيلات بمكان وقوع الجريمة ووضعه من الداخل, أو بالآثار الموجودة به والمتعلقة بالجريمة المرتكبةوا ٍجمالاً كلّ ما من شأنه أن يساعد الجهات الشرطية والقضائية, ويمكنهم من وضع تصور لكيفية وقوع الجريمة واستخلاصبعض الأدلة من المادة التي تمّ جمعها[3].

2/ الصعوبات التي تعترض معاينة مسرح الجرائم المعلوماتية : لما كان محل جرائم المعلوماتية هو برامج الحاسب الآلي وبياناته أو بواسطتها, فإن التساؤل يثور حول مدى صلاحية مسرح هذه الجرائم للمعاينةنظرا للصعوبات التي قد تحُول دون تحقيق فعالية المعاينة أو فائدتها.

---

[1]- منصور عمر المعايطة, الأدلة الجنائية والتحقيق الجنائي, دار الثقافة, عمان, الطبعة الثانية , 2011, ص 67.

[2]- عفيفي كامل عفيفي, المرجع نفسه, ص 353.

[3]- عفيفي كامل عفيفي, المرجع نفسه, ص 354.

ويمكن أن نلخص أبرز الصعوبات التي قد تعترض معاينة مسرح الجريمة المعلوماتية في الآتي[1]:

- ✓ قلة الآثار التي قد تتخلف عن هذا النوع من الجرائم, باعتبار أن محلها هو بيانات وبرامج الحاسب الآلي أي أن هذه الجرائم تقع على أشياء غير ملموسة ممّا يعني أن تخلف الآثار عنها نادر جدّا.
- ✓ الأعداد الكبيرة من الأشخاص الذين يتردّدون على مسرح وقوع الجريمة المعلوماتية خلال المدّة الزمنية التي غالباً ما تكون طويلة نسبياً بين تاريخ وقوع الجريمة وتاريخ الكشف عنها, الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها, وهو ما يلقي ضلالاً من الشك حول الدليل المستقى من المعاينة.

3/ بعض القواعد والإرشادات الفنية الواجب إتباعها عند معاينة مسرح الجريمة المعلوماتية:

تتطلب المعاينة ضرورة إتباع مجموعة من القواعد والإرشادات الفنية والعملية عند إجرائها, ونلخص أبرزها في الآتي :

- ✓ القيام بتصوير الحاسب وما قد يتصل به من أجهزة طرفية ومحتوياته وأوضاع المكان الذي يوجد به بصفة عامة.
- ✓ ملاحظة طريقة إعداد نظام الحاسب بعناية بالغة.
- ✓ التحفظ على بيانات الإدخال والمخرجات الورقية للحاسب الآلي, وهذا لرفع البصمات.
- ✓ حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة والشرائط والأقراص الممغنطة غير السليمة, وفحصها.
- ✓ يجب أن تقتصر المعاينة على مأموري الضبط القضائي, سواء كانوا من الباحثين أو من المحققين, ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحواسيب واسترجاع المعلومات, ممن تلقوا التدريب الكافي لمواجهة هذا النوع من الجرائم وكيفية التعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة[2].
- ✓ في الأخير, يجب أن تتّم هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين

---

[1]– عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, دار النهضة العربية, القاهرة, مصر, الطبعة الأولى, 2009, ص 212.

[2]– عفيفي كامل عفيفي, المرجع السابق, ص 357.

الجزائية[1].

ثانياً : ضبط الأدلة : نقصد بالضبط في هذا المجال, جمع الأدلة في الجريمة المعلوماتية, ولهذا يمكن تعريف الضبط على أنه إجراء من إجراءات التحقيق يهدف إلى وضع اليد على الأدلة المتحصل عليها وتحريزها وحفظها لمصلحة المحقق.

والضبط لا يتوقف على تحريز جهاز الحاسوب فقط,إنّما يمتد من ناحية ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم, والأهم في هذا الصدد هو أن الضبط في مجال لجرائم المعلوماتية ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الإشتباه, ما يعني أن محل الضبط ليس إلاّ أشياء ذات طبيعة معنوية معرضة بسهولة للتغيير والإتلاف[2].

1/ الإختلاف الفقهي حول مدى صلاحية جرائم الحاسب الآلي لجمع الأدلة بشأنها نظراً لكون الضبط وجمع الأدلة في هذه الجرائم محله البيانات والبرامج المعالجة آلياً , فقد ثار التساؤل حول مدى صلاحية هذه البيانات لأن تكون محلاً لجمع أدلتها, لذلك انقسم الفقه في هذا الصدد إلى اتجاهين, فيرى الأول أن بيانات الحاسب الآلي لا تصلح لأن تكون محلاً للضبط لانتفاء الكيان المادي عنها وبالتالي استحالة جمع الأدلة بشأنها.

بينما يرى اتجاهثاني أن البيانات المعالجة آلياً ما هي إلاّ ذبذبات إلكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ والتخزين على وسائط مادية وبذلك لا يمكن إنكار وجوده المادي, وبالتالي فهي تصلح لأن تكون محلاً لضبط وجمع أدلتها[3].

بهذا نرى أنه هناك خلاف جوهري بين الفقهاء حول مدى صلاحية الجرائم المعلوماتية لضبط وجمع أدلتها, فجانب من الفقه يرى بأنه لا مجال لجمع الأدلة في هذه الجرائم, بينما هناك رأي فقهي

1- محمد عبيد سيف سعيد المسماري و عبد الناصر محمد فرغلي, الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية, بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, 12-14 نوفمبر 2007, ص 18.

2- كمال أحمد الكركي,التحقيق في جر ائم الحاسوب, ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية, تنظيم أكاديمية شرطة دبي, مركز البحوث والدراسات, دبي, الإمارات العربية المتحدة, 26-28 أفريل 2003, ص 02-03.

3- عبد الفتاح بيومي حجازي,الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, المرجع السابق, ص 272.

ثاني يرى عكس ذلك ويقول بأن هذه الجرائم المعلوماتية مثل بقية الجرائم التقليدية يمكن جمع الأدلة بشأنها دون أي إشكال, طالما أن تلك البيانات التي تقع عليها هذه الجرائم يمكن أن تسجل وتحفظ على وسائط مادية فيمكن ضبطها كأدلة مادية,وقد أدّى هذا الخلاف الفقهي بالمشرع اليوم في بعض دول العالم, إن لم تكن أغلبها إلى تحديث النصوص التشريعية المتعلقة بالجوانب الموضوعية والإجرائية لمكافحة الجرائم المعلوماتية بما يتو افق وخصوصياتها.

وممّا لا شك فيه أن الضبط وجمع الأدلة في الجرائم المعلوماتية ينصب على المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة بالنظام محل الإشتباه أي على الأشياء ذات الطبيعة المعنوية, وهذا ما يثير دون أدنى شك بعض الصعوبات العملية التي تصادف رجال الشرطة أثناء قيامهم بجمع أدلة الجريمة المعلوماتية[1].

2/ الصعوبات العملية في جمع أدلة الجريمة المعلوماتية وسبل تجاوزها : إن مرحلة جمع الأدلة في الجرائم المعلوماتية تصادفها عدّة صعوبات عملية تحول في بعض الأحيان دون تمكن رجال الشرطة والتحقيق من جمع الأدلة الكافية التي تمكنهم من كشف خيوط وملابسات الجريمة.

ولعلّ أهم هذه الصعوبات, تلك الناجمة عن قلة خبرة أجهزة الشرطة بسبب قلة تدريبها في هذا المجال, ما يترتب عليه فشلها هي والأجهزة الأخرى المنوط بها التحقيق وجمع الأدلة في هذا النوع من الجرائم,كذلك قد تصادف المحقق صعوبات تحول دون ضبطه للبيانات التي تعدّ دليلاً على ارتكاب جريمة ما في العالم المعلوماتي, ومن ضمن تلك الصعوبات نذكر الآتي[2] :

- ✓ عدم وجود دليل مرئي يمكن فهمه بالقراءة باعتبار أن بيانات الحاسب الآلي التي تقع عليها الجرائم المعلوماتية أو قد تقع بواسطتها غير مرئية وبالتالي هناك عائق لجهاز الشرطة يحول بينه وبين ضبط هذه الجرائم والوقوف على أدلتها وعلى مرتكبيها.
- ✓ كذلك فإن البيانات التي يمكن التوصل إليها, فإنه يمكن محوها أو تدميرها من قبل الجاني في فترة زمنية بسيطة لا تتعدى ثوان معدودة, ويمكن للجاني تبرير موقفه بأن هناك خطأ في نظام الحاسب

---

[1]- محمد أبو العلاء عقيدة, التحقيق وجمع الأدلة في الجرائم الإلكترونية, ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية, تنظيم أكاديمية شرطة دبي, مركز البحوث والدراسات, دبي, الإمارات العربية المتحدة, 26-28 أفريل 2003, ص 02-03.

[2]- عبد الفتاح بيومي حجازي,مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, المرجع السابق, ص 214.

الآلي, وبالتالي يمكن له التنصل من المسؤولية.

- قلة وجود ضابط شرطة قضائية متخصص أو على الأقل من يساعده من ذوي الاختصاص في هذه المجال, على كيفية التعامل مع البيانات التي تعدُّ دليلاً على الجريمة المعلوماتية, الأمر الذي يؤدي إلى إغفال الدليل أو إهماله أو إتلافه أو إفساده.
- ومما يزيدالأمر تعقيداً في حالة الأنظمة الكبيرة والمتصلة بنهاية طرفية أخرى, الأمر الذي قد يؤدي إلى إنتهاك سيادة دولة أخرى موجودة بها هذه البيانات المطلوبة كأدلة من قبل سلطات التحقيق[1].

لذلك من أجل تجنب هذه الصعوبات والمعوقات العملية ومحاولةالحدّ منها, وجعل عملية جمع الأدلة وضبطها أكثر فاعلية وذات فائدة لجهات التحقيق, يجب ضبط وتحريز مجموعة من الأدلة المادية, والتي لها قيمتها الخاصة في إثبات وكشف الجريمة المعلوماتية ونسبتها إلى متهم معين, ومن بين هذه الأدلة ما سنذكره في الآتي[2]:

- الأوراق, سواء أوراق تحضيرية تمّ إعدادها بخط اليد كمسودة تصوير العملية التي يتّم برمجتها, أوراق تالفة التي تمّ طباعتها للتأكد من تمام الجريمة والتي ألقيت في سلّة المهملات, أوراق أصلية والتي قام الجاني بطباعتها وتمّ الإحتفاظ بها كمرجع أو لأغراض الجريمة, أوراق أساسية وقانونية المحفوظة في الملفات العادية أو دفتر الحسابات, وكلّها تعتبر من الأدلة التي يجب الإهتمام والإعتناء بها عند معاينة مسرح الجريمة وعدم إغفالها.
- جهاز الحاسب الآلي وملحقاته, كوحدات المعالجة المركزية ووحدات الإدخال ووحدات الإخراج ووحدات التخزين و المودم والكروت والأقراص الممغنطة وبطاقات الإئتمان, وكلّها أدلة لإثبات الجرائم المعلوماتية.

---

[1]- عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, المرجع نفسه, ص 215.

[2]- عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, المرجع نفسه, ص 60.

الفرع الثاني : مرحلة التوقيف للنظـر

تتطلب مرحلة البحث والتحري عن الجريمة المعلوماتية من ضابط الشرطة القضائية المكلف حصرياً بذلك, القيام بإجراءات اتجاه الأشياء والأشخاص الذين قد يكونون على علاقة بها, سواء بصفة مباشرة أو غير مباشرة, ومن ضمن هذه الإجراءات توقيف الأشخاص على ذمة التحري معهم لمدّة محددّة قانوناً بمكان معين وبتوافر شروط معينة لأجل سماع إفادتهم حول الجريمة المحقق فيها, يعرف هذا الإجراء قانونًا بالتوقيف للنظر, فهو من ضمن الصلاحيات الممارسة من طرف ضباط الشرطة القضائية والتي خولها لهم القانون في إطار الشرعية الإجرائية, يستمد شرعيته من المادتين 47 و 48 من الدستور والمواد 51, 51 مكرر, 51 مكرر 1, 52, 53 من قانون الإجراءات الجزائيةوينطوي كما يدّل عليه إسمه على مساس بأحد أهم حقوق الشخص وهي الحرية في التنقل.

فالتوقيف للنظر إجراء من إجراءات الضبط - بوليسي يتّم بتقييد حرية المشتبه فيه من التنقل أو مبارحة المكان الموضوع فيه, يلجأ إليه ضابط الشرطة القضائية خلال إجراءات التحري التي باشرها لأجل الكشف عن ملابسات الجريمة الواقعة محاولاً الوصول إلى مرتكبها الحقيقي ثم تقديمه أمام الجهة القضائية المختصة بالتوصل في إسنادها إليه ومعاقبته عليها متى ثبت ذلك الإسناد قانوناً وتوفرت شروط الإدانة[1].

سوف نتكلم ضمن هذا الفرع عن تعريف التوقيف للنظر وحالاته, تلي بعدها إجراءاته وأهم شروطه وذلك كما يلي :

أولاً : تعريف التوقيف للنظر وحالاته: يتفق الفقه القانوني على أن التوقيف للنظر هو استثناء من القاعدة العامة (الأصل في الإنسان البراءة), فهو كما يصفه البعض بأنه " اتخاذ تلك الاحتياطات اللازمة لتقييد حرية المقبوض عليه ووضعه تحت تصرف البوليس أو الدرك لفترة زمنية مؤقتة تستهدف منعه من الفرار وتمكين الجهات المختصة من اتخاذ الإجراءات اللازمة ضدّه "[2].

فالتوقيف للنظر هو: إجراء قانوني سالب للحرية يقوم به ضابط الشرطة القضائية لضرورة التحريات الأولية متى استوجبت ذلك أو في الحالات التي حددّها القانون وبموجبه يوضع المشتبه فيه تحت تصرف مصالح الضبطية القضائية ريثما تتّم عملية التحري وجمع الأدلة وذلك في مكان معين

1- جباري عبد المجيد, المرجع السابق, ص 41.

2- جباري عبد المجيد, المرجع نفسه, ص 42.

وطبقًا لشكليات ومدة زمنية يحدّدها القانون, وباعتبار أن التوقيف للنظر من أخطر الصلاحيات الممنوحة لرجال الضبطية القضائية لما فيه من مساس بحرية الأفراد فإن المشرع الجزائري رسم الإطار القانوني لممارسته بدقة فبين حقوق الأشخاص الخاضعين له كما وضع حالات اللجوء إليه وإجراءاته وهما ما يمثل أيضًا من بين حقوق الأشخاص الموقوفين للنظر لأنه من حق هذا الشخص أن لا يوضع في الوقف تحت النظر إلاّ ضمن الحالات التي نص عليها القانون ومن أهم هذه الحالات هي :

1/ في حالة الجنح والجنايات المتلبس بها, وذلك ما نصت عليه المادة 51 من قانون الإجراءات الجزائية والتي أدخل عليها تعديل من خلال قانون 22/06فيما يخص مدى جواز تمديد مدّة التوقيف للنظر.

2/ حالة التحريات الأولية, لقد نظمها المشرع الجزائري وأطلق عليها تسمية حالة التحريات الأولية, أي في غير حالة التلبس وذلك بموجب إحكام المادة 65من قانون الإجراءات الجزائية المعدلة أيضًا من خلال قانون 22/06 وتختلف هذه الحالة عن سابقتها فيما يخص مدة التوقيف للنظر.

3/ في حالة تنفيذ الإنابة القضائية, وذلك حسب مضمون المادة 141 من قانون الإجراءات الجزائية التي تنص على صلاحية أو سلطة ضابط الشرطة القضائية لتوقيف الأشخاص تحت النظر لمدة حدّدها القانون بـ 48 ساعة مع جواز تمديد تلك المدّة بإذن كتابي من قاضي التحقيق بعد سماع المتهم المقدم له, هذا مع إمكانية التمديد بصفة استثنائية دون تقديمه وبالتالي فهذه الحالة تختلف أساسًا عن سابقتها فيما يخص الجهة التي تمنح تمديد التوقيف تحت النظر.

وفور اتخاذ ذلك الإذن المسبب والمتمثل في توقيف الشخص للنظر, يتعين على ضابط الشرطة القضائية أن يخبر الشخص الموقوف للنظر بالحقوق المذكورة في المادة 51 مكرر 1 من قانون الإجراءات الجزائية, وهي حقه في الإتصال بأفراد عائلته وتلقي زيارتهم وبحقه في إجراء فحص طبي له عند انقضاء مدّة التوقيف للنظر, مع الإشارة إلى ذلك في محضر سماع وفي سجل خاص المعدّ خصيصًا لذاك الغرض وذلك حسب المادة 52 من قانون الإجراءات الجزائية, وذلك كلّه مع مراعاة سرية التحريات.

ثانياً : إجراءات التوقيف للنظر وشروطه : إن تحديد وشرح الإجراءات التي ينبغي على ضابط الشرطة القضائية أن يراعيها بالنسبة للتوقيف للنظر وتلزمه بها فالغرض منها الوقاية من أي شكل من أشكال التعسف أو الإخلال بحقوق وحريات المشتبه فيهم,ومن شأنها أن تجعل عمله مندرجاً في إطار الشرعية الإجرائية وذلك ضماناً لفاعلية التحريات وجعل الإجراءات المنفردة خلال تلك المرحلة بمنأى عن البطلان, ومن أهم هذه الشروط والإجراءات هي :

1/ إطلاع النيابة العامة:على ضابط الشرطة القضائية إطلاع وكيل الجمهورية فوراً بكلّ توقيف للنظر ويقدم له تقريراً يبين فيه دواعي التوقيف للنظر وهذا طبقاً لنص المادة 51 من قانون الإجراءات الجزائية "... فعليه أن يطلع وكيل الجمهورية ويقدم له دواعي التوقيف للنظر".

2/مدّة التوقيف للنظر:لقد حدّد المشرع الجزائري المدّة المقررة للتوقيف للنظر بدّقة ولم يتجاهلها, ولم يترك فيها مجالاً للسلطة التقديرية لضابط الشرطة القضائية,أي تمّ تقييده بضوابط قانونية يجب الإلتزام بها, وعكس ذلك يضفي عليه صفة عدم المشروعية على كلّ توقيف للنظر يتجاوز مدته المدّة المقررة قانوناً فيجرّمه باعتباره حبساً تعسفياً وقد حدّدها القانون في المادة 48 من الدستور بثمانية وأربعين (48) ساعة,ونصت عليها كلّ من المواد 51, 65, 141 من قانون الإجراءات الجزائية, وعند إنتهاء هذه المدّة المحدّدة قانوناً يقرر إمّا إطلاق صراح الموقوف وفوراً أو إقتياده إلى وكيل الجمهورية أو قاضي التحقيق أو القاضي المناوب بحسب الحالة غير المتوقعة.

3/آجال تمديد مدّة التوقيف للنظر:لا يجوز لضابط الشرطة القضائية أن يُمدّد فترة توقيف شخص تحت النظر من تلقاء نفسه,لأن القاعدة تقضي بعدم جواز ذلك طبقاً لنص المادة 51 فقرة 2 من قانون الإجراءات الجزائية, إلاّ أن قانون 22/06 جاء بتعديل في هذا الجانب إذ نصت المادة 51 على أنه يجوز لضابط الشرطة القضائية وضع أي شخص ممن أشير إلهم في المادة 50 في الوقف للنظر إن كانت هناك دواعي لذلك.

والجديد في نص المادة 51من قانون الإجراءات الجزائية أن المشرع أجاز تمديد الوقف تحت النظر لمرة (1) واحدة عندما يتعلق الأمر بجرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات, لأن نوعية الجريمة كانت موضوع تشريع جديد أصدره المشرع الجزائري في الآونة الأخيرة وأن خصوصية هذه الجريمة من حيث البحث على أدلة الإثبات قد تتطلب مدة زمنية معينة لضابط الشرطة القضائية حتى يستطيع التحري وجمع الأدلة بخصوصها.

المطلب الثاني : مرحلـة التحقيـق

الجرائم المعلوماتية لها خطورة خاصة تتميز بها نظراً للتقنية العالية المستخدمة في ارتكابها, وغموض شخصية مرتكبيها, كما أنها أصبحت وسيلة كذلك لارتكاب الجريمة المنظمة في ثوبها المستحدث مما خلفت ورائها الكثير من المشاكل التي تؤثر على عملية التحقيق تؤدي بها إلى الخروج بنتائج تنعكس على نفسية قاضي التحقيق بفقدانه الثقة في نفسه وفي آدائه, وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها, فخلفت تلك الجرائم المستحدثة آثاراً وتحديات بالغة أثناء التحقيق فيها للوصول إلى مرتكبي هذه الجرائم, كما أثارت تحديات قانونية وتقنية وفنية بشأن آليات مباشرة إجراءات التحقيق والتعامل مع هذه الجرائم المستحدثة.

ولهذا قسمت هذا المطلب إلى فرعين, الأول حاولت فيه التطرق إلى التفتيش واستجواب المتهم, والثاني تكلمت فيه عن الإجراءات التقنية والفنية في عملية التحقيق في الجرائم المعلوماتيـة.

الفرع الأول : التفتيش واستجواب المتهم

لقد خص المشرع الجزائري قاضي التحقيق بسلطات واسعة للقيام بمهمة التحقيق في القضايا المعروضة عليه, سواء بمناسبة اتصاله بها عن طريق وكيل الجمهورية أو أحد مساعديه بالطلب الافتتاحي لإجراء التحقيق, أو بمناسبة تقديم الطرف المتضرر من الجريمة بشكوى مصحوبة بإدعاء مدني,وخارج هاذين الطريقتين لا يمكنه إطلاقاً القيام بأعماله القضائية وإنه يمكن أن ينتدب لإجراء تحقيق تكميلي من غرفة الاتهام في قضية معينة, ولأجل محاضر الإجراءات التي يقوم بها فإنه يمسك لكل قضية يتولى التحقيق فيها ملفاً, يقوم بتشكيله منذ توصله بالقضية,وله سلطة إصدار عدّة أوامر قضائية في سبيل تأدية المهام المنوطة به, وسوف أوجز بعض من أعماله في مواجهة الجريمة المعلوماتية عبر النقاط التاليـة :

أولاً : التفتيش : إن التفتيش ليس غاية في ذاته, لكن هو وسيلة للحصول على غاية معينة, وهي البحث عن دليل يتعلق بجريمة وقعت بالفعل, وباعتبار أن التفتيش هو إجراء من إجراءات التحقيق الإبتدائي, فهو يخضع لسائر الخصائص التي تحكمه, سواء في وجوب تدوينها وسريتها على الجمهور, وجواز اتخاذها في غيبة الخصوم ووكلائهم[1].

والتفتيش بصورة عامة "هو إجراء من إجراءات التحقيق, لا تجوز مباشرته أو الإذن به إلاّ بشأن جريمة تشكل جناية أو جنحة, وقعت للبحث عن دليل يفيد في كشف الحقيقة حيال شخص قامت دلائل كافية على اتهامه فيها, بوصفه فاعلاً أو شريكاً, أو على أنه حائز لأشياء استعملت في الجريمة أو نتجت عنها, أو تعلقت بها, متى ما استلزمت ذلك ضرورة التحقيق,وتقوم به سلطة حدّدها القانون في محل له حرمة, لأنه مستودع الحق في سر الإنسان, إنّما يباشر لأن ضرورة التحقيق تقتضيه وسواء رضي به من يباشر حياله أم لم يرضى"[2].

وكأصل عام أن التفتيش تختص به سلطة التحقيق بصفة أصلية واستثناءً الشرطة والدرك متى كان لهم هذه الصفة[3].

والمشرع الجزائري لم يورد تعريفاً خاصاً للتفتيش, بقدر ما اعتبره إجراء من إجراءات التحقيق الإبتدائي, وأحاطه بضوابط صارمة في الكشف عن الأدلة, مع تميزه بالخطورة لأنه يترتب عنه مساس بحرية الأشخاص وبكرامتهم, ممّا يؤكد ذلك حرص الدستور الجزائري بهذه النقطة إذ نصت المادة 40 منه على " ولا تفتيش إلاّ بأمر مكتوب صادر عن السلطة القضائية المختصة "[4], لهذا وضع المشرع الجزائري قيوداً مشدّدة لإجراء عملية التفتيش تتجسد هذه القيود في الشروط الموضوعية والشكلية التي لا بدّ من توافرها للإقدام على عملية التفتيش, وهي كما يلي :

1- عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, المرجع السابق, ص 629.

2- سامي جلال فقي حسين, الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي - دراسة مقارنة -, دار الكتب القانونية, مصر, دون طبعة, 2011, ص 137.

3- عبد الفتاح بيومي حجازي, مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, المرجع السابق, ص 192.

4- زيدان زبيحة, الجريمة المعلوماتية في التشريع الجزائري والدولي, دار الهدى, عين مليلة, الجزائر, دون طبعة, 2011, ص 130.

1/ الشروط الموضوعية للتفتيش : ينبغي توفر مجموعة من الشروط عند إجراء التفتيش, ويمكن تلخيصها في الآتي :

أ- سبب التفتيش : يشترط لصحة التفتيش أن تكون هناك جريمة معلوماتية وقعت فعلاً , وأن يكون التفتيش بقصد ضبط أشياء تتعلق بتلك الجريمة, أو تريد كشف حقيقة مجهولة,بمعنى لا بدّ من وجود سبب وجيه للتفتيش, سواء كان منزل المتهم أو منظومته المعلوماتية,وأن يكون هناك إتهام قائم ضدّ شخص أو أشخاص معينين تورطوا في إرتكاب الجريمة المعلوماتية,وإلاّ أصبح التفتيش باطلاً , بدون أي مبرر, وتدخل في خصوصيته.

ب- الغاية من التفتيش :لا بدّ أن يكون التفتيش بقصد ضبط أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة,وإلاّ وقع التفتيش باطلاً , ولا يجوز تفتيش المدافع عن المتهم بقصد ضبط أوراق أو مستندات سلّمها إليه المتهم لأداء مهمة الدفاع عنه, ولا المراسلات المتبادلة بينهما, كما لا يجوز تفتيش منازل المحامين[1].

فتعتبر تلك الأدلة المضبوطة هي أدلة إقناع, أي الآثار التي يتركها المجرم المعلوماتي عادة في مسرح الجريمة ويتّم الاستعانة بها من طرف قاضي التحقيق لتعزيز اعترافات المتهم في حالة إعترافه وربط الجرم المنسوب إليه وهذا في حالة إنكاره, كما نصت على حجز المعطيات المعلوماتية المادة 6 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم الخاصة المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها,وحدّدت المادة 84 من قانون الإجراءات الجزائية قواعد حجز الأشياء المفيدة للتحقيق, فجميع الأجهزة أو المعدات المعلوماتية ومختلف الوثائق المضبوطة والتي تمّ حجزها يجب على الفور جردها ووضعها في أحراز مختومة ويتّم تحرير محضر بضبطها كأدلة إقناع[2].

2/ الشروط الشكلية للتفتيش : نص المشرع الجزائري في نص المادة 05 من القانون رقم 09-04 السالف الذكر وهذا ضمن الفصل الثالث, بأن التفتيش في الجرائم المعلوماتية تمّ إدراجه في إطار قانون الإجراءات الجزائية الجزائري, ومن الواضح أن طبيعة الاختلاف بخصوص موضوع التفتيش في

1- عبد الفتاح بيومي حجازي,الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, المرجع السابق, ص 631.

2- محمد حزيط,مذكرات في قانون الإجراءات الجزائية الجزائري, دار هومه, الجزائر, الطبعة التاسعة, 2014, ص 175.

مجال الجرائم المعلوماتية يختلف كلياً عن التفتيش في الجرائم التقليدية، فهو يتوقف أساساً على طبيعة المكان الذي يحتوي أجهزة الحاسب الآلي ومكوناته فيما إذا كان خاصاً أو عاماً, هذا فضلاً عن تحديد الإقليم وطنياً أم أجنبياً, وأهم هذه الشروط ما يلي :

- ✓ وجود إذن مكتوب صادر عن وكيل الجمهورية أو قاضي التحقيق, مع الإشارة فيما يتعلق بإذن التفتيش, فتبدو صعوبة في هذا الصدد في اشتراط أن يكون هذا الإذن محدّداً فيما يخص محله والأشياء التي يهدف التفتيش إلى ضبطها وهي في الأساس بيانات جوهرية يجب توافرها في إذن التفتيش حسب القواعد العامة, وهذا الشرط يتطلب أن يقوم مصدر الإذن بتحديد الشيء المراد ضبطها بطريقة فنية, الأمر الذي لا يكون في مقدوره لأنه يتطلب نوع من المعرفة الفنية يتجاوز في مداه الثقافة والمعرفة العامة أو السطحية للأمور[1].
- ✓ إستظهار الإذن قبل دخول المكان المراد تفتيشه.
- ✓ أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل المراد تفتيشه, وعنوان الأماكن المقصودة بالتفتيش.
- ✓ جواز حضور بعض الأشخاص المؤهلين والمختصين بشكل ممتاز بعمل المنظومة المعلوماتية محل البحث قصد حماية المعطيات المعلوماتية التي تتضمنها قصد تسهيل ومساعدة السلطات المكلفة بالتفتيش وهذا طبقاً للمادة 5 فقرة أخيرة من قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

كما يمكن لضابط الشرطة القضائية المناب أو قاضي التحقيق إجراء عملية التفتيش ليلاً أو نهاراً وفي أي مكان على إمتداد التراب الوطني, وبدون حضور المتهم أو صاحب المسكن ودون حضور الشاهدين إذا تعلق الأمر بتلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات,و عدم تقيدهم بالأوقات, وهو ما نصت عليه المادة 47 فقرة 4 من قانون الإجراءات الجزائية.

وفيما يتعلق بمحل التفتيش في الجريمة المعلوماتية فهو ينصب على كلّ مكونات الحاسب الآلي, سواء كانت مادية مثل (وحدة الإدخال, وحدة المعالجة الرئيسية, وحدة الإخراج, وحدة التخزين) أو معنوية مثل (برامج المعالجة, برامج التشغيل, برامج الترجمة والبرامج والمعلومات المخزنة في

---

[1]- عبد الفتاح بيومي حجازي,مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, المرجع السابق, ص 197.

الحاسوب), فكلّها تصلح لأن تكون محلاً للتفتيش ويصح الإستناد إليها كدليل على ارتكاب الجريمة, وكذلك شبكات الإتصال الخاصة به, بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش.

وتجدر الإشارة إليه, أنه لا يقتصر نطاق هذه الشبكات على النطاق الإقليمي للدولة فقط, بل إنه يمتد ليشمل النطاق الإقليمي لدولة أخرى نتيجة الربط الشبكي بين أجزاء العالم وبصفة خاصة مع ظهور شبكة الإتصالات الدولية (الإنترنت), وولوج نظم المعالجة الآلية للبيانات للبحث والتنقيب في البرامج المستخدمة وملفات البيانات المخزنة عمّا يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها إجراء قد تقتضي مصلحة وظروف تحقيق جرائم الحاسبات مباشرته وهو إجراء جائز قانوناً, فهناك بعض التشريعات تسمح بجواز إمتداد التفتيش إلى خارج الدولة في حالة إتصال حاسب الشخص بحاسب أو نهاية طرفية في هذا المجال فنجد المادة 2/17 من القانون الفرنسي رقم 239 لسنة 2003 بشأن الأمن الداخلي تجيز لرجال الضبط القضائي القيم بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية فتنص على أنه " إذا كانت البيانات مخزنة في نظام معلوماتي يقع خارج إقليم الدولة فإنه يجوز لرجل الضبط القضائي الدخول إلى هذه البيانات مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية"[1].

وتأييداً لذلك صدر عن المجلس الأوروبي توصيات تجيز أن يمتد تفتيش الكمبيوتر إلى الشبكة المتصل بها ولو كانت هذه الشبكة تقع خارج الدولة, فتنص التوصية رقم 13 لسنة 1995 المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتصلة بتقنية المعلومات على أنه " لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقاً لضوابط معينة أن تقوم بمد مجال تفتيش كمبيوتر معين يدخل في دائرة إختصاصها إلى غير ذلك من الأجهزة ما دامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها ما دام أنه من الضروري التدخل الفوري للقيام بذلك "[2].

لهذا تطرق إليه المشرع الجزائري ضمن المادة 5 فقرة 3 من القانون رقم 09-04 والتي تنص بأنه "إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقاً من المنظومة

---

[1]- محمود إبراهيم غازي, الحماية الجنائية للخصوصية والتجارة الإلكترونية, مكتبة الوفاء القانونية, الإسكندرية, مصر, الطبعة الأولى, 2014, ص 780.

[2]- محمود إبراهيم غازي, المرجع نفسه, ص 780.

الأولى, مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني, فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقًا للإتفاقيات الدولية ذات الصلة ووفقًا لمبدأ المعاملة بالمثل ".

ثانيًا : الإستجواب : يقصد بالإستجواب مناقشة المتهم بالتهمة الموجهة إليه ومواجهته بالأدلة القائمة ضدّه, والمتهم حر في الإجابة عن الأسئلة الموجهة عليه, ولا يعدُّ امتناعه قرينة ضدّه, ذلك أن الإستجواب ذو طبيعة مزدوجة, فهو أداة اتهام ووسيلة دفاع في آن واحد, بحيث يسمح للمتهم بأن يحاط بالتهمة الموجهة إليه وبكلّ ما يوجد بالملف من أدلة, ويتيح له الوقت للإدلاء بكل الإيضاحات والأدلة التي تساعد على كشف براءته أمّا الطابع الإتهامي, فيكمن في كونه الطريق المؤدي إلى الدليل الأقوى في الدعوى العمومية الذي يزيل أدنى شك في الإتهام وهو الإعتراف.

ونظرًا لخطورة الآثار التي تترتب عن هذا الإجراء,فإن القانون أحاطه بعدّة ضمانات وشكليات وأي خرق له يُعدّ تحت طائلة البطلان, وهناك أنواع ثلاثة من الإستجواب وهما (الإستجواب عند الحضور الأول, الإستجواب في الموضوع, الإستجواب الإجمالي), وسنرى بعض النقاط الأساسية للإستجواب وهي :

1/ مضمون الإستجواب وصياغته : أوجب القانون عند حضور المتهم لأول مرة أمام قاضي التحقيق وهذا بحضور أمين ضبط غرفة التحقيق, أن يتثبت المحقق من شخصيته وهويته طبقًا للمادة 100 من قانون الإجراءات الجزائية الجزائري,ثم يحيطه علمًا بالتهمة المنسوبة إليه ويثبت ذلك أقواله في المحضر,ثم يتعين على قاضي التحقيق أن يستجوب المتهم خلال مدّة 48 ساعة من حبسه[1] وهذا طبقًا لنص المادة 121 من قانون الإجراءات الجزائية الجزائري.

ولا شك أن مضمون الإستجواب في الجريمة المعلوماتية يتحدّد بمدى إلمام المحقق الجنائي لمفردات هذه الجريمة وطبيعتها, على نحو يمكنه من مواجهة التهم بالأدلة ويعطي له فرصة للدفاع عن نفسه وتفنيد هذه الأدلة[2].

2/ مباشرة الإستجواب بواسطة سلطة التحقيق : بالنظر إلى دقة الإستجواب فقد يشترط مباشرة جهة قضائية مختصة ومحايدة في النيابة العامة أو قاضي التحقيق,وخوفًا من ضياع الوقت وضياع معالم

---

[1]– أحسن بوسقيعة, التحقيق القضائي, دار هومة, الطبعة السابعة, الجزائر, 2008, ص 96.

[2]– عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, المرجع السابق, ص 687.

الجريمة, يمكن لمأموري الضبط القيام بالإستجواب, ويشترط في هذه الحالة أن يكون متصلاً بالعمل المندوب له مأمور الضبط القضائي ولازماً لكشف الحقيقة مثال ذلك أن يكون المتهم مريضاً ومهدداً بعملية جراحية تؤدي إلى تأخير التحقيق, أو يكون المجني عليه على وشك الوفاة, والحكمة من ذلك مواجهة المتهم بالمجني عليه[1].

3/ حقوق المتهم أثناء الإستجواب : من حقوق المتهم أثناء الإستجواب الحق في الصمت, فلا يجبره على الكلام إن امتنع عنه, وهو مبدأ جوهري يفرض نفسه على جميع إجراءات الدعوى الجنائية, وهذا بالنظر إلى المتهم على أنه بريء حتى يثبت العكس بحكم قضائي[2].

ونستخلص من هذا الكلام أن للمتهم الحق في حرية الكلام وعدم الإجابة على الأسئلة الموجهة عليه والتزام الصمت أثناء فترة الإستجواب.

ومن حقوقه أيضاً لا يجوز تعذيب المتهم وإكراهه على الإعتراف, وعدم تأثير قاضي التحقيق على إرادة المتهم تأثيراً مادياً أو معنوياً وإلاّ وقع الإستجواب باطلاً, مع الإشارة إلى أن الحقوق و الضمانات في الجرائم التقليدية, هي نفسها المطبقة في الجرائم المعلوماتية.

4/ حق الإستعانة بمحام أثناء الإستجواب : يعدُّ حق الإستعانة بالدفاع أثناء التحقيق ضمانة من ضمانات سلامة التحقيق وحسن سير إجراءاته, لأن وجود المحامي إلى جانب المتهم وهو يواجه إتهاماً بارتكاب جريمة, من شأنه أن يطمئن المتهم ويساعده على إظهار الحقيقة, أو إثبات براءته, كما يكون عوناً لسلطة التحقيق في تحقيق عادل, كما لا تتقيد النيابة العامة بهذا الحق إذا رأت أن مصلحة التحقيق تقتضي ذلك, فيجوز الإستجواب في غياب المحامي في أحوال وحالات التلبس, والمحقق غير ملزم بانتظاره أو الموافقة على طلب تأخير الإستجواب[3].

5/ قواعد مناقشة المتهم : وضع المشرع الجزائري في قانون الإجراءات الجزائية بعض القواعد, منها ما جاء في المادة 112 من قانون الإجراءات الجزائية, حيث نصت على " يجب أن يستجوب في

---

[1] – عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, المرجع السابق, ص 687.

[2] – محمد حزيط, المرجع السابق, ص 154.

[3] – جودة حسين جهاد و عمر السعيد رمضان, قانون الإجراءات الجنائية الإتحادي في دولة الإمارات العربية المتحدة, أكاديمية شرطة دبي, دبي, الإمارات العربية المتحدة, دون طبعة, 1994, ص 384.

الحال كلّ من سيق أمام قاضي التحقيق تنفيذًا لأمر إحضار, بمساعدة محاميه "[1], وسوف أتعرض إلى بعض النقاط الجوهرية لطريقة الإستجواب وهذا عبر الآتي :

- ✓ عزل المتهمين عن بعضهم في المناقشة والإستجواب, لأنها تعتبر أهم قاعدة حتى لا يتأثر أحدهم بأقوال الآخر أو يؤثر عليه.
- ✓ أن يكون المحقق قادرًا على قراءة لغة الجسم ونبرة الصوت اللتان يستطيع من خلالهما معرفة ما إذا كان الشخص يقول الحقيقة أم لا.
- ✓ أن يكون خبير الحاسوب حاضرًا في عملية الإستجواب من خلال إستعراض أهم الخطوات للإستجواب وضماناته[2].

يمكن القول بأن الإستجواب هو إجراء يمتاز بالدقة نظرًا لأهميته وخصوصيته في سير عملية إجراءات التحقيق الجنائي في الجرائم بصفة عامة والجرائم المعلوماتيـة بصفة خاصة.

أمّا فيما يتعلق بالمواجهة فقاضي التحقيق مخول قانونًا بإجراء مواجهة بين المتهم والشهود أو فيما بين المتهمين أنفسهم أو بين المتهم والضحية وهذا طبقًا لنص المواد 105 و106 و107 من قانون الإجراءات الجزائية, ويجب أن تتّم مواجهة المتهم بغيره أو بالمدعي المدني بحضور محاميهم أو بعد إخطارهم قانونًا إلاّ إذا تنازلوا صراحة عن ذلك,ويتّم التنويه بذلك في محضر المواجهة[3].

فالمواجهة في التحقيق تعني مواجهة المتهم بغيره ووضعه وجهًا لوجه إزاء متهم آخر أو أحد الشهود ليسمع بنفسه ما قد يصدر منهم من تصريحات تتعلق بالتهمة ووقائع الفعل المتابع من أجله, فيتّم الإجابة عنها من قبل المتهم بالتأييد أو النفي بعد أن يطلب منه قاضي التحقيق ذلك, والمواجهة أيضًا قد تدفع المتهم إلى الإعتراف بالوقائع المنسوبة إليه أو تقرير أقوال متناقضة ليست في صالحه.

---

[1]- المادة 112من قانون الإجراءات الجزائية الجزائري.

[2]- محمد نصير محمد الرحاني, مهارات التحقيق الجنائي في جرائم الحاسوب والإنترنت, دراسة على الشرطة بالمنطقة الشرقية, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, 2004, ص 20.

[3]- محمد حزيط, المرجع السابق, ص 161.

الفرع الثاني : الإجراءات التقنية والفنية في عملية التحقيق في الجرائم المعلوماتيـة

إن الأدوات الفنية التي تستخدم في بيئة نظم المعلومات, والتي يمكن باستخدامهاأن يتّم تنفيذ إجراءات وأساليب التحقيق المختلفة وبعض الوسائل الإجرائية المهمة التي تستعمل أثناء تنفيذ طرق التحقيق الثابتةوالمحددّة والأساليب المتغيرة وغير المحدّدةوالتي تثبت وقوع جريمة معلوماتية وتحدّد شخصية مرتكبها[1], وبما أن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصالوخصوصًا التي تقع بواسطة الإنترنت, تكون أصعب في الإثبات, وتحتاج إلى تدخل الجهات الأمنية أكثر من الجرائم الأخرى التي تعلن عنها,وعلى المحقق إتباع أساليب متغيرة بحيث يعالج كلّ أسلوب منها في إحدى الحالات المعينة, أو يلجأ إلى استعمالعدّة أساليب في حالات أخرى, لأنه يحتاج للوسائل المادية والمعنوية ليستخدمها في تنفيذ التحقيق, لأن التحقيق في جرائم المعلوماتية يحتاج إلى معرفة تامة وا ٍدراك لوسائل تثبت وقوع الجريمة والوصول إلى الجاني ونسبتها إليه.

سوف أتكلم في هذا الفرع عن الترتيبات التقنية التي يستعملها ضباط الشرطة القضائية في التحري والتحقيق في الجرائم المعلوماتيـة, تليها دور الشرطة العلمية والتقنية وذلك كما يلي :

أولاً : الترتيبات التقنية : منح المشرع الجزائري لضباط الشرطة القضائية رخصة للقيام بجملة من الأعمال, وهذا بموجب إذن من وكيل الجمهورية المختص أو بموجب إذن من قاضي التحقيق, بغرض وضع الترتيبات التقنية إذا تعلق الأمر بإجراء تحقيق تمهيدي بشأن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهذا بموجب المادة 65 مكرر 5 المتضمنة بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية والقانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وهذا ضمن المادة 4 والخاصة بمراقبة الإتصالات الإلكترونية, وفي سبيل ذلكتمّ إنشاء هيئة وطنيةوحدّد مهامها بغرض الوقاية من تلك الجرائم وهذا في المادة 14 من القانون رقم 09-04.

فتلك الترتيبات التقنية وضعت من أجل تهيئة ظروف خاصة في عملية التحري والتحقيق الجنائي في الجرائم المعلوماتيةنظرًا للخطورة الإجرامية لهذا الفعل وأثرها على السياسة العامة في الدولةممّا تتطلب مستلزمات التحريات أو التحقيقات القضائيـة بعض الترتيبات ومن بينـها :

[1]– خالد عياد الحلبي, المرجع السابق, ص 212.

1/ مراقبة الإتصالات الإلكترونية : وتتمثل في اعتراض المراسلات التي تتّم عن طريق وسائل الإتصال السلكية واللاسلكية, ويقصد بها البريد الإلكتروني, التنصت التلفوني, وجميع المراسلات التي تتّم عبر الحاسب الآلي.

2/ تسجيل الأصوات : إجراء ترتيبات تقنية دون موافقة المعنيين بالأمر من أجل التقاط وتثبيت, بث وتسجيلأصوات و الكلام المتفوه بهواءً ا بصفة خاصة أو سرية,من طرف شخص أو عدّة أشخاص في أماكن خاصة أو عمومية.

3/ إلتقاط الصور : حيث يتّم التقاطصور لشخص أو عدّة أشخاص في أماكن خاصة أو عامة,تتّم دون موافقة المعنيين.

4/ التسرب : نظم المشرع الجزائري إجراء عملية التسرب بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية, في الباب الثاني من الفصل الخامس, في المواد 65 مكرر 11 إلى غاية 65 مكرر 18 التي أجاز بمقتضاها لضباط الشرطة القضائية وأعوانهم القيام بعملية التسرب إذا دعت مقتضيات التحقيق لذلك, كما عرفت المادة 65 مكرر 12 من قانون الإجراءات الجزائية التسرب بأنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف, ولهذا الغرض يسمح لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب أن يستعمل هوية مستعارةكما يسمح لهم دون أن يكونوا مسؤولين جزائيًا القيام بعمليات اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو أجهزة أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها, ووضع تحت تصرفهم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو الحفظ أو الإتصالمّما يعني أن عملية التسرب تتمثل في اختراق ضابط شرطة أو عون الشرطة القضائية لتنظيم إجرامي بما يمكن من معرفة نشاطه الإجرامي وتحديد دور كلّ عنصر من عناصره[1].

[1]- محمد حزيط, المرجع السابق, ص 115.

ونظراً لخطورة هذا الإجراء والمتمثل في عملية التسرب, فقد أخضعه المشرع الجزائري لشروط وضوابط, وبعد الحصول على إذن مكتوب ومسبب من قبل وكيل الجمهورية أو من قاضي التحقيق, حتىيكون هذا الإجراء صحيحاً ومنتجاً لآثاره[1].

ثانياً : دور الشرطة العلمية والتقنية : إن علاقة الدليل العلمي بالقانون في عصرنا الحاضر, أمر ضروري نظراً لأهميته العلمية في الكشف عن الحقيقة.

وتعتبر الشرطة العلمية والتقنية أوسع مجال علمي,فهي تشمل عدّة فروع مستقلة عن بعضها البعض تعمل مع الجهات القضائية, بهدف استقصاء الحقيقة خاصة في مجال الجرائم المعلوماتيـة.

1/ الجانب التقني للشرطة العلمية : في منتصف القرن 19 بدأت العلوم الطبيعية تتطورنظراً للحاجة الملحة لها من طرف رجال القانون والباحثون, وهذا في الأحداث والوقائع والجرائم التي ترتكب والتي فاقت قدرات العقل البشري على استيعابها, وبدأت مرحلة التجريب من أجل شرح خبايا الأمن, وساعدت هذه العلوم في التحقيق الجنائي, ويعتبر « هنري فالتون ألفونس بارتيلاف » من مؤسسي الشرطة العلمية, بحيث استعمل طرق جديدة علمية من أجل اكتشاف المجرمين واكتشاف الأدلة القاطعة وتقديم الإجابة العلمية المقنعة الكافية[2].

2/ فريق التحقيق في الجرائم المعلوماتية : هناك محققون جنائيون ذوي خبرة طويلة, وهناك أخصائيون في الحاسب الآلي والشبكات, ولكن من النادر وجود شخص يمتلك المهارات في كلا الجانبين, لذا يستعين المحققون القضائيون برجال الشرطة العلمية وبعض خبراء مسرح الجريمة, حيث يكون فريق تحري متكامل يعمل على كشف الحقيقة وتقديم الأدلة, ويمكن تقسيم هذا الفريق إلى[3]:

أ) قائد الفريق : من ذوي الخبرة الطويلة في مجال التحقيق الجنائي وله دراية خاصة بالجرائم المعلوماتية والإنترنت, يتولى السيطرة الكاملة على مسرح الجريمة, ويقوم بتوزيع المهام على الفريق.

ب) محقق جنائي :واحد أو أكثر لديه خبرة بالتحقيق وإجراءاته, مع إلمامه الواسع بطبيعة الجريمة وكيفية التعامل مع الأدلة الرقمية, فيتولى البحث عن الأدلة وتلقي التصريحات.

ج) خبراء المعلوماتية والشبكات : يجمعون بين المعرفة بعلم الحاسوب والشبكات وإجراءات

---

[1]- نصر الدين هنوني و دارين يقدح, الضبطية القضائية في القانون الجزائري, دار هومه, الجزائر, دون طبعة, 2009, ص 81.

[2]- نصر الدين هنوني و دارين يقدح, المرجع نفسه, ص 81.

[3]- خالد عياد الحلبي, المرجع السابق, ص 201.

التحقيق, مهمتهم تنحصر في رفع وتحريز الأدلة الجنائية الرقمية بالطريقة الفنية المناسبة, التي لا تؤثر على سلامة الدليل وصلاحيته لإقامة الدعوى.

د) خبراء تدقيق حسابات : متخصصون في المراجعة, المحاسبة وخبير في التعامل مع الأنظمة البرمجية وتبادل النقد الإلكتروني المستخدمة في المؤسسات المصرفية, ويعمل مع خبير الحاسب الآلي, ولتحديد أسلوب الجريمة وتقدير الخسائر المادية الناتجة عن الجريمة.

هـ) خبير بصمات : لرفع البصمات من المكونات المادية للحاسوب والشبكات المتضررة, كلوحة المفاتيح والفأرة,و اتخاذ الإحتياطات اللازمة لحفظ الأدلة.

و) خبير الرسم التخطيطي وخبير التصوير : يقوم برسم تخطيطي لمسرح الجريمة بطريقة فنية ودقيقة لأماكن تواجد الأدلة والأشخاص فيه, بالإضافة إلى أهمية التصوير الفوتوغرافي والفيديو, والذي يعتبر من الوسائل الهامة لتسجيل الأدلة المرئية وغير المرئية وتقديمها في صور لتكون أدلة وقرائن حسب قوتها في الإثبات.

3/ تطبيقات تكنولوجيا المعلومات الأمنية : توجد العديد من التطبيقات العلمية لتكنولوجيا المعلومات والحاسبات الآلية, يمكن استخدامها في الجانب العملي الأمني حتى يمكن مواجهة هذا السيل من الجرائم المستحدثة, ومن بين هذه التطبيقات :

أ) نظام تحديد الأماكن GPS : وهو عبارة عن منظومة إلكترونية متكاملة, تعمل بواسطة أجهزة صغيرة, تقوم باستقبالإشارات معينة صادرة عن عدّة أقمار صناعية,يتّم من خلالها تحديد الموقع على وجه الدقةمّما يساعد الأجهزة الشرطية المختصة على سرعة القيام بالإنقاذ[1].

ب) نظام المعلومات الجغرافية GFS : تعتمد هذا النظم على استخدام البيانات المرتبطة لمواقع جغرافية معينة, سواء المناطق الجبلية أو الصحراوية أو داخل المدن, ويستعان في تشغيل هذه النظم بالخرائط الرقمية, والصور الملتقطة بالأقمار الصناعية.

ج) رصد وتتبع الأنشطة الإجرامية على عناوين الإنترنت (IP وMAC) والبريد الإلكتروني وبرامج المحادثة : إن عنوان الإنترنت Internet Protocol Address هو المسؤول عن تراسل حزم

---

[1]– محمد قطب, الظواهر الإجرامية المستحدثة وطرق مواجهتها – دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية –, الأكاديمية الملكية للشرطة, البحرين, 2010, ص 67.

البيانات عبر الإنترنت وتوجيهها إلى أهدافها, ويشبه إلى حد بعيد العنوان على مغلف رسائل البريد التقليدي بعد وضعها بصندوق البريد, وهو يتيح للموجات والشبكات المعنية بنقل الرسالة, ويوجد عنوان (IP) بكلّ جهاز مرتبط بالإنترنت ويتكون من أربعة أجزاء, والجزء الواحد له ثلاث خانات, حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية, والجزء الثاني لمزود الخدمة والثالث لمجموعة الحواسيب المرتبطة,والجزء الرابع يحدُّد الحاسوب الذي تمّ الإتصال منه[1].

وفي حالة وجود أي مشكلة أو أعمال تخريبية فإن أول ما يجب أن يقوم به المحققون هو البحث عن رقم الجهاز, وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية, ويمكن لمزود خدمة الإنترنت أن يراقب المشترك, كما يمكن للشركة التي تقدم خدمة الإتصال الهاتفي أن تراقبه أيضًا, إذا توافرت لديه أجهزة وبرامج خاصة أخرى لذلك.

وتوجد أكثر من طريقة لمعرفة عنوان (IP) الخاص بجهاز الحاسوب في حال الوصول المباشر, منها في حالة العمل على نظام تشغيل Windows بكتابة Winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان (IP)مع ملاحظة أنه قد يتغير كلما تمّ الإتصال بالإنترنت مرة أخرى, وفي حالة استخدام أحد برامج المحادثة كأداة للجريمة فإنه يتطلب تحديد هوية المتصل, كما تحدد رسالة البريد الإلكتروني وشخصية مرسلها حتى لو لم يدون معلوماته في خانة المرسل, شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة[2].

ويمكن الإعتماد عليه من خلال إنشاء وحدات مختصة مزودة بالأجهزة والمعدات التكنولوجية المتطورة,لكي يتّم رصد ومراقبة المواقع المشبوهة على الإنترنت.

د)الكشف عن شخصية مرتكبي الجريمة آليًا : عن طريق استخدام الحاسب الآلي في استخراج صحيفة الحالة الجنائية بالأحكام النهائية,الصادرة ضدّ الأشخاص وحفظ صور البصمات والتعامل معها بصورة علمية منظمة, من خلال إنشاء أرشيف إلكتروني لحفظ البصمات ومقارنتها بالبصمات التي ترفع في مكان الجريمة.

---

[1]- خالد عياد الحلبي, إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت, المرجع السابق, ص 205.

[2]- خالد عياد الحلبي, المرجع نفسه, ص 206.

هـ) إنشاء قاعدة معلومات جنائية : من خلال تشغيل حاسب آلي ذي سعة أكبر وقدرة أعلى في معالجة البيانات واسترجاعها,وربطه محلياً من خلال شبكة متطورة من النهايات الطرفية بالأجهزة المختصة.

و) إنشاء غرفة عمليات متطورة : بتزويدها بأحدث أجهزة الإتصالات السلكية واللاسلكية الإلكترونية, وربطها بالأجهزة الأمنية المختصة لنقل وتبادل المعلومات ودعم اتخاذ القرار.

ز) إنشاء معامل جنائية متنقلة : عن طريق تزويدها بالسيارات المجهزة كمعامل جنائية متنقلة مزودة بأحدث الأجهزة العلمية والمعدات والأدوات ووسائل الإتصال, للإنتقال السريع لموقع الجريمة[1].

4/ إعداد الإطارات والكوادر : أدّى التطور التكنولوجي الهائل وثورة المعلومات إلى بروز جرائم جديدة لم تكن من قبل, لهذا ذهبت العديد من الإتجاهات إلى إبراز لتنفيذ الفلسفة الحديثة لبرامج التدريب الأمني,ولعلّ أبرزها ما نلخصه في الآتي :

أ) تطبيق مبدأ الجودة : وتعني الجودة الشاملة, أداء متكامل من الأدوات والأساليب والتدريب, وتطبيق مبادئ إدارة الجودة الشاملة في إدارة التدريب الأمني يعدُّ تحسيناً مستمراً لكلّ الأنشطة والعمليات المتعلقة ببرامج التدريب الأمني[2].

ب) تطبيق التدريب عن بعد : ويقصد به نظام أو أسلوب تدريبي يستطيع المتدرب أو المرشح أياً كان موقع عمله, أن يلتحق بدورة أو برنامج تدريبي أو يحضر مؤتمراً أو ندوة أو حلقة علمية, بشكل متزامن أو غير متزامن, دون الحاجة إلى الحضور الشخصي في مكان انعقادها[3].

ج) تشجيع التعلم الذاتي: إن تواجد برامج التعلم الذاتي في الجهات الأمنية سيساعد كثيراً في ارتفاع مستوى تأهيل وتدريب رجل الأمن وإتقانه استخدام برامج الحاسوب والإنفتاح على التقنية الحديثة.

د) إعتماد البحث العلمي أساساً للتدريب حيث يُعدّ البحث العلمي أساس التقدم والتطور في أي مجال من مجالات الحياة, لذلك فإن توسيع مجال البحث العلمي في مكافحة الجريمة المعلوماتية وعرضها على رجال الأمن, سيساهم في نقل النتائج والتوصيات التي يتوصل إليها الباحثون لرجال الأمن الميدانيين وبالتالي زيادة المهارة في الآداء.

---

[1]- محمد قطب, المرجع السابق, ص 68.

[2]- محمد قطب, المرجع نفسه, ص 07.

[3]- محمد قطب, المرجع نفسه, ص 08.

المبحث الثاني : تقديـر الأدلـة في الجريمة المعلوماتيـة

الأصل أن الذي يحكم إجراءات المحاكمة في الجريمة المعلوماتية هي أن تكون المرافعات شفوية وحضورية, بحضور أطراف الدعوى الجنائية, فتطرح الأدلة عليهم لمناقشتها, سواء كانت أدلة تقليدية أو أدلة حاسب آلي ويتّم سماع الشهود,وتُعرض تلك الأدلةأمام القاضي شخصياً وهذا بحضور الخبراء الذين عليهم الإمتثال أمام المحكمة لمناقشة تقاريرهم, وقد تكون الأدلة مباشرة كالشهادة وتقرير الخبرة أو غيرها من القرائن.

فالقاضي الجنائي لكي يتوصل إلى حكم الإدانة يجب أن يصل إلى يقين لا يناقضه احتمال آخر,أو أن حكم الإدانة لا يمكن أن يُبنى على مجرد ظنون, وعلى هذا الأساس, فإن القاضي الجنائي يملك حرية تقدير تلك الأدلة, بما في ذلك أدلة الحاسوب,وفقاً لمبدأ حرية الإثبات, وحرية الإقتناع, فأكثر حالات الخطأ في تقدير الأدلة, عندما يتسرع القاضي, ويجزم بثبوت الإدانةمؤسساً هذا الجزم على دليل, أو أكثر غير مباشر, أو على قرينة من القرائن, ويترتب على ذلك عدم قدرة أدلة الإثبات على إحداث القطع واليقين, ويترتب على ذلك استمرار حالة البراءة التي يكفي لتأكيد وجودها حينئذٍ مجرد الشك في ثبوت الإدانة, هذا هو السائد في القوانين ذات الصياغة اللاتينية, فالقاضي الجنائي يصل إلى يقينية أدلة الحاسوب, عن طريق نوعين من المعرفة, أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة وفحصها, وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والإستنتاج, من خلال الربط بين هذه الأدلة, والملابسات التي أحاطت بها, فإذا لم يتوصل القاضي إلى الجزم بنسبة الجريمة المعلوماتية إلى المتهم, عليه أن يقضي حكمه بالبراءة, فالشك يفسر لصالح المتهم, ويستفيد منه المتهم المعلوماتي[1].

ولدراسة هذه المرحلة الصعبة, ارتأيت تقسيم هذا المبحث إلى مطلبين, مطلب أول أتكلم فيه عن طرح الأدلة للمناقشة, والثاني خصصته إلى الحكم الصادر في الجريمة المعلوماتيـة.

---

[1]- سامي جلال فقي حسين, المرجع السابق, ص 123.

المطلب الأول : طرح الأدلـة للمناقشـة

تعني قاعدة وجوب مناقشة الدليل في المواد الجنائية, أن القاضي لا يمكن أن يؤسس اقتناعه إلاّ على العناصر الإثباتية التي طرحت في جلسات المحاكمة, وخضعت لحرية مناقشة أطراف الدعوى, ويعدُّ مبدأ المواجهة بين أطراف الدعوى من أهم المبادئ التي يجب أن يؤسس القاضي اقتناعه على ضوئها, حيث يتطلب هذا المبدأ طرح الأدلة في الجلسة, وأن تتاح الفرصة أمام طرفي الدعوى الجنائية, لمناقشة الأدلة المقدمة من كلّ منهما, وتفنيدها, ويرتبط هذا المبدأ بالمبدأ القانوني العام, المتمثل في ضرورة احترام حقوق الدفـاع, الذي يعدُّ أحد المظاهر الأساسية لدولة القانون, والنظم الديمقراطية[1], ويقتضي مبدأ المواجهة, ضرورة حضور كلّ خصم في الدعوى, وأن يطلع خصمه على ما لديه من أدلة وأن يواجهه بها,وأن يناقش كلّ منهما الآخر, ومبدأ المواجهة, يتطلب نوعين من الضمانات,النوع الأول يكون سابقًا على عملية المواجهة بين الأطراف, ويتضمن إحاطة المتهم علمًا بالتهمة المنسوبة إليهوا ٍعطائه الوقت الكافي, والضمانات اللازمة لكي يدافع عن نفسه, والإستعانة بمحاميأمّا النوع الآخر من الضمانات فيكون أثناء عملية تقديم أدلته سواء كانت مستندات, أو سؤال الشهود, أو الخبراء, وتقديم المذكرات وغيرها,ومن ثم يناقش كلّ طرف أدلة الطرف الآخر ويحاول أن يدحضها, وعلى ضوء المناقشات التي تحصل يبني القاضي الجنائي اقتناعه على النتيجة النهائية لهذه المناقشات, وقد حرصت العديد من التشريعات الجنائية الإجرائية على النص صراحة على هذه القاعدة, مع إجماع تلك التشريعات على وجوب عرض الدليل المقدم في الدعوى للمناقشةسواء كان هذا الدليل دليلاً عاديًا, أو دليل حاسوب, فعدم عرض هذا الدليل للمناقشة يعيب الحكم, ويوجب نقضه, لأنه لم يعرض للمناقشة, وبالتالي لم تسنح للأطراف فرصة مناقشة الدليل وتفنيد ما ورد فيها,وعليه فإن أدلة الحاسوب شأنها شأن الأدلة العادية لا بدّ أن تخضع للمناقشة, ويترتب عليها النتائج التي تترتب على الأدلة العاديةفكلّ دليل يتّم الحصول عليه من خلال وسط تكنولوجيا المعلومات, يجب عرضه للمناقشة في الجلسة, كذلك بالنسبة للشهود في الجرائم المعلوماتية وخبراء النظم المعلوماتية يجب أن يمتثلوا أمام القاضي الجنائي لمناقشتهمومناقشة تقارير هم التي قدّموها من خلال خبرتهم, كذلك أدوات الجريمة المعلوماتية التي يتّم ضبطها يجب عرضها أمام

---

[1]– سامي جلال فقي حسين, المرجع السابق, ص 117.

القاضي الجنائي ليطلع عليها بنفسه, ولهذا أردت تقسيم هذا المطلب إلى فرعين, الفرع الأول تحت عنوان الخبرة القضائية, والثاني أتكلم فيه عن الشهادة.

الفرع الأول : الخبـرة القضائيـة

هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية,ويمتدّ عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات, وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه, وأن نجاح الإستدلالات وأعمال التحقيق, في هذه الجرائم يكون مرهتداً بكفاءة وتخصص هؤلاء الخبراءليكون الحكم مطابقاً للقانون, وبالنظر لما تتميز به الجريمة المعلوماتية من خصائص فبإمكان القاضي أن يستعين بالخبراءللفحص وإبداء الرأي الفني في الأمور التي تستعصي عليه فهمها وتفسيرها, وذلك حتى يمنع أي تشكيك في صحة الدليل المستمد منه.

إن حرية القاضي المطلقة في تقدير الخبرة مبدأ سائد ومعروف منذ أن ظهرت الخبرة كوسيلة وعنصر من عناصر الإثبات, فحسب المادة 213من قانون الإجراءات الجزائية الجزائري نجدها تنص على خضوع كافة عناصر الإثبات لتقدير القاضي ومن بينها الخبرة, كما أن المادة 219 من نفس القانون تركت مسألة إجراء الخبرة للسلطة التقديرية للمحكمة على أن تتبع في تلك الأحكام المتعلقة بالخبرة والمنصوص عليها في المواد من 143 إلى 156 من قانون الإجراءات الجزائية, وقد تمّ التأكيد على مبدأ حرية القاضي في تقدير الخبرة المحكمة العليا في قراراتها بقولها :" الخبرة هي طريقة اختيارية, لها قوة الطرق الأخرى للإثبات, لا تتمتع بامتياز "," إن تقرير الخبرة ما هو إلاّ عنصر إثبات يعرض على الأطراف للمناقشة, وعلى القضاة الفاصلين في الموضوع تقديره "[1].

إن حرية القاضي في تقدير الخبرة ومدى قوتها الثبوتية ترجع في الحقيقة إلى خصائص الخبرة نفسها, إذ أنها عبارة عن إبداء رأي في مسألة فنية أو علمية ليست من اختصاص القاضي, وليست دليلاً قائماً بذاته, أي أن الخبير لا يفحص ويصل إلى قيام دليل أو عدمه, وما الخبرة إلاّ تعبير عن رأي الخبير الشخصي في مسألة فنية محدودة, وهذا الرأي يخضع لمطلق تقدير القاضي في الأخذ بها أو رفضها, لأنه المختص الوحيد في إصدار حكم فاصل في جميع عناصر الدعوى وجوانبها

[1]- زبدة مسعود, القرائن القضائية, دار الأمل, الجزائر, دون طبعة, 2011, ص 156.

المختلفة, ولهذا يقال : " بأن الخبرة ما هي إلاّ عدسة مكبرة للأشياء, والقاضي له القدرةالتي تمكنه بكلّ حرية من فحص الصورة التي يراها عبر العدسة وهل هي واضحة "[1].

وا ٍذا تعارضت آراء الخبراء المعينين في نفس المسألة, فإن القاضي يحكم بالرأي الذي يقنعه هو, والذي يتفق مع الأدلة الأخرى في الدعوى, وله أن يأخذ بتقرير الخبير الذي إنتدبه قاضي التحقيق, ويلفت النظر عن رأي الخبير الذي عينته المحكمةكما له أيضً ا أن يأخذ بتقرير الخبير في مسألة لم تكن محل طلبه, إذ أن واجب الخبير أثناء تجاربه وعمله الفنيأن يثبت ما يكشفه ممّ ا يساعد على الوصول إلى الحقيقة.

وعليه فالمقصود بالخبرة هي: " مساعدة فنية تقدم للقاضي في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة أو دراية علمية لا تتوفر لديه "[2].

ويمكن تعريف الخبير المعلوماتي على أنه شخص ذو كفاءة عالية في مجال الحاسب الآلي وعلى دراية بكلّ جزئياته وملحقاته.

أولاً : الأساس القانوني للخبرة : لقد أجاز المشرع الجزائري بموجب المادة 143 من قانون الإجراءات الجزائية لقاضي التحقيق أو قاضي الحكم بندب خبير, وأوجبت المادة 146 من نفس القانون على تحديد مهمة الخبير والأسئلة الفنية أو العملية التي يطلب منه الإستفسار فيها, وأوجبت المادة 3/143 من قانون الإجراءات الجزائية على أن تجرى عمليات الخبرة في جميع مراحلها تحت إشراف قاضي التحقيق ومراقبته أو القاضي الذي تعينه الجهة لقضائية التي أمرت بإجراء الخبرةوا ٍذا لم يودع الخبير تقاريره فيالميعاد المحدّ د جاز للقاضي المكلف استبداله بغيره.

ثانيً ا : ضرورة إستدعاء الخبراء : إن مساهمة الخبراء في تحديد هوية الجاني وتقديم الأدلة المادية هي مساهمة مهمة وفعالة بالنسبة للقاضي في إصدار الأحكامنظر ً ا لطبيعة الجرائم المعلوماتية كونها في الغالب غير مرئية لأنها تتعلق بمعطيات في شكل نبضات أو ذبذبات إلكترونية تسهل على الجاني محو الأدلة وتدميرها في ثوان[3], لذلك استوجب الأمر استدعاء خبراء مختصين في هذا المجال

---

[1]- زبدة مسعود, المرجع نفسه, ص 157.

[2]- عبد الله بن سعود و محمد السراني, فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, الطبعة الأولى, 2011, ص 35.

[3]- محمد خليفة,المر جع السابق, ص 35.

من أجل الحفاظ على الأدلة الموجودة داخل الحاسب الآلي وتحديد الدليل المادي الخاص بالحاسب الآلي.

ثالثًا : مهام الخبير : بمجرد تسلم الخبير لجهاز الحاسوب, فإنه يقوم بمجموعة من المهام المنوطة به يكلفه بها القاضي نلخصها فيما يأتي[1]:

- ✓ القيام بمعاينة ودراسة أجهزة الحاسب الآلي المحجوزة واستخراج والتقاط ملفات السجل وتحليلها.
- ✓ استعمال الشبكة الإفتراضية الخاصة VPN والعمل على استرجاع الملفات المحذوفة من القرص الصلب, ودعائم التخزين الإلكتروني وا ٍعادة بناء نشاط الإنترنت من خلال البريد الإلكتروني والبيانات المخبأة.
- ✓ تحديد مستوى أمن أنظمة الإعلام الآلي والطرق التي استطاع بها الفاعل إختراق النظم المعلوماتية, مع تحديد مظاهر الحذف والتغيير والتخريب الإلكترونيد ّقة, والبحث عن وجود شيفرات خبيثة[2].

رابع ًا : حجية الخبرة في الإثبات : إن مسألة حجية الخبرة في الإثبات مسألة تعود إلى الإقتناع الشخصي للقاضي, فإذا لم يقتنع جاز له ندب خبير لمعرفة رأيه في مسألة لم يجزم فيها الخبير الأول, ويقودنا الحديث عن حجية الخبرة للحديث عن مسألة الإثبات في المواد الجزائية, إذ أن له أهمية كبرى في كشف الحقيقة وبصفة أدق للإثبات هدف أساسي يتمثل في البحث فيما إذا كان من الممكن تحويل الشك إلى يقين,وهنا تتجلى صعوبة إثبات الجرائم المعلوماتية لأنها جرائم لا تترك أثرا لها مع صعوبة الإحتفاظ الفني بآثارها وتحتاج إلى خبرة فنية وخداع وتضليل للتعرف على مرتكبيها, وتعتمد على قمة الذكاء في إرتكابهاونظر ً ا لغياب الإعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم, فمهمة فريق البحث الجنائي في جمع الأدلـة يشبه عمل المنقبين عن الآثـار.

---

[1] – حسين الشريف, الدليل المهني لقاضي التحقيق, دار الألمعية, الجزائر, الطبعة الأولى, 2010, ص 36-37.

[2] – عبد الفتاح بيومي حجازي,الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية ,المرجع السابق, ص 119-187.

الفرع الثاني : الشهـادة

إن الشهادة في الدعاوى المعلوماتية تختلف كلياً عن الشهادة في الجرائم العادية, لأن محل الجريمة المعلوماتية غالباً ما يكون برنامجاً إلكترونياً, عكس الجرائم العادية, فكشف الحقيقة يتوقف على ما يعلمه الشاهد بالخبرة النظرية لا بما يعلمه بالواقع من حقائق رآها أو سعها أو نقلت إليه[1].

أولاً : شهادة الحاسب الآلي: يلعب الحاسوب دوراً مهماً ورئيسياً في كشف الجرائم المرتكبة من خلاله, وتتبع فاعليها فيعتبر شاهداً رئيسياً على الجريمة, فمع تزايد نطاق جرائم الحاسوب وإعتماد مرتكبيها على أحدث التقنيات, فإنه أصبح ملزماً إستخدام نفس تلك التقنيات للكشف عنها, رغم الميزة التي يتميز بها مرتكبوا هذه الجرائم من ذكاء خارق وعلم بليغ بالتكنولوجيا.

ثانياً : شهادة البرنامج : تعتبر الأدلة الجنائية عبارة عن بيانات رقمية موجودة في الحاسوب وملحقاته المادية والمنقولة كالأقراص المضغوطة, والحاسوب يتكون من جزئين رئيسيين هما[2]:

المكونات المادية وهي المكونات الصلبة, واللامادية وهي البرامج والمعطيات, هذه الأخيرة تكتب بلغة ما لتنفيذ عمليات محددة, فتعتبر هذه البرامج شاهداً رئيسياً على وقوع هذه الجرائم ودليلاً قاطعاً على إثباتها.

ثالثًا : الدليل الإلكتروني : تستند كذلك عملية الإثبات الجنائي في جرائم المعلوماتية على الدليل الإلكتروني باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم الحديثة العهد, وعليه يمكن تعريفه بأنه الدليل الذي تمّ الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنت والأجهزة الإلكترونية الملحقة والمتصلة به, وشبكات الإتصالات من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة[3].

رابعاً : حجية الشهادة في الإثبات : من أهم قواعد الإثبات أنه لا حاجة لإقامة الدليل على ما تنهض به الشواهد على تقرير ثبوته, إنّما يلجأ إلى الإثبات من يدعي عكس ما تؤيده الشواهد, فإثبات الجريمة هو وجود أدلة تؤكد حصولها كالاعتراف أو الشهادة, لكن مشكل الإختصاص في هذه

---

[1]- محمد أمين الرومي, جرائم الحاسوب وحقوق المؤلف, يوم دراسي منظم بين وزارتي العدل والإتصال, الأردن, 28 أفريل 1999, ص 99-125.

[2]- عفيفي كامل عفيفي, المرجع السابق, ص 148.

[3]- خالد عياد الحلبي, المرجع السابق, ص 230.

الجرائم المعلوماتية هو المشكلة التي تعرقل الحصول على الدليل المباشر بسبب التداخل والترابط بين شبكات المعلومات, لذلك نادى البعض بضرورة إنشاء وحدات خاصة لمكافحة هذه الجرائم لإثبات الجريمة وتحديد أدلتها وفعاليتها[1].

المطلب الثاني : الحكم الصادر في الجريمة المعلوماتيـة

إن التطور المتجدّد والمستمر للمعلوماتية يجعل من صور التجريم الحالية غير قادرة على مواكبة ما يطرأ من صور إجرامية مستحدثة, فنجد في النماذج التي سنذكرها أن حجم الجريمة المرتكبة لا يتناسب والعقوبة المسطرة عليها,لذلك قيل قديماً " من أمن العقوبة أساء الأدب "[2], ولدراسة هذا الموضوع ارتأيت تقسيم هذا المطلب إلى فرعين, فرع أول بعنوان نماذج عن الأحكام الصادرة في الجريمة المعلوماتية, والثاني أتكلم فيه عن مشروعية أدلـة الحاسوب.

الفرع الأول : نماذج عن الأحكام الصادرة في الجريمة المعلوماتيـة

في حادثة هامة حول خلق فيروس شرير عبر الإنترنت عرف باسم " ميلسا "حيث تمّ إعتقال مبرمج الكمبيوتر من ولاية نيوجرسي, واتهم باختراق إتصالات عامة وهذا سنة 1999 لسرقة خدمات إلكترونية,ووصلت العقوبة الصادرة ضدّه إلى السجن أربعين عاماً وغرامة مالية تقدر بحوالي 5000 دولار, كما صدرت في هذه القضية مذكرات إعتقال بلغ عددها 19 مذكرة[3].

أولاً : النموذج الأول : يعتبر إقتحام المواقع من الجرائم الشائعة في العالم, ففي عام 1997 قام مراهق بالتسلل إلى نظام مراقبة الملاحة الجوية في مطار ماشيتوتش,مما أدى إلى تعطيله لمدّة 6 ساعات,إلاّ أن العقوبة إقتصرت على وضعه لمدّة سنتين تحت المراقبة مع إلزامه بأداء خدمة للمجتمع لمدّة 250 يوم.

---

[1]- عبد الفتاح بيومي حجازي, الإثبات في جرائم الإنترنت والكمبيوتر, المرجع السابق, ص 187.

[2]- أنظر الموقع www.OKAZ.com:sa بتاريخ 06 فيفري 2011.

[3]- محمد عبدالله المنشاوي,دراسة الإنترنت وأشهر جرائمه, قسم البحوث, جامعة القاهرة, مصر, دون طبعة, 2008, ص 129.

ثانياً : النموذج الثاني تعقب مكتب التحقيقات الفدرالي طالباً جامعياً بكلية علوم الحاسوب بجامعة nomstone الذي إعترف في قاعة محكمة بوسطن باختراقه أنظمة الحاسوب الحكومية, منها أنظمة وزارة الدفاع ووكالة ناسا, وحكم عليه ثلاث سنوات تحت المراقبة.

نستنتج أن العقوبات الحالية لا تساعد على تقليص الإرتفاع المستمر للجرائم المتعلقة بالتسلل والإقتحام إلى الأنظمة المعلوماتية.

الفرع الثاني : مشروعيـة أدلـة الحاسوب

تعرف الشرعية الإجرائية بأنها " الأصل في المتهم البراءة,ولا يجوز اتخاذ إجراء جنائي قبل المتهم إلاّ بناء على قانون, وتحت إشراف القضاء, وفي حدود الضمانات المقررة, بناء على قرينة البراءة "[1], ويفضل أغلبهم استعمال مصطلح الشرعية عند الكلام عن مبدأ " لا جريمة ولا عقوبة إلاّ بنص ", أي مبدأ شرعية الجريمة والعقاب وبالحديث عن الأدلة الجنائية وخصوصاً أدلة الحاسوب يجب أن يتّم الحصول عليها بصورة مشروعة, حتى تصلح لأن تكون أساساً لأي حكم جنائي, واختلفت النظم والقوانين الإجرائية في نظرتها إلى مشروعية الدليل الجنائي, وسوف أتعرض إلى هذه النظم ونماذج من كلا القانونين الفرنسي والياباني, وأوضح موقفهما من مشروعية أدلة الحاسوب كدليل جنائي, وذلك كالآتي :

أولاً : القانون الفرنسي : ميز قانون الإجراءات الجنائية الفرنسي بين نوعين من البطلان, الأول هو البطلان المقرر بموجب نصوص صريحة, والثاني البطلان المقرر كجزاء على مخالفة النصوص الجوهرية والمسمى بالبطلان الذاتي, ففي عام 1933 م ألغى المشرع الفرنسي التقسيم الشهير لحالات البطلان, وأصبحت المادة الجديدة كالآتي " يتحقق البطلان عندما يترتب على إغفال إجراء جوهري منصوص عليه في قانون الإجراءات الجنائية, أو نص إجرائي آخر على مساس بحقوق الطرف المعني "[2], وأكدت محكمة النقض الفرنسية على ضرورة التمييز بين رفض محكمة الموضوع قبول دليل متحصل بطريق غير مشروع, من ناحية, وبناء المحكمة اقتناعها الذاتي على مثل ذلك الدليل,

---

[1]- سامي جلال فقي حسين, المرجع السابق, ص 101.

[2]- سامي جلال فقي حسين, المرجع نفسه, ص 103.

من ناحية أخرى فالقاعدة أن القاضي الجنائي يتعين عليه أن لا يحُرم خصماً من تقديم دليل, ولو كان قد حصل عليه بصورة غير مشروعة, وهي قاعدة لازمة لتمكينه من التوصل إلى الحقيقة, ولكن تقديم مثل هذا الدليل لا يعني قبوله في تكوين عقيدة القاضي, فالقاضي له الحرية في بيان قوة الدليل في الإثبات تبعاً لاقتناعه الذاتي,وذلك تطبيقاً للمادة 427 من قانون الإجراءات الفرنسي, التي تجيز الإثبات بكافة الطرق, ويحكم القاضي بناءً على اقتناعه الذاتي,وتطبيقاً لذلك رفضت محكمة النقض الفرنسية طعن المتهم في إحدى القضايا المعروضة أمامها في 10 نيسان 1992, وتتلخص وقائع هذه القضية في أنه كان أحد مأموري الضبط القضائي يتلقى منذ توليه مهامه معلومات مفيدة في التحقيق الأولي بواسطة التليفون, أو بالفاكس خارج دائرة اختصاصه, وكان يقوم بكتابتها ويرفقها بالإجراءات, كما كان يحدث بالنسبة للمستندات التي يحصل عليها بطريق الفاكس, فقام المتهم بالطعن في هذا الإجراء أمام غرفة الإتهام على أساس أن مأمور الضبط القضائي قد تجاوز إختصاصه المكاني, وخالف الأحكام المتعلقة بسماع الشهود, ورفضت غرفة الإتهام هذا الطعن, لأنها رأت أن الإجراء الذي قام به مأمور الضبط القضائي لا يعني إنتقاله إلى خارج دائرة إختصاصه الذي يمارس فيها وظائفه عادة, علاوة على ذلك, فإن جميع المعلومات عن طريق الفاكس, أو التليفون لا يمكن تشبيهها بسماع الشهود, إنما هي رسائل لا تتعدى قيمتها المعلومات, تخضع لرقابة وتقدير قاضي التحقيق, وبادر المتهم بالطعن في قرار غرفة الإتهام بالطعن أمام محكمة النقض, التي رفضت بدورها الطعن على أساس أنه طبقاً للمادة 1/18 من القانون الإجرائي الفرنسي, فإن مأموري الضبط القضائي ليس لهم إختصاص من حيث المبدأ, إلاّ في حدود دوائر إختصاصهم الإقليمي, حيث يمارسون وظائفهم المعتادة, فليس هناك ما يمنعهم من جمع المعلومات من خارج دوائر إختصاصهم بواسطة التليفون, أو الفاكس, أو أية وسيلة أخرى للإتصال حيث إن قيمة المعلومات التي يتّم جمعها بهذه الطرق تخضع للمناقشة الحضورية للأطراف, وتخضع لتقدير محكمة الموضوع, وطبقاً لهذا القرار فإن محكمة النقض إعتبرت الإنتقال المادي للمعلومات من مكان خارج الحدود المكاني لإختصاص مأمور الضبط القضائي إلى دائرة إختصاصه لا يخالف القانون, وبالتالي يمكن الإعتماد عليها كدليل إثبات, فالمادة 1/18 من القانون السالف الذكر لا تنطبق, إلاّ في حالة الانتقال المادي لمأمور الضبط القضائي خارج حدود اختصاصه المكاني, ومحكمة النقض تمسكت بمبدأ حرية الإثبات طالما أن حقوق الدفاع تمّ مراعاتها من خلال المناقشة الحضورية للمعلومات التي يتّم

الحصول عليها, ويقع على عاتق قاضي التحقيق مهمة مراقبة صحة المعلومات التي جمعت[1].

ثانياً : القانون الياباني : أجمع القانون الياباني على وجوب أن تكون الأدلة المتحصلة عليها مشروعة, فالدستور الياباني يضمن حق المتهم في التزام الصمت,ويستبعد الأدلة التي يتّم الحصول عليها من خلال الإكراه, والهدف من ذلك هو تجنب قيام الشرطة بإكراه المتهم على الإعتراف, وعليه فإن الاعتراف تحت الإكراه يستبعد كدليل إثبات حسب قانون الإجراءات الجنائية الياباني, وعلى هذا الأساس استبعدت المحكمة العليا الاعتراف الذي يتّم الحصول عليه عن طريق الوعد والخداع[2], وثار خلاف بين الفقه والقضاء الياباني حول مدى مشروعية التنصت, والمراقبة الإلكترونية, بهدف إجراء التحريات في ظل قانون الإجراءات الجنائية الياباني, حيث إنه لا يوجد قانون ينظم هذه الطريقة, لأنها تنتهك حق الخصوصية, وأكدت المحكمة العليا أن الحياة الخاصة لها قيمة دستورية, وعلى الرغم من ذلك فإن محكمة مقاطعة (kofu) أصدرت حكماً أقرت فيه مشروعية التنصت للبحث عن دليل, وغالبية الفقه الياباني يذهب إلى إستبعاد الدليل الذي يتّم الحصول عليه بصورة غير مشروعة, سواء كانت أدلة تقليدية أم أدلة حاسوب, والمحكمة العليا قد ضيقت من نطاق تطبيق قاعدة إستبعاد الأدلة الغير مشروعة وذلك بإشتراطها أن تكون المخالفة على درجة من الجسامة, أو خطرة إلى جانب صفة عدم المشروعية لإستبعاد الدليل, ويظهر ذلك من خلال إحدى أحكامها بقولها " إن البحث عن الحقيقة يجب أن يتّم مع ضمان حقوق الإنسان, وعدالة الإجراءات أخذاً في الإعتبار المادة 31 من الدستور الياباني الذي ينص على ضرورة أن تكون المحاكمة عادلة "[3].

من خلال استعراض موقف القانونين الفرنسي و الياباني, يتبين أن كليهما قد ذهبا إلى بطلان أو إستبعاد الأدلة المتحصلة عليها بصورة غير مشروعة, وعلى هذا الأساس, فإن أدلة الحاسوب بمختلف أنواعها لو تمّ الحصول عليها بوسائل غير مشروعة كالإكراه أو التهديد, تكون معيبة يجب إستبعادها, ومن الأمثلة على ذلك تعذيب المتهم لإجباره على فك شفرة الدخول إلى حاسوبه الشخصي, لغرض استحال الأدلة منه, لاستخدامها ضدّه في القضية المتهم فيها.

---

[1]- سامي جلال فقي حسين, المرجع السابق, ص 104.

[2]- سامي جلال فقي حسين, المرجع نفسه, ص 115.

[3]- سامي جلال فقي حسين, المرجع السابق, ص 115.

من خلال ما تقدم, نجد أن المشرع الجزائري قد ساير هو كذلك أغلب التشريعات, وجعل ضوابط قانونية تتّسم بالشرعية عند كيفية جمع أو الحصول على أدلة الحاسوب من طرف ضباط الشرطة القضائية عند ممارستهم لأعمالهم وذلك ضمن المادة الأولى من قانون العقوبات التي تنص على أنه " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون ", وتمّ كريس المبدأ المتمثل في قرينة البراءة دستوريًا للشخص أثناء مختلف مراحل سير المتابعة الجزائيـة.

الخاتمـــة

وإجمالاً لما قيل, لقد أثارت الجرائم المعلوماتية تحديات لها وزنها في النظام القانوني، وعلى الأخص بالنسبة لقانون الإجراءات الجزائية وقانون العقوبات، ويرجع السبب في ذلك إلى أن القوانين العقابية تبسط حمايتها على الأشياء المادية والمرئية فقط، متجاهلة في اعتبارها المعلومات والقيم المعنوية, لأجل ذلك تناولنا أهم الجوانب الموضوعية والإجرائية لهذه الجرائم بدءاً بالإطار المفاهيمي والنظري لها, وصولاً إلى الإثبات في الجريمة المعلوماتية, وعلى ضوء ما تقدم رأينا إلى أن لجرائم المعلوماتية من الخصوصية ما حال دون إمكانية تطبيق النصوص التشريعية التقليدية بشأنها، الأمر الذي نجمت عنه صعوبات جمّة في مواجهة هذه الجرائم من حيث صعوبة كشافها وإقامة الدليل عليها, باعتبار أن محل هذه الجرائم معطيات الحاسب الآلي (برامج، بيانات، معلومات)، أضف إلى ذلك ما يتميز به مقترفوها من مستوى عالي من الذكاء وقدرتهم على إضاعة الدليل في وقت قياسي من ارتكاب الجريمة المعلوماتية.

ولعلّ هذه المميزات هي التي جعلت من جرائم المعلوماتية أحدأكبر المخاطر التي تهدّد كيانات الدول وتمس بالحقوق المالية والشخصية للأفراد، وهذا ما استدعى تدخل المشرع في أغلب البلاد لإعادة النظر في النصوص التشريعية الجزائية التقليدية لجعلها أكثر تماشيا مع خصوصيات الجرائم المعلوماتيةوهذا ما نراه جلياً في التبني الواضح للمشرع الجزائري من خلال التعديل الأخير لقانون العقوبات رقم 15/04 المؤرخ في 2004/11/10 واستحدث قسم جديد تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات, وقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء بتقنيات جديدة ومعان أخرى توضح القواعد الإجرائية في مجال تحريك الدعوى وتقفي آثار مجرمي المعلوماتية، من خلال تحديد الترتيبات التقنية لمراقبة الاتصالات الالكترونية ورصدها، وكيفيات تفتيش المنظومة المعلوماتية عن بعد، ثم إجراءات حجز تلك المعطيات المعلوماتية, ومنح صلاحيات مدنية للوقاية من تلك الجرائم,والحث بخصوص المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة المعلوماتية, وبذلك يعتبر كسياسة وقائية من الدولة، ليتدارك في الأخير الفراغ القانوني الذي كان حاصلاً في مجال هذه الجرائم, ويكون قد حقق شبه من التوازن في التصدي لتلك الجريمة المعلوماتيـة.

ومـا يمكن أن أخرج به من خلال دراستي المتواضعة هذه النتـائج الآتيـة :

- ❖ الجرائم المعلوماتية جرائم مستحدثة, تتطلب الخبرة الفنية والتقنية الكبيرتين لدى رجال الشرطة والتحقيق, للإلمام بجوانبها الإجرائية.
- ❖ قصور نصوص التشريع الجزائي التقليدية عن الإحاطة بجوانب الجرائم المعلوماتية, بإعتبار هذهالأخيرة محلها يختلف كليًا عن الجرائم التقليدية الأخرى, التي وضعت من أجلها هذه النصوص التشريعية.
- ❖ المشرع الجزائري سارع لسد الفراغ التشريعي في مجال هذه الجرائم عندما نص على ثلاث أنواع من الجرائم المعلوماتية هي (جريمة الدخول والبقاء غير المصرح به, جريمة التلاعب بالمعطيات, جريمة التعامل مع معطيات غير مشروعة).
- ❖ المشرع الجزائري أغفل في نصوصه بعض النقاط الجوهرية, عندما لم يتعرض لبعض الجرائم المعلوماتية مثل جريمة الإعتداء على سير نظام المعالجة الآلية للمعطيات, وجريمة التزوير المعلوماتي, وكذا مختلف الجرائم الإباحية التي ترتكب على الإنترنت.
- ❖ نظرًا لظهور شبكة الإنترنت أصبح العالم عبارة عن قرية صغيرة, وبالتالي فإن جرائم الحاسوب والإنترنت ترتكب في موقع ما,وتتحقق النتيجة في موقع أخر أو عدّة مواقع,ممّا يجعلها جرائم وطنية أو دولية, ومن هنا وجب تكثيف الجهود والتعاون الدولي لمكافحتها, وتطوير جهود البوليس الدولي (الإنتربول) من أجل ذلك.

بناءًا على ما تمّ ذكره, فإننا نورد بعض التوصيات, والتي نأمل أن تؤخذ بعين الإعتبار لدى رجال القانون والإختصاص وهذا في الآتـي :

- ❖ إصدار تشريعات جديدة أو تعديل التشريعات الجزائية القائمة, لمواجهة الجرائم المعلوماتية, وذلك بتحديد الجرائم وتقرير العقوبات المناسبة لها, بغية حماية النظام المعلوماتي واستيعاب التطور التكنولوجي الحاصل على العالم.
- ❖ تبني خطة واسعة للتدريب ورفع مستوى الكفاءة المعلوماتية في القطاع الوظيفي للدولة, مع تخصيص دورات تدريبية مكثفة وعقد ندوات علمية وقانونية, لفائدة القضاة والنيابة العامة والشرطة القضائية لرفع مستوى الكفاءة لديهم في استخدام التقنية المعلوماتيـة.

- ❖ الإهتمام بالتأهيل المستوى العالي والمناسب, لكوادر الأجهزة الشرطية والقضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار, مع إنشاء شرطة متخصصة لمكافحة الجريمة المعلوماتيـة وتخصيص مكاتب أمنية على المستوى الوطني تعالج قضايا الإجرام المعلوماتي.
- ❖ يجب على الوزارة المعنية, وضع الحماية للقيم الاجتماعية والأخلاقية والمحافظة على العادات والتقاليد بإغلاق النوافذ التي تطلُّ على المواقع الإلكترونية الإباحية والجنسية, وتوعية المجتمع بخطورة هذه المواقع, حتى لا تتفكك الأسر الجزائرية.
- ❖ حث الدول العربية مجتمعة على إبرام اتفاقية فيما بينها على غرار الاتفاقية الأوربية, بغية تعزيز روابط التعاون القضائي والشرطي بجميع صوره, لمواجهة التحديات الإجرائية الناجمة عن الجرائم المعلوماتية عبر الوطنية.
- ❖ وضع إستراتيجية دولية للتعاون في المجال التشريعي المتعلق بجرائم المعلوماتية, والحث على التكامل فيما بين قوانين العقوبات في مختلف دول العالم, بهدف تسهيل تعقب وملاحقة وتسليم مجرمي المعلوماتية.
- ❖ وضع تقنية البصمة الإلكترونيةو التوقيع الإلكتروني,لكلّ من يريد التفاعل أو الولوج في شبكة الإنترنت,مع تعميمه وتوظيفه على كلّ قطاعات الدولـة, بحيث يصبح في متناول موظفي ومؤسسات الدولة, قصد الحماية الفعالة التي توفرها تلك التقنية.
- ❖ السماح للشركات العالمية في مجال الإنترنت للسوق الإلكترونية أو البورصات والمواقع التفاعلية (Yahoo, Facebook, Ebay, Google, Amazam) للإستثمار في السوق الجزائريـة عن طريق عقود عادلة ومفيدة, وتسمح للدولة الجزائرية بتحقيق مكسب إقتصادي وا ٍجتماعي و خاصة أمني, ما دامت تلك الشركات تملك خاصيـة تكنولوجيا الأمن الإلكتـروني.

وفي الأخير ليسعني إلاّ أن أقول بأ المشرع الجزائري ظلّ متشبثا باحترام حقوق الإنسان من خلال جعل المساس بها استثناء وفي أطر قانونية تتمثل في الأذونات والتصريحات من طرف النيابة العامـة.

أولاً : النصوص القانونية :

1.الأمر رقم 66-155 المؤرخ في 18 جوان 1966 والمتضمن قانون الإجراءات الجزائية الجزائري المعدل والمتمم .

2.الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم .

3.القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات, جريدة رسمية, عدد 71, المؤرخة في 11 نوفمبر 2004 .

4.القانون رقم 04-14 المؤرخ في 27ر مضان 1425 هجرية, المعدل والمتمم والمتضمن قانون الإجراءات الجزائية, الجريدة الرسمية, العدد 71 الصادرة بتاريخ 10 نوفمبر 2004.

5.القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها, الجريدة الرسمية, عدد 47 المؤرخة في 16 أوت 2009 .

6.القانون رقم 96-392 المؤرخ في 13 ماي 1996, المتضمن تعديل قانون العقوبات الفرنسي .

ثانيـ ا : المؤلفات :

* المؤلفات بالغة العربية :

01.أحسن بوسقيعة, التحقيق القضائي, دار هومة, الجزائر, الطبعة السابعة, 2008 .

02.أحمد خليفة الملط, الجرائم المعلوماتية, دار الفكر الجامعي, الإسكندرية, مصر, الطبعة الثانية, 2006 .

03.أسامة عبد الله قايد, الحماية الجنائية للحياة الخاصة وبنوك المعلومات, دار النهضة العربية, القاهرة, مصر, دون طبعة, 1994 .

04.آمال قارة, الحماية الجزائية للمعلوماتية في التشريع الجزائري, دار هومة, الجزائر, الطبعة الثانية, 2007.

05.جباري عبد المجيد, دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة, دار هومة, الجزائر, الطبعة الثانية, 2013 .

06.جميل عبد الباقي الصغير, جرائم التكنولوجيا الحديثة, دار النهضة العربية, دون مكان نشر, دون طبعة, دون سنة نشر.

07.جودة حسين جهاد و عمر السعيد رمضان, قانون الإجراءات الجنائية الإتحادي في دولة الإمارات العربية المتحدة, أكاديمية شرطة دبي, دبي, الإمارات العربية المتحدة, دون طبعة, 1994 .

08.حسين الشريف, الدليل المهني لقاضي التحقيق, دار الألمعية, الجزائر, الطبعة الأولى, 2010 .

09.خالد عياد الحلبي, إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت, دار الثقافة, عمان, الطبعة الأولى, 2011 .

10.خالد ممدوح, أمن الجريمة الإلكترونية, الدار الجامعية, الإسكندرية, مصر, دون طبعة, 2008 .

11.خالد ممدوح, حجية البريد الإلكتروني في الإثبات, دار الفكر الجامعي, القاهرة, مصر, دون طبعة, 2001

.
12.رؤوف عبيد, مبادئ القسم العام من التشريع العقابي, دار الفكر العربي, القاهرة, دون طبعة, مصر, 1979 .
13.زبدة مسعود, القرائن القضائية, دار الأمل, دون طبعة, الجزائر, 2011 .
14.زيدان زبيحة, الجريمة المعلوماتية في التشريع الجزائري والدولي, دار الهدى, عين مليلة, الجزائر, دون طبعة, 2011.
15.زينات طلعت شحادة, الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية, مكتبة صادر ناشرون, بيروت, لبنان, 2006 .
16.سامي جلال فقي حسين, الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي – دراسة مقارنة –, دار الكتب القانونية, دون طبعة, مصر, 2011 .
17.سامي علي حامد عياد,الجريمة المعلوماتية وا إجرام الإنترنت, دار الفكر الجامعي, الإسكندرية, 2007 .
18.سمير عالية, شرح قانون العقوبات – القسم العام –, المؤسسة الجامعية للدراسات, بيروت, لبنان, دون طبعة, دون سنة نشر.
19.عبد الحكيم رشيد توبة, جرائم تكنولوجيا المعلومات, الطبعة الأولى, دار المستقبل, عمان, الأردن, 2009.
20.عبد الفتاح بيومي حجازي, الجريمة في عصر العولمة– دراسة في الظاهرة الإجرامية المعلوماتية–, الطبعة الأولى, دار الفكر الجامعي, الإسكندرية, 2007 .
21.عبد الفتاح بيومي حجازي, الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية, الطبعة الأولى, دار النهضة العربية, القاهرة, مصر, 2009 .
22.عبد الفتاح بيومي حجازي,مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت, دار الكتب القانونية, المحلة الكبرى, مصر,2007 .
23.عبد الله بن سعود و محمد السراني, فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني, الطبعة الأولى, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, الطبعة الأولى, 2011 .
24.عبد الله عبد الكريم عبد الله, جرائم المعلوماتية والإنترنت, الجرائم الإلكترونية– دراسة مقارنة –, الطبعة الأولى, منشورات الحلبي, بيروت, لبنان, 2007 .
25.عفيفي كامل عفيفي, جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون, منشورات الحلبي الحقوقية, بيروت, لبنان, دون طبعة, 2003 .
26.علي القهوجي, الحماية الجنائية لبرامج الحاسوب, الدار الجامعية للنشر, الإسكندرية, دون طبعة, 1997.
27.عماد مجدي عبد الملك, جرائم الكمبيوتر والإنترنت, دار المطبوعات الجامعية, مصر, دون طبعة, 2011

.
28.عمر ممدوح خليل, حماية الحياة الخاصة في القانون الجنائي, دار النهضة العربية, القاهرة, مصر, 1983
.
29.محمد أمين الشوابكة, جرائم الحاسوب والإنترنت, الطبعة الأولى, دار الثقافة, عمان, الأردن, 2006 .
30.محمد حزيط, مذكرات في قانون الإجراءات الجزائية الجزائري, دار هومه, الطبعة التاسعة, الجزائر, 2014.
31.محمد خليفة, الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, دار الجامعة الجديدة, الأزاريطة, الإسكندرية, دون طبعة, 2007.
32.محمد عبد الله أبو بكر سلامة, موسوعة جرائم المعلوماتية– جرائم الكمبيوتر والإنترنت–, منشأة المعارف, مصر, 2006 .
33.محمد عبدالله المنشاوي, دراسة الإنترنت وأشهر جرائمه, قسم البحوث, جامعة القاهرة, مصر, دون طبعة, 2008 .
34.محمد علي العريان, الجرائم المعلوماتية, دار الجامعة الجديدة للنشر, الإسكندرية, مصر, 2004.
35.محمود إبراهيم غازي, الحماية الجنائية للخصوصية والتجارة الإلكترونية, مكتبة الوفاء القانونية, الطبعة الأولى, الإسكندرية, مصر, 2014 .
36.مسعود خثير, الحماية الجنائية لبرامج الكمبيوتر, دار الهدى, الجزائر, دون طبعة, 2010 .
37.منصور رحماني, الوجيز في القانون الجنائي العام, دار العلوم, عنابة, الجزائر, دون طبعة, 2006 .
38.منصور عمر المعايطة, الأدلة الجنائية والتحقيق الجنائي, دار الثقافة, الطبعة الثانية, عمان, 2011 .
39.منير محمد الجنبيهي و ممدوح محمد الجنبيهي, جرائم الإنترنت والحاسب الآلي وسبل مكافحتها, دار الفكر الجامعي, مصر, 2004 .
40.نبيل صقر, الوسيط في شرح جرائم الأموال, الطبعة الأولى, دار الهدى, عين مليلة, الجزائر, 2012.
41.نصر الدين هنوني و دارين يقدح,الضبطية القضائية في القانون الجزائر ي, دار هومه, دون طبعة, الجزائر 2009.
42.هدى حامد قشقوش, جرائم الحاسب الإلكتروني في التشريع المقارن, دار النهضة العربية, الإسكندرية, القاهرة, الطبعة الأولى, 1992.
43.هشام محمد فريد رستم, قانون العقوبات ومخاطر تقنية المعلومات, مكتبة الآلات الحديثة, القاهرة, مصر, 1995.
44.هلالي عبداللاه أحمد, إلتزام الشاهد والإعلام في الجرائم المعلوماتية, دراسة مقارنة, القاهرة, دار النهضة العربية, 1997.

*** المؤلفات بالغة الأجنبية :**

1. David Thampson, Current trends in computer crime, control computer quarterly, Vol, n1, 1991.

2. J.PRADEL,les infractives à l'informatique, R.I.D.C,1990 – 2.

3. Linant de bellefonds (Xavier) et autres, pratique de droit informatique, 1998, op,cit.

ثالثًا : <u>المقالات والمجلات</u> :

1. جريدة الشروق, الشروق تغوص في عالم الجريمة الإلكترونية بالجزائر, محتالون يؤسسون حكومة موازية على الفايسبوك, الخميس 02 أفريل 2015, العدد 4695.

2. حكيم سياب, " السمات المميزة لجرائم المعلوماتية عن الجرائم التقليدية ", مجلة الدراسات والأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009.

3. رامي حليم, "جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات",مجلة الدراسات و الأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009.

4. عبد المجيد بوناب, " الحرب الإلكترونية, قمة الصراع العالمي وحصاد العولمة التقنية ", مجلة العلم والإيمان, العدد 33, الجزائر, ماي 2009.

5. عطاء الله فشار, " مواجهة الجرائم المعلوماتية في التشريع الجزائري ", مجلة الدراسات والأبحاث, العدد الأول, جامعة الجلفة, الجزائر, 2009.

6. سميرة معاشي, مجلة المنتدى القانوني, دورية تصدر عن قسم الكفاءة المهنية للمحاماة, جامعة محمد خيضر بسكرة, الجزائر, العدد السابع 2010.

رابعًا : <u>البحوث والمؤتمرات</u> :

1. رحاب عميش, الجريمة المعلوماتية, ورقة عمل مقدمة إلى المؤتمر المغاربي حول المعلوماتية والقانون, أكاديمية الدراسات العليا, طرابلس, ليبيا, 28 – 29 أكتوبر 2009.

2. كمال أحمد الكركي, التحقيق في جرائم الحاسوب, ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية, تنظيم أكاديمية شرطة دبي, مركز البحوث والدراسات, دبي, الإمارات العربية المتحدة, 26–28 أفريل 2003.

3. محمد أبو العلاء عقيدة, التحقيق وجمع الأدلة في الجرائم الإلكترونية, ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية, تنظيم أكاديمية شرطة دبي, مركز البحوث والدراسات, دبي, الإمارات العربية المتحدة, 26–28 أفريل 2003.

4. محمد أمين الرومي, جرائم الحاسوب وحقوق المؤلف,يوم دراسي منظم بين وزارتي العدل والإتصال, الأردن,

28 أفريل 1999.

5. محمد سامي الشوا, الجرائم المعلوماتية للتعدي على الذمة المالية للغير, بحث مقدم إلى مؤسسة الأعمال الإلكترونية بين الشريعة والقانون, كلية الشريعة والقانون وغرفة التجارة والصناعة, دبي, الإمارات العربية المتحدة, من 10-20 ماي 2003.
6. محمد عبيد سيف سعيد المسماري و عبد الناصر محمد فرغلي, الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية, بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, 12-14 نوفمبر 2007.
7. محمد قطب, الظواهر الإجرامية المستحدثة وطرق مواجهتها – دراسة مقارنة بين القانون الوضعي والشريعة الإسلامية –, بحث غير منشور, الأكاديمية الملكية للشرطة, البحرين, 2010.
8. محمد نصير محمد الرحاني, مهارات التحقيق الجنائي في جرائم الحاسوب والإنترنت, دراسة على الشرطة بالمنطقة الشرقية, جامعة نايف العربية للعلوم الأمنية, الرياض, السعودية, 2004.
9. يونس عرب, جرائم الكمبيوتر والإنترنت, – إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات –, ورقة عمل مقدمة إلى مؤتمر الأمن العربي, تنظيم المركز العربي للدراسات والبحوث الجنائية, أبو ظبي|الإمار ات العربية المتحدة, 10-12 فيفري 2002.

خامسـ ًا : <u>مواقع الإنترنت</u> :

1.http://www.elfagr.org.

2. www.OKAZ.com:sa