جامعة الدكتور مولاي الطاهر – سعيدة –
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة لنيل شهادة الماستر في العلوم القانونية والإدارية
تخصص : علم الإجرام
بعنوان :

الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

من إعداد الطالب :

□ بريكي توفيق

تحت إشراف الدكتور :

عياشي بوزيان

أعضاء لجنة المناقشة

الدكتور : عياشي بوزيان	مشرفا ومقررا
الدكتور : بن عيسى أحمد	رئيسا
الدكتور : عثماني عبد الرحمن	عضوا مناقشا
الأستاذ : شيخ قويدر	عضوا مناقشا

بسم الله الرحمن الرحيم

« رب إشرح لي صدري
ويسر لي أمري
وأحلل عقدة من لساني يفقه
قولي »

صدق الله العظيم

سورة طه الآية 25 – 28

السنة الجامعية : 2016/2015

كلمة شكر وعرفان

بادئا ذي بدء أشكر الله عز وجل الذي أنار لي الدرب وفتح لي أبواب العلم وأمدني بالصبر والإرادة. وأتوجه بجزيل الشكر إلى الأستاذ المشرف الدكتور "عياشي بوزيان" الذي تشرفت بإشرافه وتوجيهاته القيمة ونصحه السديد أعانه الله تعالى في كل درب سلكه فقد كان نعم الأستاذ ونعم الأخ ونعم المشرف.

دون أن يفوتني شكر وتقدير وإحترام السادة الأساتذة أعضاء اللجنة الموقرة التي قبلت مناقشة هذه المذكرة المتواضعة وجزاهم الله عني خير الجزاء.

شكرا لكم جميعا.

بريكي توفيق

الإهـداء

إلى روح والدي العزيز عبد السلام الذي أرجو من الله عز وجل أن يسكنه فسيح جنانه.

إلى التي أهدتني روح الحياة وقدمت لي آيات الحب والحنان.

إلى من وضعت الجنة تحت قديمها إلى أمي الحبيبة أطال الله عمرها.

إلى أسرتي المتواضعة زوجتي وريحانتا قلبي العزيزتين "رتاج" ، "وريمان".

إلى العائلة الكريمة التي زرعت السعادة في قلبي وتذوقت معهم لذة الحياة.

إلى الخال الطيب والأخ الحنون الأستاذ المحامي "عبد الله بريكي ".

إلى كل من عرفني من قريب أو بعيد.

جزاهم الله عني كل الجزاء.

بريكي توفيق

قائمة المختصرات

ق.إ.ج.ج..... قانون الإجراءات الجزائية الجزائري

ق.ع.ج.....قانون العقوبات الجزائري

ج.ر..... الجريدة

الرسمية

ج.....الجزء

ط..... الطبعة

ص.....الصفحة

س.....السنة

ع.....العدد

مقدمة

مقدمة :

شهد العقد الأخير من القرن العشرين وبدايات القرن الحادي والعشرين تقدما هائلا في مجال التكنولوجيا عامة وتكنولوجيا المعلومات والإتصالات خاصة ومازال ينمو حتى يومنا هذا ويتسارع بخطى واسعة وسريعة أكثر من الأمس وأفرز هذا العصر العديد من آليات تصنيع المعرفة والمزيد من الوسائل التكنولوجية الحديثة التي جعلت العالم قرية كونية صغيرة.

كما أن العصر الراهن يعرف بعصر الثورة العلمية والمعلوماتية والتكنولوجية كما يعرف بعصر التلاحم العضوي بين الحواسيب والعقل البشري فالحواسيب غزت كل مجالات النشاط الإنساني المعاصر.

وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق في مجال تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة فإن هذه الثورة التكنولوجية المتنامية رافقتها في المقابل جملا من الإنعكسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة والإنحراف عن الأغراض المتوخاة منها فقادت إلى تفشي ظاهرة من الظواهر الإجرامية المستحدثة ألا وهي ظاهرة الجرائم المعلوماتية التي لم تعد تقتصر على إقليم دولة واحدة بل تجاوزت حدود الدول وهي جرائم مبتكرة ومستخدمة تمثل إحدى صور الذكاء الإجرامي مما صعب من مهمة إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية كما كشف عن عدم قدرة قواعد الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أو على صعيد الملاحقة الجنائية الدولية.

ولحداثة ظاهرة الجرائم المعلوماتية إهتم الباحثون بالبحث عن تعريف ملائم لهذه الظاهرة لكن دون جدوى وفي هذا الإطار تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن إرتكابها في بيئة الكترونية .

ويعتبر هذا التعريف من أفضل التعريفات التي تناولت ظاهرة الإجرام المعلوماتي.

وتكتسي معالجة هذا النوع من الجرائم أهمية بالغة بالنظر إلى الإشكالات العملية التي تطرحها وإرتباط ظهورها بتكنولوجيا الحاسوب والانترنت مما أسفر عن تميزها بمجموعة من الخصائص جعلتها تختلق عن غيرها من الجرائم واستوجب ضرورة التعامل معها بما يتلاءم مع هذه الخصوصية ناهيك عن أن مرتكبيها يختلفون عادة عن المجرمين التقليديين باعتبارهم أشخاصا على مستوى عالي من العلم والمعرفة فالفاعل في الجرائم المعلوماتية أو ما يسمى بالمجرم المعلوماتي ليس شخصا عاديا إنما شخص ذو مهارات تقنية عالية قادر على استخدام قدراته لتغيير المعلومات أو تقليد البرامج أو تحويل الحسابات عن طريق إستعمال الحاسوب بشكل غير مشروع.

فموضوع دراستنا يتمثل في معرفة القواعد الإجرائية الخاصة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي تضمنها قانون 04/09 المؤرخ في 05 أوت 2009 وكذا استحداثه بموجب المرسوم الرئاسي 261/15 المؤرخ في 2015/10/08 للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، إذ تعد هذه القواعد آليات وضعها المشرع تسمح للمتحري عن انتهاكات قانون العقوبات بإستعمال وسائل قانونية جديدة تتلاءم وخصوصية هذه الجرائم إذ أن قواعد

قانون الإجراءات الجزائية التي تعد الآن تقليدية لم تعد تكفي وتسمح بالتحري والتحقيق وضبط الأدلة الجزائية في هذا الفضاء الإفتراضي المتميز بسهولة إختفاء آثاره ومحو أدلته.

وعليه ارتأينا دراسة هذا الموضوع في فصلين على النحو التالي :

تناولنا في الفصل الأول : الإطار المفاهيمي للجرائم التكنولوجية وخصائصها والحماية الجزائية للنظم والمعلوماتية بالجرائم المرتبكة عبرها وهيئات مكافحتها.

ثم تطرقنا في الفصل الثاني إلى آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال من خلال الدليل الرقمي وطرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفصل الأول :
الإطار المفاهيمي
للجرائم التكنولوجية
و
هيئات مكافحتها

الفصل الأول : الإطار المفاهيمي للجرائم التكنولوجية وهيئات مكافحتها.

لقد عاشت المجتمعات حقبة من الزمن في حالة ذهول وإنبهار لما حققه الكمبيوتر من سرعة في القيام بالعمليات الحسابية ثم تطور ليشمل أعمال التخزين واستيعاب كم هائل من المعلومات وترتيبها بدقة متناهية حتى أصبحت المعلومات التي كان أمر حفظها وتخزينها يستلزم أماكن واسعة وجهدا كبيرين في متناول الأيدي بجهد بسيط ووقت قصير. هذه المميزات العالية جعلت الإستعانة بالحاسوب واستخدامه ضرورة لا غنى عنها لدى أجهزة الدولة والأشخاص الاعتباريين والطبيعيين.

كما أن المعلوماتية تطورت بشكل سريع جدا بفضل تطوير وسائل الإتصال التي تعتمد على الإتصالات الرقمية حيث تسمح بنفي معنى المكان والزمان ونقل المعلومة صوتا وصورة عبر الانترنت بصفة آلية وفي أي مكان من العالم دون إن يكون لها مركز قيادة أو سلطة مركزية مطلقة تتحكم فيها وأمام انخفاض مستوى الأمن في شبكة الانترنت إستفحلت بعض الآثار السلبية لظاهرة المعلوماتية حتى أصبحت تهدد كيان المجتمع اجتماعيا وأخلاقيا خصوصا بظهور أنماط إجرامية لم تكن معروفة من قبل فالشرط الذي قطعته المعلوماتية في تطورها هو نفسه الشوط الذي تأخرت به التشريعات ولاسيما الجنائية منها التي أصبحت عاجزة عن مواجهة مخاطر هذه الظاهرة الإجرامية المستحدثة.

وما يجب إدراكه أن هذه التطورات المذهلة في تكنولوجيات الإعلام والإتصال واكبته جهود دولية للتعاون فيما بين الدول والمؤسسات لخلق مجتمع دولي يسوده التفاهم وتنموا بين أطرافه روح الإحترام بغض النظر عن إختلاف لغاتها وتعدد عقائدها والإتصالات هي العامل المرجح لتحقيق هذه الأغراض.

وتعتبر منظمة اليونسكو UNESCO للتربية والثقافة هي إحدى الوكالات المتخصصة في الأمم المتحدة التي لها باع طويل فيما يخص الأنشطة العالمية المتعلقة بالإتصالات وتقنية المعلومات ولذلك يطلق على المجتمع الدولي اليوم أنه مجتمع المعلومات أو مجتمع الإتصالات.[1]

المبحث الأول : مفهوم الجرائم التكنولوجية والحماية الجزائية للنظم المعلوماتية.

لعل ما يجب الإشارة له في البداية أن الجرائم التي نحن بصدد الحديث عنها هي " الجرائم المعلوماتية " وقد اختلفت المصطلحات الدالة عليها ، فالبعض يطلق عليها جريمة "الغش المعلوماتي " والآخر يسميها "الجريمة المعلوماتية " وثالث يصفها بظاهرة "الإختلاس المعلوماتي" وغيرهم يرمز لها

بـ" الجنح المعلوماتية " مما يصعب معه التقرير بإمكان إيجاد تعريف موحد بإعتبار أن هذه الظاهرة حديثة مما يخشى معه حصرها في نطاق محدد.[2] ولما كانت الجرائم المعلوماتية ظاهرة حديثة لإرتباطها بتكنولوجيات الحاسوب فقد بذل المهتمون بدراسة هذا النمط من الإجرام جهدا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعتها لكن بدون جدوى حتى قيل إن الجريمة المعلوماتية تقاوم التعريف.[3] باعتبارها ظاهرة إجرامية مستجدة ومتميزة من حيث وسيلة إرتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي المجسد لها .

[1] عبد الفتاح بيومي حجازي ، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة للطبعة الأولى 2009 دار النهضة القاهرة ، ص12.

[2] الدكتور : عياشي بوزيان ، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الإقتصادية وآليات مكافحتها ، مجلة الدراسات ، العدد الرابع ، ديسمبر 2016 ، ص 160 ، 161.

[3] هشام فريد رستم ، مخاطر تقنية المعلومات ، مكتبة الآلات الحديثة الطبعة الأولى 1994 ، ص 49.

وما حاولنا التطرق له من خلال هذا المبحث هو التعريف بالجرائم التكنولوجية والخصائص التي تميزها عن باقي الجرائم.

المطلب الأول : ماهية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و خصائصها.

أحاط بالجريمة التكنولوجية شأنها في ذلك شأن كل ظاهرة جديدة الكثير من التساؤلات التي تتعلق بتحديد مفهومها وخصائصها والتمييز بينها وبين ما يقترب منها من ظواهر.

والحقيقة أن تحديد مفهوم الجرائم التكنولوجية وتحديد حجمها هو خطوة أولى للتعرف على هذه الظاهرة من جميع جوانبها القانونية وما يتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها وسنحاول من خلال هذا المطلب الوصول إلى تعريف يتلاءم مع طبيعة الجريمة التكنولوجية لننتقل بعد ذلك إلى خصائص هذه الجريمة.

الفرع الأول : التعريف بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

تعرف الجريمة عموما بأنها :« كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية ».[1]

وعرفها البعض الآخر بأنها « عدوان على مصلحة يحميها القانون ويختص القانون الجنائي بالنص عليها وبيان أركانها والعقوبة المقررة لفاعلها ».[2]

أما بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال بإعتبار أن المشرع الجزائري قد اختار لها هذا الإسم بدلا من جرائم المعلوماتية فإنه عرفها في المادة 2 فقرة أ من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

[1] أ حسن بوسقيعة "الوجيز في القانون الجزائي العام " دار هومة ، الجزائر ، الطبعة الخامسة 2007 ، ص 20.

[2] حسن عبيد "الجريمة الدولية " دراسة تحليلية وتطبيقية ، دار النهضة العربية سنة 1990 ، ص 25.

ومكافحتها بقوله « يقصد في مفهوم هذا القانون بما يأتي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب و يسهل ارتكابها عن طريق منظمة معلوماتية أو نظام للإتصالات الإلكترونية ».

ومن هذا التعريف يمكن أن نحصي ثلاث أنواع من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وهي :

1. جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات في المواد 394 مكرر إلى 394 مكرر 7 وهي أفعال الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات وكذلك فعل الإدخال أو الإزالة أو التعديل بطريق الغش لمعطيات في نظام للمعالجة الآلية.
2. الأشكال التقليدية المجرمة كالغش والنصب عن طريق شبكة الإنترنيت.
3. الجرائم المعروفة بالمحتوى كجرائم القذف والسب وتحريض القصر على الفسق والدعارة .

وتوجد عدة تعريفات للجرائم المتصلة بتكنولوجيات الإعلام والإتصال أوردها الفقهاء ولكنها تعد في أغلبها ضيقة لأنها تقتصر على الأنظمة المعلوماتية وخاصة منها المرتكبة عن طريق جهاز الحاسوب غير مبرزين الأفعال التي ترتكب بواسطة أو ضد أنظمة الاتصالات كجرائم القذف والسب بإستعمال البريد الإلكتروني أو غرف الدردشة في مواقع الانترنيت وكلها تعد من تكنولوجيات الإتصال فالأنظمة المعلوماتية مرتبطة ببعض بواسطة شبكات الإتصال هذه الشبكات تسمح لنظم المعلوماتية بمشاركة البرامج والمعطيات والأجهزة التابعة لها. وفي الوقت الحاضر شبكة الأنترنت هي مثال عن نوع الشبكات المعلوماتية حيث تتصل أجهزة الحاسوب فيما بينها وتتم عمليات تبادل المعطيات من خلالها.

ولكن يجب التطرق إلى هذه التعريفات حتى يمكننا مقارنتها بالتعريف الذي أورده المشرع لهذه الجرائم.

هي « كل فعل أو امتناع عمدي ينشا عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال المادية أو المعنوية ».[1]

وهي «كل سلوك سلبي أو إيجابي يتم بموجبه الإعتداء على البرامج أو المعلومات للإستفادة منها بأية صورة كانت ».[2]

وهي «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها » وهو تعريف لمجموعة من الخبراء في منظمة التعاون الاقتصادي والتنمية (OC DE) ويؤخذ على هذا التعريف إبتعاده عن مبدأ لا جريمة ولا عقوبة ولا تدابير امن إلا بقانون.

وهناك تعريف آخر للجرائم المعلوماتية للدكتور هلالي عبد الله أحمد بأنها :« عمل أو امتناع يأتيه الإنسان إضرار بمكونات الحاسب وشبكات الإتصال الخاصة به والتي يحميها قانون العقوبات ويفرض لها عقابا ».[3]

وقد عرفها الدكتور محمد شوقي بأنها « كل فعل غير مشروع إقترن بالتواصل مع منظومات معلوماتية وشبكات الاتصالات في حين يكون غياب هذا التواصل مانعا لارتكاب هذا الفعل غير المشروع ».

أما بالنسبة للتعريف الذي جاء به المشرع للجرائم المتصلة بتكنولوجيات الإعلام والإتصال بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل

[1] محمد سامي الشواء ، ثورة المعلوماتية وانعكاساتها على قانون العقوبات ،الطبعة الثانية ، دار النهضة العربية القاهرة ، 1998، ص 6.

[2] محمد حامد الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، طبعة الأولى ، دار الثقافة للنشور والتوزيع ، عمان ، 2004 ، ص 154.

[3] الدكتور طارق إبراهيم الدسوقي عطية ، النظام القانوني للحماية المعلوماتية " دار الجامعة الجديدة للنشر ، الإسكندرية ، 2009 ، ص 158.

ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية فقد وفق برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية ولولا هذه النظم المعلوماتية وشبكات الاتصالات ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم وهو ما يوافق تماما التعريف الذي جاء به الدكتور محمد شوقي.

الفرع الثاني : خصائص الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي وقد كان لظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالانترنيت أثره في إعطاء شكل جديد للجريمة المعلوماتية ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود وسوف نحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية ثم سنتناول بالدراسة أهم السمات التي تميز المجرم المعلوماتي.[1]

أولا : خصائص الجرائم المعلوماتية.

تتميز الجرائم التكنولوجية بجملة من الخصائص لعل أبرزها ما يلي :

أ. جرائم مستحدثة :

[1] محمد فواز محمد مطالقة ، آليات الوفاء بالبدل المالي عن طريق الإنترنيت ، مقال منشور بالدليل الإلكتروني .

بحيث ظهرت تبعا للتطور الهائل في مجال التقنية العالية وهو ما جعل أمر تحديد هذا النمط من الإجرام وإدراجه ضمن طائفة الجرائم التقليدية المعروفة تكتنفه صعوبات ترجع إلى الطبيعة الخاصة بها باعتبارها تطال المعلومات ومن ذلك جرائم السطو على أرقام بطائق الائتمان ، فقد أدى إعتماد هذه البطائق المصرفية للوفاء بالمعاملات التي تتم عبر الانترنت إلى إمكانية قرصنتها واختراق البيانات الخاصة بها واستخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطائق الأصليين وكذلك تحويلها الأرقام وهمية تمكن الجناة من الحصول على أموال الغير وتعد شبكة الانترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم بإعتبارها ترتكب عبر هذه الشبكة ومن النماذج المدللة على ذلك ما قام به أحد الأشخاص المغاربة الذي سهلت له إقامته بروسيا الإبحار في عالم الإنترنت والولوج إلى مواقع إلكترونية خاصة من بينها موقع "ميرك " إذ تمكن من الحصول على مجموعة من الأرقام السرية الخاصة ببطائق الائتمان مقرصنة واستغلها في إقتتناء المجلات والملابس الشخصية وبعد عودته إلى المغرب قام بقرصنة مبالغ مالية من مؤسسة ويسترن يونيون وبيع وحدات خاصة بالإتصالات الهاتفية عبر موقع سكايب كما أن تردده على نادي الانترنيت ساعده في التعرف على أشخاص آخرين أطلعوه على كيفية شراء الملابس والقبعات ذات الشهرة العالمية بإستعمال بطائق إئتمان تخص أجانب يقيمون خارج المغرب. [1]

ب.جرائم عابرة للحدود الوطنية :

فالعالم الآن أصبح قرية يمكن التجول في أنحائها بمجرد الضغط على فأرة الحاسوب المرتبطة بشبكة الأنترنت ، فيمكن لشخص ما أن يرتكب جريمة ما في دولة ما تكون آثارها في دولة أو دول عديدة

[1] الدكتورة هدى قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1992 ، ص53.

أخرى وهذا ما نسميه تلاشي الحدود بين الدول في العالم الإفتراضي وخير مثال على ذلك القضية التي حدثت خلال سنة 1989 والمسماة مرض نقص المناعة المكتسبة (الإيدز) التي تتلخص وقائعها في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي تهدف في ظاهرها إلى تقديم بعض النصائح المتعلقة بمرض نقص المناعة المكتسبة غير أن هذا البرنامج يحوي فيروسا يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل وتظهر عبارة على الشاشة يطلب فيها الفاعل مبلغ مالي يرسل على عنوان معين لقاء حصول المتضرر على مضاد للفيروس وبتاريخ 03 فبراير 1990 تم إلقاء القبض على المتهم "جوزيف بوب" في أوهايو بالولايات المتحدة الأمريكية وتم تسليمه للمملكة المتحدة بطلب من هذه الأخيرة باعتبار أن فعل الإرسال تم داخلها إقليميا وتم توجيه أحد عشرة تهمة إبتزاز إليه وقعت معظمها في دول مختلفة إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية وعلى الرغم من ذلك فإن للقضية أهمية لسببين :

- **الأول** : تعد المرة الأولى التي يقدم فيها متهم للمحاكمة بتهمة إعداد برنامج خبيث (فيروس) .
- **الثاني** : تعد المرة الأولى التي يتم فيها تسليم متهم في جريمة مرتبطة بتكنولوجيات الإعلام والإتصال وبسبب تزايد هذا النوع من الإجرام الذي انتشر في الكثير من الدول ولم تعد هناك دولة بمنأى عنه تعالت الأصوات من أجل التصدي لهذه الظاهرة وذلك في إطار تعاون دولي بمقتضاه يتم توحيد القواعد القانونية إلى حد معين مع إحترام سيادة الدول في سن قوانينها التي تتناسب ومبادئها والتي

تجرم التصرفات التي يتم بها الإعتداء على النظم المعلوماتية وشبكات الإتصال المختلفة حتى لا يفلت مجرمو المعلوماتية من قبضة القانون.[1]

ج. **أسلوب إرتكابها** :

تعد الجرائم المعلوماتي من الجرائم الهادئة التي لا تحتاج إلى عنف في إرتكابها ، فالتقنية والخبرة في مجال المعلوماتية تكفيان لوحدهما لإرتكاب أخطر الجرائم التي قد تهز كيان مؤسسة مالية ما أو فرد له اعتماد مالي تم الكشف عن رقم اعتماده السري.

د. **صعوبة اكتشافها ونسبتها لشخص معين** :

لأن الجرائم المعلوماتية ترتكب بهدوء فإن اكتشافها يكون في كثير من الأحيان بمحض الصدفة ولأن مستعملي تكنولوجيا الإعلام والإتصال غير مجبرين على الكشف عن هويتهم عند استعمالهم لهذه التكنولوجيات وخاصة عند تواصلهم بشبكة الانترنيت يكون من الصعب التوصل إليهم والكثير من مرتكبي الأفعال الضارة والمحرمة لا ينالون جزاءهم لعدم إمكانية التوصل إليهم وخاصة في الدول التي لا تملك التقنية والمهارات اللازمة في المؤسسات الأمنية أو خلال التحقيق في تلك الجرائم من طرف سلطتها القضائية.

هـ. **صعوبة إثباتها** :إن التحقيق في الجرائم المعلوماتية يتطلب الإلمام بتقنيات تكنولوجيات الإعلام والإتصال ومواكبة التطور السريع الذي يحدث كل يوم في هذا المجال فيستحيل الإلمام بكل جوانب هذه التقنيات ولكن مسايرتها والتعاون فيما بين التقنيين قد يسهل استخلاص الدليل الإلكتروني من

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، الطبعة لأولى ، 2008 ، ص52، 53.

بيئته الإفتراضية والتحقق من سلامته ويستلزم لذلك أن تقوم سلطات التحقيق بالتدريب والتأهيل اللازمين والإستعانة بذوي الخبرة الأكفاء حتى تكون أعمالهم في التحري والتحقيق على قدر من المهنية التي يمكن بها تقديم دليل الكتروني موثوق إلى القضاء.

مع العلم أن الدليل الإلكتروني يترك دائما آثارا في حالة محوه أو تعديله والخبير فقط من يكتشف التلاعبات التي تحدث في النظم المعلوماتية التي يحدثها المجرمون لمحو آثار جرائمهم والآثار التي توصل إليهم وسيكون في هذا الموضوع توضيحات أكثر عن التكلم في البحث والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال في الفصل الثاني من هذه الدراسة.

و. **إنها جريمة منظمة :**

في البداية إعتبرت الجرائم المتصلة بتكنولوجيات الإعلام والإتصال كسلسلة متتابعة من الإعتداءات على الشبكات ولكنها تلونت بصبغة المافيا أي الجريمة المنظمة منشئة بذلك سوق سوداء حقيقة للمعلومات المقرصنة ابتداء من التعدي على حقوق الملكية الفكرية والفنية والغش في البطاقات البنكية.[1]

ز. **ضرورة وجود حاسوب ومعرفة تقنية به :**

والمقصود من وجود الحاسوب هنا أن تتم الإستعانة به كوسيلة لتنفيذ هذه الجرائم كإستعماله في معالجة المعلومات المقرصنة من بطائق الإئتمان بعد ربطه بآلة تقوم بتسجيل ونقل تلك المعلومات ويتم نسخها على بطاقة أخرى تحمل إسم مرتكب الجريمة أو اسم مستعار تستخدم في سحب الأموال من الشبابيك الأوتوماتيكية وهذا النوع من الجرائم يتطلب إلماما كافيا بمهارات ومعارف فنية كالمعرفة التقنية بالحاسوب

[1] كوثر فرام ، الجريمة المعلوماتية على ضوء العمل القضائي المغربي ، بحث نهاية التدريب بالمعهد العالي للقضاء ، فترة 2009/2007 ، ص 11.

واستخدامه لأن مقترفي هذه الجرائم من المختصين في معالجة المعلومات آليا وعلى دراية فائقة بمجال الحاسب الآلي .[1]

ثانيا : خصائص المجرم المعلوماتي .

يتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين ونذكر منها:

أ. المهارة المطلوبة لتنفيذ النشاط الإجرامي :[2]

والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الإجتماعي مع الآخرين إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم بل من الخبرة المكتسبة في هذا المجال .

ب.معرفة كافة الظروف المحيطة بالجريمة :

[1] جميل عبد الباقي الصغير الانترنت والقانون الجنائي الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، دار النهضة العربية القاهرة ، طبعة 2001، ص 19.

[2] الطالبة حاجب هيام ، الجريمة المعلوماتية ، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء ، الدفعة 16 ،2005/2008 ، ص 10.

إذ ان المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

ج. السلطة التي يتمتع بها المجرم المعلوماتي :

وهي التي تمكنه من ارتكاب جريمته فقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

د. الباعث وراء ارتكاب الجريمة:

قد لا تختلف في الكثير من الأحيان عن الباعث لإرتكاب غيرها من الجرائم الأخرى فالرغبة في تحقيق الربح المادي وبطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله وأخيرا الإنتقام من رب العمل أو أحد الزملاء.

المطلب الثاني : الحماية الجزائية للنظم المعلوماتية والجرائم المرتكبة عبرها.

تطورت أشكال الجريمة المرتكبة عبر هذه التكنولوجيات وأصبح ما يسمى بـ " عولمة الجريمة " [1] فأصبحت تحديات الجريمة عابرة الحدود قضية تهدد الأمن الوطني والدولي في آن واحد بما تقدمه من تسهيلات للأنشطة الإجرامية للأفراد أو للمنظمات (المافيا والجماعات الإرهابية) وذلك بخلقها بيئة خصبة للأنشطة الإجرامية ويطرح السؤال نفسه حول مدى كفاية آليات مكافحة هذه الجرائم سواء من الناحية التقنية العلمية المستخدمة أو من حيث تأهيل العناصر البشرية القادرة على إكتشاف الجريمة ذات الطبيعة التقنية المعقدة والتحقيق فيها والقدرة على التعامل مع مختلف القرائن والأدلة الرقمية ناهيك عن قصور التشريعات الوطنية في معظم الدول لمكافحة هذا الإجرام والأمر المهم الذي يجب تذكره أن الجريمة في مظهرها القديم لم تختف بل اتسع نطاقها ليحتل العالم الافتراضي أي الانترنيت وباقي تكنولوجيات الإعلام والإتصال وظهرت علاوة على ذلك أنماط من الجرائم المستحدثة زادت في حجم الضحايا والخسائر وفي كافة المستويات فنحن نشاهد بما لا جدال فيه تنامي هذا الإجرام لأن المجرمين يستوعبون بسرعة امتيازات الشبكات الرقمية التي تسمح لهم بارتكاب الجرائم على أوسع نطاق بإمكانات مادية ضئيلة مع القليل من الخطر.[2]

وبسبب هذا الحجم المتزايد للجرائم المتصلة بتكنولوجيات الإعلام والإتصال قسمنا هذا المطلب إلى فرعين أولهما أهم الجرائم الماسة بالأشخاص وثانيهما أهم الجرائم الماسة بانظمة المعالجة الآلية للمعطيات.

[1] عبد الله ، عبد الكريم عبد الله،جرائم المعلوماتية والانترنيت (الجرائم الإلكترونية)، منشورات الحلبي القانونية ، ط 1، بيروت 2007 ، ص 22.

[2] عبد الله ، عبد الكريم عبد الله ، المرجع السابق ، ص 22.

الفرع الأول: أهم الجرائم الماسة بالأشخاص بواسطة تكنولوجيات الإعلام والاتصال.

ونتناول فيه مجموعة من الجرائم أهمها :

1) انتحال الشخصية :

انتحال الشخصية يرتكز على أخذ اسم الغير من أجل التنكر أو إخفاء نفسه أو التهرب من مسؤولياته وبالتالي المتابعة الجزائية ويمكن تعريفها عمليا بأنها "أيا كان يستعمل أو يستغل بعلم المعلومات الشخصية لشخص آخر لغاية غير مشروعة" والهدف الوحيد هو ارتكاب جريمة للحصول على امتياز مادي .

لا يوجد انتحال للشخصية في التشريع العقابي الجزائري إلا في ثلاث حالات :

1. انتحال اسم عائلة خلاف اسمه في محرر عمومي أو رسمي أو في وثيقة إدارية معدة لتقديمها للسلطة العمومية وذلك بموجب المادة 247 من قانون العقوبات .
2. أحكام المادة 248من قانون العقوبات التي نصت على من تحصل على صحيفة السوابق القضائية باسم الغير وذلك بانتحال اسما كاذبا أو صفة كاذبة.
3. انتحال اسم الغير في ظروف أدت الى قيد حكم في صحيفة السوابق القضائية لهذا الغير أو كان من الجائز أن تؤدي إلى ذلك (م 249 من قانون العقوبات).

2) جرائم الإعتداء على حرمة الحياة الخاصة وصور الأشخاص :

الحق في الحياة الخاصة هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسان وهناك الكثير من التعريفات لهذا الحق نظرا لإختلاف نطاق الخصوصية من فرد لأخر فهناك من يجعل حياته

الخاصة كتابا مفتوحا وهناك من يجعلها سرا غامضا كما يختلف مضمون الحياة الخاصة من مجتمع لآخر نتيجة لإختلاف القيم الأخلاقية والتقاليد والثقافة والدين مع وجوب التأكيد على أن الخلاف ينصب على نطاق الحق في الحياة الخاصة لكنه لا يمتد إلى الحق في الخصوصية فهو حقيقة مؤكدة لجميع الأفراد في كل المجتمعات.[1]

فقد عرفه الفقيه ALLEN WESTIN بأنه :« الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات في أن يحددوا لأنفسهم متى وكيف وبأي قدر يمكن إيصال المعلومات الخاصة بهم إلى غيرهم ».[2]

والحق في الحياة الخاصة حظي بحماية دستورية حيث نصت عليه مواد الدستور المادة 34 تنص على أنه « تضمن الدولة عدم انتهاك حرمة الإنسان...»

وتنص المادة 39 « لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون سرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة ».

وبالنسبة لقانون العقوبات فقد جرم أفعالا تمس الحياة الخاصة للأشخاص كجريمة الوشاية الكاذبة (المادة 300 ق.ع) جريمة إفشاء السر المهني في غير الحالات المحددة قانونا (م301 . ق.ع) كذلك جريمة إتلاف الرسائل أو المراسلات الموجهة للغير وفضها مع سوء النية (م 303 و م 137 ق.ع) .

جرائم القذف والسب التي تمس الإعتبار والشرف (م 296 إلى 299 ق.ع) وتقضي م 303مكرر03 ق.ع على مسؤولية الشخص المعنوي عن الجرائم المذكورة آنفا.

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، المرجع السابق ، ص165.

[2] مشار إليه عند نهلا عبد القادر المومني ، ص 165.

وبالنسبة للقانون رقم 03/2000 المؤرخ في 05 أوت 2000 الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية فقد نصت م 127 منه في الفصل المتعلق بالأحكام الجزائية على ما يلي « تطبيق العقوبات المنصوص عليها م 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال ».

نسري نفس العقوبات على شخص مرخص له بتقديم خدمة مواصلات سلكية ولاسلكية وكل عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية والذي في إطار ممارسة مهامه وزيادة على الحالات المقررة قانونا ينتهك بأي طريقة كانت سرية المواصلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية واللاسلكية أو الذي أمر أو ساعد في إرتكاب هذه الأفعال.

ويعاقب بالحبس من شهرين إلى سنة وبغرامة مالية من 5000. دج إلى 1000000 دج أو بإحدى هاتين العقوبتين كل شخص غير الأشخاص المذكورين في الفقرتين السابقتين إرتكب الأفعال المعاقب عليها بموجب هاتين الفقرتين.

علاوة على العقوبات المنصوص عليها في الفقرات 1 و 2و 3 المشار إليه أعلاه يمنع المخالف ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية أو اللاسلكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس سنوات.

كذلك من المؤكد أن تقديم شخص عن طريق الانترنت مجموعة من الصور أو المعلومات عن الغير ولو كان من مجموعة المحيطة به يخلق قناة ممتازة للإعتداءات على الحياة الخاصة أو الحق في الصورة وحتى

القذف ومثال ذلك حالة نشر صور للأصدقاء في بطاقته ، هذا النشر العلني يمكن أن يشكل إعتداء على حق الصورة إذا لم يوافق الشخص صاحب الصورة على ذلك قبل النشر وتقضي المادة 303 مكرر 01 « يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من إحتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير أو استخدم بأي وسيلة كانت التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون...» وتنص المادة 303 مكرر على أنه « يعاقب الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك :

1. بالتقاط أو نقل أو تسجيل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
2. بالتقاط أو تسجيل أو نقل صور لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في إرتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة ويضع صفح الضحية حدا للمتابعة الجزائية.

3) الاعتداءات على القصر :

عبر العالم هناك فئات كثيرة ومتزايدة ممن يفضلون التنقل عبر مواقع بذيئة بواسطة الشبكات الرقمية وفي الواقع من السهل جدا أن يجد الشخص المواد (الأفلام والصور) الفاحشة عبر الأنترنيت حيث يكون فالكل يستطيع زيارة هذه المواقع من أجل الطباعة ، تنزيل الملفات ....فالجنس والمنتجات التي تحتوي الإباحية حاضرة وبكل قوة عبر الشبكة ، فمنتجيها يميلون دائما لإمتلاك التكنولوجيات الحديثة وخاصة

منها الإجتماعية فهي تهيء لهم استغلالها (الإنترنت) وكذلك الهواتف النقالة وهذه الصناعة تعد من أكبر الصناعات عبر الأنترنت بجانب صناعة الألعاب ، أما المواقع الإباحية فلا تعد ولا تحصى والعشرات منها تظهر كل يوم أشكال خدماتها تختلف من موقع لآخر ولكن هذه المضامين تنتج على أنها للكبار غير أنه ليس كل مستعملي الأنترنت كبارا فالقصر والأطفال يعدون من أكثر الشرائح استعمالا للانترنت ودخولهم المواقع الإباحية أمر يحدث كثيرا سواء بالمصادفة وأحيانا أخرى بإيعاز من أصفائهم على سبيل الفضول.

فالقصر يستعلمون يوميا الانترنت بمعدلات عالية 12 % منهم يمضون أكثر من ثلاث ساعات في المراسلات الإلكترونية و 87 % وقعوا في محتويات سيئة خلال تنقلهم عبر الانترنت ، فالصور والأفلام الإباحية التي تتضمن أطفالا هي شكل خاص وخطر من الإستغلال الجنسي للأطفال والذي يتخذ مدى عالمي مع تطور إستعمال الشبكات الرقمية والانترنت سهل هذا النوع من العروض الإباحية في أكثر من 100000 موقع.

كما أن هذه المواقع يسهل الوصول إليها من طرف البالغين المنحرفين وحتى الأشخاص العاديين ولكن التعود على مشاهدتها يودي في كثير من الأحيان إلى جرائم بشعة ضد الأطفال من أشخاص مقربين في محيطهم نتيجة للمشاهدة المفرطة للمواقع الإباحية بصفة عامة.

تنص المادة 333 كرر من قانون العقوبات على : « يعاقب بالحبس من شهرين إلى سنتين وبغرامة من 500 إلى 2000 دج كل من صنع أو حاز أو إستورد أو سعى في استيراد من أجل التجارة أ وجر أو لصق أو أقام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في

التوزيع كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء ».

وتنص المادة 347 فقرة 1 من ق. ع على أنه « يعاقب بالحبس من ستة أشهر إلى سنتين وبغرامة من 1000 إلى 20.000 دج كل من قان علنا بإغراء أشخاص من أي من الجنسين بقصد تحريضهم على الفسق وذلك بالإشارة والأقوال أو الكتابات أو بأية وسيلة أخرى ».

أما المادة 342 فقرة 1 من قانون العقوبات فتنص على أنه :« من حرض قصرا لم يكملوا الثامنة عشر على الفسق أو فساد الأخلاق أو تشجيعهم عليه أو تسهيله لهم بصفة عرضية ، يعاقب بالحبس من خمس سنوات إلى عشر سنوات وبغرامة من 2000 إلى 100000 دج ».

بإستقراء المادتين 333 مكرر و 347 من قانون العقوبات نجد أن المشرع حرض على تجريم أية مادة بذيئة تؤدي إلى إفساد الأخلاق وذلك إذا تم بيعها أو إحرازها بقصد البيع أو التوزيع او العرض ونلاحظ أن المشرع لا يعاقب على إحراز المواد البذيئة إلا إذا اتجهت النية إلى بيعها فمن حاز مواد إباحية مخلة بالحياء في بريده الإلكتروني الخاص دون أن تتجه نيته إلى بيعها أو وتوزيعها فإنه لا يعد مرتكبا لجريمة ضد الآداب والأخلاق العامة وحتى تعد جريمة قائمة وفقا لنص المادة 333 مكرر يجب أن يتم بيع أو عرض أو توزيع هذه المادة أو حيازتها من أجل عرضها أو توزيعها أو بيعها وهذه الأفعال يمكن تصورها في نطاق شبكة الانترنت أو باستعمال الهاتف النقال.[1]

[1] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت ، الجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، ط 1، 2007.

ويستوي لدى المشرع أن تكون تلك المواد مطبوعة أو مخطوطة ولا يهم الدعامة التي تكون عليها لوحات زيتية أو صور شمسية أو شرائط ممغنطة فالمشرع وسع من نطاق التجريم بقوله :« أو أنتج أي شيء مخل بالحياء » حيث شمل كل المواد المخلة بالحياء وطرق صنعها ونقلها فعرض هذه المواد عن طريق الهواتف النقالة والأنترنت وتوزيعها بشتى الطرق تحقق الركن المادي للجريمة ، أما بالنسبة للمادة 347 ق.ع فهي الخاصة بالإغراء العمومي وتقوم بتوافر ثلاث أركان :

فعل الإغراء ، العلنية ، القصد الجنائي.

ويقصد بالإغراء «كل دعوة موجهة إلى شخص بسواء كان ذكرا أو أنثى مجهولا أو معروفا لإتيان الفجور وذلك مهما كانت الوسيلة المستعملة ».[1]

ويجب أن يكون الإغراء في مكان عمومي ولا يشترط القانون الإعتياد.

والوسائل التي عددها المشرع في المادة 347 الإشارة أو القول أو الكتابة أو أية وسيلة أخرى تتوافر فيها العلنية تصلح للإغراء فهل تدخل الإنترنت كوسيلة من وسائل الإغراء ؟ بحسب القضاء الفرنسي على قضاة الموضوع تحديد الوسيلة المستعملة للإغراء في حكم الإدانة.

يجب أن تتوافر النية لدى من يحرض على الفسق لقيام الجريمة .[2]

الفرع الثاني : أهم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جرم المشرع الجزائري في القسم السابع مكرر من قانون العقوبات الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وتم إدراج هذا القسم بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل

[1] أ حسن بوسقيعة " الوجيز في القانون الجزائي الخاص "، الجزء الأول ، دار هومة ، الجزائر ، ط 09 ، 2008 ،ص 127.

[2] أ حسن بوسقيعة ، المرجع السابق ، ص 123،ص 124.

والمتمم لقانون العقوبات ليواجه المشرع الجرائم الحديثة المتصلة بتكنولوجيات الإعلام والإتصال هذه الجرائم محددة بموجب المواد 394 مكرر إلى 394 مكرر 6 أحكام هذه المواد تعاقب على الاختراقات غير المصرح بها داخل نظم المعالجة الآلية للمعطيات.

وقبل التطرق إلى هذه الجرائم يجب أولا التعريف بأنظمة المعالجة الآلية للمعطيات حيث لم يقم المشرع بتعريفها على غرار المشرع الفرنسي وقد عرفها الفقه الفرنسي بأنها « كل مركب يتكون من وحدة أو مجموعة وحجات للمعالجة ، ذاكرة ، برامج ، معطيات ، أجهزة ، لإدخال أو لإخراج ، أجهزة الربط التي تعمل فيما بينها لتحقيق نتيجة محددة ، هذا المركب يكون خاضعا لنظام حماية ».[1]

وسوف نتطرق إلى أهم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون التشريع الجزائري .

1. جريمة الدخول غير المشروع في المنظمة المعلوماتية.

يعتبر قانون العقوبات الجزائري من القوانين العربية السابقة إلى هذا الموضوع بل أنه من التشريعات المواكبة للتشريعات الغربية حيث خطا المشرع الجزائري هذه الخطوة بالمبادرة إلى تعديل قانون العقوبات بمقتضى القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع مكرر بمحتوى المادة 394 مكرر إلى 394 مكرر 7 ويبدو أن المشرع الجزائري.

لم يكتف بذلك بل قطع أشوطا أخرى في إيجاد فرض حماية جنائية على الحياة الخاصة للأفراد حين بادر بتعديل جديد لقانون العقوبات وهو الذي جاء به القانون رقم 06 /23 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 وإقراره المادة 303 مكرر إلى 303 مكرر 3 وهو بذلك يضع

[1] آمال قادة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة ، الطبعة الثالثة، 2007، الجزائر ، ص 102.

سياجا لحماية خصوصية الأفراد تحسبا للاستخدام السيء للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال وما يرتبط بها من تقنيات مثل ما يسمى بالبلوتوت وغيره قد نصت المادة 394 مكرر من قانون العقوبات على ما يلي :

« يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.00 دج كل من يدخل أو ينتهك عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك ».

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج.

يلاحظ أن المشرع الجزائري جرم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية وإعتبر هذا التصرف في حد ذاته يشكل جريمة إذا يستخلص لأول وهلة أن مجرد إختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية بعد إنتهاك للنظام المعلوماتي بطريقة غير مشروعة.[1]

ويمكن حسب مفهوم النص أن الجريمة تتحقق بالصور التالية :

- بمجرد الوصول إلى نظام معلوماتي لكن بطريق الغش أي أن الجريمة عمدية هنا تقوم بتوافر القصد الجنائي العام.

[1] هدى حامد قشوش ، المرجع السابق ، ص 55.

- أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه ووضح من نص المادة 394 مكرر ق.ع أن جريمة الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك أي أضرار بالمعلومات ودون تحديد للزمن ذلك أن جريمة الدخول غير المشروع هي جريمة وقتية كما نرى على عكس جريمة البقاء في المنظومة التي تعد من الجرائم المستمرة.

2. جريمة البقاء في المنظومة المعلوماتية :

لاحظنا أن نص المادة 394 مكرر يجرم الدخول وكذلك البقاء فيها ومما يتعين الوقوف عنده هنا هو أن المشرع فرق بين فعل الدخول غير المشروع وبين البقاء دون وجه قانوني أو مصلحة قانونية.

ويمكننا إيعاز ذلك إلى سبب بسيط يبرر هذه التفرقة وهو أنه وإن كان الدخول عن طريق الخطأ ينتهي معه الجرم فإن البقاء عن قصد يشكل جرما قائما بذاته ينم عن إرادة الجاني في الإضرار بالغير.

ويؤكد توافر القصد الجنائي لديه ولم نجد في القانون المقارن رأيا يحدد بدقة زمن إنتهاء جريمة الدخول وبداية جريمة البقاء في المنظومة أو في جزء منها غير أن البعض إعتبر أن بدايتها تكون منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام المعلوماتي [1] لكنه ومع ذلك يظل الغموض قائما حول مدة البقاء داخل المنظومة ويطرح صعوبة حول تحديد زمن البقاء ويجب التفرقة هنا بين البقاء الحاصل عن جريمة الدخول غير المشروع وبين البقاء الناتج عن الدخول المسموح به لكون الجاني رفض الخروج بعد إستيفاء الوقت المسموح له بالدخول فيه للنظام وفي كل الحالات التي يتضح أن المشرع ربط البقاء كتصرف إرادي من قبل الجاني بسوء النية أي عن طريق الغش ويستوي في ذلك أن يكون الدخول أو البقاء في النظام

[1] عبد القادر القهوجي ، الحماية الجنائية لبرنامج الحاسوب الآلي ، الدار الجامعية للطباعة والنشر بيروت ، 1999 ، ص 36.

المعلوماتي كله أو حتى في جزء منه ذلك أن الاعتداء قد يستهدف جهاز الحاسوب نفسه بكيانه المنطقي.

فيستهدف الإعتداء كل المعطيات المخزنة فيه أو يستهدف المعدات المتصلة به وواضح أن المشرع الجزائري لم يكتف بتجريم الدخول أو البقاء غير المشروعين في النظم المعلوماتي بل تجاوز ذلك على تجريم مجرد المحاولة وذلك حسب العبارة الواردة في نص المادة 394 مكرر بالقول « أو يحاول ذلك » غير أن ما يمكن إشارته هنا وهو من الصعوبة بمكان وهو ما يتعلق بفكرة الإثباتات وما من شأنه إعطاء تصور يفيد بأن هناك شروع أو محاولة طالما أن الجريمة في حد ذاتها تطرح إشكالا في الإثبات.

والملاحظ أن المشرع الجزائري يستند في العقوبة وجعلها مضاعفة بنص المادة 394 مكرر ق.ع إذا ترتب عن الدخول أو البقاء في النظام حذف أو تغيير لمعطيات المنظومة إذ نص في الفقرة (2) من المادة المشار إليها على ما يلي :« تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ».

ويتضح من هنا أن الحرص على حماية نظام المعلوماتية لم يتوقف عند تجريم الدخول إليه أو البقاء فيه بل في مواجهة ما هو أخطر منها وهو ما يترتب عنها من نتائج ومنها :

1. حذف البيانات أو المعطيات أو تغييرها.

2. تخريب نظام اشتغال المنظومة.

إن حصول عملية التحريف أو التغيير في المنظومة تعد أبرز صور الجريمة لكونها تجسد الركن المادي للجريمة وتعطي إنطباعا على بلوغ المجرم مبتغاه ويجسد الركن المادي هنا بإحداث تغيير في البيانات وذلك بمحوها كليا أو جزئيا أو تشويهها بحيث تصبح غير صالحة للاستعمال في ذات الوقت يتحقق الركن المعنوي لهذه

الجريمة بتوافر العلم بأن تتجه إرادة الجاني لتحقيق نتيجة تصرفه ومن ثم فإن جريمة الإتلاف والتخريب جريمة عمدية وهي لا تقتصر على تغيير في البيانات بل قد تصل إلى تخريب نظام إشتغال المنظومة كما تصورها نص المادة 394 مكرر ق.ع وبصدد ذلك ضاعف المشرع العقوبة ومن المؤكد هنا إن تحقيق جريمة الإتلاف أو التخريب والتغيير في المعطيات الإلكترونية ومما سبق تكون قائمة ، أما في حال الإتلاف المادي للأجهزة بالكسر أو الحرق أو غيرها فنكون هنا بصدد جريمة منصبة على أموال مادية وتطبق بشأنها أحكام المادة 407 وما بعدها من قانون العقوبات.

وإذا كنا نوهنا بالتطور الذي عرفه التشريع الجزائري في مجال مواكبة الثورة المعلوماتية والرقمية فإننا نلاحظ بأن المشرع الجزائري حذا حذو المشرع الفرنسي بل نكاد نجزم بأنه جعل نص المادة 394 مكرر من قانون العقوبات متطابقا مع نص المادة 1/323 من قانون العقوبات الفرنسي والتي تنص على أن «الدخول أو البقاء بطريق الغش داخل كل أو جزء من نظام المعالجة الآلية للمعطيات يعاقب عليه بالحبس لمدة سنة وبغرامة قدرها 10.000 فرنك وإذا ترتب عن ذلك حذف أو تغيير لمعطيات مخزنة في النظام أو إتلاف تشغيل النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها 200.000 فرنك».

ويتعين الإشارة هنا إلى أن المشرع الفرنسي أصدر عدة قوانين تنصب حول المعالجة الآلية للمعلومات منها القانون رقم 17 لسنة 1978 والذي سمي بقانون المعلوماتية والحريات ثم القانون الصادر بتاريخ 1982/06/12 المتعلق بإثبات التصرفات القانونية ذات المعالجة الإلكترونية.

- قانون العقوبات الجديد رقم 336/92 الصادر سنة 1992 والذي بدأ تطبيقه لسنة 1994.

3. جريمة إدخال معطيات في نظام المعالجة الآلية للمعطيات أو إزالتها بطرق تدليسية.

نصت المادة 394 مكرر 1 من قانون العقوبات الجزائري على ما يلي:

« يعاقب بالحبس من سنة أشهر إلى ثلاث سنوات بغرامة 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها». يبدو أن المشرع الجزائري لكي يعطي حضوضا أوسع لفكرة الحماية الجنائية للمنظومة المعلوماتية وبالتالي حماية الحياة الخاصة تدرج في وضع سياج متكامل ومترابط بتصور السلوكات التي تنطوي على أفعال قد يقدم عليها الجناة وتشكل خرقا أو مساسا بقدسية الحياة الخاصة للأفراد أو لمؤسسات الدولة والمحتواة بشبكة نظام المعلوماتية من بيانات ومعطيات وبرامج وما يتبعها من نتاج فكري لذلك نلاحظ أن المشرع بادر برفع العقوبة في المادة 394 مكرر (1) وجعلها تبدأ من 06 أشهر إلى ثلاث سنوات وبغرامة من 500.000 إلى 2000.000 دج على خلاف ما نص عليه في المادة 394 مكرر ذلك أنه وإن إعتبر المشرع مجرد الدخول إلى المنظومة المعلوماتية أو جزء منها أو البقاء فيها بطرق تدليسية بشكل جريمة دون إقترانه بأي تصرف آخر كما تفطن المشرع إلى تصور ما قد يترتب عن فعل الدخول أو البقاء من المساس بالمعطيات أو البيانات المخزنة من خلال التجول في النظام سواء كان هذا المساس عن عمد أو عن غير عمد.

لأنه جاء إثر تصرف جرمه القانون على خلاف حال الدخول إلى النظام عن طريق الخطأ وتأتي المرحلة اللاحقة كما جاء بها النص وهو قيام الجاني بإدخال معطيات أو برامج جديدة أو معلومات وهمية أو مزيفة ومعلوم أن أي تدخل في نطاق البيانات يعد تدخلا في الكيان المنطقي للحاسوب الآلي كما

سبقت الإشارة إليه والمقصود بإدخال المعطيات في المنظومة هو إدراج برنامج ما والذي هو عبارة عن تعليمات بلغة ما توجه إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة هي بمثابة هدف الجاني لذلك فإن البرنامج الجديد إما أن يكون برنامجا وهميا يهدف إلى التمويه والتضليل في إرتكاب الجريمة وتغيير الحقيقة وتعتبر مرحلة إدخال البيانات أو البرامج أو المعطيات الجديدة كما سماها المشرع الجزائري أهم المراحل في الجريمة الإلكترونية فهي التي تمهد لمرحلة أخطر وهي مرحلة إستقلال البيانات.

فقد يعمد المجرم الإلكتروني إلى إدخال بيانات جديدة على فاتورة الهاتف قبل طبعها وإرسالها أو بيانات متعلقة بحساب بنكي ومن الأمثلة الواقعية قيام طالب بتغيير درجاته المسجلة على الحاسوب أو القيام بالتسجيل الإلكتروني مكان طالب آخر في الجامعة بواسطة اقتناص البيانات.[1]

ويلاحظ المشرع وفي نص المادة 394 مكرر 1 إعتبر كذلك إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملا مجرما أيضا فلا يتوقف الأمر على إدخال معطيات جديدة في النظام بل قد يعمد المجرم بعد الدخول غير المشروع إلى إتلاف البيانات المخزنة أو المتبادلة عبر شبكة الانترنت أو تعطيلها.

ومما يلاحظ هنا أن المشرع قصد بإزالة المعطيات المخزنة إتلافها أو محوها كليا فالنص لم يستثن بأن تكون الإزالة جزئيا أو كليا والأرجح أن يشمل المعنيين معا طالما أن كليهما يشكل فعلا ينطوي على خطورة كبيرة من شأنها إلحاق الأذى بالغير.

[1] ذلك ما حدث فعلا بالنسبة للتلميذ الناجح في المرتبة الأولى في شهادة البكالوريا لسنة 2008 من ولاية قالمة الذي إكتشف بأن شخصا آخر انتحل صفته وسرق بياناته وسجل نفسه مكانه في إختيار لا يرغب به في الجامعة (عن جريدة الشروق اليومية عدد 2362 ليوم السبت 2008/07/26).

ويستوجب هنا حسب رأينا أن يصدر الفعل من شخص يكون دخل إلى النظم بطريق الغش أو على عكس ذلك إذ أنه ليس بالضرورة أن يقترن التصرف المنصب على إزالة البيانات أو التعديل فيها بفعل الدخول غير المشروع الذي يعد جرما في حد ذاته كما أسلفها ولكن التصرف هنا قد يصدر عن فئة العابثين والذين يطلق عليهم (الهاكرز أو الكراكز).

المبحث الثاني : هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

تمتاز الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بعلاقتها الوطيدة بوسائل الإتصال الحديثة وشبكة الأنترنت المتوافرة في كل بقاع العالم.

فجرائم التزوير والإحتيال الإلكتروني ونشر الصور الإباحية والدعارة بمختلف صورها وخاصة دعارة الأطفال التي وجدت لها مرتعا خصبا في مواقع الأنترنت المنتشرة في كل مكان وبكل اللغات وكذلك إستعمال تكنولوجيات الإعلام والإتصال في تنفيذ جرائم الإرهاب والتخريب والجريمة المنظمة تزيد من خطر استعمال هذه التقنيات والتي هي في نفس الوقت لا غنى للناس عنها لذلك فإن إلزامية اللجوء إلى هيئات متخصصة وأشخاص ذوي خبرة عالية في مجال التكنولوجيات الحديثة قد يساهم في ردع هذا النوع من الجرائم بالرغم من أن الكثير منها يتم دون متابعات جزائية إما لعدم إكتشافها أو لعدم التبليغ عنها أو لبطأ رد الفعل القضائي غير المتخصص إتجاهها وفي هذا المجال استلزم إنشاء خلايا متخصصة في كشف هذه الجرائم والتحقيق فيها عبر جميع وحدات الدرك الوطني مع إدراج التكوين المتخصص لرجال القضاء الذين سيحكمون في هذا النوع من الجرائم.

كذلك فإن السمات الدولية لهذه الجرائم بإعتبارها عابرة للحدود في كثير من الأحيان تجعل من تطبيق القوانين الوطنية الجزائية للعديد من الدول لقمعها يشكل تحديا فعليا لممارسة الإختصاص القضائي لهذه الدول وهو ما يرتبط أساسا بسيادتها الوطنية وبتطبيق قوانينها الوطنية على جرائم مرتكبة في إقليمها وهو ما يجعل التعاون الدولي وإعداد قوانين جزائية متناسقة بين الدول لمكافحة هذه الجرائم أمرا حتميا.

المطلب الأول : مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الوطني.

إن الجرائم المعلوماتية تعد من الجرائم الحديثة المرتبطة بتطور تكنولوجيات الإعلام والإتصال التي تستدعي إمكانات وخبرات تقنية لا يمكن مواكبتها إلا بإنشاء هيئات ومراكز متخصصة لمكافحة الجرائم المتصلة بها وبتجنيد العاملين في قطاع العدالة عن طريق التكوين المتخصص الذي يهدف إلى توسيع معارفهم بتلك التكنولوجيات ولمعرفة كيفية استخلاص الأدلة الرقمية وكيف يتم الحكم بواسطتها.

بالإضافة إلى أن الجرائم المعلوماتية تقف بجنب جرائم أخرى كثيرة متعددة ومتنوعة ولكنها في النهاية تعد من أهم الجرائم المستحدثة لأمر واحد وهو أن جميع الجرائم يمكن استعمال تكنولوجيات الإعلام والاتصال في ارتكابها ومثال ذلك جرائم تبييض الأموال ، الإرهاب ، الجريمة المنظمة ، جرائم الفساد ، وتأتي الجرائم التقليدية كالسرقة والنصب والقتل ومن خلال ذلك نرى أن استعمال أجهزة الإعلام الآلي وتكنولوجيات الإعلام والإتصال متوافرة للجميع بمن فيهم المجرمين بمختلف أنواعهم وصفاتهم أساليبهم في ارتكاب جرائمهم.

لهذا سنتناول في هذا المطلب السلطات المتخصصة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها « تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وتحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم » أمامها مهام فقد أوردتها المادة 14 من نفس القانون .

أ. تنظيم الهيئة :

بإستقراء نصوص القانون 04/09 فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة.

ب.مهام الهيئة .

للهيئة مهمتان رئيسيتان هما :

1. الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

وتكون بتوعية مستعملي تكنولوجيات الإعلام والإتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات ومن أهم هذه الجرائم التجسس على الإتصالات والرسائل الإلكترونية ، التلاعب بحسابات العملاء أو بطاقات ائتمانهم....إلخ

2. مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال :

بحسب المادة 14 من القانون 04/09 فهناك نوعان من المكافحة التي تقوم بهما هذه الهيئة :

أ. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة ب من القانون 04/09.

ب. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم مشاركتها مع المنظمات المماثلة لها على مستوى الدول بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم.

الفرع الثاني الضبطية القضائية ودررها في مواجهة جرائم تكنولوجيات الإعلام والإتصال .

إن لسلطة الضبط القضائي دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها أما بالنسبة للجرائم المستحدثة فإنها تلقي المزيد من الأعباء على عاتق هذه السلطة وكذلك الأمر بالنسبة للسلطات القضائية وذلك نظرا لضعف خبرة كل منهما في مواجهة هذه الجرائم.

فمن المتصور أن يجد ضباط الشرطة القضائية أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم وقد يفشل جهاز الضبط القضائي في تقدير أهمية الجريمة نظرا لنقص الخبرة والتدريب.[1]

نظرا لهذه الأسباب كانت من أولويات السياسية الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تكوين وتأهيل سلك ضباط الشرطة القضائية وأعوانهم.

فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال فبموجب هذا العمل فإن الكثير من إطارات الدرك الوطني استفادوا من تكوين خاص في جامعات سويسرا وأمريكا وكندا سواء في المجال التقني (الإعلام الآلي) أو القانوني الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذلك تم التكوين في مؤسسات وطنية مثل مركز الدراسات والبحوث في الإعلام العلمي والتقني الذي عرض تكوينا في الأمن المعلوماتي في إطار التكوين كل سنة هذا البرنامج التكويني يهدف إلى تطوير كفاءات سلك الدرك الوطني حتى تكون أكثر عملية في مجال مكافحة الجرائم المعلوماتية كما أن إطارات الدرك

[1] عبد الفتاح بيومي ،المرجع السابق ،ص 232.

الوطني تساهم في عدة ملتقيات وطنية ودولية تنصب موضوعاتها في إطار الجرائم المتصل بتكنولوجيات الإعلام والإتصال .

لهذا فإن التدريب الجيد لعناصر الأمن والدرك الوطنيين والحملات التحسيسية للمواطنين ستحد من انتشار هذه الجرائم وفي حالة وقوعها فإن المجرمين ينالون عقابهم إمكانية الوصول إليهم عبر إجراءات قانونية تتسم بالشرعية .

الفرع الثالث : السلطة القضائية في مواجهة الجرائم المعلوماتية.

منذ سنة 2003 وفي إطار إصلاح العدالة قامت وزارة العدل بإطلاق برنامج تكوين خاص بالقضاة هدفه رفع مستوى أداء القضاة ليواكب التطور القانوني الجاري الخاص بجرائم المعلوماتية لأجل هذا تم إجراء أولا دمج مادة « الجريمة المعلوماتية » في برنامج تكوين طلبة المدرسة الوطنية للقضاة على شكل ملتقيات ينشطها خبراء ، العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة وإطارات وزارة العدل في إطار التعاون الثنائي.

وقد جاء في اتفاقية التمويل الجزائرية الأوروبية لمشروع دعم إصلاح العدالة في الجزائر: أن هذا المشروع يهدف إلى دعم التخصص وتكوني القضاة داخل وخارج الوطن للاستجابة للمتطلبات المستجدة الناتجة عن لتزايد المستمر للمنازعات التي يجب عليهم الفصل فها.

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص وما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتم لقانون الإجراءات الجزائية على أنه يجوز تمديد دائرة الإختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم

المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف كما نصت المادة 40 مكرر من ق. إ . ج على أنه « تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 40 ، 37 ، 329 من هذا القانون مع مراعاة أحكام المواد 40 مكرر 1 إلى 40 مكرر 5 أدناه ».

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة وهو الأمر الذي نعتقد أنه جعل المشرع الجزائري يتفادى هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية.[1]

فيتجنب إنشاء هيئات قضائية جديدة لكنه يوسع دائرة الإختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها اختصاص نوعي معين في مواد معين دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن اختصاصها العادي وهذا ما يجعلنا نعتقد من جانب آخر أن التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية.

[1] عمار بوضياف ، النظام القضائي الجزائري ، دار ريحانة طبعة 2003 ، ص 229 ، 230.

المطلب الثاني : مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال على الصعيد الدولي.

إن السبيل إلى مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على المستوى الدولي لا يتم إلا عن طريق تعاون الدول فيما بينها وهذا التعاون يتم غالبا في شكل اتفاقيات ثنائية أو متعددة الأطراف ولكن ذلك لا يمنع من ظهور تنازع حول تطبيق القوانين الجزائية الوطنية لدول مختلفة.

وقد تطرح بعض العوائق عند إجراء التحقيقات القضائية للكشف عن أدلة الاتهام والتي هي في هذه الحالة متوافرة في أقاليم عدة دول باعتبار أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي في الكثير من الأحيان من الجرائم المنظمة العابرة للحدود وبالتالي يكون اللجوء إلى تعاون دول حقيقي بموجب قوانين وطنية أمر لا بد منه لمكافحتها ومعاقبة فاعليها .

الفرع الأول : مبدأ الإقليمية في مواجهة جرائم المعلوماتية.

لقد تأثر مبدأ إقليمية القوانين الجزائية بالعولمة التي أعادت طرح الخلاف حول مفهومه التقليدي بإعتباره مبرزا لسيادة الدول على إقليمها وجرائم المعلوماتية لا تعرف الحدود المرسومة للدول ولقد تخطتها كلية فهذه الجرائم يمكن إن ترتكب في عدة دول في آن واحد .

فالبنسبة للاختصاص الإقليمي لقضاء نظم قانون العقوبات وقانون الإجراءات الجزائية قواعد إسناد الإختصاص متعلقة بمكان ارتكاب الفعل المجرم من جهة ومن جهة أخرى بجنسية الفعل كما أن بعض الدول كفرنسا تأخذ بجنسية الضحية لانعقاد الإختصاص لقضائها.

وإذا تعلق الأمر بقواعد إسناد الإختصاص بتطبيق مبدأ الإقليمية المادة 3 فقرة 1 من قانون العقوبات التي تنص على أنه « يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية » كما

تنص المادة 585 من قانون الإجراءات الجزائية على أنه « كل من كان في إقليم الجمهورية شريك في جناية أو جنحة مرتبكة في الخارج يجوز أن يتابع من أجلها ويحكم عليه فيها بمعرفة جهات القضاء الجزائرية ».

إذا كانت الواقعة معاقبا عليها في كلا القانونين الأجنبي والجزائري يشترط أن تكون تلك الواقعة الموصوفة بأنها جناية أو جنحة قد تثبت ارتكبها بقرار نهائي من الجهة القضائية الأجنبية وعليه فلكي يسأل الشريك لا بد من توافر أمرين :

- أن يكون الفعل مجرما في كلا البلدين.
- أن يصدر حكم الإدانة على الفاعل الأصلي في البلد الذي ارتكبت فيه الجناية أو الجنحة.

أما فيما يخص الجنايات والجنح المرتكبة من طرف جزائريين خارج الإقليم الوطني (المادة 582 من ق. ج) فإن قانون العقوبات الجزائري يطبق عليها ولكن بتوافر الشروط التالية :

- يجب أن تكون الواقعة المرتكبة جناية أو جنحة في نظر القانون الجزائري ولم يشترط المشرع أن تكون الواقعة تشكل جناية في نظر تشريع الدولة التي ارتكبت فيها بعكس الجنحة التي أوجب المشرع أن تكون كذلك في نظر تشريع الدولة التي ارتكبت فيها .
- يجب إن يكون المتهم جزائريا وقت ارتكاب الجريمة أو بعد ارتكابها (المادة 584 ق.ج)
- يجب أن يعود المتهم إلى الجزائر.
- يجب ألا يكون المتهم قد حكم عليه نهائيا في الخارج إذ لا يجوز محاكمته مرتين على واقعة واحدة.

- إذا كانت الجريمة موصوفة جنحة وكانت قد ارتكبت ضد أحد الأفراد (الضرب ، الجرح العمد ، السرقة ....) فإن المادة 583 من ق.إ.ج توقف تطبيق قانون العقوبات الجزائري على شكوى من الطرف المتضرر أو بلاغ من سلطات الدولة التي ارتكبت فيها الجريمة.[1]
- وفي الأخير فإن الجنايات والجنح المرتبكة ضد جزائريين في الخارج من طرف أجانب فلا ولاية للقضاء الجزائري عليها إلا في حالة واحدة حددها المشرع بالمادة 591 ق. إ.ج وهي في حال ارتكاب جناية أو جنحة على متن طائرة أجنبية إذا كان الجاني أو المجني عليه جزائريا.

الفرع الثاني : التعاون الأمني الدولي .

إن مكافحة أساليب الإجرام المعلوماتي لا يتحقق إلا إذا كان هناك تعاون دولي على المستوى الإجرائي الجزائي بحيث يسمح بالاتصال المباشر بين أجهزة الأمن في الدول المختلفة وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المعلوماتية وتعميمها لأن هذا النوع من الجرائم ذو بعد دولي وبالتالي فهي عابرة للحدود ذلك أنها قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية التي لا تعتد بسيادة الدولة التقليدية ويتحقق بذلك الفعل الإجرامي على الرغم من التباعد الجغرافي بين الجاني والمجني عليه ، هذا النوع من الجرائم يشكل إذا صورة من صور العولمة عل اعتبار أنها لا تعترف بالحدود القائمة بين الدول سواء الجغرافية أو السياسية هذا ما أدى إلى تصنيفها على أنها من قبيل الجرائم الدولية مما يعني إمكانية خضوعها لأكثر من قانون جنائي.[2]

[1] أحسن بوسقيعة ، الوجيز في القانون الجزائي العام ، المرجع السابق ، ص81.

[2] الدكتور عياشي بوزيان ، مجلة الدراسات الحقوقية ، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية ودافعها في الجزائر ، العدد الرابع ، ديسمبر 2015.ص187.

لذلك أصبحت الحاجة ملحة إلى تعاون أجهزة الأمن بين الدول وتنسيق العمل فيما بينها لضبط المجرمين وقد تبلور هذا النوع من التعاون الدولي في إنشاء منظمة دولية تهدف إل تأكيد وتشجيع التعاون بين سلطات الأمن في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة وتبادل المعلومات والبيانات فيما بينها والتعاون في ضبط المجرمين بمساعدة أجهزة الأمن في الدول الأطراف ومدها بالمعلومات المتوافرة لديها على إقليمها أي أن عضو الأنتربول لا يقوم بنفسه بإجراء القبض على المجرم بل إن هذا العمل منوط بجهاز الأمن الوطني في الدولة التي يتواجد المجرم على إقليمها الأم الذي يؤكد على احترام السيادة الوطنية.

لذلك فإن من الأهمية بمكان تدعيم القانون بين أجهزة الشرطة في هذه الدول المختلفة بناء على اتفاقيات دولية ولهذا التعاون أهمية بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم المعلوماتية قد تم ارتكابها عبر شبكة الأنترنت من خلال موقع موجود في الخارج فغنها تقوم بالإبلاغ عن هذه شبكة إلى سلطات الأمن بالدولة التي تم منها البث.[1]

يجمع الأنتربول المعلومات عن الجرائم المعلوماتية ويحفظها ويحللها ويتبادلها مع جميع بلدانه الأعضاء عبر منظومة الأنتربول العلمية للاتصالات الشرطية .

ومن المهم في التحقيقات الجارية بشان الإجرام المعلوماتي أن تسارع الشرطة إلى ضبط الأدلة المتعلقة بالبيانات الرقمية وهي على حالتها الأصلية قدر الإمكان وقد كون الأنتربول شبكة من المحققين العاملين

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق ، ص 594.

في الوحدات الوطنية المعنية بجرائم الكومبيوتر تعرف باسم شبكة النقاط المرجعية الوطنية لتسير الإتصالات الميدانية بين البلدان الأعضاء وتسرعها قدر الإمكان .

كما استحدثت فرق للأنتربول تعنى بجرائم تكنولوجيا المعلومات لتسيير إنماء الإستراتيجيات والتقنيات والمعلومات بشان أحدث الأساليب الإجرامية في جرائم تكنولوجيات المعلومات وكمثال على الأنشطة المقدمة من طرف هذه الفرق ما قامت به الفرق العاملة الأوربية التي أعدت « دليل الأنتربول بشأن جرائم تكنولوجيا المعلومات » الذي يجمع ويصف بالتفصيل أدوات التحقيقات.

الفرع الثالث المساعدة القضائية الدولية :

لما كانت جرائم المعلوماتية ذات طابع عالمي وبالتالي يمكن أن تتعدى آثارها عدة دول فإن ملاحقة مرتكبي هذه الجرائم وتقديمهم للمحاكمة وتوقيع العقاب عليهم يستلزم القيام بأعمال إجرامية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها مثل : سماع الشهود ، أو طلبات الحصول على معطيات معينة مخزنة في نظام معلوماتي موجود داخل إقليم دولة أخرى أو حول إلكترونيا عن طريق الشبكة ويمكن مراقبتها أو إعتراضها في إقليم تلك الدول أو اللجوء إلى الإنابة القضائية أو تقديم المعلومات التي يمكن أن تساهم في التحقيق حول هذه الجرائم وكل ذلك لا يتحقق بدون مساعدة الدول الأخرى لذلك تضم معظم الاتفاقيات الخاصة بالجرائم التقليدية نصوص تقضي بضرورة اللجوء إلى المساعدة المتبادلة بهدف تحقيق السرعة والفاعلية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم.[1]

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق، ص 597.

فالمساعدة القضائية تعني عموما كل الأشكال المتعلقة بتطبيق بعض السلطات الردعية في إطار التحريات المتعلقة بجرائم تكنولوجيات المعلومات وعليه فللمساعدة القضائية صور عديدة نتناول منها يأتي :

أ. **نقل إجراءات الردع** :

ويقصد به قيام دولة بناء على اتفاقية باتخاذ إجراءات جزائية بصدد جريمة ارتكبت في دولة أخرى وذلك إذا توافرت شروط معينة :

1. أن يكون الفعل المنسوب إلى شخص يشكل جريمة في الدولة الطالبة والدول المطلوب إليها.
2. أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة.
3. أن يكون الإجراء المطلوب اتخاذه يؤدي للوصول إلى الحقيقة كأن تكون أدلة الجريمة موجودة في الدولة المطلوب إليها.

إن ممارسة الإختصاص في القضايا العابرة للحدود يمكن أن تسبب مطالبة تنافسية للاختصاص والتي من الممكن في النهاية أن تتسبب في تعدد المتابعات القضائية وتخلق خلافات بين الدول إن تقنية نقل الإجراءات تقدم آليات جد فعالة لحل هذه المشاكل وحماية حقوق الضحايا واستعادة المجرم للمجتمع وقد أقر المجلس الأوروبي اتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنظمة إمكانية محاكمة الجاني طبقا لقوانينها بناء على طلب دولة أخرى طرف هذه الاتفاقية بشرط أن يكون الفعل معاقب عليه في الدولتين وبالنسبة للجزائر فقد تم إبرام العديد من الاتفاقيات الثنائية من بينها الإتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا الموقعة

بمدريد في 07 أكتوبر سنة 2002 (المرسوم الرئاسي رقم 23/04 مؤرخ في 07 فيفري 2004 الجريدة الرسمية العدد 08).

ب.تبادل المعلومات :

هو ما نصت عليه المادة 17 من القانون 04/09 المتضمن بقواعد الخاصة للوقاية من الجرائم بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نصت على أنه « يتم الاستجابة لطلبات المساعدة الجزائية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل » كما أن هناك مظهر آخر لها يتعلق بصحيفة السوابق القضائية للمتهمين من خلالها تتعرف الجهات القضائية على الماضي الجزائي للشخص المحال لها والتي تساعد في تشديد العقوبة في حال العودة أو في وقف تنفيذها إلا أن تدويل صحيفة السوابق العدلية لا يتم إلا بواسطة اتفاقات تبادل المعلومات بين الدوليتين الطالبة والمطلوب منها.[1]

ج. تبادل الإنابة القضائية الدولية :

ويقصد بها إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الإجراء في الفصل في مسألة معروفة على السلطة القضائية في الدولة الطالبة ويتعذر عليها

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق، ص 598.

القيام به بنفسها وهو ما أبرزته المادتين 16 و 17 من القانون 04/09 السالف الذكر والذي عبرت عنه باتخاذ إجراءات تحفظية ولا يكون ذلك إلا بالإنابة القضائية.

شروط قبول المساعدة القضائية الدولية :

- لقد أورد المشرع الجزائري في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مجموعة من الشروط لقبول المساعدة القضائية الدولية :

أ. بالنسبة لكيفية إرسال طلبات المساعدة سواء من وإلى الجزائر فإنه يتم غالبا بالطريق الدبلوماسي وهو كما نعلم يتسم بالبطء وكثرة شكلياته وهو ما يتعارض مع نظم المعلومات التي تتميز بسرعة عبور وتبادل المعلومة من خلال شبكات الاتصال الحديثة والانترنت ولان الجريمة المعلوماتية لها ثلاث ميزات :

- سرعة فقدانه.
- صعوبة اكتشافها.
- عابرة للحدود الوطنية.

فإن تلك الطريق لا يمكن إعتمادها دائما في مجال الجرائم المتعلقة بتكنولوجيات الإعلام والإتصال لهاذ نجد أن المشرع الجزائري أراد استثناءا في المادة 16 فقرة 2 من القانون 04/09 «يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدآ المعاملة بالمثل قبول طلبات المساعدة القضائية إذا وردت عن طريق وسائل الإتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها» وبهذا الصدد أوجبت المادة 36 من

القانون رقم 06/05 المتعلق بمكافحة التهريب والمعدل بالأمر رقم 09/06 « على أنه في حالة توجيه الطلب إلكترونيا من طرف السلطات الأجنبية يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا ».[1]

ب.أورد المشرع في المادة 18 فقرة 1 من القانون 04/09 مجموعة من القيود على طلبات المساعدة القضائية الدولية تمنع الإستجابة لها وذلك إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام غير أنه يمكن الاستجابة إلى طلبات المساعدة القضائية شريطة المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.[2]

ج. بحسب نص المادة 16 فقرة 1 من القانون 04/109 أدرج المشرع مبدأ ازدواجية التجريم وإن لم يكن قد صرح به وتنص المادة على أنه «في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني » بالتالي لا يمكن للدولة تقديم المساعدة القضائية لدولة أخرى في تحقيقات أو تحريات تخص أفعال غير مجرمة لديها وعليه فإنه بالنسبة للأحكام الموضوعية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال يجب على الدولة إعداد نصوص متناسقة قدر الإمكان مع النصوص التشريعية لباقي الدول وهو ما يدعدى بتنسيق القوانين الوطنية الجزائية وذلك لاجتناب وجود منافذ أو تفسيرات متضاربة ب للشروط الواجب توفرها لتبرير الجريمة وفي الواقع وحتى في حالة عدم استخدام قاعدة ازدواجية التجريم في كل حالات المساعدة القضائية فإن هذه القاعدة هي في كثير ما الأحيان ضرورية للوصول إلى أدلة الإدانة.

[1] الأستاذ زيحة زيدان ،الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للنشر عين مليلة الجزائر، طبعة 2011 ص145.

[2] الدكتور عياشي بوزيان ، المرجع السابق ، ص 157.

الفصل الثاني :
آليات البحث والتحري للكشف
عن الجرائم المتصلة
بتكنولوجيات الإعلام والاتصال.

الفصل الثاني : آليات البحث والتحري للكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

إن إصدار المشرع للقانون 04/09 المتضمن القواعد الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قد أرسى قواعد إجرائية جديدة تخضع لها السلطة القضائية وأعوانها تطبيقا لمبدأ الشرعية الذي يعد حجر الزاوية في الإجراءات القانونية للتحقيق في الجرائم المرتكبة ومتابعة فاعليها وتوقيع العقوبة المناسبة عليهم [1] هذه الإجراءات الجديدة والتي يستطيع بها رجل الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية التي أرساها قانون الإجراءات الجزائية لذلك سيكون تقسيم هذا الفصل إلى مبحثين :

- المبحث الأول : الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .
- المبحث الثاني :أساليب التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

[1] د.حاتم حسين بكار « أصول الإجراءات الجنائية وفق أحدث التعديلات التشريعية والاجتهادات الفقهية والقضائية » منشأة المعارف بالإسكندرية مصر 2007 ، ص 24

المبحث الأول : الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

لقد أنتجت حالة الصراع بين المجتمعات وبين الجريمة في ثوبها الجديد الناجمة من استعمال تكنولوجيات الإعلام والاتصال نظرة جديدة إلى الإثبات الجنائي تمثلت في سؤال فرض نفسه على دراسات القانون الجنائي يتناول في موضوعه البحث في مدى إمكانية تجاوب وسائل الإثبات الجنائي التي يمكن نعتها الآن بالتقليدية مع التقنيات الجيدة لتكنولوجيات الإعلام والاتصال وهذا التساؤل يقودنا في الحقيقة إلى الإقرار بان ظاهرة جديدة برزت لتنظم بجدارة إلى المفاهيم التقليدية للدليل ، وهي هنا الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والانترنت ، بحيث يصح أن يطلق على الارتباط بين الظاهرة الرقمية الجديدة وبين الإثبات الجنائي تسمية جديدة "الدليل الرقمي" أو "الدليل الإلكتروني" حسبما أطلق عليه المشرع الأوربي هذا المصطلح .[1] وهذا فعلا ما قام به المشرع الجزائري محتذيا بذلك ما قامت به التشريعات المقارنة من تبني وسائل جديدة للبحث والتحري في هذه الجرائم.

فالإستعانة بالدليل الرقمي لم تعد محل شك في قيمته كدليل يتلاءم مع مفهوم الأدلة التي يعرفها القانون في صيغته التقليدية وذلك لأمر مهم وهو تقنينه بقانون بسبب إدخاله في المنظومة القانونية .

المطلب الأول : الدليل الرقمي في إثبات الجريمة المعلوماتية.

كما أثرت الثورة المعلوماتية على نوعية الجرائم التي صاحبتها وظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية فإنها في المقابل أيضا أثرت على إثباتها فأصبحت الأدلة التقليدية التي جاءت بها نصوص القانون الإجراءات الجزائية غير قادرة على إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق

[1] فتحي محمد أنو عزت « الأدلة الإلكترونية في المسائل الجنائية » ، دار الكفر والقانون مصر ، ط 1، .2010 ، ص581.

تقنية تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة

الفرع الأول : مفهوم الدليل الرقمي وخصائصه.

أولا : تعريف الدليل الرقمي.

إن تقييم أي نظام قانوني لا يمكن أن يصل إلى نتائج صحيحة إلا إذا توافر لدى المقوم تصورا واضحا لذلك النظام وعليه فإنه من الواجب ليتسنى فهم ماهية هذا النوع من الأدلة لابد من تناول تعريفه . وقد وردت بشأن الدليل الرقمي عدة تعريفات أهمها :

« أنه الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء ».[1]

وهناك من يعرفه « بأنه معلومات يقبلها المنطق والعقل ويعتمدها العلم ، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة لنظم المعلوماتي وملحقاتها وشبكات الاتصال ، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمات لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه أو أنه ذلك الدليل الذي يجد له أساس في العلم الافتراضي يقود إلى الجريمة ».[2]

[1] ممدوح عبد الحميد عبد المطلب « البحث والتحقيق الجنائي الرمي في جرائم الحاسب الآلي والانترنت » دار الفكر القانوني ، مصر ، 2006 ، ص 08.

[2] عمر محمد يونس ،« مذكرات في الإثبات الجنائي عبر الانترنت » ندوة الدليل الرقمي بجامعة الدول العربية ، 2006، ص 05.

أو أنه « الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو لإدانة فيها ».

وقد عرفت مجموعة العمل العلمية للأدلة الرقمية الدليل الرقمي عام 1999 «بأنه معلومات ذات قيمة إثباتية مخزنة و منقولة في شكل ثنائي ».

والتعريف الذي أخد به التقرير الأمريكي المقدم لندوة الأنتربول العلمية حول الدليل الرقمي عام 2001 اعتبر أن الدليل الرقمي هو عبارة عن بيانات يمكن إعدادها وتراسلها وتخزينها رقميا لتمكين الحاسوب من تأدية مهام ما.

ويستخلص من التعريفات السابقة أن الدليل الرقمي هو أي معلومات سواء كانت من صنع الإنسان أو تم استخلاصها من الحاسوب بقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة أو الجاني أو المجني عليه.

وبالنظر إلى جملة التعريفات السابقة يمكن أن نلاحظ أن منها من ألحق مفهوم الدليل الرقمي بمفهوم البرنامج على الرغم من اختلافهما فالفرق بينهما يكفي في الوظيفة التي يؤديها كل واحد منهما ، فبرامج الحاسب الآلي لها دور كبير في القيام بمختلق العمليات التي يحتويها نظام المعالجة الآلية والذي لا يقوم

بعملية إلا عن طريق مجموعة من البرامج تسمح بالقيام بمختلف العمليات عند إعطاء أوامر بذلك أما الدليل الجنائي الرقمي فله أهمية كبري ودور أساسي في معرفة كيفية حدوث جرائم الاعتداء على نظم المعالجة الآلية بهدف إثباتها ونسبتها إلى مرتكبها.

كما حصرت بعض التعريفات السابقة الأدلة الرقمية في تلك الأدلة التي يتم استخراجها من الحاسب الآلي وهو ما يعد تضييقا لدائرة التقنية فهي كما يمكن أن تستخلص من الحاسب الآلي فمن الممكن أيضا الحصول عليها من أي وسيلة تقنية أخرى كالهواتف النقالة الذكية.

والتعريف الأكثر شمولا هو الذي يعرف الدليل الرقمي بأنه «طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى أحد الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب Le disque dur والرسائل الإلكترونية المخزنة والمنقولة رقميا».

ثانيا : خصائص الدليل الرقمي.

تقوم خصائص الدليل الرقمي على مدى ارتباطه بالبيئة التي يحيا فيها وهي البيئة الافتراضية والتي انعكست على طبيعة هذا الدليل فأصبح يتصف بعدة خصائص جعلته يتميز على الدليل الجنائي التقليدي منها :

1/ الدليل الرقمي هو دليل علمي :

إن الدليل الرقمي يحتاج إلى بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات ذات المبنى العملي ومن ثمة فإن، ما ينطبق على الدليل العملي ينطبق على الدليل الرقمي فالدليل العملي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة أن القانون مسعاه العدالة وأما العلم فمسعاه الحقيقة وإذا للدليل العلمي منطقه الذي يجب ألا يخرج عليه ، إذ يستبعد تعارضه مع القواعد العملية السليمة فإن الدليل الرقمي له ذات الطبيعة فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه.[1]

2/الدليل الرقمي من طبيعة تقنية :

إن الطبيعة التقنية للدليل تقضي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها فلا تنتج التقنية سكينا يتم به اكتشاف القاتل ، أو اعترافا مكتوبا أو مالا في جريمة الرشوة ، أو بصمة إصبع وإننا تنتجه التقنية هو نبضات رقمية تتشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها ومثل هذا الأمر يجعلنا نقرر ، أنه لا وجود للدليل الرقمي خارج

[1] عمر محمد بن يونس المرجع السابق ص 977.

بيئته التقنية وأنه لكي يكون هناك دليل رقمي يجب أن يكون مستوحا أو مستنبطا من البيئة الرقمية أو التقنية.[1]

وهي في إطار جرائم المعلوماتية ممثلة في العالم الرقمي أو العالم الافتراضي وهو العامل الكامن في الحاسوب.

ونتيجة للطبيعة التقنية للدليل الرقمي فإنه اكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ بحيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير[2] بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل باستخدام البرامج والتطبيقات الصحيحة.

3/الدليل الرقمي دليل متنوع ومتطور :

يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة الرقمية إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن في حال المراقبة عبر الشبكات وقد يكون بيانات مفهومة كما لو كان وثيقة (Document) معدة بنظام المعالجة الآلية كما من الممكن أن يكون صورة ثابتة أو متحركة

[1] خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الطبعة الأولى 2009 ، ص 56.

[2] عمر محمد بن يونس المرجع السابق ص 17.

(أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الإلكتروني وقد يكون أيضا مرتبطا بالتشفير وهذا التنوع إنما يعد تعبيرا عن اتساع قاعدة الدليل الرقمي بحيث يمكنه بهذه الصور أن يشمل أنواعا متعدد من البيانات الرقمية التي تصلح منفردة أو مجتمعة لأن تكون دليل بالإدانة أو البراءة.

وأما عن كون الدليل الرقمي دليل متطورا فهي خاصية تكاد تكون تلقائية نظرا لارتباطه بالطبيعة التي تتم عبرها حركة الاتصال عبر الانترنت والعالم الافتراضي اللذان لا يزالان في بدايتهما ولم يصلا بعد إل منتهاهما ولن يكون من السهل احتواؤهما.

4/ الدليل الرقمي صعب التخلص منه:

إن القاعدة التي تسري على كافة ما يتعلق بهيكلة تكنولوجيا المعلومات هي أنه كلما حدث اتصال بتكنولوجيات المعلومات في معنى إدخال بيانات إلى ذلك العالم(Input) من الصعب التخلص منها ولو كان ذلك باستخدام أقوى أدوات الإلغاء في الحاسوب (ERASE .REMOVE .DELETE) لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوافر على برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب[1].

ويمكن إعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية إذ يمكن التخلص بسهولة من الأوراق والأشرطة المسجلة إذا حملت في طياتها دليل الجريمة بتمزيقها أو حرقها ، كما يمكن

[1] عمر محمد أبوبكر بن يونس المرجع السابق ص 17.

أيضا التخلص من بصمات الأصابع بمسحها من موضعها كما يمكن التخلص من الشهود بتهديدهم أو قتلهم كما يحدث في بعض الدول الغربية أو استبعادها أصلا في الإثبات إذا مضى عليه مدة طويلة من الزمن قد لا يكون بعدها الشاهد قادرا على التذكر وكل ذلك يجعل عملية التخلص من هذه الأداة أمرا سهلا ومن إمكانية استرجاعها أو استرداد الدليل المستمد منها مستحيلا بعد تدميرها أما بالنسبة للأدلة الرقمية فإن الحال غير ذلك حيث يمكن استرجاعها بعد محوها وإصلاحها بعد إتلافها وإظهارها بعد إخفائها مما يؤدي إلى صعوبة التخلص منها ، كما أن نشاط الجاني في عملية محو الدليل يشكل في حد ذاته دليلا ضد الجاني لأنه هذا النشاط يتم تسجليه في الحاسب الآلي ويمكن استخلاصه لاحقا ويترتب على هذه الخاصية مسائل قانونية هامة أبزرها مسألة التخلص أو إخفاء الدليل وهو يعد فعلا آخر موضوع التجريم بمقتضى القانون ، فإن ثبت أن مرتكب الجريمة المعلوماتية قد استخدم من البرمجيات من اجل التخلص من الدليل فإنه يمكن متابعته وإدانته بالنصوص القانونية التي تجرم مثل هذه الأفعال.

5/ الدليل الرقمي ذو طبيعة رقمية ثنائية (1 – 0) :

إن الآثار التي يتركها مستخدم النظام المعلوماتي والتي تشمل الرسائل المرسلة منه أو التي استقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي وشبكة الاتصالات تكون على الشكل الرقمي فالبيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أو حروف أو أرقام أو صور أو فيديو تتحول إلى صيغة رقمية ، حيث ترتكز تكنولوجيات المعلوماتية الحديثة على تقنية الترقيم التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي قوامة الرقمان (0) ، (1) فأي شيء في العالم الرقمي يتكون من الصفر والواحد فالكتابة مثلا في العالم الرقمي ليس لها الوجود

المادي الذي نعرفه وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد وهو الرقم الثنائي (0) ، (1) وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة.[1]

إن هذه الخصائص السالف ذكرها أكسبت الدليل الرقمي طابعا متميزا جعلت منه الدليل الأفضل لإثبات الجرائم المعلوماتية لأنه من طبيعة الوسط الذي ارتكبت فيه سواء كانت هذه الجرائم مرتبكة بواسطة نظام المعاجلة الآلية أو كانت تشكل إعتداء ومساس بنظام ا لمعالجة الآلية.

الفرع الثاني : أشكال الدليل الرقمي وأنواعه.

أولا أشكال الدليل الرقمي : ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال.

1. **الصورة الرقمية** : وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديلة للصورة التقليدية.
2. **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية وتشمل المحادثات الصوتية على الانترنت.
3. **النصوص المكتوبة** : وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي.

[1] سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير جامعة باتنة ، 2013 ،ص125.

ووفقا لما قررته وزارة العدل الأمريكية سنة 2002 فإن الدليل الرقمي يمكن أن يأخذ الأشكال التالية :[1]

السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات البرامج معالجة الكلمات وغرف المحادثة على الانترنت.

السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبر مخرجات برامج لم يلمسها الإنسان مثل LOGFILES السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب بعد معالجتها من خلال برامج معينة.

كما أن هناك [2]من يقسم أشكال الدليل الرقمي تقسيما يتطابق مع تقسيم الجريمة عبر الحاسب الآلي على النحو التالي :

- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها.
- أدلة رقمية خاصة بالشبكة العالمية للمعلومات.
- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

بالإضافة إلى هذا التقسيم فإنه يوجد من الفقه من إعتمد في تحديد أشكال الدليل الرقمي على أشكال المخرجات الكومبيوترية إذ يأخذ الدليل الرقمي بحسب هذا التقسيم ثلاثة أشكال :

- مخرجات ذات طبيعة ورقية يسجل فيها المعلومات على الورق ويستخدم في ذلك الطابعات.
- مخرجات ذات طبيعة الكترونية تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية.

---

[1] سلطان محيا الريحاني « الجرائم المعلوماتية » بحث منشور على الموقع الإلكتروني.http/www.ATSLP.com بدون ترقيم.

[2] ممدوح عبد الحميد عبد المطلب ، المرجع السابق ، ص 88.

- مخرجات مرئية معروضة بواسطة شاشات الحاسب الآلي ذاته ويتمثل هذا الشكل في عرض البيانات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به .

ثانيا :أنواع الدليل الرقمي .

يأخذ الدليل الرقمي نوعين رئيسيين :

أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون وسيلة إثبات فأما النوع الأول فيمكن إجماله في ما يلي :

السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الإنسان في إنشائها.

السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الجهاز ، ومن أمثلة ذلك البيانات التي تم إدخالها على الأدلة وتم معالجتا لتكون وسيلة إثبات فهي تلك الأدلة التي تنشأ دون إرادة الشخص ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية الرقمية وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال النظام المعلوماتي ، وشبكة الاتصالات والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها فالاتصالات التي تتم عبر المنظومة المعلوماتية المرتبطة بشبكة فالإتصالات وكذا المراسلات الصادر عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك.

وتبدو أهمية التمييز بين هذين النوعين في كون أن النوع الأول من الأدلة الرقمية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها لذلك فإن عادة ما يعمد إلى حفظه للاحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه كما يكون من السهل الحصول عليه ، بينما النوع الثاني من الأدلة الرقمية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها ويكون الحصول عليه بإتباع تقنيات خاصة لا تخلو من الصعوبة وهو على العكس من النوع الأول إذا لم يعد ليحفظ ما يجعله عرضة للفقدان بسهولة.[1]

المطلب الثاني : مصادر الحصول على الدليل الرقمي.

إن مصادر الحصول على الدليل الرقمي تكمن في البيئة الرقمية التي ارتكبت فيها الجريمة المعلوماتية وتتمثل في أجهزة الحواسيب الخاصة بالجاني والمجني عليه وكذا أجهزة مقدم الخدمة .

وهذه المصادر قد تكون على سبيل المثال لا الحصر إذا إن التطور العلمي والتقني قد يسفر عن أنواع جديدة من المصادر التقنية ، إذ المقصود هنا من أين يمكن لجهات التحقيق والتحري عن الجريمة المعلوماتية إستخلاص الدليل الرقمي.

الفرع الأول : فحص جهاز الحاسوب الخاص بالجاني والمجني عليه.

إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقيق وبيان الطريقة التي قام بها هذا لأخير في ارتكاب جرائمه ، مما لا شك فيه أن المجني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ، ما قام

[1] طارق محمد الجملي ، « الدليل الرقمي في الإثبات الجنائي »ورقة عمل مقدمة من للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة 28 - 2009/10/29 المرجع السابق.

به الجاني من جرائم وبالتالي فإن فحص جهاز الحاسوب الخاص به يمكن المحقق من معرفة الدخول وتتبع مصدره.

ويمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال أجهزة الحاسوب سواء الخاصة بالجاني أو المجني عليه عن طريق البحث في المصدرين التاليين :

أولا : أنظمة الحاسوب وملحقاتها.

تعد الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للأفراد فهذه الحواسيب تحتوي على الكثير من المعومات المتعلقة بنشاطات الأفراد ورغباتهم وعملية حجز الحاسوب يقصد تفحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المعلوماتية بإعتبار أن هذا الجهاز هو وسيلة تنفيذها والحاسب الآلي في ذاته يقوم في تركيبته على أمرين هما القطع الصلبة (HARDWARE) والقطع المرنة أو البرمجيات (SOFTWARE) وهناك عنصر ثالث يتوزع بين البرمجيات والقطع الصلبة وهو عنصر المعلوماتية. [1]

لذلك فإن الأمر يستلزم أن يكون الفحص ماديا ومعنويا للارتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل .

وقد تعتمد عملية الفحص على الحاسوب ذاته أي ما يسمى بالفحص الذاتي من خلال قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص ومثل هذه العملية تتطلب من القائم

[1] حسين بن سعيد الفاغري ،« الجدول الدولية في مواجهة جرائم الإنترنت » 2007، ص 425.

بها مهارة عالية أو قد يتم الفحص عن طريق الإستعانة بجهاز آخر للبحث ويجب أن تشمل عملية الفحص على ما يلي :

1/فحص القرص الصلب :

يحتوي القرص الصلب بداخله على مجموع البيانات الرقمية ذات الطابع الثنائي والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (0-1) وتتم عملية فحص القرص الصلب إما كليا أو جزئيا ، فالفحص الجزئي يؤدي إلى التعرف على محتوى البيانات والتي يؤدي التعامل معها إلى الكشف عن القيمة الإسترادادية للبيانات المخزنة فيه سواء كانت محتويات المكتوبة ، صور أو أصوات....إلخ.

بالإضافة إلى إمكانية معرفة ما تم حذفه من بيانات وبرامج بالإستعانة ببرمجيات خاصة للقيام بذلك[1] والمثال المستخدم هنا هو حالة البحث في ملفات النسخ وهذه الأخيرة هي عبارة عن ملفات تأخذ نسخة احتياطية عن كل صفحة يتم الولوج إليها عبر الانترنت كما توجد ملفات خاصة بالتنزيل مهمتها استقبال الملفات التي يتم تحميلها على جهاز الحاسب الآلي من خارجه وعبر الانترنت فهذه الملفات مركزها القرص الصلب.

وللتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم بها ضبط الحاسوب ومهارة الشخص القائم بإستخلاص البيانات دون العبث بمحتوياتها لذلك فإنه عند ضبط جهاز الحاسب الآلي ، على المحقق أن ينتزع القرص الصلب من الجهاز الخاص به ويحافظ عليه من

[1] عمر محمد أبوبكر بن يونس ، المرجع السابق ص 17.

الارتجاج أو الاصطدام بأي شيء ، وعدم محاولة تفريغ أي بيانات متواجدة عليه وذلك تفاديا لفقد أي بيانات ، وتسليمه إلى الفني الخبير المختص الذي يقوم بتحليل النسخ التي تصدر من القرص ويعرض ما توصل إليه على المحقق.

وهنا لا بد من مراعاة شرط سلامة جهاز الحاسب الآلي الذي يعني صحة حركة القطع الصلبة فيه وذلك لتجنب الوقوع في مأزق رفض المحكمة الاعتداد بالدليل المنبثق عنه فشرط سلامة الحاسوب مطعن رئيسي على كل دليل تم الحصول عليه بحيث يجب الكشف على حركة الحاسوب بداية والإقرار بسلامته.[1]

2/ فحص البرمجيات :

يتطلب في هذه الحالة أن نميز بين الفحص الداخلي للبرمجيات والفحص الخارجي لها ، فالفحص الداخلي يتم من خلال البحث في البناء المنطقي للبرمجة مما يوحي بأن هناك جهودا تجديدية في إعداده للعمل حين إنزاله على جهاز الحاسب الآلي من خلال تتبع خطوات منطقة تعبر عن هذا الجهد.

وأكثر ما يتم البحث عنه في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار ذلك أن النسخ عبر الانترنت لا يشبه النسخ باستخدام برمجيات المعالجة فالأول نسخ عبر العالم الافتراضي والثاني يتم باستخدام مصنف متداول في العالم المادي وتفيد وسيلة النسخ في ترتيب كيفية حدوث الجريمة.

أما في حالة الفحص الخارجي والذي يتم اللجوء فيه إلى النسخ الأصلية للمقارنة بينهما وبين النسخة محل الاشتباه وكل ذلك للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة.

[1] خالد ممدوح إبراهيم ، المرجع السابق ،ص 215.

وفي كلتا الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة التي يمكن أن تؤثر في الحاسوب وتجعله محل شك تهتز معه قيمة الدليل يكون لهذا القصور أثره في عملية تقييم الدليل المستمد من البرمجيات ذاتها.

3/فحص النظام المعلوماتي :

إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب وتعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات.[1]

يمكن استرجاعها عبره تكون مخزنة في ملفات على أي شاكلة يمكن أن تكون عليها الحركة الإسترادادية ما دام موضوعها يشكل جريمة.

والحقيقة أن على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم والكم الهائل من المعلومات المخزنة فيه.

بالإضافة إلى أن عملية تخزين البيانات لا تتخذ شكلا محددا أو إنها تتنوع أساليبها والتي يصل مداها إلى حد إمكانية تخزين البيانات بشكل آمن في الحاسوب بنظام التشغيل أو بنظام إخفاء البيانات المعلوماتية بحيث لا يظهر الملف حتى في حالة البحث الآلي للحاسب عنه والذي قد يحتوي على مواد إجرامية ، وتفوت الفرصة بسب هذه التقنية على المحققين من الوصول إليه .[2]

ثانيا : فحص أنظمة الإتصال بالأنترنت :

[1] سعيداني نعيم ، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير جامعة باتنة ،2013،

[2] خالد محمود إبراهيم ، المرجع السابق.

يقصد بنظام الإتصال بالانترنت بالمفهوم الإجرائي هو تلك الإجراءات أو المراحل المتبعة حال استخدام الإتصال بالانترنت ومن أهم المسائل المثارة في صدد فحص أنظمة الإتصال بالانترنت سعيا وراء البحث عن دليل هي مسألة تحديد مكان الجريمة أو جهاز الحاسب الآلي الذي انطلق منه النشاط الإجرامي ، وذلك من خلال تتبع الحركة العكسية لمسار الإنترنت أي تتبع الحركة التراسلية للنشاط الممارس من خلال الأنترنت فالحاسوب بمجرد أن يتعرف على المسار يقوم تلقائيا بإختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات.

ويستخدم في عملية تتبع حركة مسار الانترنت نظام فحص الكتروني يطلق عليه اسم علم البصمات المعاصر وما يتم التوصل إليه بعد ذلك هو عنوان رقمي PROTOCOL ADRESSE IPLNTERNETيسمى وهو عبارة عن بروتوكول لعنونة البيانات والمواقع في شكل الانترنت وبمقتض هذا البروتوكول (IP)يتم التعرف على الكومبيوتر الموصول بشبكة الانترنت من خلال عناوين عددية حيث لكل كمبيوتر بها عنوانه الوحيد والخاص به تماما يسمىIPADRESSE وكل عنوان(IP) مكون من جزئين الأول يشكل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة ويعمل بروتوكول(IP) بشكل متزامن مع بروتوكول التحكم بالنقل وهذان البروتوكولان التحكم بالنقل(PROTOCOL TRANSMISSION CONTROL) TCP وهذان البروتوكولان TCP/IP هما من عائلة بروتوكولات الإتصال بين عدة أجهزة من الحواسيب طورت أساسا لنقل البيانات بين أنظمة(UNIX) ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الإنترنت ويرتكز البروتوكولان (TCP/IP) معا على تقنية التبديل المعلوماتي بواسطة الحزم

المعلوماتية بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلة الموصولة فيما بينها ، وحزمة المعلومات جزء أو قسم من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقم خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه وعند كل وصلة تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرها نحو الوصلات التالية الأقرب إلى جهة المقصد النهائية . ويعتبر نظام (TCP/IP) من أكثر البروتوكولات المستخدمة في شبكة الأنترنت فهو جزء أساسي منه لذلك تبرز أهمية الإستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها هذا البروتوكول في تحقيق الجرائم المعلوماتية حيث تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي من خلال الفترة الزمنية لإقتراف الجريمة.

وجدر الإشارة إلى أنه في إطار فحص نظام الإتصال بالإنترنت كمصدر يمكن من خلاله البحث عن الدليل الرقمي يتضمن أيضا لزوم فحص الخادم وهو حاسب ضخم مهمته تخفيف حركة الإتصال بالمواقع والصفحات التي تتم استضافتها على هيئة رقمية لذلك فإنه يطلق على الخادم Lieu De Stockage Numirisées de donnés.

الفرع الثاني : تعاون مزودي الخدمة مع جهات التحقيق.

لما كان الدليل الرقمي قابعا في البيئة التقنية ويتسم بخصائصها وهي خصائص تبني على أساس الطبيعة المرنة التي عليها العالم الإفتراضي ، فإن للفاعل إمكانية إزالة الدليل من على بعد باستخدام التقنية ذاتها من أجل ذلك إستلزم الأمر وضع إطار قانوني وهو نظام إلزام مزودي الخدمة بحفظ المعطيات وهذا ما

تضمنه قرار الجمعية العامة للأمم المتحدة رقم (63/55) المؤرخ في 2001/01/22 والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وذلك في الفقرة "و" من المادة الأولى منه والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الوصول إليها وهو ما أكده المشرع الجزائري بموجب المادة 10 من الفصل الرابع في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تحت عنوان " إلتزامات مقدمي الخدمات مساعدة السلطات ".

أولا : المقصود بمزودي الخدمات.

حسب المادة الأولى فقرة "ج" من اتفاقية بودابست فإن مزود الخدمة هو كل من يقوم بخدمات الإتصال أو خدمات معالجة البيانات أو خدمات التخزين البيانات وقد يكون جهة عامة أو جهة خاصة وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذي يشكلون مجموعة مغلقة.

ويعرف قانون حماية الحياة الخاصة في مجال الإتصالات الإلكترونية في الولايات المتحدة الأمريكية نوعين من مزودي الخدمة.

النوع الأول : مزود خدمة الاتصالات الإلكترونية ويقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الاتصالات الإلكترونية.

النوع الثاني : وهو مزود خدمة الحوسبة عن بعد ويقصد به كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الإلكترونية.

وقد عرفه المشرع الجزائري مزود الخدمة (مقدم الخدمة) بموجب الفقرة (د) من المادة الثانية في القانون 04/09 بأنه :

1. كل كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام الاتصالات.
2. وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

وعلى هدي ذلك فإن، المراسلة بالبريد الإلكتروني والتي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها بعد فإنها تستقر في حالة تخزين إلكتروني وتكون في هذه المرحلة النسخة من الإتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في انتظار استقبال المرسل إليه لها من مزود الخدمة ، وبمجرد استلام المرسل إليه المراسلة بالبريد الإلكتروني فإن، الإتصال يكون قد وصل إلى وجهته الأخيرة ، وهنا يكون موقف مزود الخدمة يتراوح بين أمرين إما أن يقوم بمسح تلك الرسالة أو يقوم بالاحتفاظ بها.

ثانيا : التزامات مقدمي الخدمة.

ألزم المشرع الجزائري مقدمي الخدمات بحفظة المعطيات وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين في انتظار اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره.

وما تجدر الإشارة إليه في هذا الإطار أنه ليس أي معطيات معلوماتية محل اعتبار من المشرع بل حصر المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة في المعطيات المتعلقة بحركة السير(معطيات المرور) ، وهي كما عرفها في المادة الثانية فقرة (ه) من القانون 04/09 « أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الإتصالات توضح مصدر الإتصال ، الوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ، ونوع الخدمة » وقد حصر المشرع معطيات المرور التي ألزم في المادة 11 مزودي الخدمة بحفظها في :

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

-الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال وكذا عناوين المواقع المطلع عليها.

وقد عرفت اتفاقية بودابست في مادته الأولى الفقرة "د" هذا النوع من المعطيات بأنها صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد ، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد سلك الإتصالات ومن مصدرها إلى الجهة المقصودة ، وهي بذلك تشمل طائفة من المعطيات تتمثل في مصدر الإتصال ، ووجهته المقصودة ، وقت أو زمن الإتصال ،

حجم الإتصال ومدته ونوع الخدمة المؤداة. وبما أن حفظ المعطيات إجراء وقتي وإحتراما للحق في الخصوصية فإن المشرع الجزائري وضع التزاما على مزودي خدمة بإزالة المعطيات التي يقومون بتخزينها بعد سنة [1]من تاريخ التسجيل وعلى غرار المشرع الجزائري نجد المشرع الفرنسي حرص بدوره في نطاق التخزين التلقائي للمعطيات المتعلقة بالاتصالات الإلكترونية و ذلك بموجب المادة 32 من قانون البريد والإتصالات الإلكترونية المضافة بموجب المادة 29 من القانون رقم 1062/2001 المعدلة بالمادة 20 من القانون 239/2003 المؤرخ في 2003/03/18 المتعلق بالأمن الداخلي على ضرورة مسح المعطيات المخزنة بعد الإحتفاظ بها لمدة أقصاها سنة إذا دعت مقتضيات البحث والتحقيق والمتابعة القضائية ذلك.

وقد رتب المشرع الجزائري مسؤولية إدارية وأخرى جزائية على تقاعس مزودي الخدمة عن حفظ المعطيات المذكورة لإمكانية أن يشكل هذا التقصير عرقلة للسير العادي للتحريات القضائية.

واسترشادا بما ذكر فإن مزودي خدمات الانترنت يعتبرون مصدرا لجهات البحث والتحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في نفسا الوقت بوضعها تحت تصرف هذه الجهات إذا تم طلبها.

[1] المادة 11 من القانون 04/09 «....تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.....».

المبحث الثاني : أساليب التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

منذ سنة 2006 فإن الإجراءات الجزائية تكيفت مع خاصيتي التبخر والعالمية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، فكان من أولويات المشرع الجزائري تدعيم الإجراءات الجزائية بوسائل قانونية للتحقيق من أجل جمع الأدلة الرقمية تحت شروط تجعل منها أدلة أصيلة على الصعيد القانوني :

-القانون رقم 22/06 المؤرخ في 2006/12/20 المعدل لقانون الإجراءات الجزائية الذي حوى مجموعة من الإجراءات الجديدة لمكافحة أنواع محددة من الجرائم ومنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات والجريمة المنظمة العابر للحدود .

-القانون رقم 04/09 المؤرخ في 05 / أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يحوي هذا القانون تدابير مهمة لتدعيم فعالية وسعة التحريات والتحقيقات الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

وعلاوة على الأدوات المدرجة في قانون الإجراءات الجزائية الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مثل اعتراض المراسلات ، أوجد المشرع وسائل أخرى أكثر فعالية مثل : التفتيش المعلوماتي ، حجز المعلومات ، التفتيش عن بعد ، أدرجها ضمن القانون 04/09 السالف ذكره ، إن الروح العامة لهذه القوانين الإجرائية هي السماح بوضع الأدوات المعلوماتية في متناول مختلف القائمين على مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال فبطبيعة الحال ليس هناك ما يبرر ترك هذه الأدوات في متناول مرتكبي هذه الجرائم وعليه فقد تم تقسيم هذا المبحث إلى مطلبين :

- الأول : مراقبة الإتصالات الإلكترونية.

- الثاني : تفتيش المنظومة المعلوماتية .

المطلب الأول : مراقبة الإتصالات الإلكترونية.

إن الإتصالات الالكترونية قد عرفها المشرع بأنها « أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية » المادة 02 فقرة (و) من القانون رقم 04/09 فالاتصالات الإلكترونية تشمل الإتصالات السلكية أو الخلوية (الهاتف النقال) ، الفاكس ، البريد الإلكتروني ، مواقع الدردشة على الانترنت وحتى المنتديات المختلفة وساحات الرأي والنقاش(FACEBOOK, MSN, SKYPE.....) وحتى المنتديات المختلفة وساحات الرأي والنقاش Forum on line التي تسمح بنقل وتبادل الأفكار والمعلومات.

الفرع لأول : مفهوم مراقبة الإتصالات الإلكترونية.

لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الإتصالات الإلكترونية ولكن بعض التشريعات قد عرفته مثل التشريع الأمريكي والكندي فقد عرفها المشرع الأمريكي بأنها « عملية الإستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز الكتروني أو أي جهاز آخر » المادة 2510-4 من قانون الإتصالات الفدرالي الأمريكي وطبقا لقانون الإتصالات الإلكترونية لسنة 1986 أصبح التعريف المذكور يتسع ليشمل الإتصالات الإلكترونية الأخرى.[1]

وقد وضع الفقه العديد من التعريفات لمراقبة الإتصالات الإلكترونية منها :

[1] ياسر الأمي فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجنائية ، دار المطبوعات الجامعية ، الإسكندرية ، مصر ، الطبعة الأولى 2009 ، ص 138.

1. ذهب رأي إلى تعريف المراقبة الإلكترونية بأنها تعتمد الإنصات والتسجيل ومحلها المحادثات الخاصة سواء أكانت مباشرة أو غير مباشرة أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الإتصال السلكية واللاسلكية .

2. ورأي آخر ذهب إلى أن المراقبة هي نوع خاص من استراق السمع يسلط على الأحاديث الشخصية والمحادثات التليفونية خلسة دون علم صاحبها بواسطة أجهزة الكترونية ، أسفر عنها النشاط العلمي الحديث فهو ينص على أي حديث شخصي يكون للإنسان مع غيره ، ويكون له صفة شخصية كما ينص على المكالمات التلفونية ليشمل المكالمات اللاسلكية أيضا ويتم هذا الإجراء بغض الحصول على دليل غير مادي يحتج به في مجال الدعاوى والتحقيقات ويخلص هذا الرأي إلى أننا لا نكون بصدد مراقبة إلا إذا توافرت الشروط الآتية :

-إستراق السمع وهو يقع على الأحاديث الشخصية والمكالمات السلكية واللاسلكية التي يجريها الأفراد.

- أن يتم استراق السمع خفية دون علم صاحب الحديث ، وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة التي أسفر عنها النشاط العلمي المعاصر.

- أن يكون إستراق السمع لهذه الأحاديث بغرض تقديم دليل يصلح للإثبات في الدعاوى والتحقيقات.[1]

[1] أحمد محمد حسان ، نحو نظرية عامة لحماية الحق في الحياة الخاصة ، دار النهضة العربية ، 2001 ، ص141.

3. ويمكن تعريف المراقبة بأنها إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاص تأمر به السلطة القضائية في الشكل المحدد قانون بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعا ويتضمن من ناحية استراق السمع إلى الحديث ، ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك.[1]

4. ومراقبة الإتصالات الإلكترونية هو إجراء خاص يتم بإشراف قضائي بحسب الحالات ، وتعرف بأنها تقنية تقوم على تدخل وسطي لتحويل مسار في خط مشترك بوسيلة ممغنطة ، من أجل التسجيل والمحادثة ، وهي تمثل فائدة أكيدة لفاعلية المتابعات الجزائية.

وقد تبنى المشرع الجزائري مراقبة الاتصالات الإلكترونية كإجراء خاص لعمليات الوقاية من جرائم محددة هي : الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو كإجراء تقتضيه التحريات والتحقيقات القضائية (المادة 4 . أ من قانون 09/ 04).

وهذا إجراء ليس جديدا على المنظومة القانونية الإجرائية الجزائية ، فقد نص عليها المشرع قبلا في قانون الإجراءات الجزائية في النص المتعلق بإعتراض المراسلات وتسجيل الأصوات والتقاط الصور (المواد من 65 مكرر 05 إلى غاية المادة 65 مكرر 10 من ق.إ.ج) ولكنه إقتصر تطبيق أحكام هذه المواد على مجموعة من الجرائم وهي جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية ، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، وهي هنا محددة على سبيل الحصر وبالتالي لا يمكن اعتراض مراسلات في إطار تحريات الشرطة القضائية أو تحقيقات قضائية في جرائم غير تلك المذكورة في

[1] ياسر الأمير فاروق ، المرجع السابق ، ص 141.

المادة 65 مكرر 5 من ق.إ.ج وعليه بالنص على مراقبة الإتصالات الإلكترونية في القانون 04/09 فإن المشرع قد أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني لإستكمال التحريات أو التحقيقات حتى في جرائم تقليدية إن صح قول ذلك ومثال ذلك : جريمة الزنا المنصوص عليها في المادة 339 من قانون العقوبات بحيث يمكن إثباتها حتى برسالة إلكترونية في بريد المتهم الإلكتروني كإثبات تقبله المحكمة.

الفرع الثاني : حالات اللجوء إلى المراقبة الإلكترونية.

نص القانون رقم 04/09 المؤرخ في 2009/08/05 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 03 منه على ما يلي :

« مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات ، والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجرائية الجزائية وفي هذا القانون وضع ترتيبات تقنية مراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية ».[1]

ومن الواضح أن مراقبة الإتصالات حدها القانون على سبيل الاستثناء وفي حالات محددة حصريا في المادة 04 من القانون المشار له وهي :

[1] الأستاذ : زيجة زيدان ، المرجع السابق ، ص127.

أ. الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة (المادة 4 من القانون 04/09) : المراقبة الوقائية كمبدأ عام لا تطبق على متابعة قضائية لجريمة مرتبكة ولكن تخص كشف خطر أو تهديد لأمن الدولة.

وعليه فإن هذه الجرائم لم ترتكب ولكن المشرع سمح في إطار الوقاية من هذه الجرائم بإجراء عمليات المراقبة للاتصالات الإلكترونية للأشخاص أو مجموعات يحتمل تورطهم مستقبلا بالقيام بالأفعال الموصوفة جرائم إرهاب أو تخريب أو الجرائم الماسة بأمن الدولة ، والاحتمال هنا ليس لدرجة توافر دلائل قوية تربط هؤلاء الأشخاص بارتكاب تلك الأفعال ، وإنما مجرد الشكوك ولو بسيطة ، فالوقاية لا تفترض القيام بأعمال تحضيرية لارتكاب هذه الأفعال ، وإنما مجرد تكهنات أو حتى دلائل بسيطة قد توحي بأن هؤلاء الأشخاص يمكنهم ارتكاب تلك الأفعال .

غير ، هذا الإجراء لا يمنح إلا بشروط خاصة حددها المشرع بنص المادة 4 فقرة 3 من لقانون 04/09 ولقد شدد المشرع في الفقرة الأخيرة من المادة 4 بأن الترتيبات التقنية الموضوعة لمراقبة الإتصالات الإلكترونية في هذه الحالة هي موجهة حصرا لتجميع وتسجيل المعطيات ذات صلة بالوقاية من تلك الأفعال ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

ب. في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني واحتمال اكتشاف جريمة قبل وقوعها وخاص بنوعية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو احتمال ضئيل فما يعرف عن الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال أنها صعبة الاكتشاف ولا يتم اكتشافها أحيانا إلا مصادفة فيكف عن ها الاحتمال الوارد في نص المادة 4 فقرة ب من القانون 04/09 وإن كان هذا الأمر يدخل أيضا في إطار الوقاية من هذه الجرائم .

ج. لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى مراقبة الاتصالات الإلكترونية .

د. في إطار تنفيذ المساعدة القضائية الدولية المتبادلة كما هو منصوص عليه في المواد 16،17، 18 من القانون 04/09.

المطلب الثاني : تفتيش المنظومة المعلوماتية .

يقصد بالتفتيش التقصي والبحث عن الأدلة سعيا وراء ضبطها ، يقصد الإستعانة القانونية بها لإدانة المتهم وبالتالي ينبغي القيام بضبط ما يترتب عليه التفتيش وتحريزه بطريقة عليمة حتى لا يفقد قيمته القانونية حال تفقده أمام القضاء إذا تطلب الأمر ذلك.[1]

فقد نصت المادة 5 فقرة 1 من قانون 04/09 « يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى :

-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

-منظومة تخزين معلوماتية.

[1] مبروك نصر الدين ، محاضرات في الإثبات الجنائي ، الجزء الأول (النظرية العامة للإثبات الجنائي) ، دار هومة ، الجزائر ، 2007 ، ص 337.

أما بالنسبة للمنظومة المعلوماتية فقد عرفها المشرع في المادة 02 (ب) بأنها « أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين ».[1]

الفرع الأول :حالات اللجوء إلى تفتيش النظم المعلوماتية.

أولا : حالات تفتيش النظم المعلوماتية.

بحسب نص المادة 05 من قانون 04/09 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته ، فإن حالات اللجوء إلى تفتيش النظم المعلوماتية هي نفسها الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية للإتصالات وهما الحالتين المتعلقتين بالوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة ، وكذلك حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني ، فالتفتيش هنا وخلافا للتفتيش التقليدي عن الأدلة التي تثبت وقوع الجريمة ونسبتها إلى المتهم إنما هي حالة إجراء تفتيش وقائي قد تسفر عنه أدلة يمكن أن تكون إثبات لتخطيط مسبق يراد به إرتكاب جرائم ذات خطورة على الأمن الداخلي للدولة وكما نعلم فإن الأحكام العامة للتفتيش تقضي بأنه « الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة

[1] أوضحت المذكرة التفسيرية لاتفاقية بودابست إن المقصود بالنظام المعلوماتي هو جهاز يتكون من مكونات مادية MATERIEL (WORD . HARD) ومكونا منطقية LOGICIEL (SOFTWARE) وذلك بغرض المعالجة الآلية للبيانات الرقمية.

جناية أو جنحة واقعة بالفعل وترجع نسبتها إلى متهم معين وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية ».[1]

وبناء على ذلك فإن سبب التفتيش في الجرائم التقليدية بوصفه من إجراءات التحقيق هو :

1. وقوع جناية أو جنحة.

2. اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها.

3. توافر إمارات قوية أو دلائل على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره.

هذه القواعد لا يمكن أن تكون سبب لتفتيش نظم المعلوماتية لأنه طبقا لنص المادة 05 فقرة 01 من قانون 04/09 أجازت التفتيش يقصد الوقاية من جرائم حددها المشرع لم ترتكب ولكن تعد أسلوبا وقائيا فقط ، وهو ما يعد إعتداء فعلي على الحياة الخاصة للأشخاص لأن القانون لم يحدد صفات من يقع عليهم هذا التفتيش هل هم مجرمون سابقون أم أشخاص لهم علاقة بمجرمين ارتكبوا هذه الأفعال ، وقد أسال هذا الموضوع الحبر في كثير من الدول خاصة منها الأوربية ، فالكثير مننها (ألمانيا ، سويسرا) منعت اللجوء إلى أسلوب التفتيش الوقائي لأنه يعد اعتداء فعليا على الحياة الخاصة للأفراد التي كفلها الدستور ، ولا يمكن اللجوء إليه إلا في حالة الوقوع الفعلي للجريمة .

والحالتين الأخريين هما :

- حالة اللجوء إلى تفتيش نظم المعلوماتية لمقتضيات التحريات والتحقيقات فقد تعطي نتيجة تهم الأبحاث الجارية دون اللجوء إلى تفتيش هذه المنظومة المعلوماتي .

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق ، ص 396.

- وأخيرا حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ثانيا : إجراءات تفتيش نظم المعلوماتية.

إذن التفتيش :

لم ينص المشرع في المادة 05 من قانون 04/09 صراحة على وجوب استصدار إذن بتفتيش نظم المعلوماتية من طرف ضباط الشرطة القضائية في حالة التحريات المتعلقة بالجرائم المتلبس بها أو في حالة التحريات كما هو الحال بالنسبة كمراقبة الإتصالات الإلكترونية حيث أن المشرع نص صراحة على منح الإذن لضباط الشرطة القضائية يسمح لهم بتنفيذ هذا الإجراء ولكن بالرجوع إلى الفقرة 05 التي نصت على أنه « يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية... » فقد نصت أن قيام ضباط الشرطة القضائية لتفتيش نظم المعلوماتية يكون بناء على قواعد قانون الإجراءات الجزائية التي تفرض على ضابط الشرطة القضائية عند انتقاله إلى مساكن الأشخاص الذين يظهر ، أهم ساهموا في الجناية أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش لا يكون إلى بإذن مكتوب صادر من وكيل الجمهورية و قاضي التحقيق مع وجوب الاستظهار بها لأمر قبل الدخول إلى المنزل والشروع في التفتيش ويكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها (المادة 44 ، ق. إ.ج)كذلك نص المادة 64 ق.إ.ج التي تحيل أحكام المواد من 44 إلى 47 من ق.إ.ج فيما يخص التحريات الأولى التي يجريها ضباط الشرطة القضائية كما أن الدستور نص على وجوب أن يتم التفتيش بأمر مكتوب صادر عن السلطات القضائية المختصة (المادة 40 من دستور 1996).

وعليه فإن تفتيش النظم المعلوماتية تعرف نفس الحماية ونفس الحدود المادية والجغرافية كالتي تطبق في العالم المادي الملموس لباقي الجرائم.

التفتيش عن بعد :

قضت المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بمكافحة جرائم تكنولوجيات الإعلام والإتصال على « إمكانية الدخول بغرض التفتيش إلى منظومة معلوماتية ولو عن بعد ».حيث أجاز المشرع الجزائري القيام بتفتيش.

المنظومة المعلوماتية عن بعد ويقتضي ذلك الدخول إليها دون إذن صاحبها والولوج إلى الكيان المنطقي للحاسوب فالتفتيش هنا يستهدف أشياء معنوية وفنية وليست مادية كالبرامج وقواعد البيانات ولأنه هذه قد تكون وسيلة لارتكاب جريمة أو تخزين معلومات بشأنها لا سميا إذا كان هذه المعلومة غير مرتبطة بعد بأية دعامة مادية وإن كان المشرع الجزائري قد أجاز إفراغ أو نسخ تلك المعلومات المشكوك فيها أو التي من شانها الإفادة في الكشف عن الجريمة أو مرتكبيها والمنسوبة على دعامة تخزين الكترونية قابلة للحجز .

ج. التسخير :

(المادة 05 فقرة 04 من قانون 04/09 والمادة 49 من ق.إ.ج) من أجل جمع عناصر الدليل الرقمي فإن القضاة (وكيل الجمهوري ، قاضي التحقيق بحسب الحالة يمكنهم اللجوء لمختلف التصرفات وأساليب التحقيق ومن ذلك التسخير.

التسخير عبارة عن إجراء من طرف قاضي أو ضابط شرطة قضائية يفوض فيه شخص لتقديم عمل لا يمكنه القيام بنفسه لنقص الوسائل أو لانعدام الإختصاص التقني الضروري.

1. في الجنايات والجنح المتلبس بها :

لضابط الشرطة القضائية إن اقتضى الأمر ذلك إن يستعين بأشخاص مؤهلين لإجراء معاينات لا يمكن تأخيرها (المادة 49 ق.إ.ج) وهو حكم عام في قانون الإجراءات الجزائية وهذا لمساعدته في الكشف عن الأدلة والمحافظة عليها ولا يأتي ذلك إلا بالإستعانة بأهل الخبرة والمعرفة التقنية.

2. التحريات الأولية والتحقيق القضائي :

بناء على نص المادة 05 فقرة 04 من قانون 09/04 « يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بإتخاذ التدابير اللازمة لحماية المعطيات المعلوماتية التي تتضمنها » فالتسخير يتم من طرف السلطات المكلفة بالتفتيش : ضابط الشرطة القضائية بإذن من قاضي التحقيق أو وكيل الجمهورية ، الأشخاص سواء من القطاع العام أو الخاص لهم إطلاع كافي بتكنولوجيات الإعلام والإتصال ، وقد حدد المشرع هذا الإطلاع على النحو التالي:

-دراية المسخر بعمل المنظومة المعلوماتية.

-دراية المسخر بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها المنظومة المعلوماتية.

-وهدف التسخير مساعدة السلطات التفتيش في عملها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

الفرع الثاني : حجز المعطيات المعلوماتي .

1. تعريف حجز (ضبط) الدليل الإلكتروني .

يقصد بالضبط هنا ضبط الأشياء لأنها من إجراءات جمع الأدلة ، وهو جائز سواء كان الشيء مملوك للمتهم أو لغيره من الأشخاص ، وتنظم الضبط (الحجز) قواعد قانون الإجراءات الجزائية من حيث التحديد من يقع عليه الضبط ومن يقوم بالضبط ويمكن تعريف الضبط بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة ، والضبط هو الغاية من التفتيش ونتيجة المباشرة المستهدفة ، ولذلك يتعين عند إجرائه إن تتوافر فيه نفس القواعد التي تنطبق بشأن التفتيش ، يؤدي بطلان التفتيش إلى بطلان الضبط.[1]

ويترتب على هذا الارتباط بين التفتيش والضبط ، أن الضبط لا يجوز أن يقع على شيء إلا وصفه دليلا من أدلة الجريمة التي تجري التفتيش بشأنها ولذلك فإن يباشر من أجل الحقيقة المطلقة ، بمعنى أنه ما دام التفتيش يستهدف ذات فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة لأنه ما يضبط في الحاليتين تحقق العدالة الجنائية ، لذلك يقول فوستنان هيلي :

[1] محمد سعيد تمور ، أصول الإجراءات الجزائية (شرح لقانون أصول المحاكمات الجزائية) ، دار الثقافة للنشر والتوزيع ،عمان الأردن ، الطبعة الأولى ، 2005 ، ص 359.

« إنه لما كان التفتيش يباشر للكشف عن الحقيقة ، سواء كان في إدانة المتهم أو براءته فإن ينبغي ألا يقتصر الضبط على الأشياء التي تؤدي إلى إدانة المتهم دون غيرها بل إنه يتعين أن ينصب أيضا على الأشياء التي تفيد الحقيقة أيا كانت وإن أدت إلى تبرئة المتهم ».[1]

ومالا يلاحظ بالنسبة لضبط الأدلة الرقمية في قانون 04/09 هو استعمال المصطلح مغاير لما اعتاد عليه في قانون الإجراءات الجزائية ، فاستبدل مصطلح الضبط بمصطلح الحجز ، أي حجز الأدلة الرقمية.

2. إجراءات حجز المعطيات المعلوماتية.

يمكن لضباط الشرطة القضائية حجز كل الأشياء والوثائق التي استعملت في الجريمة أو شكلت نتيجة لها ، عندما تكون هذه المضبوطات ضرورية لكشف الحقيقية.[2]

إن الدعائم الرقمية (الإلكترونية) مثل الأقراص المضغوطة ، مفاتيح USB الهواتف النقالة يمكن وضعها في أحراز حسب قانون الإجراءات الجزائية .

ومن المناسب كنتيجة تنسيق إجراءات حجز واستغلال المعطيات المعلوماتية قصد جعلها مفهومة وقابلة لإدراك من طرف الأشخاص الذين ستظهر عليهم كدليل كما أنه من الضروري توضيح أساليب جمع الأدلة الرقمية والحفاظ على سلامتها كذلك مع وجوب حماية هذا الإجراء (حجز الدليل) على الشبكة المعلوماتية ، كمثال بروتوكولات نموذجية لجمع الأدلة الرقمية تسمح بحماية الإجراءات وذلك بتقليص خطر إبطالها إجرائيا.

أساليب حجز المعطيات المعلوماتية :

[1] فوستنان هيلي ، الجزء الثالث ، فقرة 1275 ، ص 499 ، منقول عن مصطفى محمد موسى ، المرجع السابق ، ص 209.

[2] المادة 42 فقرة 03 ، ق.إ.ج (حالة التلبس) ، المادة 81 ،ق.إ.ج (التحقيق القضائي).

لقد إعتمد المشرع في حجز المعطيات المجرمة على أسلوبين متمثلين في نسخ المعطيات أوحجبها (تجميدها)

أ. نسخ المعطيات الرقمية .

إن المعطيات الرقمية المعلوماتية المجمعة يمكن نسخها على جميع دعائم التخزين وهذا الذي يناسب تسمية الحجز المعلوماتي الذي هو غير متعارض مع الضبط المادي التقليدي لدعائم التخزين المعلوماتي المستخرجة من نفس مكان التفتيش بدل حجز القطع الصلبة التي تتضمن المواد الممنوعة فيتم مثلا نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها ، أو نسخ البيانات التي يتم وضعها في إطار برمجية تحوي قنبلة زمنية موقوتة وهنا نجد أسلوب النسخ يصلح تماما أن ينتج عنه دليل رقمي مقبول أمام القضاء[1] وهذا ما نصت عليه المادة 06 من قانون 04/09 بقولها : « عند ما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها وأنه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز».

وأخيرا في نص المادة 06 فقرة 03 من قانون 04/09 أجاز المشرع استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات المبحوث عنها من أجل جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

ب.الحجز عن طريق منع الوصول على المعطيات.

[1] فتحي محمد أنور عزت ، المرجع السابق ، ص 636.

أوجب المشرع على السلطة التي تقوم بالتفتيش ، استعمال التقنيات المناسبة لـ :

- منع الوصول إلى المعطيات التي تحويها المنظومة المعلوماتية.

- منع نسخ تلك المعطيات.

وما نلحظه بالنسبة لهذه المادة هو كيف يمكن لضباط الشرطة القضائية تقديم الدليل الإلكتروني أمام القضاء ، إذا ما استحال فتحه ، وهذا ما لم تجيب عليه المادة 07 من قانون 04/09.

المعطيات المحجوزة ذات المحتوى المجرم.

سمحت المادة 08 من قانون 04/09 « للسلطات التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة » وكمثال على ذلك حجب المواقع التي تحوي مثال شعارات تمس برموز الدولة.

أما بالنسبة للقانون المقارن نجد أن المشرع الفرنسي منح لوكيل الجمهورية ولقاضي التحقيق حسب الحالة بإعطاء أوامر للقيام بحذف المعطيات نهائيا من الدعائم التي تم نسخها ، والتي المعطيات المعلوماتية في حال استعمالها أو حيازتها تكون مجرمة أو تشكل خطر على أمن الأشخاص أو الممتلكات ، مثال ذلك ، الصور الخاصة بالاعتداءات الجنسية على القصر.

في حالة الحجز الذي بتم بحضور شخص شهد التفتيش طبق لمواد قانون الإجراءات الجزائية ، فإن تحليل المعطيات لا يستوجب أن يكون بحضوره .

الخاتمة

الخاتمة :

إن إصدار المشرع الجزائري لقانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها ليكون بذلك أرسى قواعد إجرائية جديدة للكشف عن الجرائم المعلوماتية ومعاقبة مرتكبيها فقد شملت مواده الكثير من الآليات المستحدثة والمتمثلة في :

1. نصه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها وإن لم يتم تنصيبها لحد الساعة.
2. كذلك بالنسبة للقواعد المتعلقة بالإختصاص الإقليمي للقانون الجزائري حيث تم التوسع في الإختصاص الإقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني نظرا لما يمكن لهذه التكنولوجيات الحديثة من القيام به في حالة استغلالها ضد مصالح الدولة ولو في أقاليم دول أخرى من طرف جزائريين أو جانب ، أيضا فإن عالمية إستغلال تكنولوجيات الإعلام والإتصال وخاصة الأنترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من إختصاص القانون الجزائي لأكثر من دولة مما قد ينجر عنه تنازع في الإختصاص ، مما قد ينشأ للمجرمين أماكن لا قانون فيها فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعالا جدا ولا يتأتى ذلك إلا باستعمال الطرق الحديثة للتواصل ما بين السلطات القضائية دون المرور بالطرق الدبلوماسية المعقدة وهو ما تم تشريعه فعلا ضمن هذا القانون.

3. كذلك الأمر بالنسبة لتنسيق القوانين الجزائية العالمية سيؤدي بالتأكيد لإحكام قبضة العدالة على المجرمين في أي دولة يكون فيها.

4. أيضا فإن لطرق التحري في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ميزاتها والتي تبناها المشرع في القانون 04/09 فالمراقبة الإلكترونية للإتصالات وتفتيش النظم المعلوماتية أعطى لها القانون صفة الشرعية القانونية بتقنينها وإدخالها ضمن الترسانة الإجرائية الجزائية في القانون الجزائري ، تسمح للمتحرين عن الجرائم والمحققين فيها فسحة قانونية لتقديم الأدلة اللازمة لإدانة المتهم أو تبرئته.

5. كما يلعب مقدمو الخدمات بما لديهم من تقينا متماشية مع تطور التكنولوجيات الحديثة للإعلام والإتصال دورا مهما في مكافحة هذا النوع من الإجرام وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن الجرائم المرتكبة بواسطة أو ضد هذه التكنولوجيات أيضا الإلتزام بما قرره المشرع بحفظ للمعطيات المعلوماتية يسمح للمتحرين تتبع الجريمة وحركة المجرمين وبالرغم من جهود المشرع لوضع قواعد إجرائية تتماشى والجرائم المعلوماتية إلا أن هناك بعض الملاحظات التي سجلناها عبر دراستنا تتمثل في النقاط التالية :

1. إن تنصيب هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الواردة في القانون 04/09 أمر مهم يجب على السلطات المعنية الإسراع في تجسيده على أرض الواقع للتصدي لهذا النوع من الإجرام ومكافحتة وكذلك تقديم المساعدة للسلطات القضائية في التحقيقات الجارية حول هذه الجرائم .

2. تعد مراقبة الإتصالات الإلكترونية وتفتيش النظم المعلوماتية من أهم وأخطر الإجراءات التي جاء بها قانون 04/09 فهذين الإجراءين خلفا صراعا كبيرا في كثير من الدول الأوروبية فسويسرا وألمانيا مثلا لم تسمحا بالقيام بالمراقبة الإلكترونية والتفتيش في المنظومة المعلوماتية إلا إذا وقعت الجريمة فعلا ، وليس كتدبير وقائي من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ، وهذا لأن هذين الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد فكان جديرا بالمشرع وضع قيود قانونية لتبرير اللجوء هذين الإجراءين كما هو الحال بالنسبة للحالة (أ) من المادة 04 من القانون 04/09.

3. لاحظنا كذلك بالنسبة لإلتزامات مقدمي الخدمات بأنواعهم أن المشرع ألزمهم في المادة 12 من القانون 04/09 بسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها وجعل الدخول إليها غير ممكن ولم يدرج المشرع أي مسؤولية على عاتقهم في حالة إمتناعهم عن القيام بهذا الإلتزام على عكس نظيره المشرع الفرنسي لهذا كان جديرا بالمشرع إدراج عقوبات جزائية على مقدمي الخدمات المقصرين في أداء واجبهم القانوني.

4. عدم الإقتصار عند التجريم والعقاب على أنماط السلوك المحظور حاليا بل يجب مراعاة الأبعاد المستقبلية لأن تكنولوجيا المعلومات والحواسيب في تطور سريع بل يكاد يكون مذهل.

5. وأخيرا إن صدور القانون 04/09 يعد تحديا فعليا للسلطات القضائية وأعوانها من أجل تطبيقه نظرا لخصوصية الإجراءات التي جاء بها ، فيكون لزاما عليها أن تساير التقدم التكنولوجي الحاصل على مستوى الإعلام والإتصال من تكوين جيد يسمح بفهم وتطبيق هذه التقنيات حتى تكون

عمليات البحث والتحري أكثر فاعلية وكذلك الحكم القضائي في الدعاوى الجزائرية المتعلقة بهذه الجرائم مبنيان على فهم جيد للوقائع خاصة إذا كانت مرتبطة بجرائم تقنية بحتة.

قائمة المصادر والمراجع.

المراجع :

1.أحسن بوسقيعة "الوجيز في القانون الجزائي العام " دار هومة ، الجزائر ، الطبعة الخامسة 2007.

2.أحمد محمد حسان ، نحو نظرية عامة لحماية الحق في الحياة الخاصة ، دار النهضة العربية ،2001 .

3.الأستاذ : زيجة زيدان ، الجريمة المعلوماتية في التشريع الجزائري والدولي ، دار الهدى للطباعة والنشر ، الطبعة الأولى ، سنة 2011 .

4.آمال قادة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة ، الطبعة الثالثة، 2007، الجزائر .

5.جميل عبد الباقي الصغير الانترنت والقانون الجنائي الأحكام الموضوعية للجرائم المتعلقة بالانترنت ، دار النهضة العربية القاهرة ، طبعة 2001.

6.حسن عبيد "الجريمة الدولية " دراسة تحليلية وتطبيقية ، دار النهضة العربية سنة 1990 .

7.حسين بن سعيد الفاغري ،« الجدول الدولية في مواجهة جرائم الإنترنت » 2007.

8.خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية ، دار الفكر الجامعي، الطبعة الأولى 2009 .

9.د.حاتم حسين بكار « أصول الإجراءات الجنائية وفق أحدث التعديلات التشريعية والاجتهادات الفقهية والقضائية » منشأة المعارف بالإسكندرية مصر 2007 .

10. الدكتور : عياشي بوزيان ، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الإقتصادية وآليات مكافحتها ، مجلة الدراسات ، العدد الرابع ، ديسمبر 2016 ، ص 160 ، 161.

11. الدكتور طارق إبراهيم الدسوقي عطية ، النظام القانوني للحماية المعلوماتية " دار الجامعة الجديدة للنشر ، الإسكندرية ، 2009 .

12. الدكتور عياشي بوزيان ، مجلة الدراسات الحقوقية ، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية ودافعها في الجزائر ، العدد الرابع ، ديسمبر 2015.

13. الدكتور عياشي بوزيان ، مجلة الدراسات الحقوقية مكتبة الرشاد للطباعة والنشر ، الجزائر العدد الرابع طبعة 2015 .

14. الدكتورة هدى قشقوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، الطبعة الأولى ، دار النهضة العربية ، القاهرة ، 1992 .

15. سلطان محيا الريحاني « الجرائم المعلوماتية » بحث منشور على الموقع.

16. طارق إبراهيم الدسوقي عطية ، النظام القانوني للحماية المعلوماتية ، دار الجامعة الإسكندرية ، مصر ، 2009 .

17. طارق محمد الجملي ، « الدليل الرقمي في الإثبات الجنائي »ورقة عمل مقدمة من للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة 28 - 2009/10/29 المرجع السابق.

18. عبد الفتاح بيومي حجازي ، الجرائم المستحدثة في نطاق تكنولوجيا الإتصالات الحديثة للطبعة الأولى 2009 دار النهضة القاهرة .

19. عبد الفتاح بيومي حجازي الإثبات الجنائي في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية، مصر 2007 .

20. عبد القادر القهوجي ، الحماية الجنائية لبرنامج الحاسوب الآلي ، الدار الجامعية للطباعة والنشر بيروت ، 1999.

21. عبد الله ، عبد الكريم عبد الله ، جرائم المعلوماتية والانترنيت (الجرائم الإلكترونية) ، منشورات الحلبي القانونية ، ط 1، بيروت 2007 .

22. عمار بوضياف ، النظام القضائي الجزائري ، دار ريحانة طبعة 2003 .

23. عمر محمد يونس ،« مذكرات في الإثبات الجنائي عبر الانترنت » ندوة الدليل الرقمي بجامعة الدول العربية ، 2006.

24. فتحي محمد أنور عزت ، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية ، دار الفكر والقانون ، مصر ، طبعة ، 2010 .

25. فوستنان هيلي ، الجزء الثالث ، فقرة 1275 ، منقول عن مصطفى محمد موسى ، المرجع السابق .

26. مبروك نصر الدين ، حاضرات في الإثبات الجنائي ، الجزء الأول (النظرية العامة للإثبات الجنائي) ، دار هومة ، الجزائر ، 2007 .

27. محمد أمين الشوابكة، جرائم الحاسوب والأنترنت ، الجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، ط 1، 2007.

28. محمد حامد الهيتي ، التكنولوجيا الحديثة والقانون الجنائي ، طبعة الأولى ، دار الثقافة للنشور والتوزيع ، عمان ، 2004 .

29. محمد سامي الشواء ، ثورة المعلوماتية وانعكاساتها على قانون العقوبات ،الطبعة الثانية ، دار النهضة العربية القاهرة ، 1998، .

30. محمد سعيد تمور ، أصول الإجراءات الجزائية (شرح لقانون أصول المحاكمات الجزائية) ، دار الثقافة للنشر والتوزيع ،عمان الأردن ، الطبعة الأولى ، 2005 .

31. محمد فواز محمد مطالقة ،آليات الوفاء بالبدل المالي عن طريق الإنترنيت ، مقال منشور بالدليل الإلكتروني.

32. ممدوح عبد الحميد عبد المطلب « البحث والتحقيق الجنائي الرمي في جرائم الحاسب الآلي والانترنت » دار الفكر القانوني ، مصر ، 2006 .

33. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، الطبعة لأولى ، 2008 .

34. هدى حامد قشوش ، جرائم الحاسب الإلكتروني في التشريع المقارن ، ط1 ، دار النهضة العربية سنة 1992.

35. هشام فريد رستم ، مخاطر تقنية المعلومات ، مكتبة الآلات الحديثة الطبعة الأولى 1994 .

36. هلا عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، الطبعة لأولى ، 2008 .

37. ياسر الأمي فاروق ، مراقبة الأحاديث الخاصة في الإجراءات الجنائية ، دار المطبوعات الجامعية ن الإسكندرية ، مصر ، الطبعة الأولى 2009 .

النصوص القانونية :

- القانون 04/09 المؤرخ في 05 أغسطس 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.
- المرسوم الرئاسي رقم 261/15 المؤرخ في 08 أكتوبر 2015 المتضمن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام والإتصال ومكافحتها.
- الأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو سنة 1966 يتضمن قانون العقوبات المعدل والمتمم بآخر تحيين بالقانون رقم 01/14 المؤرخ في 04 فبراير سنة 2014.
- الأمر رقم 66- 156 المؤرخ في 18 صفر عام 1386 الموافق لـ 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم حسب آخر تعديل له الأمر رقم 11-02 المؤرخ في 23 فبراير سنة 2011.
- دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر في 28 نوفمبر 1996 ، الجريدة الرسمية رقم 76 المؤرخة في 08 ديسمبر 1996.

المذكـرات :

- سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير جامعة باتنة ، 2013.
- كوثر فرام ، الجريمة المعلوماتية على ضوء العمل القضائي المغربي ، بحث نهاية التدريب بالمعهد العالي للقضاء ، فترة 2009/2007 .
- الطالبة حاجب هيام ، الجريمة المعلوماتية ، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء ، الدفعة 16 ،2008/2005 .

الجرائـد :

- عن جريدة الشروق اليومية عدد 2362 ليوم السبت 2008/07/26.

مواقع الانترنت :

- http//www.ATSLP.com
- WWW.ARAVLAWINF.COM

الفهـــرس