جامعة زيان عاشور بالجلفة

كلية الحقوق والعلوم السياسية

قسم الحقوق

سبل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

مذكرة ضمن متطلبات نيل شهادة الماستر حقوق

تخصص إدارة ومالية

إعداد الطالبين :

- بن يحي عبد الفتاح
- كـــراك فتيحـــة

إشراف الأستاذ:

- د. بن يحي أبو بكر الصديق

لجنة المناقشة:

1-.....عمـــــران عطيـــة..... رئيسا

2- .....بن يحي أبو بكر الصديق.....مقررا

3- .....صدارة محمـــد.....مناقشا

الموسم الجامعي : 2017 / 2018

شكر وعرفان

نشكر الله عز وجل ونحمده حمدا كثيرا مباركا فيه الذي هدانا بعونه وأتممنا هذا العمل ، فلك الحمد ربي كما ينبغي جلال وجهك وعظيم سلطانك.

يتقدم الطلبة الذين سهروا على إعداد هذه المذكرة المتواضعة بالشكر والعرفان إلى الأستاذ الفاضل ، الدكتور/ بن يحي ابو بكر الصديق ، الذي كان يمد العون بكل سخاء دون أن يبخل علينا بما كان في وسعه تقديمه ، فكانت نعمة المرشد ونعمة الموجه ..... شكرا أستاذتا الفاضل دمت في خدمة الطلبة خاصة طلبة العلوم القانونية والإدارية .

كما لا يفوتنا أن نشكر كل أساتذة القسم 02 تخصص ماستر إدارة ومالية و كافة أساتذة كلية الحقوق بجامعة زيان عاشور وجميع مؤطريها وكذا جميع العاملين من رجال ونساء الذين أدو الواجب أمام الطلبة فبفضل الله ثم بفضلهم إستطعنا أن نجتاز مرحلة كان طلب العلم أول راياتها والصدق والأمانة وحب الوطن والمهنة إلى آخر دربها.

شكرا جزيلا

الإهداء

نهدي هذا العمل المتواضع إلى كل عائلاتنا المحترمة، عائلة بن يحي وكذا عائلة كراك خاصة الأم كراك بنت دريدي وبنات الأخت كراك خديجة وحليمة، والى كل الأصدقاء إضافة إلى طلبة ماستر إدارة ومالية وخاصة القسم 02 ، كما نتقدم بإهداء هذا العمل البسيط إلى كل من ساهم من بعيد أو قريب لإنجاح هاته المذكرة ونتمنى النجاح للجميع والتوفيق في العلم والعمل ومسار مهني مشرف إنشاء الله.

مقدمة

مقدمـــة

يظل التطور الهائل الذي شهده مجال تكنولوجيات الإعلام والاتصال بشكل لم يعد أحد في العالم بمنأى عن تأثيرها المباشر والمتواصل في حياة الأفراد والمجتمعات، لتشمل كل مجالات حياتنا، فبحدودها غير المتناهية أصبحت اليوم بوسائلها الرقمية عامل مؤثر على سلوكيات الأفراد والمجتمعات، ونلاحظ ما فعلته مواقع عديدة وأهمها YouTube، Facebook في التأثير على توجهات مجتمعات بأكملها، فالانترنت بعالمها الافتراضي أصبحت جزءا مؤثر على توجهات الشعوب، ويعتمد الانتصار القوي للمعلوماتية على عناصر مهمة تتمثل في تطور الحاسوب وتقدم علم الالكترونيات بسرعة وانتشاره الواسع وتعدد مهامها:

– سرعة الانتشار: لقد عمل الباحثون والعلماء في مجال تكنولوجيات الإعلام والاتصال لنحو أكثر من نصف قرن من تطور علم الإلكترونيك و تقنيات الاتصال الحديثة أدى إلى دخول العالم في عصر * ثورة المعلومات *

– إن عالمية هذه التكنولوجيات التي تبحث في كل يوم عن امتيازات تعبر الحدود عبر العالم سواء من حيث عالمية عملها وكذلك من حيث عالمية تنفيذها، فالكل يستطيع استعمالها واستغلالها.

– أما تعدد مهامها فهو الذي يطرح إشكالات تتمثل في المحافظة على الحرية الشخصية للأفراد، فبعد أن أصبح العالم قرية رقمية، يظهر جليا أن احترام الحريات الأساسية للأفراد بدأ يتضاءل إلى أن ينعدم، بسبب الانتهاكات العديدة سواء من طرف الدول أو من طرف الأشخاص للحياة الخاصة للأفراد.

فالانترنت مثلما شبهها البعض بأرض أمريكا في القرن التاسع عشرة بأنها أرض السيئ والجيد(Leonard Cohen)، فعالم الانترنت له سحر مغري ومقلق في آن واحد، فقد أصبح فجأة فن جديد للحياة، فالكل يجد فيه رغباته بدون مراعاة للعمر أو الثقافة، ولأنه

ليس هناك لعبة في الواقع بدون قاعدة ولا أفق بلا حدود، وكذلك مثل باقي النشاطات الفردية والاجتماعية لا مجتمع بدون قاضي.

وكان لزاما بسبب هذا التداخل الواسع بين العالم الافتراضي وعالمنا أن يندرج في إطار قانوني حتى لا تكون الانترنت وباقي تكنولوجيات الإعلام والاتصال مجال يزدهر فيه الإجرام ، ولا أن تقيد الحريات فيها إلى حد تختنق فيه الحرية التي تعد المحرك الحقيقي والذي هو شعار التطور الذي تؤول إليه المجتمعات بعد انتشار تكنولوجيات الإعلام والاتصال و إنشاء الحكومات الرقمية لجعل كل شيء رقمي.

ولكن التوفيق بين الواقعة والحق كما نعرفه دائما صعب، حيث منذ نصف قرن من ولادة الانترنت وأقل من 20 سنة من دخولها في بلادنا وضعت عبر دول العالم المتحضر ونحن في إثرهم ركيزة قانونية تشريعية وتنظيمية متشعبة ومتنامية والتي أوجدت بطبيعة الحال عددا متزايدا من التطبيقات والترجمات العملية والقانونية لها، فالمشرع والفقه والقضاء هم الركائز الثلاثة للقانون سخرت لعالم الانترنت، بنشاط وفاعلية يبرزان سرعة العمل المتزامن مع تنامي تكنولوجيات الاتصال والتطبيقات القانونية المرافقة لها،إنما يصطلح عليه حديثا بالقانون العقابي السيبيري(المعلوماتي) وهو المرتبط بالجرائم المرتكبة عبر الانترنت وباستعمال التكنولوجيات الحديثة للإعلام والاتصال يبرز وبشكل دائم ومتطور الأفعال والوقائع المجرمة وتعيينها بذاتها وكيفية تطبيقه، محددا بذلك تميزه وانفراده .

فموضوع دراستنا هو جانب من هذا القانون المتمثل في دراسة القواعد الإجرائية الخاصة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي تضمنها قانون 04/09 المؤرخ في 05 أوت 2009، إذ تعد هذه القواعد سبل وضعها المشرع، تسمح للمتحري عن انتهاكات قانون العقوبات التي تتم بواسطة أو ضد إحدى تكنولوجيات الإعلام والاتصال، باستعمال وسائل قانونية جديدة تتلاءم وخصوصية هذه الجرائم، إذ بدون هذه الآليات لا يمكن للمتحري أو المحقق الكشف عن مرتكبي هذه الانتهاكات وتقديمهم

للمحاكمة وعرض الأدلة التي هي في شكل الكتروني وفي عالم افتراضي لأن قواعد قانون الإجراءات الجزائية التي تعد الآن تقليدية لم تعد لتكفي وتسمح للتحري والتحقيق وضبط الأدلة الجزائية في هذا الفضاء الافتراضي المتميز بسهولة اختفاء آثاره ومحو أدلته.

إذ يوجد اختلاف جوهري في المبادئ التي تحكم آليات مكافحة هذه الجرائم، فخصائص هذه الأخيرة تفرض إيجاد قواعد إجرائية مختلفة سواء من حيث الأشخاص والهيئات التي تساهم في مكافحتها، لأنها ستكون متخصصة في هذا النوع من التكنولوجيات وبالتالي يسمح لها ذلك بمعرفة الانتهاكات القانونية التي قد تتعرض لها، كذلك فإن قواعد الاختصاص الإقليمي ستتغير لأن هذه الانتهاكات لم تعد تجري في مكان إقامة مرتكبها ولكن قد ترتكب في أماكن متعددة وفي وقت واحد ومن أشخاص مختلفون في جنسياتهم، مما يستدعي تعاون دولي لمكافحة هذا الإجرام الجديد.

أما بالنسبة لطرق الكشف عن الجريمة ووسائل إثباتها فإنها تستدعي آليات مستحدثة تتوافق وطبيعة هذه الجرائم وأساليب ارتكابها التي تتم دائما بواسطة التكنولوجيات الحديثة للإعلام والاتصال.

تهدف هذه الدراسة إلى توضيح وتحليل قانونيين لقواعد إجرائية خاصة وجديدة تحكم البحث والتحري في جرائم مستحدثة تتسم بالسرعة في التطور وتنامي في الجمهور المتأثر بها، تجعل رجال الفقه والقضاء كما المتأثرين بها(الفاعل والضحية) مكلفون بتطبيق أحكامها بالرغم مما تحويه من تغيرات وتقلبات مرتبطة بها.

كما نهدف لوضع تطبيقات عملية من خلال تجارب سابقة في الفقه والقانون المقارن تسمح بالاستفادة من تجاربهم وتطبيق أمثل للقواعد الجديدة المكرسة في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن هذا الموضوع الذي نتناوله بالدراسة يحوي نظرة تشريعية وقانونية لمكافحة جرائم جديدة لم يتناولها فقهاؤنا بالدراسة والتحليل الجديرين بها، وذلك لحداثة دخول هذه التكنولوجيات

إلينا فوسائل الإعلام والاتصال الجديدة والانترنت لم ينتشر استعمالها إلا وفقا لمخطط وطني يقضي بنشر استعمالها عبر الوطن لتكون في متناول الجميع بمن فيهم منتهكي قانون العقوبات.

وبالرغم من حداثة هذه التكنولوجيات إلا أن آثارها امتدت إلى كل مناحي حياة الأفراد والمجتمعات، فكان لزاما أن نواكب عمل المشرع بالتوضيح والتحليل لتغطية الفراغ الفقهي وكذلك نقص التطبيقات القضائية لهذا القانون بالرغم من الانتهاكات العديدة التي تصحب هذه التكنولوجيات في واقعنا.

وما نلحظه في الدراسات المماثلة هو أنها تتناول الجانب الموضعي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أي أنها تعرف بهذه الجرائم وتبين أنواعها، أما بالنسبة لآليات مكافحتها فليس هناك دراسة مماثلة سواء في الفقه الجزائري أو في الفقه المقارن في الدول العربية، وسبب ذلك هو عدم تبني أكثر الدول العربية والكثير من الدول النامية لهذا النوع من التشريعات الحديثة، وأما بالنسبة للقانون 04/09 المؤرخ في 2009/08/05 فهو قانون إجرائي حديث بالنسبة للمنظومة التشريعية في الجزائر ولم يتناوله الفقهاء عندنا بالدراسة، لهذا كانت الدراسة مستحيلة بمراجعنا وما كان علينا إلا الاستعانة بالمراجع الأجنبية في فرنسا تحديدا لسبقها في تناول الموضوع سواء من قبل المشرع بإصداره العديد من القوانين المتعلقة بهذا الموضوع أو الاجتهادات القضائية المختلفة وعمل أساتذة القانون، فكانت هناك دراسات عديدة سواء كتب قانونية، أو مقالات علمية منشورة في جرائد متخصصة في القانون بالإضافة إلى المواقع المختلفة في الانترنت التي تناولت نقاطا مختلفة في دراستنا، ولأن المشرع الجزائري قد استوحى جانب كبير من مواد القانون 04/09 من اتفاقية بودابست لسنة 2001، المتعلقة بالإجرام المعلوماتي (Convention sur la cybercriminalité) المتضمنة توصيات حول تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسوب، و كذلك توصيات حول كيفيات تفتيش وحجز المعطيات المجرمة داخل منظومة معلوماتية، بالإضافة

لسماح الاتفاقية بإعداد نظم مراقبة للاتصالات المختلفة سواء عبر الانترنت أو عبر الهاتف الأرضي والنقال، واحتوت الاتفاقية نصوصا حول تجريم وعقاب الانتهاكات المتصلة بتكنولوجيات الإعلام والاتصال، هذه الاتفاقية كانت مصدرا مهما للمشرع الجزائري للتشريع العقابي بجانبيه الموضوعي والإجرائي، لهذا كان الاعتماد على ما تم دراسته في القانون المقارن تسهيلا للدراسة والبحث في القانون 04/09.

واعتمادا على ما سبق طرحه يمكن أن نلخص وبشكل أساسي محاور دراستنا لتكون إجابة على إشكالية هذا البحث المتمثلة في:

– كيف تم تنظيم آليات وسبل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في القانون 04/09؟

ويتبع هذا التساؤل مجوعة من الأسئلة يمكن طرحها وهي:

– كيف يمكن لنواب العامون ووكلاء الجمهورية و ضباط الشرطة القضائية وأعوانهم إلى غاية قضاة الحكم أن يتعاملوا بكل موضوعية وفهم للتحري والتحقيق ثم الحكم في قضايا مواضيعها تتميز بالخصوصية ؟

– وهل القواعد الإجرائية في قانون الإجراءات الجزائية وخاصة منها إجراءات البحث والتحري والتفتيش وضبط الأدلة يمكنها أن تستوعب الجرائم الحديثة والمتنامية المرتبطة بتكنولوجيات الإعلام والاتصال؟

– تعد الانترنت ووسائل الاتصال الحديثة منطقة تدخل واسعة للكثيرين يقومون بتسييرها وتقديم الخدمات فيها واستعمالها، فكيف تعامل المشرع لتنظيم هؤلاء جميعا، وتحديد مسؤولياتهم في حالة ارتكاب جرائم يمكنهم إما منعها أو التدخل للحد منها؟

كل هذه التساؤلات سيتم الإجابة عليها وفقا لمنهجين علميين هما المنهج التحليلي الذي يوافق تماما طريقتنا في الإجابة عن تساؤلاتنا، وكذلك سنعتمد في تحليلنا لهذا القانون على المنهج المقارن خاصة فيما يتعلق بالدراسات الفقهية والأحكام القضائية في فرنسا والتي

تساعدنا في فهم مقصد المشرع من وضع أحكام قانون 04/09 و دورها في مكافحة هذا النوع من الإجرام.

وعليه ستتم دراستنا لهذا الموضوع وفق خطة منهجية من فصلين على النحو التالي:

الفصل الأول: هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الأول: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال محليا

المبحث الثاني: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال دوليا

الفصل الثاني: الدليل وطرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الأول: الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الثاني: طرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

الفصل الأول:
هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

الفصل الأول: هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

باختلاف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بتقنية التنفيذ العالية المعتمدة على وسائل الاتصال الحديثة وشبكة الانترنت المتوافرة في كل بقاع العالم، كما أن سرعة التنفيذ والأثر الذي تخلفه على المجتمعات يعد مهولا، فجرائم التزوير والاحتيال الالكتروني، ونشر الصور الإباحية، والدعارة بمختلف صورها وخاصة دعارة الأطفال التي وجدت لها مرتعا خصبا في مواقع الانترنت المنتشرة في كل مكان وبكل اللغات، وكذلك استعمال تكنولوجيات الإعلام والاتصال 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 (الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها) 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 اكتشافها أو لعدم التبليغ عنها أو لبطء رد الفعل القضائي غير المتخصص اتجاهها، وفي هذا الحال 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، والذي يعد جزء منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتي تكون من اختصاص هيئات قضائية متخصصة للفصل فيها (الأقطاب الجزائية).

كذلك فإن الصفات الدولية لهذه الجرائم باعتبارها عابرة للحدود في كثير من الأحيان تجعل من تطبيق القوانين الوطنية الجزائية للعديد من الدول لقمعها يشكل تحديا فعليا لممارسة الاختصاص القضائي لهذه الدول، وهو ما يرتبط أساسا بسيادتها الوطنية وبتطبيق قوانينها الوطنية على جرائم مرتكبة في إقليمها أو التي تمس بمصالحها ومؤسساتها، وهو ما يجعل التعاون الدولي وإعداد قوانين جزائية متناسقة بين الدول

لمكافحة هذه الجرائم أمرا حتميا، وإلا فإن الكثير من المجرمين سيجدون لأنفسهم منافذ تمنع توقيع العقاب عليهم لارتكابهم تلك الجرائم، وذلك لعدم تمكن بعض القوانين الجزائية من الوصول إليهم بسبب تنازع القوانين الجزائية من جهة، ولقصور تطبيق القوانين الوطنية على هذا النوع من الجرائم من جهة أخرى.

لهذا فإن دارستنا لسبل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تبدأ:

أولا: بمعرفة مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الوطني، وثانيا: نتناول مكافحة هذه الجرائم على الصعيد الدولي.

المبحث الأول: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الوطني

يمكننا طرح تساؤل يسمح لنا بالإجابة عنه بتحديد عناصر هذا المبحث والذي هو كالآتي:[1]

هل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (الجرائم المعلوماتية) تتطلب سلطات أو هيئات أو أشخاص يتمتعون بقدر كاف من المعرفة التكنولوجية الحديثة لوسائل الإعلام والاتصال؟ أم أنه يمكن للسلطات الحالية متابعة مجرمي تكنولوجيات الإعلام والاتصال ومساءلتهم بما لديها من أساليب تقليدية في البحث والتحري عنهم وتقديم أدلة تثبت إدانتهم؟.

الإجابة عن هذا التساؤل يقودنا إلى أنه:

01-إن الجرائم المعلوماتية تعد من الجرائم الحديثة المرتبطة بتطور تكنولوجيات الإعلام والاتصال التي تستدعي إمكانات وخبرات تقنية لا يمكن مواكبتها إلا بإنشاء هيئات ومراكز متخصصة لمكافحة الجرائم المتصلة بها، وبتجنيد العاملين في قطاع العدالة عن

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص 231.

طريق التكوين المتخصص الذي يهدف إلى توسيع معارفهم بتلك التكنولوجيات، ولمعرفة كيفية استخلاص الأدلة الرقمية، وكيف يتم الحكم بواسطتها.[1]

02-إن 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، وحتى الجرائم التقليدية كالسرقة والنصب والقتل. ومن خلال ذلك نرى أن استعمال أجهزة الإعلام الآلي و تكنولوجيات الإعلام والاتصال متوافرة للجميع بمن فيهم المجرمين بمختلف أنواعهم وصفاتهم وأساليبهم في ارتكاب جرائمهم.

لهذا سنتناول في هذا المبحث السلطات المختصة بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المطالب التالية:

المطلب الأول: الهيئات الوطنية للوقاية والمكافحة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

حيث أن المشرع الجزائري حاول أن يواكب الترسانة العالمية من القوانين والإجراءات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال بإنشاء هيئات للمكافحة والوقاية.[2]

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

حيث أن المشرع نص على هذه الهيئة في القانون 04/09 في المادة 13 والمرسوم الرئاسي 15/261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة تكنولوجية الإعلام والاتصال الصادر بتاريخ 8 أكتوبر 2015، هي سلطة إدارية مستقلة لدى وزير العدل تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل .

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص 231.

[2] عبد الفتاح بيومي حجازي، المرجع نفسه، ص 231.

تتشكل من أعضاء معينين من الحكومة وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء ومسئولي مصالح الأمن وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكري والدرك والأمن الوطني وفق لقانون الإجراءات الجزائية مهامها :

01-حماية النظام العام

02-سرية المراسلات والاتصالات

03-التحريات والتحقيقات القضائية

04-الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها

05- إجراء التفتيش والحجز داخل المنظومة معلوماتية

الفرع الثاني: السلطة الوطنية للتصديق الالكتروني

وحسب المادة 16 من القانون رقم 04/15 الصادر بتاريخ 01 فبراير 2015 المتعلق بتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والذمة المالية

مهامها[1] : تحددت حسب المادة 18 من القانون 04/15

- إعداد سياستها للتصديق الالكتروني وسهر على تطبيقها.
- إبرام الاتفاقيات الأطراف المتبادل على المستوى الدولي.
- اقتراح مشاريع تمهيدية لنصوص التشريعية و التنظيمية المتعلقة بهذا المجال.
- القيام بعمليات التحقيق عل مستوى السلطتين الحكومية والاقتصادية المتعلقة بهذا المجال.

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

الفرع الثالث : السلطة الحكومية لتصديق الالكتروني

المنصوص عليها في المادة 26 من القانون 04/15 تنشا على مستوبا الوزير المكلف بالبريد وتكنولوجية الإعلام والاتصال حكومية لتصديق الالكتروني تتمتع بذمة المالية وشخصية المعنوية المستقلة مهامها :[1]

01- إعداد سياسة التصديق الالكتروني التي تعرض على السلطة الوطنية للمصادقة.

02- الاحتفاظ بشهادات التصديق الالكتروني المنتهية صلاحيتها.

03- نشر الشهادات التصديق الالكتروني للمفتاح العمومي للسلطة الوصية.

04- إرسال كل المعلومات الخاصة بنشاط التصديق الالكتروني إلى السلطة الوصية (دوريا أو بناء على طلب).

05-القيام بعملية التدقيق.

الفرع الرابع : سلطة الاقتصادية للتصديق الالكتروني

نصت عليها المادة 29 من القانون 04/15 تتعين هذه السلطة المكلفة بضبط البريد والمواصلات السلكية ولإسلكية في مفهوم هذا القانون مهامها حسب المادة 30 من نفس القانون السابق:

01- اتخاذ الإجراءات والتدابير لازمة لضمان الاستمرارية الخدمات في حالة عجز المؤدي للخدمة.

02- السهر على وجود منافسة فعلية ونزيهة بين مؤدي خدمات التصديق الالكترونية.

03- التحكيم في المنازعات القائمة بين مؤدي خدمات التصديق الالكتروني.

04- إعداد دفتر الشروط المحدد لشروط وقيمة التصديق الالكتروني وعرضه على السلطة الوصية للموافقة عليه.

05- القيام بتبليغ النيابة العامة بكل فعل ذي طابع جزائي.

[1] القانون رقم 04/15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني الصادر في 01 فيفري 2015

قراراتها ذات صفة إدارية قابلة لطعن أمام السلطة الوطنية في اجل شهر من تاريخ تبليغ ولا يكون لهذا الطعن اثر موقف والقرارات الصادر عن السلطة الوطنية فهي قابلة لطعن أمام مجلس الدولة في اجل شهر من تاريخ تبليغ ولا يكون لهذا الطعن اثر موقف المادتين 31 و32 من القانون 04/15 .

المطلب الثاني: دور الضبطية القضائية في إجراءات مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن لسلطة الضبط القضائي دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها.[1]

أما بالنسبة للجرائم المستحدثة فإنها تلقي المزيد من الأعباء على عاتق هذه السلطة وكذلك الأمر بالنسبة للسلطات القضائية، وذلك نظرا لضعف خبرة كلا 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، وللسبب ذاته سيفشل التحقيق في جمع أدلة جرائم تكنولوجيات الإعلام والاتصال، كما أن المحقق وفي بعض التحقيقات قد يدمر الدليل بمحوه للقرص الصلب بخطأ منه أو بإهماله، ولهذا كان لازما تبني إستراتيجية واضحة في مجال البحث عن أدلة إثبات الجريمة المعلوماتية، من حيث إعداد ضباط الشرطة القضائية وحتى قضاة النيابة العامة والتحقيق وقضاة الحكم[2].

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

---

[1] القانون السابق.

[2] القانون السابق.

2 عبد الفتاح بيومي حجازي، المرجع السابق، ص 232.

هذا البرنامج التكويني يهدف إلى تطوير كفاءات سلك الدرك الوطني، حتى تكون أكثر عملية في مجال مكافحة الجرائم المعلوماتية[1].

كما أن إطارات الدرك الوطني تساهم في عدة ملتقيات وطنية ودولية تنصب موضوعاتها في إطار الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. بينما مصالح الأمن الوطني هي غائبة عن مجارات تكريس مكافحة هذه الجرائم ماعدا ما يتم تنظيمه من معارض وملتقيات تتعلق بالموضوع، وكذلك المشاركة والمساهمة في ملتقيات ومؤتمرات وطنية ودولية تتناول بالخصوص حقوق المؤلف في البيئة الرقمية[2] .

هذا ما استجد في الجزائر بينما في الأنظمة المقارنة فنجد أنه في فرنسا مثلا تم تأسيس العديد من الهيئات التي تختص بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نذكر على سبيل المثال[3]:

- الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال السابق ذكرها، من أجل مكافحة أفضل ضد هذه الجرائم، وهذه المصلحة الخاصة بالشرطة القضائية لما بين الوزارات تحوي أعوان الشرطة، وأعوان الدرك، الذين يشتركون باختصاصهم في مكافحة هذه الآفة.
- مديرية مراقبة الإقليم مختصة بتسريع عمليات التحريات القضائية المتعلقة بأعمال القرصنة على الأنظمة الآلية للمؤسسات ذات التدابير الحصرية أو معطيات مصنفة للدفاع.

كما أن الدرك الوطني الفرنسي أنشأ منذ سنة 1998 إدارة مكافحة الجرائم المعلوماتية ضمن المصلحة التقنية للأبحاث القانونية والوثائقية، كل هذه الترسانة من

---

[1]Hadjira BOUDER: Orientations de la politique pénale de prévention et de lutte contre la criminalité liée aux TIC en Algérie, centre de recherche sue l'information scientifique et technique, CERIST,03 Rue des frères Aissiou, Benaknoun, Alger, Algérie,www.alexalaw.com [28/02/2011]

[2]أنظر المرجع السابق.

[3]France, de la sécurité intérieure et des Libertés Locales, le 25 février 2005, Thiery BRETON ,Chantier sur la lutte contre la cybercriminalité, Rapport remis à Monsieur le ministre de l'Intérieur en www.4law.co.il ,P 04. [04/03/2011].

الهيئات والمؤسسات لمكافحة الجرائم المعلوماتية بمختلف أشكالها ما هي إلا دليل على خطورة وتشعب هذا النوع الجديد من الإجرام، وهو ما يجب على السياسة الجنائية الجزائرية أن تتبِعْهُ ، لأنه يلاحظ تباطؤ كبير في مجارات هذه الجرائم، وإفلات الكثير من المجرمين من العقاب خاصة فيما يتعلق بالاعتداءات على الأشخاص والأموال التي تتم بواسطة شبكة الانترنت، وكذلك ما وصلنا إليه من تبادل للصور عبر الهواتف المحمولة عبر Bluetooth التي تحمل في طياتها خدش للحياء العام، وصور لأشخاص أبرياء التقطت لهم تلك الصور بعلم منهم أو بدون علمهم، ولكن وظفت تلك الصور لتكون أفعالا إجرامية يعاقب عليها القانون، ولأنه لا توجد سياسة وقائية تحسيسية فإن فاعلي هذه الجرائم يتمادون في ارتكاب جرائمهم بدون متابعات قضائية تحد من إجرامهم، لهذا فإن التدريب الجيد لعناصر الأمن والدرك الوطنيين والحملات التحسيسية للمواطنين ستحّدّ من انتشار هذه الجرائم، وفي حالة وقوعها فإن المجرمين ينالون عقابهم لإمكانية الوصول إليهم عبر إجراءات قانونية تتسم بالشرعية.

المطلب الثالث: السلطة القضائية في مواجهة الجرائم المعلوماتية

إن السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين[1]، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإنّ حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي[2].

ومنذ 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

[1] Hadjira BOUDER: op. cit, page 11

[2]Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, Droit pénal appliqué», 2010, ECONOMICA ,Paris France, page 206.

تكوين طلبة المدرسة الوطنية للقضاء على شكل ملتقيات ينشطها خبراء، العديد من دورات التكوين في مختلف مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال منظمة بالخارج لصالح القضاة و إطارات وزارة العدل في إطار التعاون الثنائي، ومنها: التعاون الجزائري الفرنسي، الجزائري البلجيكي، والجزائري الأمريكي الذي تناول خاصة التكوين المتخصص في الملكية الفكرية المتمحورة حول التزوير المتصلب البيئة الرقمية[1].

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية (ق إ ج) على أنه يجوز تمديد دائرة الاختصاص 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 40مكرر 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، 329من هذا القانون مع مراعاة أحكام المواد من 40مكرر 1إلى 40 مكرر 5أدناه ".

و إذا 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 لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية[2]، فيتجنب إنشاء هيئات قضائية جديدة لكنه يوسع من دائرة الاختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها اختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن

[1]Hadjira BOUDER: op. cit, page 12

[2]عمار بوضياف، المرجع السابق، ص 229.

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.

هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسوم التنفيذي 348/06 المؤرخ في 05أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق(جريدة رسمية رقم:63) في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، ولأن الجريمة المنظمة تشمل جرائم جد متنوعة تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وترتكب من طرف عدة أفراد يتصرفون بطريقة منظمة، تعد الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإن الحركة المتزايدة والضرورية أدت إلى تركيز الاختصاص القضائي في إطار الاهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة[1].

المبحث الثاني: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الدولي

لا يمكن مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بفاعلية إل إذا قبلت الدول المعنية التعاون الكامل فيما بينها، وهذا التعاون غالبا ما يكون في شكل اتفاقيات ثنائية أو متعددة الأطراف في المواد الجزائية ولكن ذلك لا يمنع من ظهور تنازع حول تطبيق القوانين الجزائية الوطنية لدول مختلفة على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة، فمن المحتمل أن يكون عدد من الدول المعنية بجريمة

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. page 207.

معلوماتية يثير عدد من المشاكل فكيف يتم تحديد أي من تلك الدول تم فيها ارتكاب الجريمة؟ وأي من هذه الدول مختصة في عقاب مرتكبي هذه الجريمة؟.

وفي حالة الإجابة عن هذه التساؤلات قد 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 دولي حقيقي وبموجب قوانين وطنية، أمر لا بد منه لمكافحتها ومعاقبة فاعليها وهذا ما سنتناوله تباعا في هذا المبحث.

المطلب الأول: مبدأ الإقليمية في مواجهة جرائم المعلوماتية

لقد تأثر مبدأ إقليمية القوانين الجزائية بالعولمة، التي أعادت طرح الخلاف حول مفهومه التقليدي باعتباره مبررا لسيادة الدولة على إقليمها، وجرائم المعلوماتية لا تعرف الحدود المرسومة للدول، ولقد تخطتها كلية، فهذه الجرائم يمكن أن ترتكب في عدة دول وفي آنٍ واحد، وبالنتيجة، معطيات رقمية افتراضية غير مادية ومكان لوقوع الجريمة ليس بالضرورة موجودا على إقليم الدولة أو في نطاق اختصاص جهازها القضائي عندما تظهر التأثيرات المادية (الواقعية) للجريمة[1].

واختصاص القضاة هو " صلاحية التحقيق أو الحكم في قضية أو دعوى ما للفصل فيها "[2] وعندما نتحدث عن الاختصاص فنعني بذلك " سلطة المحكمة وصلاحياتها في النظر في القضية المطروحة أمامها إن لجهة " الشخص« المحال أمامها، أم لجهة » الجريمة « المسندة إلى الفاعل أو باقي المدعى عليهم من شركاء أو متدخلين أو محرضين، أم لجهة » المكان " حيث وقعت الجريمة "[3] وهو يعد من النظام العام الذي يمكن إثارته في كل

[1]Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, op. cit. page 158.

[2]عمر السعيد رمضان، أصول المحاكمات الجزائية في التشريع اللبناني، منشورات الدار المصرية للطباعة والنشر،الطبعة الأولى، 1971، ص 404.

[3] إلياس أبو عيد، نظرية الاختصاص في أصول المحاكمات المدنية والجزائية، منشورات زين الحقوقية، 2004، لبنان، ص 469.

وقت من الإجراءات، وكذلك للقاضي أن يثيره من تلقاء نفسه، وللسؤال حول الاختصاص الإقليمي هو سؤال مهم وأساسي فيما يخص التحقيقات الأولية أو القضائية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ذلك لأنه في كثير من القضايا المطروحة التحقيق فيها عابر للحدود، وعناصرها الدولية تجعلها السبب في صعوبات تتعلق بتحديد الجهة القضائية المختصة إقليميا للفصل في تلك القضية[1].

الفرع الأول: التذكير بالقواعد

1- بالنسبة للاختصاص الإقليمي للقضاء، نظم قانون العقوبات وقانون الإجراءات الجزائية قواعد إسناد الاختصاص متعلقة بمكان ارتكاب الفعل المُجرم من جهة، ومن جهة أخرى بجنسية الفاعل (كما أن بعض القوانين كفرنسا تأخذ بجنسية الضحية لانعقاد الاختصاص لقضائها)[2].

2- يتعلق الأمر بقواعد إسناد الاختصاص بتطبيق مبدأ الإقليمية المادة 3فقرة 1 من قانون العقوبات (ق ع) التي تنص على أنه " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية "، كما تنص المادة 586من ق إ ج على " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر "، وقد أقرت أحكام القضاء الفرنسي- باعتبار قواعدها مطابقة لأحكام القانون الجزائري فيما يخص الاختصاص الإقليمي- بأنه في حالة ارتكاب الجريمة في الخارج وأنتجت آثارها في فرنسا فإن الاختصاص ينعقد للقضاء الفرنسي، فالمادة 113-2 من قانون العقوبات الفرنسي والتي تقابلها المادة 586ق إ ج وضعت مبدأ المسؤولية الموسعة للقضاء الجزائي الوطني، معتنقة بذلك نظرية كلية الحضور كلما كان هناك ارتباط بالإقليم الوطني وبالقانون الجزائي في حالة أن جزء من الجريمة ارتكب في الإقليم[3].

[1]Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, op. cit. page 158.
[2]Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, op. cit. page 158
[3]Yann PADOVA, Administrateur des services de l'Assemblée nationale, Un aperçu de la lutte contre la cybercriminalité en France, Revue de science criminelle 2002 France, p. 768.

وعليه فإن الفقه الفرنسي بناء على هذه الاجتهادات القضائية يؤكد على أن تمركز الموزعين الذين يتم بواسطتهم نشر عبر الانترنت محتويات قابلة أن تكون أسس لجرائم لا يؤثر على الاختصاص القضائي الوطني ما دامت الجرائم يمكن الوصول إليها من داخل الإقليم الوطني[1].

3- تنص المادة 585من ق إ ج والتي تقابلها المادة 113- 5 من قانون العقوبات الفرنسي على أنه "كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة في الخارج يجوز أن يتابع من أجلها ويحكم عليه فيها بمعرفة جهات القضاء الجزائرية إذا كانت الواقعة معاقبا عليها فيِ كِلا القانونين الأجنبي والجزائري بشرط أن تكون تلك الواقعة الموصوفة بأنها جناية أو جنحة قد ثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية "، وعليه فإنه لكي يسأل الشريك يجب توافر أمرين:

- أن يكون الفعل مجرما في كلا البلدين.

- أن يصدر حكم الإدانة على الفاعل الأصلي في البلد الذي ارتكبت فيه الجناية أو الجنحة[2].

هذا الحكم ينطبق على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة في آن واحد في الإقليم الوطني وفي الخارج[3].

4- أما بالنسبة للجنايات والجنح المرتكبة من طرف جزائريين خارج الإقليم الوطني (المادة 582 من ق إ ج) فإن قانون العقوبات الجزائري يطبق عليها ولكن بتوافر الشروط التالية:

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. page 158.

[2]Yann PADOVA, op. cit, p. 76.9

[3] بن محمد محمد، تنازع الاختصاص في الجرائم الالكترونية، مقال مأخوذ من مجلة دفاتر السياسة والقانون، صادرة عن كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، العدد الثاني، جانفي 2010، ص 149.

– 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 أن يكون المتهم جزائريا وقت ارتكاب الجريمة أو بعد ارتكابها (المادة 584ق إ 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، جرح عمد، سرقة..) فإن المادة 583من ق إ ج توقف تطبيق قانون العقوبات الجزائري على شكوى من الطرف المضرور أو بلاغ من سلطات القطر الذي ارتكبت فيه تلك الجريمة[1](وهي نفس الأحكام الواردة في المادة 113–6 من قانون العقوبات الفرنسي).

وفي الأخير فإن الجنايات والجنح المرتكبة ضد جزائريين في الخارج من طرف أجانب فلا ولاية للقضاء الجزائري عليها إلّا في حالة واحدة حددها المشرع بالمادة 591ق إ ج وهي حالة ارتكاب جناية أو جنحة على متن طائرة أجنبية إذا كان المجني عليه جزائريا، بعكس القانون الفرنسي الذي يأخذ بمبدأ شخصية النص الجزائي على إطلاقه (الإيجابي والسلبي) فيطبق على كل جناية أو جنحة معاقب عليها بالحبس مرتكبة من طرف فرنسي أو أجنبي خارج الإقليم الفرنسي إذا كان الضحية من جنسية فرنسية وقت ارتكاب الجريمة مع وجوب توافر نفس الشروط الوارد ذكرها مسبقا[2].

5– معايير الاختصاص الإقليمي المنصوص عليها في المواد 16، 37، 40، 329من ق إ ج هي مكان ارتكاب الجريمة، محل إقامة أحد الأشخاص المشتبه في مساهمتهم في

[1]أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، الطبعة الخامسة،2007، صفحة 81.

[2]أحسن بوسقيعة، المرجع نفسه، صفحة 82.

اقتراف الجريمة، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر، ولجنسية مرتكب الجريمة أثر في الاختصاص القضائي.

6- الجنايات والجنح الماسة بالمصالح الأساسية للجزائر: وهو مبدأ الاختصاص العيني، وطبقا لهذا المبدأ يطبق القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف النظر عن جنسية مرتكبها[1]،ويعتمد هذا المبدأ على حق الدولة في الدفاع عن جميع صور الاعتداء على مصالحها الحيوية والأساسية ولو وقعت تلك الجرائم خارج إقليمها تكريسا لمبدأ عدم المساس بسيادة الدولة. فالمادة 588من ق إ ج والمادة 15من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كرست هذا المبدأ، ونلاحظ بالنسبة للمادة 588 ق إ ج أنها حددت اختصاص القضاء الجزائري في الجرائم المرتكبة من أجنبي بالخارج وحصرتها في الجرائم المرتكبة ضد أمنها أو جريمة تزييف النقود الوطنية أو أوراق مصرفية مع توافر شرط القبض على المجرم في الجزائر أو حصلت على تسليمه لها مع توافر الشروط التي نصت عليها المادة 589ق إ ج.

الفرع الثاني: تكييف الاختصاص وفق المنازعات

إن عنصر العالمية للانترنت يحث مجرمي المعلوماتية بالتلاعب بالحدود مما يجعل تطبيق قواعد الاختصاص الإقليمي معقدة في المواد الجزائية، ومثال ذلك يمكن للنيابة العامة أن تقرر عدم اختصاصها بناء على عناصر أجنبية في الوقائع بالرغم من أن جزء من تلك الأفعال قد وقعت في مجال اختصاصها.

و الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في غالب الأحيان لها ميزات دولية، غير أن التحقيقات فيها هي بحد ذاتها تعد معطيات تدار وتسير بالقانون الوطني، وفي هذا الصدد فإن تدفق المعلومات عبر تيار حر وهو الانترنت والتحقيق فيها من قبل

[1] بن محمد محمد، المرجع السابق، ص 151.

سلطات مخولة لذلك لا بد أن تكون مقيدة باختصاصها الإقليمي الوطني وبمبدأ السيادة[1].

وفي غياب اتفاق دولي لتوسيع الاختصاص، وتشريع دقيق في مجال الاختصاص القضائي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فإن الاجتهاد القضائي الفرنسي[2] حدد حالة بحالة قواعد الاختصاص المتوافقة مع هذا النوع من الإجرام:

1- العنصرية والرجعية وجرائم الصحافة: تبنى الاجتهاد القضائي الفرنسي تصورا واسعا لمحل الجريمة، فالقانون الفرنسي يُطبق متى أمكن الوصول إلى الخبر عبر الانترنت، فقد اعتبر أن النيابة العامة مختصة إقليميا أين تم نشر الخبر، وفي حالة أن المحتوى صادر عن موقع أجنبي ومحمل في فرنسا مثلا فإن السلطات القضائية الفرنسية مختصة إجمالا، كما لو أن الجريمة قد ارتكبت بالكامل في الإقليم الفرنسي.

إلا أنه بقرار صادر في 08ديسمبر 2009 اعتبرت الغرفة الجنائية بمحكمة النقض الفرنسية أنه " مكان ارتكاب الجريمة هو المكان الذي تم فيه التلفظ بالتهديد(توجيه التهديد) وليس في الدول بعد أن نقل الخبر فيها عبر التلفاز أو الإعلام المكتوب أو الرقمي والذي تم من خلاله علم الضحية به".

2- جرائم التقليد عبر الانترنت: في مواد التقليد المعلوماتي تكون مختصة إمّا محكمة المكان الذي تم فيه فعل التقليد و إما مكان نشره.

هذا الرفض لتنظيم الاختصاص القضائي الفرنسي المستند على معيار قابلية الوصول عن طريق محرك البحث Google، لأن محكمة الاستئناف بباريس وضعت معيار جديد للاختصاص الإقليم يقوم على مميزات "الإرتباط الكافي والأساسي بين هذه الوقائع والضرر المدعى به "[3].

---

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. page 160.

[2] لغياب الاجتهاد القضائي الجزائري في هذه القضايا المستحدثة.

[3] 06 juin 2007, legalis.net,art.1944, V. Répertoire de droit pénal et de procédure pénale © EditionsDalloz 2011, disponible sur:www.dalloz.fr

وأخيرا قامت محكمة باريس بإصدار أمرين لها في 16 ماي 2008 باحتفاظ قاضي فرنسي باختصاصه في مواد تقليد العلامات التجارية عبر الانترنت مُستندة على واقعة أن الأفعال المجرمة التي يمكن الوصول إليها لها أثار اقتصادية على المجتمع الفرنسي "غير هام بأن هذا الموقع يدار في اسبانيا ويصعب الوصول إليه بمحركات البحث في فرنسا ."[1]

3- جرائم المساس بأنظمة المعالجة الآلية للمعطيات: تقع هذه الجرائم غالبا في آن واحد وفي أماكن مختلفة ونتيجة لذلك قد يحدث تعقيدا في سير الإجراءات .

إن الاجتهاد القضائي الفرنسي مثل محل تنفيذ هذه الجرائم بمكان الموقع الالكتروني(web) أين أتلف، أنشأ سير،غذي، روقب، مستقلا في ذلك عن موقع الخادم الضروري لقيامه بعمله[2].

وكذلك الأمر فإن محكمة الاستئناف سايرت تعليل النيابة العامة فيما يخص المعنى الموسع الذي تبناه القضاء الفرنسي لعبارة " الفعل المكون""**acte constitutive** " وقبلت اختصاص القانون الفرنسي فقط عندما تظهر آثار الجريمة في فرنسا.

ففي حالة أن هناك عناصر مكونة لجريمة الدخول بطرق الغش لنظام معالجة المعطيات أو جريمة إتلاف المعطيات أو التلاعب بها (بالتعديل، المحو..) موجودة داخل الإقليم الوطني فإن القانون الجزائي الوطني يطبق[3].

المطلب الثاني: ضرورة التعاون الدولي في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن الحاجة إلى تنسيق دولي وثيق في مجالات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ترتبت قبل كل شيء عن الحركة الكبيرة للمعلومات في الأنظمة المعلوماتية،

[1]V. Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011.
[2]TGI Paris, ord.16 mai 2008 legalis.net,art.2419.
[3]Ca Paris,13 ch. Section A, 25 septembre2007.

هذه الحركة سمحت بارتكاب جرائم عن طريق جهاز للإعلام الآلي (الكمبيوتر) في دولة ما في حين أن نجاح الفعل الإجرامي يكون بتنفيذه في دولة أخرى. كما أن هذا النوع من الإجرام يتطلب تعاون دولي فّعّال لمكافحته[1]، والذي هو مهم من أجل حماية فعالة أيضا لأنظمة الاتصالات العابرة للعديد من الدول، أضف إلى ذلك أن تصدير البرامج المعلوماتية للخارج تبرر أيضا ضرورة تنظيم قانون دولي لحمايتها.

ونتيجة لذلك فإن الانترنت بقدر ما هي فضاء مفتوح للاتصالات فإنها تخلصت من كل قيود الإقليمية، وتسمح بنشر كل أنواع المعلومات بدون عقبات جغرافية. وبالمقابل، القانون الجزائي هو تعبير عن سيادة الدول، وفي هذا السياق فإنه يحوي البعد الإقليمي للدولة، وعلى ذلك فجزائيا قاضي التحقيق والشرطة القضائية يتحرون تقليديا وأساسا لتحديد موقع مرتكب الجريمة وتحديد هويته، وحفظ عناصر الأدلة من أجل تجسيد الجريمة التي يمكن أن تكون قد ارتكبت على إقليم دولة أخرى، وبموجب النظام القانوني الوطني المطبق داخل الدولة التي تصل إليها المعلومة، فإن هذه الأخيرة يمكن أن تعد إما مشروعة أو غير مشروعة، يرجع هذا غالبا للوظيفة المتغيرة لمبادئ حرية التعبير واحترام الحياة الخاصة [1]، وخير مثال على ذلك قضية Yahoo حيث أنه بتاريخ 22 ماي 2000 أمر قاضي الاستعجالات بباريس بإلزام الشركة الأمريكية Yahoo بإيجاد حلول تقنية من أجل منع وصول مستعملي الانترنت بفرنسا لموقع البيع بالمزاد لمنتجات نازية، خرقا لأحكام نصوص قانون العقوبات الفرنسي، الأمر الاستعجالي أرفق بتقرير كتب من طرف مجموعة من الخبراء يفصلون فيه الإجراءات القابلة للعمل بها وخاصة في مجال تصفية مستعملي الانترنت بتوظيف عناوينهم الالكترونية من أجل توقيف الاضطراب غير المشروع للنظام العام، ومن أجل أن يصبح هذا الأمر نافذا يجب على الأقل الموافقة عليه من قاضي أمريكي، وبالفعل قام القاضي الأمريكي من المجلس

[1]Anne BRISSET-GIUSTINIANI, Aspects juridiques de l'émergence d'une sécurité européenne des réseaux et des systèmes d'information, Mémoire D.E.S.S. Droit de l'Internet-administrations-entreprises, Université PantheonSorbonne paris I, disponible sur: www.univ-paris1.fr/.../2004_sept_OK_Brisset_ Giustinani_ Version_ ...[06/06/2011].

القضائي لمقاطعة شمال كاليفورنيا بفحص الأمر أولا من حيث مطابقته للدستور الأمريكي الحامي لحرية التعبير، وفي حكمه بتاريخ 07نوفمبر 2001اعتبر القاضي جيرمي فوجيل Jeremy FOGEL أن القرارات الفرنسية تكون بوضوح غير متلائمة مع أول تعديل إذا هي أصبحت مطبقة في الولايات المتحدة الأمريكية، إن فرنسا لها السيادة من أجل وضع الحدود لحرية التعبير في إقليمها، هذا المجلس لا يمكنه تنفيذ قرار أجنبي لا يحترم الدستور الأمريكي، إلا في حالة إلغاء حرية التعبير المحمية داخل حدودنا الإقليمية، إن المجلس ملتزم حتما ببعض الأحكام التي هي على قدر من المشاركة الجوهرية في الثوابت، وخاصة في فكرة أساسية وجوهرية للتعديل الأول، الذي بمقتضاه أنه من الأحسن السماح بتعبير غير عنيف لأراء مزعجة أفضل من وضع أفكار حكومية في مجال التعبير[1]،يتعلقا لأمر بوضوح بأن الجهود نحو تعاون دولي لوحدها التغلب على خطر إزالة فاعلية الرد القضائي بسبب التعارض الموجود بين الفضاءات القانونية الوطنية[2]، ومن المهم ملاحظته أن التشريعات الوطنية في مجال الجريمة المعلوماتية في مجملها حديثة الصدور وبعض الفوارق يمكن إيجادها، خاصة في حالات تجريم القرصنة، فمثلا في الولايات المتحدة الأمريكية الدخول غير المشروع للنظام المعلوماتي لا يعد مجرما إلا إذا وقع على أجهزة الكمبيوتر للمؤسسات العامة، وأما في اليابان فإن هذه الجريمة لم توضع قواعد تجريمها إلّاّ في سنة 1999[3]، وبالنسبة لنا فإن أحكام المساس بأنظمة المعالجة الآلية للمعطيات ومن بينها الدخول غير المشروع للأنظمة المعلوماتية لم يتم تجريمه إلا في سنة 2004بموجب تعديل قانون العقوبات بالقانون رقم: 15/04 المؤرخ في 10نوفمبر 2004.

[1]Source, Les Échos,28 novembre 2001, Les associations plaignantes ont cependant annoncé leur intention de faire appel de ce jugement qui est accessible sur le site : www.eff.org/Legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/.
[2]V. Yann PADOVA. , p. 775.
[3]Ibid. op. cit , p. .577

وللتعاون الدولي صور عديدة يهمنا منها التعاون القضائي الدولي الذي أدرجه القانون04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي خصص الفصل السادس منه والأخير للتعاون والمساعدة القضائية الدولية التي سنتناولها في المطلب التالي.

المطلب الثالث: وسائل التعاون القضائي على الصعيد الدولي

يعد التعاون الأمني والمساعدة القضائية في قضايا المعلومات من أهم صور التعاون الدولي القضائي في مجال الجرائم العابرة للحدود ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الأول: 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.

فإنه يصعب على الدولة بمفردها القضاء على جرائم المعلوماتية العابرة للحدود، لأن جهاز الأمن في هذه الدول أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الأمن بين الدول وتنسيق العمل فيما بينها لضبط المجرمين ومكافحة نشاط الإجرام المعلوماتي الذي يتجاوز حدود الدولة، وقد تبلور هذا النوع من التعاون الدولي في إنشاء المنظمة الدولية للشرطة الجزائية (الإنتربولInterpol)[1] وتستهدف هذه المنظمة 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

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة الإسكندرية، مصر 2009، صفحة 594-594.

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 الانتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل أن هذا العمل منوط بجهاز الأمن الوطني في الدولة التي يتواجد المجرم على إقليمها، الأمر الذي يؤكد على احترام السيادة الوطنية.

ولذلك فإنه من الأهمية تدعيم التعاون بين أجهزة الشرطة في هذه الدول المختلفة بناء على اتفاقيات دولية، ولهذا التعاون أهميته بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن إحدى الجرائم المعلوماتية قد تم ارتكابها عبر شبكة الانترنت من خلال موقع موجود في الخارج فإنها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات الأمن بالدولة التي تم منها البث[1].

يجمع الانتربول المعلومات عن الجرائم المعلوماتية ويحفظها ويحللها ويتبادلها مع جميع بلدانه الأعضاء عبر منظومة الانتربول العلمية للاتصالات الشرطية، وتستهدف الأوجه الأخرى لبرنامج الانتربول الخاصة بالإجرام السيبيري(المعلوماتي)[2]:

– تيسير التعاون الميداني بين البلدان الأعضاء من خلال إعداد لائحة بأسماء ضباط الاتصال المتيسرين على مدار الساعة للمساعدة في التحقيقات بشأن الإجرام المعلوماتي،

– زيادة تبادل المعلومات بين البلدان الأعضاء بشأن الأساليب الجرمية المتبعة في الإجرام المعلوماتي عن طريق الفرق العاملة الإقليمية وحلقات العمل التدريبية،

– إنماء شراكات إستراتيجية مع منظمات دولية أخرى وهيئات القطاع الخاص.

وفي إطار تنسيق الموارد الميدانية في التحقيقات الجارية في مجال تكنولوجيا المعلومات بالتعاون مع الدول الأعضاء، قامت الانتربول في مارس 2008 بطلب من دولة كولومبيا إجراء فحوص أدلة جنائية مستقلة على أجهزة ومعدات كمبيوتر ضبطت خلال عملية

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

[2] أنظر النشرة الإعلامية في موقع المنظمة عبر الانترنت: www.interpol.int

لمكافحة المخدرات والإرهاب نفذت ضد معسكر للقوات المسلحة الثورية (الفاك) وذلك لتحديد ما إذا كان جرى التلاعب بمضمون أي من المعدات بعد ضبطها.أجرى فريق خبراء الأدلة الجنائية التابع للإنتربول دراسة فنية مستقلة وأصدر تقارير خلص لغياب أي دليل يشير إلى تعديل ملفات المستخدمين أو تحريفها أو الإضافة عليها أو حذفها.

ومن المهم في التحقيقات الجارية بشأن الإجرام السيبيري المعلوماتي أن تسارع الشرطة إلى ضبط الأدلة المتعلقة بالبيانات الرقمية وهي على حالتها الأصلية قدر الإمكان، وأن تتعاون عبر الحدود حين وقوع هجوم سيبيري يشمل عدة بلدان. وقد كون الانتربول شبكة من المحققين العاملين في الوحدات الوطنية المعنية بجرائم الكمبيوتر– تعرف باسم شبكة النقاط المرجعية الوطنية – لتيسير الاتصالات الميدانية بين البلدان الأعضاء وتسرعها قدر الإمكان، ونقاط الاتصال هذه متيسرة على مدار الساعة وطوال أيام الأسبوع ويمكنها تلقي أو تقديم المعلومات وطلبات المساعدة، وتعتبر شبكة النقاط المرجعية المركزية الوطنية شرطا أساسيا لاستحداث منظومة الإنذار المبكر. وقد بادر أكثر من 120 مكتبا مركزيا إلى تعيين نقاط مرجعية مركزية وطنية.

كما استحدثت فرق للإنتربول تعنى بجرائم تكنولوجيا المعلومات لتيسير إنماء الإستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيات المعلومات، وكمثال على الأنشطة المقدمة من طرف هذه الفرق ما قامت به الفرق العاملة الأوربية التي أعدت " دليل الانتربول بشأن جرائم تكنولوجيا المعلومات " الذي يجمع ويصف بالتفصيل أدوات التحقيقات وهو متوفر على موقع الانتربول على الويب[1].

[1]أنظر النشرة الإعلامية في موقع المنظمة عبر الانترنت: www.interpol.int.

الفرع الثاني: المساعدة القضائية الدولية في المواد الجزائية

1- أشكال 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 إجرائية 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 اعتراضها في إقليم تلك الدولة، 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 تتضمن معظم الاتفاقيات الخاصة بالجرائم التقليدية نصوص تقضي بضرورة اللجوء إلى المساعدة المتبادلة، بهدف تحقيق السرعة والفاعلية في إجراءات ملاحقة وعقاب مرتكبي هذه الجرائم[1].

وتعرف المساعدة القضائية الدولية بأنها " كل إجراء قضائي تقوم به دولة منشأ لتسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[2] ، كما يمكن تعريفها أيضا بأنها " الإجراء الذي يسمح لسلطة قضائية لدولة بتوجيه إنابة قضائية إلى سلطات قضائية مختصة في دول أخرى من أجل تنفيذ جيد لها[3]، 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 ما يأتي:

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي- النظام القانوني للحماية المعلوماتية- (مرجع سابق) ص: 597.

[2] سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، (دراسة مقارنة) رسالة دكتوراه، كلية الحقوق جامعة عين شمس، سنة 1997صفحة 425، عن طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، ص: 597.

[3] Mohamed CHAWKI, Combattre la cybercriminalité, Edition de Saint Amans France, 2008, page. 314.

أ-**نقل إجراءات الردع Transmission des proceduresrepressive**: 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 الشخص يشكل جريمة في الدولة الطالبة والدولة 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[1].

إن ممارسة الاختصاص في القضايا العابرة للحدود يمكن أن تسبب مطالبة تنافسية للاختصاص والتي من الممكن في النهاية أن تتسبب في تعدد المتابعات القضائية وتخلف خلافات بين الدول، إن تقنية نقل الإجراءات تقدم آليات جد فعالة لحل هذا المشكل.

وخلاصة الاتفاق بينهما هو أن الدولة يمكن أن تتنازل عن حقوقها القضائية لصالح دولة أخرى بناء على الاتفاقية مما يسمح بتسوية تنازع الاختصاص، هكذا مبادرة زيادة على ذلك تتميز بالإدارة الجيدة للعدالة الجزائية وحماية لحقوق الضحايا واستعادة المجرم للمجتمع[2]، وقد أقر المجلس الأوربي اتفاقية نقل الإجراءات الجنائية، التي تعطي لأطراف المنضمة إمكانية محاكمة الجاني طبقا لقوانينها، بناء على طلب دولة أخرى طرف هذه الاتفاقية، بشرط أن يكون الفعل معاقبا عليه في الدولتين، وبالنسبة للجزائر فقد تم إبرام العديد من الاتفاقيات الثنائية من بينها الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا، الموقعة بمدريد في

[1] طارق إبراهيم الدسوقي عطية، مرجع سابق، صفحة 599.

[2]Mohamed CHAWKI, op. cit. page 316.

7 أكتوبر سنة 2002 (المرسوم الرئاسي رقم 23/04مؤرخ في 7فيفري 2004، الجريدة الرسمية عدد 08).

ب-**تبادل المعلومات:** وهو ما نصت عليه المادة 17من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نصت على أنه " يتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل "، فتبادل المعلومات يشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، كما أن هناك مظهرا آخر لها يتعلق بصحيفة السوابق القضائية للمتهمين، من خلالها تتعرف الجهات القضائية على الماضي الجزائي للشخص المحال لها، والتي تساعد في تشديد العقوبة في حالة العود أو في وقف تنفيذها، إلا أن تدويل صحيفة السوابق القضائية لا يتم إلا بواسطة اتفاقات تبادل المعلومات بين الدولتين الطالبة والمطلوب منها[1]، وخير مثال على ذلك ما أوردته المادة 15 فقرة 1 و2 من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا السالفة الذكر التي نصت على أنه "1- تتبادل وزارتا العدل الطرفين بيانات عن الأحكام المقيدة في صحيفة السوابق القضائية والصادرة من الجهات القضائية لكل منهما ضد رعايا الدولة الأخرى والأشخاص المولودين في إقليمها.

2 -وفي حالة المتابعة أمام جهة قضائية تابعة لأحد الطرفين المتعاقدين يمكن للسلطة القضائية المختصة أن تحصل من السلطات المختصة للطرف الآخر على صحيفة السوابق القضائية الخاصة بالشخص محل المتابعة . "

ج-**تبادل الإنابة القضائية الدولية:** ويقصد بها طلب إجراء قضائي من إجراءات الدعوى الجزائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها لضرورة ذلك الإجراء في الفصل

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

في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[1]، وهو ما أبرزته المادتين 16و 17من القانون 04/09 السالف الذكر، والذي عبرت عنه باتخاذ إجراءات تحفظية، ولا يكون ذلك إلا بالإنابة القضائية.

2- 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 القضائية سواء من أو إلى 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، ولأن الجريمة المعلوماتية لها ثلاث ميزات:

- سرعة فقدانها(متبخرة)
- صعوبة اكتشافها
- عابرة للحدود الوطنية

فإن تلك الطريق لا يمكن اعتمادها دائما في مجال التحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولهذا نجد أن المشرع الجزائري أورد استثناء في المادة 16 فقرة 2 من القانون04/09 التي تنص على أنه " يمكن في حالة الاستعجال ومع مراعاة للاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها "[2]

[1] بن محمد محمد، مرجع سابق، ص 156.

[2] بن محمد محمد، مرجع سابق، ص157.

بناء على ما أوردته الفقرة 2 من المادة 16 نجد أن المشرع قد سمح باستعمال مختلف وسائل الاتصال في حالة الاستعجال، فاتحا بذلك المجال لاحتمال توافر وسائل اتصال جديدة مستقبلا، والوسيلتين المذكورتين في المادة: الفاكس والبريد الالكتروني استعملهما المشرع على سبيل المثال وليس الحصر، وفي أرينا قد أخذ المشرع بميزات الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وما تتطلبه إجراءات جمع الأدلة لهذه الجرائم من سرعة في احتوائها حتى لا يتم فقدانها أو إتلافها.

ب- أورد المشرع في المادة 18 فقرة 1 من القانون 04/09 مجموعة من القيود ترفض بموجبها طلبات المساعدة القضائية الأجنبية وهي طلبات المساعدة التي من شأنها المساس بالسيادة الوطنية أو النظام العام، وهذا أمر يترك للدولة (وزارة العدل غالبا بحسب الاتفاقيات الدولية الثنائية) في تقدير تنفيذ أو عدم تنفيذ ما يطلب إليها.

ج- بحسب نص المادة 16 فقرة 1 من القانون 04/09 أدرج المشرع مبدأ ازدواجية التجريم La double incrimination و إن لم يكن قد صرح به و تنص المادة على أنه " في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني"، وبالتالي لا يمكن للدولة تقديم المساعدة القضائية لدولة أخرى في تحقيقات أو تحريات تخص أفعالا 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 يدعى بتنسيق القوانين الوطنية الجزائية وذلك لاجتناب وجود منافذ، أو تفسيرات متضاربة للشروط الواجب توافرها لتبرير التجريم[1].

[1]Mohamed CHAWKI, op. cit. page 315.

وفي الواقع وحتى في حالة عدم استخدام قاعدة ازدواجية التجريم في كل حالات المساعدة القضائية، فإن هذه القاعدة هي في الكثير من الأحيان ضرورية من أجل " إتمام أعمال التحقيق أو الوصول إلى أدلة الإدانة أو إلى الملفات أو الوثائق"[1].

[1]Article 3 de la convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959, voire Mohamed CHAWKI, Combattre la cybercriminalité, page 315.

خلاصة الفصل الأول

لقد تم البحث في هذا الفصل عن دور السلطات القضائية والأمنية في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك بنص المشرع على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و إن لم يتم بعد إنشاؤها ولا حتّى صدور مرسوم تنظيمي يعين أعضاءها وتنظيمها، إلاّ أننا واعتمادا على القانون المقارن حاولنا قدر المستطاع معرفة المهام المستقبلية المنوط لها من أجل مكافحة فعالة لهذه الجرائم.

ثم أبرزنا دور الضبطية القضائية في مكافحة هذا النوع من الإجرام من خلال الدور الذي يلعبه الدرك الوطني خاصةً في هذا المجال، من ناحية إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتوزيع أفراد مختصين يشكلون خلايا عبر كامل وحدات الدرك الوطني للكشف والتحقيق عن هذه الجرائم، كذلك الأمر بالنسبة لسلك القضاة الذين حرصت وزارة العدل على تكوين متخصص لهم، سواء بالداخل أو في الخارج لتعزيز معارفهم ولو قليلا حول تقنيات التكنولوجيات الحديثة للإعلام والاتصال، لِما لهم من دور في تطبيق القانون وإدانة مرتكبي هذه الجرائم.

وأخيرا تناولنا أهمية التعاون الدولي في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، باعتبار أن هذه الأخيرة في أوقات كثيرة تكون عابرة للحدود، كما يمكن للأجانب المساس بمصالح وطنية ومؤسسات مالية أو اقتصادية وطنية لدولة ما دون أن يبرحوا أماكنهم في أوطانهم، وهذا ما أكده المشرع الجزائري في مواد القانون 04/09 في الفصل السادس والأخير والذي تناول فيه الاختصاص القضائي الجزائي والمساعدة القضائية الدولية المتبادلة بين الجزائر والدول المعنية بها.

الفصل الثاني:
الدليل وطرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

الفصل الثاني: الدليل وطرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن نشوء القوانين المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيات الإعلام والاتصال ومكافحتها ، الذي جاء بقواعد تنظيمية وإجرائية تخضع لها السلطة القضائية وأعوانها تطبيقا لمبدأ الشرعية وذلك للتحقيق في الجرائم المرتكبة ومتابعة فاعليها وتوقيع الجزاءات المناسبة لهم، وهذه الإجراءات الجديدة التي يستطيع بها رجال القانون ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية ، لذلك سيكون تقسيم هذا الفصل على نحو يسمح بالتعرف على الأدلة الرقمية وأساليب التحقيق فيها وفقا للمبحثين التاليين:

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

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

المبحث الأول: الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تقوم فكرة الدليل على حجية الإثبات عموما وعلى احترام الحريات المحمية دستوريا، فأجهزة العدالة الجزائية وهي تسعى إلى رصد ونسب جريمة ما إلى مرتكبها، تكون ملزمة بإحداث توافق بين الجريمة ومرتكبها، يصل إلى أقوى مدى له في تسمية الجريمة باسمه[1].

يقصد بالإثبات "إقامة الدليل على وقوع الجريمة، وعلى نسبتها إلى المتهم"، ومن ثم فإنه حين يثار موضوع الإثبات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فإن الأمر يرتبط بنقطتين: الأولى: هي موضوع الدليل الذي تسعى إليه العدالة الجزائية بقصد التوصل إلى إثبات النقطة الثانية وهي المتعلقة بالحقيقة الواقعية وهي الواقعة بأشخاصها أي الواقعة الإجرامية التي حدثت ومرتكبيها، والتي يرتب عليها القانون جزاءات سواء من حيث القاعدة الموضوعية أو من حيث القاعدة الإجرامية، وفي كل من الأمرين، يضع القانون الإجرائي تلك الضمانة الخطيرة التي تتعلق بالمحافظة على الحقوق والحريات الشخصية أثناء سير العدالة باتجاه أهدافها، نحو ترتيب الآثار الجزائية المترتبة على إحقاق العدالة، وهي ضمانة مكفولة بقوة القرار القضائي المتمثل في الحكم الذي يصدره قاضي الموضوع ذاته.

على أن ما يهمنا هنا هو السعي إلى بحث الإثبات الجزائي في الجرائم الناشئة عن استعمال تكنولوجيات الإعلام والاتصال[2]، فالبحث في الإثبات ووسائله في إطار مدى

[1] فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون المنصورة، مصر الطبعة الأولى سنة 2010، ص 581.

[2] فتحي محمد أنور عزت، المرجع نفسه، ص 582.

اتفاقها مع التقنية الحديثة يبدو غير ذي معنى إذ لم يكن مدعما بتوفيق من قبل التقنية ذاتها مع كل ما يتم إثباته في هذا الشأن[1].

فقد 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 الجديدة لتكنولوجيات الإعلام والاتصال، وهذا التساؤل يقودنا في الحقيقة إلى الإقرار بأن ظاهرة جديدة برزت لتنضم 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 للدليل هي الدليل الرقمي أو الدليل الإلكتروني، حسبما أطلق عليه المشروع الأوروبي هذا المصطلح[2]، وهذا فعلاً ما قام به المشرع الجزائري محتذيا بذلك بما قامت به التشريعات المقارنة، من تبني وسائل جديدة للبحث والتحري في هذه الجرائم، فإضافة للوسائل التقليدية (التلبس، التفتيش، التسرب، اعتراض المراسلات،... الخ) احتوى قانون 04/09 نظماجديدة للتحري والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من أهمها المراقبة الإلكترونية، بالإضافة إلى تفتيش النظم المعلوماتية وكيفية حجز الدليل الإلكتروني و الحصول على الإدانة الجنائية، أو ما يثبت حقوق العدالة عموماً، سواء حق المجتمع في الإدانة أو حقه أيضاً في ثبوت براءة الشخص المتهم، فالاستعانة بالدليل الرقمي لم تعد محل شك في قيمته كدليل يتواءم مع مفهوم الأدلة التي يعرفها القانون في صيغته التقليدية وذلك لأمر مهم وهو تقنينه بقانون بسبب إدخاله في المنظومة القانونية، وعلى ذلك سوف نتناول بالدراسة مناقشة هذه النقاط فيما يلي:

[1] فتحي محمد أنور عزت، المرجع نفسه، ص 632.

[2] فتحي محمد أنور عزت، المرجع السابق ، ص 633 .

المطلب الأول: مفهوم الدليل الرقمي

يعرف الدليل في اللغة بأنه المرشد، وما يتم به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات[1]، ويعرف الدليل اصطلاحا بأنه " ما يلزم العلم به علم شيء آخر" وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته أو ما يمكن التوصل به إلى معرفة الحقيقة[2].

وقد جاءت كلمة الدليل في القرآن الكريم في قوله تعالى(أَلَمْ تَرَ إِلَىٰ رَبِّكَ كَيْفَ مَدَّ الظِّلَّ وَلَوْ شَاءَ لَجَعَلَهُ سَاكِنًا ثُمَّ جَعَلْنَا الشَّمْسَ عَلَيْهِ دَلِيلًا) (الفرقان الآية 45)، ويستخدم الدليل في الاصطلاح الشرعي بمعنى البينة، والتي تعني بدورها الحجة والبرهان، فمن المتفق عليه لدى الفقهاء أن البينة اسم لكل ما يبين الحق ويظهره[3].

وفي الاصطلاح القانوني تعددت وجهات نظر القانونيين في معنى الدليل، وأهمها التعريف الذي جاء به بعض الخبراء الذين عرفوه بأنه " البرهان القائم على المنطق والعقل في إطار من الشرعية الإجرائية لإثبات صحة افتراض أو لرفع درجة اليقين الإقناعي في واقعة محل خلاف"[4]، وعرفه الدكتور أحمد فتحي سرور بأنه " الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها، والمقصود بالحقيقة في هذا الصدد هو كل ما يتعلق بالوقائع المعروضة عليه لإعمال حكم القانون عليها "[5].

ولكن الدليل في البيئة الرقمية يتميز عن غيره من الأدلة، وذلك لخصوصية الجريمة التي ينتج عنها لذلك فإننا سنتناوله كالتالي:

---

[1]منصور عمر المعايطة، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للنشر والتوزيع ، عمان الأردن، الطبعة الأولى ، 2009، ص 27.

[2]محمد حماد الهيثي، التحقيق الجنائي والأدلة الجرمية، دار المناهج للنشر والتوزيع، عمان الأردن، طبعة أولى، 2010، ص 16.

[3]منصور عمر المعايطة، المرجع السابق، ص 27.

[4]منصور عمر المعايطة، المرجع نفسه، ص 29.

[5]أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1981، ص 373.

الفرع الأول: تعريف الدليل الرقمي.

الفرع الثاني: معايير تقدير الأدلة الرقمية.

الفرع الأول: تعريف الدليل الرقمي

يمكن تعريف الدليل الرقمي،مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها لاستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرائية ويعود تسميتها بالدليل الرقمي لظهورها في شكل أرقام ويتم تحويل هذه الأرقام عند عرضها في شكل مستند ،صور تسجيل[1].

كما عرفته المنظمة العالمية لدليل الكمبيوتر في أكتوبر 2001بأنه: المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية، وقبل ذلك عرفته في سنة 2000بأنه: المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة[2]، ويؤخذ على هذين التعريفين ما يلي:

1- تجاهل التعريف الصادر سنة 2001الجهة التي يستقدم إليها الدليل الرقمي، في حين حدد تعريف مارس 2000هذه الجهة وخصصها في المحكمة.

2- تجاهل تعريف مارس 2000الصيغة التي تم بها تخزين المعلومات في حين حدد تعريف أكتوبر 2001الصيغة الرقمية التي تم تخزين المعلومات بها.

والتعريف الأكثر شمولاً في نظرنا 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 LeDisque Dur، والرسائل الإلكترونية المخزنة أو المنقولة رقميا ".[3]

---

[1] عبد الفتاح بيومي، الحجازي دليل الرقمي والتزوير في جرائم الكمبيوتر والانترانت بهجات للطباعة والتجليد ، مصر 2010.

[2] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009، ص 213.

[3] Mélanie CLEMENT-FONTAINE: Définitions et cadre juridique de la preuve numérique, Colloque du 13/04/2010. La preuve numérique à l'épreuve du litige. Les acteurs du litige à la preuve numérique(l'information numérique fait la preuve), Site de Compagnie nationale des experts

الفرع الثاني: معايير تقدير الأدلة الرقمية (صحة وخطأ الأدلة الرقمية)

حتى يمكن اعتمادها كدليل رقمي يجب أن تتوافر في المعلومة الرقمية معايير دقيقة قبل أن تكون موضوع تفسير تقني يحدد تصنيفها القانوني.

ولكن الدليل في البيئة الرقمية يتميز عن غيره من الأدلة، وذلك لخصوصية الجريمة التي ينتج عنها لذلك فإننا سنتناوله كالتالي:

أولا: المعلومة الرقمية قبل الدليل:

تذكير بخصائص المعلومات الرقمية:

المعلومة الرقمية هي «ESI» Electronically Stored Information أو L'information numérique :

أ- سهلة النسخ: فالموسوعة العالمية Encyclopédie Universalise هي صور يمكن نسخها في دقيقة تقريباً بواسطة USB.

ب – غنية كمياً: لأنه يقدر بأنه 100مليار حزمة إلكترونية تحول يومياً عبر العالم، كما أنَّ الأنظمة الرقمية هي كثيرة إلى أبعد الحدود.

جـ- غنية نوعياً أكثر من الأوراق: ومثال ذلك ميزات أو بيانات تعريف ملف معلوماتي ليس هناك ما يعادلها في عالم الكتابة غير الرقمية.

د – المعلومة الرقمية عطوبة: سواء عن طريق الخطأ أو عمداً .

هـ – المعلومة الرقمية متعلقة قليلاً ببيئتها (الأجهزة، البرامج)، كما لا يمكنها الاستغناء عن هذه البيئة أحيانا، وأحيانا أخرى يكون صعبا استغلالها.

و- هذه المعلومة قابلة للمحو والحذف ولكن ليس بسهولة.

ز – وأخيرا فإن هذه المعلومة الرقمية غير ثابتة، إذ يمكنها أن تظهر على شكل حركي يصعب بذلك إيجادها.

de justice en informatique et associées: www.cnejita.org/.../CNEJITA-ACTESCOLLOQUE13042010-A5-V5.1-pdf.[28/02/2011]

ثانيا: من معلومة رقمية إلى دليل رقمي:

معايير تصنيف المعلومة الرقمية:

معيار الأصالة والصحة يضمن أصل المعلومة، معيار السلامة يضمن محتوى المعلومة، ومعيار التتبع يعني في أي شروط تم فيها نسخ المعلومة، وأخيًارً معيار الاستمرارية يعد كماليا ولكن لا يمكن إهماله وهو مرتبط بالحفظ الجيد للمعلومة. [1]

هذه المعايير هي اختبارات للمعلومة الرقمية لكي تصبح دليلاً رقمياً يقبل في المحكمة لإدانة أو براءة أحدهم، كما أن لها هدفين:

1- تسمح للدليل الرقمي بتأكيد صلاحيته في مواجهة النزاع فيه أو معارضته (رفضه).

2-تسمح أيضا بتنظيم أساليب صالحة للمعارضة أو الطعن في أدلة الطرف الآخر .

1-معيار أصالة الدليل الرقمي (مصداقيته): Critère d'authenticité

وهو معيار ضروري جدًا، والذي حتى بدون حق الوقوع في الخطأ يكون مصير أحدهم معتمدا عليه (بالإدانة أو البراءة) فمثلا : حساب منشأ في موقع الرسائل Lotus Note هو شديد الأمان لأن تسيير بيانات التعريف مقامة على وسائل (إمكانات) التشفير التي تضمن تعريف صاحب الحساب، ولكن على النقيض تعريفات Windows لملفات البيانات(Methadone's) يمكن بسهولة تغييرها سواء عن طريق الخطأ أو عمدا، كذلك طلب بسيط لملف يغير من هذه البيانات التعريفية، وبالتالي تعد هذه البيانات متبخرة جدا، أي لا يمكن الاعتماد عليها كأدلة للتحقيق، وعليه يجب أخذ العديد من الاحتياطات قبل استعمال هذه المعلومات للتأكد بأنه لم يتم تعديلها بطريقة إرادية أو عن طريق الخطأ.[2]

[1] مصطفى محمد موسى، المرجع السابق، ص 213.

[2]Serge MIGAYRON: Critères d'appréciation technique, vraies et fausses preuves numérique, Colloque du 13/04/2010. La preuve numérique à l'épreuve du litige. Les acteurs du litige à la preuve numérique(l'information numérique fait la preuve),.
Site de Compagnie nationale des experts de justice en informatique et associées: www.cnejita.org/.../CNEJITA-ACTESCOLLOQUE13042010-A5-V5.1-pdf.

1- معيار سلامة الدليل الرقمي (صحته): Critère d'intégrité ويعد هذا المعيار أساسي:

في حالة النسخ البسيط لملف، حيث تتوافر آلية تسمى حساب البصمة الرقمية "Hash" مع اللوغارتمية MD5 كمثال التي تسمح بأن يسند إلى ملف أو إلى مجموعة من الملفات سلسلة أحرف أو أرقام وحيدة (نتحدث عن وظيفة في اتجاه وحيد أو نهائي)، في حالة أن الملف تم تعديله ولو قليلاً، فإن بصمته الرقمية تتغير تماما، حتى في حالة ملف بمثل حجم موسوعة عالمية (حوالي 7 ملايين حرف) ففي حالة تغيير حرف واحد فقط (نقطة النهاية غيرت بمسافة) فإن البصمات المحصل عليها مختلفة تماما كالتالي:

Empreinte MD5 avant: A64C0C668E613B5D10B936F6BD2ED75D
Empreinte MD5 après: A616D59F9FC2E2671BB84F3621E41595

يعد هذا اللوغاريتم حساس جداً لكل التغييرات حتى التافهة منها، فلا يمكن حدوث أي خطأ باستعماله.

وفي حالة نسخ دعامة للمعطيات مثل القرص يمكن استعمال العديد من أساليب النسخ: نسخ بسيط أو منطقي يكفي إذا لم نكن نبحث عن ملفات تم محوها (محذوفة)، أو بالمقابل النسخ يتم فيزيائيًا أي (bit à bit) وهو يسمح بالبحث عن بقايا محتملة لملفات محذوفة.[1]

وهكذا هناك العديد من أساليب الكشف عن التغييرات المحتملة في البيانات الرقمية التي يمكن اعتبارها دليًلاً رقميا لجريمة ما، حتى ولو كانت تلك البيانات تخضع لأنظمة معقدة أو متحركة، فإن الخبراء الرقميين يمكنهم تتبعها والكشف عنها.

[1]Serge MIGAYRO, op.cit. Site de Compagnie nationale des experts de justice en informatique et associées: www.cnejita.org/.../CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1-pdf.

3- معيار التتبع: Critère de tractability

معيار التتبع هو معيار مرافق للمعيارين السابقين (أصالة وسلامة الدليل الرقمي) حيث نلاحظ في الأمثلة السابقة ضرورة أن العمليات التي تتم يجب أن توصف بدقة، وهناك أساليب للتتبع سواء يدوية أو آلية، ومثال مبسط لذلك النسخ على قرص ليزر (Gravure d'un CD Rom) يسمح بتوضيح أهمية معيار التتبع:

1- قرص ليزر تم النسخ إليه بنجاح بواسطةGraveur de Windows7 ؛

2-قرص ليزر تم النسخ إليه بنجاح بواسطة Logiciel de graveur specialize - Windows7(Eazy Creator) ،

3-قرص ليزر تم النسخ إليه بواسطة Windows XP؛

4- قرص ليزر تم النسخ إليه بواسطة برنامج Eazy Creator،Windows XP.

إن الملف الذي تم نسخه إلى القرص أنشئ بتاريخ 1 جانفي، تم نسخه إلى الأقراص في 15جانفي، ونلاحظ في كل حالة تواريخ الإنشاء والتعديل للملف المنسوخ في الجدول التالي:

	Onglet General Créé le	Onglet General Modifié le	Onglet Statistiques Créé le	Onglet Genera l Modifié le
Easy Creator Windows7	1er janvier	1er janvier	1er janvier	1er Janvier
Graveur Windows 7	1er janvier	1er janvier	1er janvier	1er Janvier
Easy Creator	1er janvier	1er janvier	1er janvier	1er

Windows XP				Janvier
Graveur Windows XP	15 janvier	1er janvier	1er janvier	1er Janvier

نلاحظ أنه في حالة استعمال ناسخ Windows XP، فإن تاريخ النسخ استعمل كتاريخ لإنشاء الملف، على أنه في باقي الحالات فإن تاريخ إنشاء الملف الأصلي للملف بقي محفوظا، وبالتالي نجد أنه باستعمال ناسخ على القرص CD Rom وبدون العلم بالإجراء المستوجب فإن عرض حالة إنشاء الملف سيكون خاطئا . ولذلك يكون من الضروري مرافقة كل عمليات النسخ للملفات الرقمية بتتبع دقيق[1].

4- معيار الحفظ (الاستمرارية) واستغلال الدليل الرقمي: Critère de conservation

من أجل الحفظ الجيد للأدلة الرقمية يجب الاهتمام بمدة صلاحية الدعامات الرقمية Les supports لحفظ البيانات وهذا الأمر يتعلق بـ: DVD وCD، إذ بمرور الوقت لا يمكن متابعة تسجيل فيديو على CD أو DVD مرت عليه سنوات من الحفظ ليس بسبب البرنامج ولكن بسبب تلف الدعامة المادي التي تكون من هذا النوع، كذلك الأمر بالنسبة لإمكانية استغلال الدليل إذ يجب أن يكون مقروء و واضحا[2].

المطلب الثاني: الطرق التقنية للتحقيق في جرائم تكنولوجيات الإعلام والاتصال

الفرع الأول: تقنيات التحقيق

مهما كان نوع القضية، فالتحقيقات في دعامة معلوماتية تجيب دائما على نفس الإشكالية: تحليل الدليل الرقمي (القرص الصلب، مفتاح USB، بطاقات الذاكرة...) لا يجب أن يتغير خلال العمليات التقنية، وهو يعد تحدٍ مهم لأن أطراف الدعوى بإمكانهم

[1]Serge MIGAYRO, op.cit. Site de Compagnie nationale des experts de justice en informatique et associées:www.cnejita.org/.../CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1-pdf.

[2] إذ أن بعض الملفات تكون إما غير مرئية أو مشفرة مثلا.

اعتباره معيبا لعدم حفظ سلامة الدليل الرقمي، أو للمتهم أن يفند التحقيق التقني للصور غير المشروعة التي وجدت في جهازه في حالة أن بايت واحد (وحدة قياس في المعلوماتية) من الدليل الرقمي قد تغير.

فالتغيرات قد تكون غير عمديه: مثلا يكفي فقط تشغيل الحاسوب في محيط Windows، حتى يتم تغيير العديد من ملفات النظام (تاريخ آخر تعديل مثلا)، وهو ما يدعى " أعراض القارئة المدمرة " في اللغة المعلوماتية، وتجدر الإشارة إلى أنه في حالة التحقيق التقني للبحث عن أدلة رقمية لإدانة أو تبرئة المتهم يجب احترام منهجية الفحص وبصرامة من أجل تجنب أي معارضة لاحقة.

إذن يجب على المحقق عند أي معالجة داخل دعامة معلوماتية إجراء البصمة الرقمية لكامل المعطيات المتواجدة في الدعامة، ويتم حساب بصمة الدعامة عن طريق لوغاريتم رياضي يدعى اللوغاريتم "hache"، فأي تعديل خاص بسلامة الدعامة التي يتم فحصها يؤدي إلى تغيير في قيمة هذه البصمة.[1]

ويمنع أي تشغيل للدعامة التي يتم فحصها داخل نظام تشغيلها، أو أي نظام للتشغيل بدون حماية الكتابة في الدعامة المعلوماتية، وفي حالة الإهمال فيما يخص هذا الأمر يؤدي إلى تعديلات لا يمكن التحكم بها في بعض الملفات، وخاصة في تواريخ التعديل، ومن ثَم تعد قابلة للتلف إذا قام التحقيق بإعادة تشكيل " الجدول الزمني المعلوماتي" للمعني (سواء المتهم أو الضحية)، وفي المرحلة الثانية من الضروري إنشاء نسخة كاملة للدعامة (النسخ "bit àbit") باستعمال جهاز لحماية الكتابة، هذه النسخة بكل الوحدات (les octets) للقرص الصلب تسمح باسترداد المعطيات المتوفرة في الدعامة وكذلك مجموع المعطيات التي تم محوها: أي في حالة محو المعطيات المجرمة من طرف المجرم، فإنها لا تحذف ماديا وإنما "الرابط" بين هذه المعطيات هو من يمحى، فالمعطيات

[1] مصطفى محمد موسى، المرجع السابق، ص 214.

تبقى في ذاكرة الدعامة ويمكن بالتالي إيجاد الملفات المحذوفة عن طريق فحص الهوامش العلوية (les en-têtes) لمختلف الملفات (ملفات الصور، ملفات النصوص...).

وفي الأخير يجب حساب البصمة الرقمية للنسخة المنجزة، وكذلك حساب بصمة رقمية أخرى للدعامة المعلوماتية ذاتها عند انتهاء المعالجة، وتسمح المقارنة بين البصمات الثلاث(البصمة الأولية للدعامة، البصمة المتعلقة بالنسخة، والبصمة النهائية للدعامة) بضمان ما يلي:

– المعالجة التقنية المختلفة تكون على النسخة المنجزة من الدعامة، فلا تغير من سلامة الدعامة: فالدليل الرقمي لا يمكن بكل تأكيد أن يتضرر من عمليات المعالجة.

– قيمة البصمة يمكن مراقبتها بتحقيق لاحق في حالة خبرة مضادة : ومثال ذلك الفحص الجديد للمعطيات يتم تماما بنفس المعطيات التي تم بها الفحص لأول مرة.

– النسخة المنجزة، وبالتالي العمل على المعطيات بها، مع الأخذ في الحسبان أن كل بايت "bit " من الدعامة تم نسخه.

العناصر التي يتم فحصها أثناء التحقيق الرقمي تكون مختلفة بحسب طبيعة الدعامة التي يتم فحصها، وكذلك طبعا لطبيعة القضية، ونقدم مثالين لدعامتين مختلفتين، القرص الصلب لجهاز الحاسوب، وهاتف نقال حيث يتم فحص كل منهما على النحو التالي:[1]

إذا تعلق الأمر بدعامة معلوماتية مثل القرص الصلب لجهاز الحاسوب، يمكن للمحقق القيام بالفحوصات التالية تبعا للأدلة الرقمية التي يجب البحث عنها:

– عرض آثار التصفح عبر الانترنت المخزنة داخل القرص الصلب للحاسوب لاحتمال وجود عناوين مختلفة لمواقع بالانترنت وملفات تمت زيارتها من مستعمل ما، كذلك تواريخ المرتبطة بهذه الزيارات، مجموع هذه العناصر المخزنة داخل الذاكرة المخفية للانترنت يتم رفعها (تحميلها) حالما تتم زيارة موقع الانترنت ويتم تسجيله على القرص

[11] Myriam QUÉMÉNER, Yves CHARPENEL Cybercriminalité, Droit pénal appliqué ،2010 ،ECONOMICA ,Paris France, page.170

الصلب للمستخدم داخل فهرس خاص في النظام، هذه الطريقة للتسجيل في الخفاء تسمح بتسريع الوقت للزيارات الأخرى لنفس الموقع.

– فحص ملفات البريد الالكتروني (الايميل) وملفات السجل للمحادثات عبر البريد الفوري.

– إعادة تشكيل نظام الملفات في حالة البحث عن أدلة داخل دعامة معلوماتية تم إعادة تشكيلها "Formaté " من طرف المتسبب في ذلك.

– استرداد الملفات الممحوة من طرف المعني وإعادة تشكيل هذه الملفات بمساعدة علامات البداية والنهاية للملفات، انطلاقا من منطقة الذاكرة غير المخصصة للدعامة المعلوماتية . [1]

أما إذا تعلق الأمر بالهاتف المحمول، فيتم الفحص على العناصر الثلاث التالية:

– ذاكرة البطاقة SIM.

– ذاكرة الهاتف المحمول.

– الملفات التي يتم تسجيلها من طرف مقدم الخدمة (أرقام المتصلين، والأرقام التي تم الاتصال بها وتواريخها، والبريد الصوتي).

الاستفادة من البطاقة SIM يتم باستعمال قارئ البطاقات الذكية " Carte à puce " وهو برنامج للقارئة، وتسمح هذه العملية باسترداد مجموع الدليل الهاتفي وكذلك الرسائل القصيرة الموجودة والمحذوفة.

الاستفادة من ذاكرة الهاتف المحمول تتم بتشغيل الهاتف ببطاقة SIMللاختبارات ويتم استعمال برنامج خاص بقارئة المعلومات الموجودة في الهاتف (الرسائل القصيرة، الصور، الأفلام...). أما الاستفادة من الملفات المقدمة من طرف مقدمي خدمة الهاتف فيتم

[1] Jean-François TYRODE, Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercrimi-nalité en droit européen, mémoire de master droit de l'Internet-Administration-Entreprises, Université PARIS 1-PANTHEON-SORBONNE, année universitaire 2006-2007,p 22-25. disponible sur www.univparis1.fr/.TYRODE_ MEMOIRE.pdf [03/09/2012].

بمساعدة طلب قضائي للمتعامل من أجل التمكن من الحصول على قائمة الاتصالات المختلفة خلال فترة زمنية تهم التحقيق[1].

الفرع الثاني: أدوات التحقيق

خلال تفحص دعامة معلوماتية فإن المعالجة التي تتم خلالها تؤدي إلى خطر أكيد مع عدم السيطرة يتمثل في تغير المعطيات، وعليه يجب خلال التحقيق القضائي الحفاظ على سلامة الدعامة الموضوعة في أحراز مختومة، بطريقة تثبت أن التحقيقات لم تغير بشكل غير مقصود الأدلة التي يتم بحثها داخل الدعامة، وبالتالي تجنب أي منازعة لاحقة.

ومن الضروري أيضا استعمال برامج خاصة تسمى "bloqueurs en écriture " وتعني تقريبا توقيف الكتابة، فبمجرد وصل أي دعامة يتم فحصها: القرص الصلب ، بطاقة الذاكرة، مفتاح USB، أو بطاقة SIM للقيام بأي إجراء في التحقيق، فإن برنامج وقف الكتابة يسمح بالوقف (verrouiller) المادي ضد أي كتابة أو محو لا إرادي للمعطيات المعلوماتية.

في المجمل أدوات التحقيق تتضمن مجموعة من البرامج و مختلف أجهزة القارئة (lectures)، تقوم مختلف أجهزة الأمن بجلبها أو حتى بصنعها لمساعدتها في مختلف التحقيقات.

المطلب الثالث: المبادئ العامة للأدلة الرقمية

خلف التعقيد التقني الملازم للعالم الرقمي فإن التحريات الخاصة بجرائم هذا العالم تواجه تحد آخر وهو احترام المبادئ الرئيسة للأدلة الجنائية، وبانبثاق إجراءات خاصة

[1]Jean-François TYRODE, Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercrimi-nalité en droit européen, mémoire de master droit de l'Internet-Administration-Entreprises, Université PARIS 1-PANTHEON-SORBONNE, année universitaire 2006-2007,p 22-25. disponible sur www.univparis1.fr/.TYRODE MEMOIRE.pdf [03/09/2012].

للتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال فلا يمكنها أن تحيد عن هذه المبادئ.

إن تطبيق قانون العقوبات على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يصطدم أحيانا بصعوبة إقامة الأدلة، والتي هي خصوصاً متبخرة (Volatiles) ومسألة حفظ المعطيات في هذا الصدد تصبح حاسمة، وبالرغم من هذه الصعوبات فإن تطبيق تلك المبادئ يكون بلا تمييز على جميع أنواع التحقيقات سواء على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أو غيرها.

و إذا كان تقديم الأدلة في المواد الجزائية حر بناء على نص المادة 212 من قانون الإجراءات الجزائية فهي ليست أقل خضوع المراعاة المبادئ التالية التي تفرض التنبه والحيطة في كل وقت من طرف القائمين على الإجراءات الجزائية، فعندما يتحرى العون القضائي (خاصة ضباط وأعوان الشرطة القضائية) عن الدليل فإنه يحترم مبدأي المشروعية والقانونية، وعليه فالمتحرين عن الدليل لا يمكنهم إلا استعمال الأدلة التي في طبيعتها منصوص عليها قانونا وتحترم الحقوق والحريات الأساسية.

وبقدر الضغوط والعراقيل الخاصة التي تمارس على المتحرين في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي هي في تطور تقني وقانوني. في حين أن المجرمين المعلوماتيين لا يتوانون على استعمال آخر ما توصلت إليه تكنولوجيات الإعلام والاتصال، فالمشرع بحاجة إلى فسحة من أجل دمج هذه التطورات ضمن الترسانة القانونية الإجرائية.[1]

كذلك وفي التطبيقات القضائية المقارنة فإن محكمة النقض الفرنسية تحكم قبضتها بقوة على حالات اللجوء لكل تقنيات التحري التي لا تتجاوب مع مقتضيات مبدأي قانونية ومشروعية الدليل، تاركة للمشرع الاهتمام بتعديل . في وقت الحاجة . "الحدود" بين وسائل

[1] مصطفى محمد موسى، المرجع السابق، ص 213.

التحقيق المشروعة أو غير المشروعة[1]، ففي حالة اللجوء إلى دليل ناتج عن جريمة تمت عن طريق تحريض من الشرطة فإن هذا الدليل لا يقبل طبقاً لمبدأ مشروعية الأدلة الجنائية، مع ذلك يلاحظ فقهاء القانون المقارن في فرنسا أن هناك تمييز واقع بين الأدلة المقدمة من طرف ضباط الشرطة القضائية الذين يُفَرَض عليهم جمعها قانونيَاً، وبين تلك الأدلة المقدمة من طرف باقي الأطراف الأخرى في الدعوى الجزائية (المدعي المدني، أو المتهم نفسه) فالغرفة الجنائية بمحكمة النقض الفرنسية[2] أكدت التساهل فيما يتعلق بمبدأ المشروعية بقولها » حيث أنه لا توجد أحكام قانونية لا تسمح للقاضي الجزائي أن يستبعد استعمال أدلة متحصل عليها من شخص قدمه لجهاز التحقيق لسبب واحد، لأنه تم الحصول عليه (الدليل) بطريق غير مشروعة أو غير قانونية،ولأنه يخصه فقط، وبتطبيق المادة 927ق إ ج قدر القاضي قيمته الثبوتية بعد أن أخضعه لمواجهة بين الخصوم، فإن محكمة الاستئناف قد بررت قرارها.

جزاء الإخلاء بالمبدأ:

توضيحا لما يتعلق بالمحافظة على مجال التحقيقات الرقمية واعتبارا للمبادئ الرئيسية للإجراءات الجزائية المستخدمة، فإننا سنورد مثالاً من التطبيقات القضائية المقارنة التي توضح جزاء الإخلال بمبدأ مشروعية الأدلة الجنائية كالتالي:

– أصدرت محكمة النقض الفرنسية قرارا في 04جوان2008[3] انتقدت فيه إجراء تم فيه استغلال معلومات محصلة من طرف السلطات الأمريكية عن تواجد جرائم حبس صور تحوي مواد إباحية للأطفال عن طريق الانترنت (Cyberpédopornographiques)، حيث أنه تم التعرف على مواطن فرنسي بعدما قام بالاتصال بموقع يحوي صور للاستغلال الجنسي للأطفال (Pédophiles)، وبتبليغ من السلطات الأمريكية، أدت هذه الوقائع إلى فتح تحقيق ثم متابعة وإدانة من طرف السلطات القضائية الفرنسية.

[1]Myriam QUÉMÉNER, Yves CHARPENEL Cybercriminalité, Droit pénal appliqué ،2010 ،ECONOMICA ,Paris France, page.171

[2] Crim.27 janvier 2010, pourvoi n° 09-83.395

[3]Cass. Crim, 04 juin2008, bulletin criminel 2008, n° 141.

محكمة النقض الفرنسية لاحظت بأن الموقع المجرم تم إنشاؤه من طرف مصلحة شرطة نيويورك الخاصة بجرائم المعلومات للبحث عن مرتكبي الأفعال من هذا النوع (Pédophiles) عن طريق الانترنت، واعتبرت أن الأدلة المقامة ضد المتهم ليست مشروعة، لأنها وقعت نتيجة تحريض، وهو مبدأ غير مرخص به في القانون الفرنسي.

وبما أن التحريات تمت وفقا : "لخدعة من طرف السلطات الأمريكية لحث المعني لارتكاب الجريمة" فلا يمكن اعتبارها قد راعت مبدأ المشروعية، والمتابعات يتم إلغاؤها بالرغم من تحقق إدانة المتهم بالجرائم التي أخذ عليها[1].

هذه القضية التي أحاطت بمنطق إلزامية احترام مبدأ المشروعية، كما تظهر أهمية خضوع القانون الجزائي السيبيري (للعالم الافتراضيCyber droit pénal) للقواعد التقليدية للإجراءات الجزائية، والاهتمام من أجل مكافحة أفضل للجرائم المتصلة بتكنولوجيات الإعلام والاتصال برصد الأدوات التشريعية الخاصة بها.

المبحث الثاني: طرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن الجرائم المرتكبة عن طريق الشبكة المعلوماتية الانترنت والشبكات الرقمية تتطور بدون توقف مرتبطة بالتطور التكنولوجي.[2]

ومنذ سنة 2006فإن 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:

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit.page.172.
[2] http://fr.wikipedia.org/wiki/surveillance , le 09/07/2011

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

– القانون رقم 04/09 المؤرخ في 05أوت2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، يحوي هذا القانون تدابير مهمة لتدعيم فعالية وسرعة التحريات والتحقيقات الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

وعلاوة على الأدوات المدرجة في قانون الإجراءات الجزائية الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثل اعت ارض 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 السيبرية (المعلوماتية) Cyber-outil في متناول مختلف القائمين على مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فبطبيعة الحال ليس هناك ما يبرر ترك هذه الأدوات في متناول مرتكبي هذه الجرائم.

وقبل التطرق لعناصر هذا المبحث كان أجدر بنا تناول تعريف التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهو ما يعرف بالتحقيق الرقمي، وهو مجموعة الأساليب المتبعة من أجل معرفة وتقديم معطيات مخزنة (الدليل الرقمي) في وسيلة الكترونية ممغنطة أمام جهة قضائية.[1]

وعليه فإن تقسيمنا للمبحث يكون بالبحث:

[1] مصطفى محمد موسى، المرجع السابق، ص 214.

أولا: في مراقبة الاتصالات الالكترونية؛ ثانيا: سنتطرق إلى التفتيش الالكتروني ؛ وثالثا نتناول دور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

المطلب الأول: مراقبة الاتصالات الإلكترونية

المراقبة هي عملية ملاحظة أنشطة الأشخاص أو مجموعة من الأفراد، والرقابة قد تكون خفية أو ظاهرة، وعلى كل حال فإن التكنولوجيات الحديثة للمعلوماتية قدمت نطاقا جديدا لتطبيق الرقابة[1].

أما الاتصالات الالكترونية فقد 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 2 . و من القانون رقم 04/09 فالاتصالات الالكترونية تشمل هنا: الاتصالات السلكية ، أو الخلوية (الهاتف النقال)، الفاكس، البريد الالكتروني، مواقع الدردشة على الانترنت (Face book, MSN, Skype..)، وحتى المنتديات المختلفة وساحات الرأي والنقاش (online forum) التي تسمح بنقل وتبادل الأفكار والمعلومات.

الفرع الأول: مفهوم مراقبة الاتصالات الالكترونية

لم يعرف المشرع الجزائري على غرار العديد من المشرعين عملية مراقبة الاتصالات الالكترونية، ولكن بعض التشريعات قد عرفته مثل التشريع الأمريكي والكندي، فقد عرفها المشرع الأمريكي بأنها » عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز الكتروني أو أي جهاز آخر « المادة 2510 – 4 من قانون الاتصالات الفدرالي الأمريكي لسنة 1968، وطبقا لقانون الاتصالات الالكترونية لسنة 1986أصبح التعريف المذكور يتسع ليشمل الاتصالات الالكترونية الأخرى[2].

وقد وضع الفقه العديد من التعريفات لمراقبة الاتصالات الالكترونية منها:

[1] http://fr.wikipedia.org/wiki/surveillance , le 09/07/2011

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

1- ذهب رأي إلى تعريف المراقبة الالكترونية بأنها تعمد 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 الاتصال السلكية واللاسلكية[1].

2- وذهب أري آخر إلى تعريفها بأنها تعني من ناحية التنصت الاعتراض- interception على المحادثات ومن ناحية أخرى تسجيلها enregistrement بأجهزة التسجيل ويكفي لمباشرة إحدى هاتين العمليتين(التنصت أو التسجيل) لقيام المراقبة[2].

3- 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 ينصب على أي حديث شخصي يكون للإنسان مع غيره، ويكون له صفة شخصية، كما ينصب على المكالمات التلفونية ليشمل المكالمات اللاسلكية أيضا ويتم هذا الإجراء بغرض 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: [1] استراق السمع وهو يقع على الأحاديث الشخصية والمكالمات السلكية واللاسلكية التي يجريها الأفراد [2] أن يتم استراق السمع خفية دون علم صاحب الحديث، وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة التي أسفر عنها النشاط العلمي المعاصر[3] أن يكون استراق السمع لهذه الأحاديث بغرض تقديم دليل يصلح للإثبات في الدعاوى والتحقيقات[3] .

4- ويمكن تعريف المراقبة بأنها إجراء تحقيق يباشر خلسة، وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانون بهدف الحصول على دليل

---

[1]عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية،و199، ص 404، مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 139.

[2]محمد أبو العلا عقيدة، مراقبة المحادثات التليفونية دراسة مقارنة، دار الفكر العربي، 1994، ص 15، مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 139.

[3]أحمد محمد حسان، نحو نظرية عامة لحماية الحق في الحياة الخاصة، دار النهضة العربية، 2001، ص 141، مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 141.

غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع إلى الحديث، ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك[1]. التعريفات السابقة أوضحت مضمون المراقبة فهي تعني من ناحية التنصت ومن ناحية أخرى التسجيل، كما أشارت هذه التعريفات إلى محل المراقبة وهي الأحاديث الشخصية والمحادثات السلكية واللاسلكية، فضلا عن ذلك فقد بينت بعض التعريفات ضرورة حصول التنصت أو التسجيل خلسة دون علم صاحب الحديث وبواسطة إحدى الوسائل أو الأدوات العلمية الحديثة، وأفصحت بعض هذه التعريفات عن الغرض من المراقبة وهو الحصول على دليل غير مادي يصلح للإثبات في الدعاوى والتحقيقات، كما تناولت الطابع القانوني للمراقبة والذي يكون بإذن مسبق من طرف السلطة القضائية، إلا أنه يؤخذ عليها أنها حددت الغرض من المراقبة على الحصول على دليل لجريمة وقعت بالفعل وهو الأمر الذي يتنافى مع الهدف الحقيقي من المراقبة وهو الوقاية من الجرائم التي يمكن ارتكابها وهي محددة على سبيل الحصر في القانون ومن بينها الإرهاب واحتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني (القانون 04/09 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

5- ومراقبة الاتصالات الالكترونية هو إجراء خاص يتم بإشراف قضائي بحسب الحالات، وتعرف بأنها تقنية تقوم على تدخل وسطي لتحويل مسار في خط مشتِرك بوسيلة ممغنطة، من أجل التسجيل والمحادثة، وهي تمثل فائدة أكيدة لفاعلية المتابعات الجزائية[2].

[1] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، الطبعة الأولى، 2009، ص 150.

[2] Myriam QUÉMÉNER, Yves CHARPENEL,op. cit, page 174.

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

وهذا الإجراء ليس جديدا على المنظومة القانونية الإجرائية الجزائية، فقد نص عليه المشرع قبلا في قانون الإجراءات الجزائية في الفصل المتعلق باعت ارض المراسلات وتسجيل الأصوات والتقاط الصور(المواد من 65 مكرر إلى غاية المادة 65 مكرر 10 من ق إ ج)، ولكنه قصر 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 المادة 65 مكرر 5 من ق إ ج، وعليه بالنص على مراقبة الاتصالات الالكترونية في القانون 04/09 فإن المشرع قد أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني لاستكمال التحريات أو التحقيقات حتى في جرائم تقليدية إن صح قول ذلك، ومثال ذلك: جريمة الزنا المنصوص عليها في المادة 339 من قانون العقوبات حيث يمكن إثباتها حتى برسالة الكترونية في بريد المتهم الالكتروني كإثبات تقبله المحكمة.[1]

[1] وهي تختلف عن التفتيش الوقائي الذي لا يعّدّ قضائيا لأنه غير مسبوق بإذن قضائي وهو يقع صحيحا ويرتب آثاره القانونية، وتبرره حالة التلبس الظاهرة، ومثال ذلك تفتيش المسافرين قبل ركوبهم الطائرة تأمينا لسلامة الطائرات وركابها، فهو لا يستهدف ضبط أشياء تفيد التحقيق في جريمة وقعت بالفعل، بل يجد هذا التفتيش مشروعيته في حالات استثنائية تبرره ويحتمل فيها أن تكشف عن جريمة، وينحصر هدفه في التحري عن "جريمة محتملة"ومثال ذلك التفتيش الإداري لأعوان الجمارك بتفتيشهم للمسافرين.أنظر في ذلك سليمان عبد المنعم، أصول الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2008، ص 670.

الفرع الثاني: حالات اللجوء إلى المراقبة الالكترونية

يمكن اللجوء إلى المراقبة الالكترونية إذا توافرت إحدى الحالات التالية:

أ- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة (المادة 4 من القانون 04/09): والمراقبة الوقائية كمبدأ عام لا تطبق على متابعة قضائية لجريمة مرتكبة، ولكن تخص كشف خطر أو تهديد لأمن الدول، وتشمل البحث عن المعلومات السياسية، الاقتصادية والعسكرية، والشخص الذي يخضع لهذا الإجراء التقني ليس موضوع إجراءات قضائية، ولا يمكنه التمتع بحقوق الدفاع التي يتمتع بها المتهم في مفهوم قانون الإجراءات الجزائية، فهذا الشخص ليس في أغلب الأحيان مشتبه فيه لارتكاب جريمة في مفهوم قانون العقوبات ولكن شخصه أو نشاطاته يُمكن أن تمثل خطرا على الأمن الداخلي[1]. وعليه فإن هذه الجرائم لم ترتكب ولكن المشرع سمح في إطار الوقاية من هذه الجرائم بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص 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، و إنما مجرد الشكوك ولو بسيطة، فالوقاية لا تفترض القيام بأعمال تحضيرية لارتكاب هذه الأفعال و إنما مجرد تكهنات أو حتى دلائل بسيطة قد توحي بأن هؤلاء الأشخاص يمكنهم ارتكاب تلك الأفعال.

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

[1] Suisse« Nouvelles technologies et droit », voir l'article " La surveillance préventive en Suisse: les moyens techniques",
http://ntdroit.wordpress.com,

ب–في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني: واحتمال اكتشاف جريمة قبل وقوعها وخاصة بنوع 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، فكيف عن هذا الاحتمال الوارد في نص المادة 4 فقرة ب من القانون 04/09، و إن 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 اللّجوء إلى مراقبة الاتصالات الالكترونية.

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

الفرع الثالث: العمليات الإجرائية[1]

هناك نوعان من الإجراءات الُمطبقة على مراقبة الاتصالات الالكترونية حددها المشرع باعتبار نوع الجرائم التي يتم مراقبة مرتكبيها:

الأحكام العامة: المنصوص عليها في قانون الإجراءات الجزائية المتعلقة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، تطبق على الحالات: ب، ج، د من المادة 4 بما أن المشرع لم ينص على قواعد خاصة بها ليتم منح الإذن بمراقبة اتصالات شخص أو مجموعة من الأشخاص نظرا لخطورة هذا الإجراء وما يرتبه من نتائج متعلقة بالمساس بحق عدم التعرض للحياة الخاصة للأفراد إلا بإذن مكتوب من السلطات القضائية، حيث أن المادة 3 من قانون 04/09 صّرحت بأنه "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**

[1] Myriam QUÉMÉNER, Yves CHARPENEL,op. cit, page 173.

قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها "، وعليه فإن الحالات التي لم يرد بشأن تنظيمها، قواعد و إجراءات معينة يتم بواسطتها الترخيص بمراقبة الاتصالات الالكترونية فهي بالتالي تخضع لأحكام قانون الإجراءات الجزائية وفقا لصريح نص المادة 3 المذكورة آنفا، وهي تكون كالتالي:

أولا: الجرائم المعنية والعمليات الإجرائية:

أ-**الجرائم التي يطبق عليها الإجراء**[1]:

1- الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 5 كالتالي:

جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد،

2- في الفقرات ب، ج ، د من المادة 4 من قانون 04/09 لم يحدد المشرع الجرائم الخاضعة للمراقبة الالكترونية سوى تلك الاعتداءات على منظومة معلوماتية تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني (الفقرة ب من المادة 4)، وكذلك لم يحدد المشرع نوع الجرائم التي يصعب الوصول في التحريات والتحقيقات القضائية الجارية في شأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى هذه المراقبة ، وبالتالي فإن جميع جرائم القانون العام يمكن أن يلجأ فيها المحقق لهذه المراقبة في حالة ضرورتها.

ونلاحظ تراجع المشرع عن حصر الجرائم التي يمكن اللجوء فيها إلى المراقبة الالكترونية والتي تشمل اعتراض المراسلات بكل أنواعها.

ب- نوعية العملية أو الإجراء: وتتمثل في:

[1] الحقوق الجزائية، محاضرة الأستاذة طالبي حليمة في مقياس قانون الإجراءات المقدمة لطلاب السنة أولى ماجستير، دفعة 2009 – 2010 كلية والعلوم السياسية، قسم الحقوق، جامعة ورقلة، يوم الأحد 22نوفمبر 2009.

– اعتراض المراسلات بواسطة وسائل الاتصال السلكية واللاسلكية

– التقاط الصور في الأماكن الخاصة

– تسجيل الكلام أو الأصوات (أو تثبيتها أو البث فيها) بصفة خاصة أو سرية في الأماكن العمومية أو الخاصة.

– ثانيا: الإذن

أ– الجهة القضائية وضرورة الإجراء: إذا اقتضت ضرورة التحري في الجرائم المتلبس بها أو التحقيق الأولي (مرحلة جمع الاستدلالات) أو التحقيق القضائي (التحقيق الابتدائي) يجوز للقاضي على مستوى اختصاصه (نيابة أو قاضي تحقيق) أن يأذن بإجراء اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، وتتم هذه العملية تحت المراقبة المباشرة للقاضي المكلف بالملف (وكيل الجمهورية أو قاضي التحقيق)[1].

ب– العناصر التي يتضمنها الإذن: يشترط في الإذن تحديد العناصر التالية لشرعيته (شرعية الإجراء):

– التعريف بالعملية: الاتصالات المطلوب اعتراضها وتسجيلها أو الصور التي يتم التقاطها

– الأماكن المقصودة (سكنية أو غير سكنية)

– طبيعة الجريمة التي تبرر الإجراء: كالجرائم المذكورة، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تبطل الإجراءات العارضة.

– شكل الإذن ومدته: يسلم مكتوبا ولمدة أربعة أشهر قابلة للتجديد عند الضرورة، ويسمح بالدخول للأماكن السكنية أو غير السكنية في أي مواعيد (خارج تلك المحددة في

[1] الحقوق الجزائية، محاضرة الأستاذة طالبي حليمة في مقياس قانون الإجراءات المقدمة لطلاب السنة أولى ماجستير، دفعة 2009 – 2010 كلية والعلوم السياسية، قسم الحقوق، جامعة ورقلة، يوم الأحد 22نوفمبر 2009.

الشريعة العامة بموجب المادة 47 ق إ ج)، وبغير رضا أو علم أصحاب الأماكن خلافا للشريعة العامة.

ثالثا: الإجراءات

أ- **سرية الإجراءات وكتمان سر المهنة:** تنفذ العملية المأذون بها بسرية ويتم مباشرة الإجراء من جهة دون علم أو رضا الشخص أو الأشخاص المعنية بها أو صاحب الأماكن، ومن جهة أخرى دون المساس بالسر المهني المقرر بنص المادة 45 فقرة 4 من ق إ ج.

ب- **التسخير:** يجوز لوكيل الجمهورية أو قاضي التحقيق أو لضابط الشرطة القضائية (المأذون له من وكيل الجمهورية أو بناء على إنابة قضائية من قاضي التحقيق) أن يسخر كل عون مؤهل لدى أي مصلحة عامة أو خاصة (وحدة أو هيئة ..) مكلفة بالاتصالات السلكية أو اللاسلكية من أجل تكليف هذا العون بالجوانب التقنية للعملية المراد القيام بها.

ج- **المحاضر:** يحرر الشخص المكلف بالعملية محضرا يحتوي على كل العناصر الجوهرية : التاريخ، ساعات بداية العملية ونهايتها، مع نسخ المراسلات والصور...تسجيل المحادثات المفيدة لإظهار الحقيقة وعند الضرورة اللجوء إلى مترجم.

ويوضع هذا المحضر بين أوراق ملف الدعوى أمام القاضي المكلف به (وكيل الجمهورية أو قاضي التحقيق).

د- **حدود استعمال المعطيات المتحصل عليها:** إن المعطيات التي يتم الحصول عليها عن طريق مراقبة الاتصالات الالكترونية لا تستعمل إلاَّ في الحدود الضرورية للتحريات والتحقيقات القضائية تحت طائلة العقوبات المنصوص عليها في قانون العقوبات (المادة 9 من القانون 04/09).

– لا يعد اعتراض المراسلات بمفهوم المادة 65 مكرر 5 من قانون الإجراءات الجزائية واقعة الاتصال بالشبكة الرقمية وبدون اللجوء إلى تعديلات مسبقة في البرنامج المراقب، قارئة ما يستطيع أي مستعمل قراءته.[1]

حكم المادة 4 فقرة 3 من القانون 04/09: وهي الأحكام المتعلقة بحالة اللجوء إلى المراقبة الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة (الحالة أ):

أ– **الإذن:** يقدم الإذن بناء على تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها، وتكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في هذه الحالة موجهة حصرا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

ب– **الجهة المختصة بتقديم الإذن:** حصر المشرع النائب العام لدى مجلس قضاء الجزائر بتقديم هذا الإذن لخطورة الإجراء المتمثل في الوقاية من تلك الجرائم المحددة على سبيل الحصر في نص المادة 4 فقرة أ المذكورة آنفا.

أ– يباشر عملية المراقبة على سبيل الحصر ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته دون غيرهم من ضباط الشرطة القضائية على المستوى الوطني.

ب– مدة الإذن حددها المشرع ب ستة (6) أشهر قابلة للتجديد.

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

المطلب الثاني: تفتيش المنظومات المعلوماتية:

ونتناول فيه ما يلي:

الفرع الأول: المفاهيم الأولية

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

فقد نصت المادة 05 فقرة 01 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.

أما بالنسبة للمنظومة المعلوماتية فقد عرفها المشرع في المادة 02 فقرة (ب) بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين[2] ولتيسير هذا المفهوم يجب أن

[1] مروك نصر الدين، المرجع السابق، ص 337.

[2] أوضحت المذكرة التفسيرية لاتفاقية بودابست أن المقصود بالنظام المعلوماتي: هو جهاز يتكون من مكونات مادية (Hard MatérielWard)، ومكونات منطقية Logiciel (Software) وذلك بغرض المعالجة الآلية للبيانات الرقمية وهو يشمل وسائل لإدخال Des Moyennes d'acquisition وإخراج وتخزين De stockage البيانات Les données،Data وهذا الجهاز قد

نتطرق إيجازا لأمرين هما التعرف على مكونات الحاسب الآلي ثم نتناول الشبكات التقنية الإلكترونية التي تربط الحواسيب ببعضها.

أولا: مكونات الحاسب الآلي الرقمي: تنقسم مكونات الحاسب الآلي إلى أجهزة وبرامج :

* **الأجهزة:** يشمل نظام الحاسب الآلي الرقمي المتكامل على وحدة نظام وملاحق خارجية

أ- وحدة النظام التي تحوي وحدة المعالج Processeur والذي به تنفذ الأوامر التي يطلب من الحاسب القيام بها، وهي إما أن تكون أوامر رياضية كعمليات الجمع والطرح، والمعادلات الرياضية الأكثر تعقيدا، أو أوامر منطقية كاختبار محتويات حقل معين لمعرفة هل هو أقل من، أو أكثر من حقل ثان، وتتم كتابة الأوامر المطلوب من الحاسب تنفيذها في شكل برنامج يكتب بإحدى لغات الحاسب (C) (Java) (Basic) ويخزن البرنامج في وحدات التخزين، وعند تشغيله يقوم نظام التشغيل بنقل نسخة منها إلى الذاكرة الإلكترونية والتي تقوم بدورها بنقل أوامر البرنامج واحداً تلوى الآخر إلى المعالج لكي ينفذها.

- وحدة الحاسب والمنطق: وتقوم بتنفيذ كل العمليات الحسابية والمنطقية على البيانات الواردة إليها.

- وحدة التحكم Unité du Contrôle وهي تتحكم في تدفق البيانات بين أجهزة الحاسب والتنسيق بينها وتتحكم في عملية الإدخال والإخراج.

- الذاكرة العشوائية: تستخدم للتخزين المؤقت للبرامج والبيانات قيد الاستخدام.

- القرص الثابت: الذي يتولى مهمة التخزين الرئيسي للنظام، حيث أن نظام التشغيل وملفات البرامج والبيانات تخزن في القرص الثابت (الصلب). [1]

ب- الملحقات الخارجية هي أدوات الإدخال، لوحة المفاتيح، الفأرة، الماسح الضوئي، وأدوات الإخراج: شاشة الحاسب، الطابعات... الخ.

يكون منفردا أو متصلاً بمجموعة من الأجهزة المماثلة عن طريق الشبكة Les réseaux. وكلمة آلية Automatisée تعني دون تدخل بشري، ومعالجة البيانات Traitement des données تعني مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي Un programme informatique، الأمن المعلوماتي،طارق إبراهيم الدسوقي، ص 45.

[1] مروك نصر الدين، المرجع السابق، ص 337.

* **البرامج:** وهي نوعان،برامج نظم التشغيل والبرامج التطبيقية

برامج نظم التشغيل: هذه البرامج تتحكم في سمات عمليات الحاسب والتي تتضمن استقبال وإخراج المعلومات والتحكم في الذاكرة والتخزين، وإدارة التطبيقات ومثال ذلك نظام التشغيل Microsoft Windows

برامج التطبيقات: وهي برامج مصممة لأداء وظيفة معينة مثل معالجة النصوص أو إدارة قاعدة البيانات:

وتستخدم قاعدة البيانات مجموعات البيانات على الحواسيب، كما يستخدم لمتابعة وإدارة عمليات الاتصال، التحكم في المخازن إلى غيرها من الوظائف المختلفة بحسب الأداء الذي أصدرت من أجله. [1]

ثانيا: الشبكات التقنية الإلكترونية

وهي تلك الشبكات التي تربط الحواسيب فيما بينها وهي ثلاث أنواع: الانترنت، الانترانت، وكالإكسترانت؛ فالأولى أي الانترنت هي من الشبكات الواسعة النطاق، أما الثانية والثالثة فهي تعد شبكات محلية لها أدوار وظيفية معينة.

شبكة الانترانت: وهي عبارة عن شبكة من الحاسبات الآلية الرقمية الخاصة بمؤسسة ما (المصارف والبنوك مثلاً، وشركات التامين)، تمكن شبكات الانترانت الأشخاص العاملين في نفس المؤسسة بالاتصال ببعضهم البعض والوصول إلى المعلومات بطريقة أسرع وأفضل وأكثر كفاءة وأقل تكلفة من الأساليب التقليدية المعتادة، فمن خلال الانترانت من إنجاز الاجتماعات وتحضير المذكرات وإرسال البريد.

تعتبر الانترانت نسخة مصغرة من الانترنت تعمل داخل المؤسسة ولا يمكن لأحد الوصول إليها إلا لمن يعمل داخل المؤسسة ولديه كلمة السر للدخول إلى الانترانت

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، مصر، الطبعة الأولى 2009 ، ص 75.

الخاصة بهذه المؤسسة، وفي نفس الوقت لا يمنع هذا النوع من الشبكات من التواصل بشبكات أوسع نطاق منها كالإكسترانت أو الانترنت.[1]

شبكة الإكسترانت: وهي عبارة عن شبكات من الحاسبات الآلية الرقمية خاصة بعدة مؤسسات (مجموعة مصارف مثلاً) وعليه تعتبر الإكسترانت نسخة مصغرة من الانترنت تعمل داخل عدة مؤسسات ولا يمكن لأحد الوصول إليها إلا لمن يعمل ويتعامل مع إحدى هذه المؤسسات ولديه كلمة السر للدخول إليها.

الانترنت: وهي شبكة عالمية للاتصال عن بعد تربط الملايين من أجهزة الحاسوب المرتبطة والمتناثرة بشتى بقاع الأرض، من خلال خطوط وتقنيات الاتصال عن بعد، كالخطوط الهاتفية أو الأقمار الصناعية أو الألياف الضوئية، يستخدمها الأفراد والمؤسسات للتواصل وتبادل المعلومات وإنجاز المعاملات بصورة لحظية على مدار الساعة، وتوفر خدمات عديدة من أجل ذلك، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الانترنت.

وتعتبر الانترنت شبكة ذات نطاق دولي تتألف من شبكات متصلة فيما بينها وتوفر لملايين المستخدمين معلومات مختلفة في شكل نصوص أو أصوات أو صور أو رسوم... الخ. ومن جهة أخرى تعد الانترنت شبكة مفتوحة ذات امتداد عالمي فضلا عن كونها شبكة إعلامية وتفاعلية تحولت من كونها "سوق للأفكار" إلى "سوق تجاري".[2]

تؤمن شبكة الانترنت مجموعة من الخدمات تتمثل في:

1- خدمات الاتصال؛

2- خدمات التجارة الإلكترونية؛

3- شبكة الويب العالمية؛

4- البريد الإلكتروني؛

---

[1] مصطفى محمد موسى، المرجع السابق ، ص 75.

[2] فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، طبعة 2010، ص 33.

5- منتديات المحادثة؛

6- خدمات تبادل الأخبار والمناقشة؛

7- خدمة نقل الملفات.

الفرع الثاني: حالات اللجوء إلى تفتيش النظم المعلوماتية و إجراءات تفتيشها

أولا: حالات تفتيش النظم المعلوماتية:

بحسب نص المادة 05 من قانون 04/09 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ فإن حالات اللجوء إلى تفتيش النظم المعلوماتية هي نفسها الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية للاتصالات، وهما الحالتين المتعلقتين بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب 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 الاقتصاد الوطني. فالتفتيش هنا وخلافاً 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 ارتكاب 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 – جناية أو جنحة – واقعة بالفعل وترجح نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية "[1].

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

[1] طارق إبراهيم الدسوقي عطية ، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية ، دار الجامعة الجديدة، مصر، 2009 ، صفحة 396. (نقض 16أكتوبر 1967، مجموعة أحكام النقض ، س 18رقم 195ص 965).

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 طبقاً لنص المادة 05 فقرة 01 من قانون 04/09 أجازت التفتيش بقصد الوقاية من جرائم حددها المشرع لم ترتكب ولكن تعد أسلوبا وقائيا فقط، وهو ما يعد اعتداء فعلي على الحياة الخاصة للأشخاص لان 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 الأوروبية، فالكثير منها (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 القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تفتيش هذه المنظومة المعلوماتية.

- وأخيرا حالة تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ثانيا: إجراءات تفتيش نظم المعلوماتية:

أ - إذن التفتيش:

لم ينص المشرع في المادة 5 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[1] الأولية كما هو الحال بالنسبة لمراقبة

[1] مروك نصر الدين، المرجع السابق، ص 338.

الاتصالات الالكترونية، حيث أن المشرع نص صراحة على وجوب 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 أنهم ساهموا في الجناية أو أنهم يحوزون أوراق أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش لا يكون إلا بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر 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 44إلى 47 من ق إ ج فيما يخص التحريات الأولية 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).

ومع وجوب أن يتضمن إذن التفتيش بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان (المادة 44 الفقرة 03 ق إ ج).[1]

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

ب- التفتيش عن بعد :

قضت المادة 05 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على: " إمكانية الدخول بغرض

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

التفتيش إلى منظومة معلوماتية ولو عن بعد "، فماذا قصد المشرع بالتفتيش عن بعد للنظم المعلوماتية؟

لم يعرف المشرع هذا المفهوم الجديد الذي يحمل في طياته الكثير وإن كانت قاعدة عدم التوسع في التفسير فيما يخص قواعد القانون الجنائي تفرض علينا عدم الإسهاب في هذا الموضوع، ولكننا سنحاول تقديم مفهوم قريب بحسب ما تم الوصول إليه في الأنظمة المقارنة.

وعليه فإن التفتيش عن بعد قد يحوي المفهومين التاليين:

المفهوم الأول: التفتيش عن بعد الذي نصت عليه الفقرة الثانية من المادة 05 والتي قضت بأنه: " في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقاً من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك ."

فقد صرحت المادة 05 الفقرة 02 بإمكانية الدخول إلى منظومة معلوماتية موجودة على جهاز آخر متصل بالجهاز الأول ولكن في مكان مختلف تماماً عنه داخل الدولة ومتصلان فيما بينهما بشبكة اتصالات أيا كانت، يمكن الدخول إلى هذه المنظومة سواء كان الجهاز الثاني ملك للمتهم أو لشخص آخر فلا فرق، ما دامت هناك دلائل على إمكانية وجود المعطيات المبحوث عنها في ذلك النظام، وعليه فإن التفتيش عن بعد في هذه الفرضية يقتضي: [1]

1- وجود دلائل أو أسباب تدعو للاعتقاد بأن الكشف عن المعطيات يكون بالبحث في المنظومة الثانية.

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق ، صفحة 397 .

2- إعلام السلطة القضائية: فلم يفرض المشرع طلب إذن ثان يسمح بهذا التفتيش وإنما مجرد إعلام السلطة القضائية التي تولت أمر هذا التفتيش (وكيل الجمهورية، أو قاضي التحقيق بحسب الحالة).

المفهوم الثاني: والذي نراه مرجحاً لأن المادة 05 في فقرتها الأولى نصت ".. ولو عن بعد " قبل ذكر الأنظمة التي يمكن تفتيشها، ثم تناولت حالة اتصال الحاسوبين وإمكانية الدخول إلى النظام الثاني، فما كان على المشرع سوى أن يذكر هذا الأمر دون تناوله مسبقا، فقد قدم المشرع في هذه الحالة إمكانية تفتيش المنظومة المعلوماتية عن بعد على سبيل التفتيش الوقائي أو التفتيش الافتراضي (La perquisition en ligne, Cyber perquisition) وهو يختلف عن مراقبة الاتصالات الإلكترونية من حيث التقنية، فالمراقبة تعني اعتراض المراسلات (E-Mail, SMS، غرف الدردشة) وكشف محتواها بدون الدخول إلى النظام المعلوماتي للجهاز الذي يتم مراقبته، أما التفتيش عن بعد فهو يتم عن طريق برنامج تجسس (حصان طروادة) يسمح بالولوج للنظام المعلوماتي المستهدف ومعرفة كلما يحصل فيه من عمليات (تسجيل البيانات، الحفظ، تحويل...) وكأن المراقب يشاهد ما يشاهدها لشخص المعني بالتفتيش على جهازه[1].وهذا يعد أمر خطير لأنه يمس مباشرة بالحياة الخاصة بالأشخاص بما تحويه تلك الأنظمة من بيانات شخصية قد لا تهم أبدا في التحقيقات والتحريات التي تتم، فما كان على المشرع أن يطلق هذه المادة على هذا النحو، وإنما كان عليه أن يحدد ما يريده بالضبط. لأنه بالنظر للمادة 04 من قانون 04/09 الخاصة بمراقبة الاتصالات الإلكترونية فقد أعطى المشرع ضمانات كافية تسمح بعدم تجاوز سلطات الضبط القضائي اختصاصها وخاصة في حالة المراقبة الوقائية، فالرقابة فيها لا تتم إلا بواسطة ضباط الشرطة القضائية المنتمين إلى هيئة الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ويتم تقديم الإذن حصرا من طرف النائب العام لمجلس قضاء الجزائر العاصمة، وأعتقد أن هذا يعد ضمانا كافيا لحماية الحياة الخاصة للأشخاص لعدم

التوسع في المراقبة: سواء من حيث الاختصاص أو من حيث السلطة التي تسمح بهذا الإجراء.[1]

وهذا ما لا نجده في تفتيش المنظومات المعلوماتية والتي تعد الآن وفي كثير من الأحيان مذكرات للحياة اليومية للأفراد، فالكثير من الأشخاص يضعون في أجهزتهم صورهم، أفكارهم، ومعتقداتهم يناقشونها عبر الانترنت سواء مع العائلة أو الأصدقاء أو حتى عن طريق غرف الدردشة (Chat) ولكن لا يصل بهم الأمر لأن يكونوا مخططي جرائم، كما نلاحظ في القانون المقارن التفتيش عن بعد لا يمكن أن يكون وقائيا وإنما يتم فقط كتحريات أو تحقيقات لجرائم معينة على درجة من الخطورة قد ارتكبت فعلا أو لوجود دلائل أو احتمالات قوية تهدد الأمن الوطني.

جـ- حالة وجود معطيات مبحوث عنها يمكن الدخول إليها انطلاقا من المنظومة الأولى ولكن مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني: وهي الحالة التي نصت عليها المادة 05 فقرة 03 من قانون 04/09 فإن كان الأمر كذلك فلا يمكن تفتيش تلك المنظومة وإنما يجب الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، فبالرغم من إمكانية تفتيشها من الناحية الفنية داخل النطاق الإقليمي، إلا أن ذلك لا يتم إلا بعد موافقة الطرف الأجنبي، وهو أمر متعلق بسيادة الدول على أراضيها وهذا يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإلكتروني.

و يجدر التنبيه أنه يمكن بناء على اتفاقيات دولية ثنائية أو متعددة الأطراف السماح بتفتيش نظم المعلوماتية خارج إقليم الدولة وبدون إذن الدولة المعنية الطرف في الاتفاقية، ولكن بالطبع في حدود معينة يسمح بها التعاون الدولي ووفقا لمبدأ المعاملة بالمثل بين

[1] طارق إبراهيم الدسوقي عطية ، المرجع السابق ، صفحة 398 .

أطراف الاتفاقية الدولية[1]، من أجل معرفة المعطيات الموجودة في خادم موجود بالخارج؛ فإن فتح تحقيق قضائي يسمح بتحرير إنابة قضائية دولية يمكن أن يتم اللجوء إليها، تمثل في غالب الأحيان عقبة وقتية للحصول عليها، وفي هذه الحال يمكن للمجرم المعلوماتي أن يستغل هذا الوقت لنقل وإخفاء المعطيات.

د – **التسخير**: (المادة 05 فقرة 04 من قانون 04/09والمادة 49 من ق إ ج) من أجل جمع عناصر الدليل الرقمي، فإن القضاة (وكيل الجمهورية، 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 به بنفسه لنقص الوسائل أو لانعدام الاختصاص التقني الضروري.

1– في الجنايات والجنح المتلبس بها: لضابط الشرطة القضائية إن اقتضى الأمر ذلك أن 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 يتأتى ذلك إلا بالاستعانة بأهل الخبرة والمعرفة التقنية.

2– التحريات الأولية والتحقيق القضائي: بناء على نص المادة 05 فقرة 04 من قانون 04/09 يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو باتخاذ التدابير اللازمة لحماية المعطيات المعلوماتية التي تتضمنها، فالتسخير يتم من طرف السلطات المكلفة بالتفتيش: ضابط الشرطة القضائية بإذن من قاضي التحقيق أو وكيل الجمهورية، لأشخاص سواء من القطاع العام أو

[1] المادة 32من الاتفاقية الأوروبية بشأن الجرائم المعلوماتية التي أعدها المجلس الأوروبي وتم التوقيع عليها في بودبست في 2001/11/23 إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: "الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور والثانية إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش، أنظر خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص206.

الخاص لهم إطلاع كاف بتكنولوجيات الإعلام والاتصال، وقد حدد المشرع هذا الإطلاع على نحو:

– دراية المسخر بعمل المنظومة المعلوماتية.

– دراية المسخر بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها المنظومة المعلوماتية.[1]

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

الفرع الثالث: حجز المعطيات المعلوماتية

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 تحديد من يقع عليه الضبط ومن يقوم بالضبط.

ويمكن أيضاً تعريف الضبط بأنه: العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة، والضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوافر فيه نفس القواعد التي تنطبق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط[2].

ويترتب على هذا الارتباط بين التفتيش والضبط؛ أن الضبط لا يجوز أن يقع على شيء إلا وصفه دليلا من أدلة الجريمة التي يجري التفتيش بشأنها، ولذلك فإنه يباشر من أجل الحقيقة المطلقة، بمعنى أنه ما دام التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبط ما يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة، لأن ما يضبط في الحالتين يحقق العدالة الجنائية، لذلك يقول فوستان هيلي: " إنه لما كان التفتيش يباشر

[1] فوستان هيلي – الجزء الثالث – فقرة 1257، ص 499، منقول عن مصطفى محمد موسى، المرجع السابق ص:208.

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

للكشف عن الحقيقة، سواء كان في إدانة المتهم أو براءته فإنه ينبغي ألا يقتصر الضبط على الأشياء التي تؤدي إلى إدانة المتهم دون غيرها، بل أنه يتعين أن ينصب أيضا على الأشياء التي تفيد الحقيقة أيّاً كانت وإن أدت إلى تبرئة المتهم ".[1]

وما يلاحظ بالنسبة لضبط الأدلة الرقمية في قانون 04/09 هو استعماله لمصطلح 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 الحقيقة.[2]

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

الحجز يشمل المعطيات التي يمكن الدخول إليها أثناء التفتيش في القرص الصلب، وفي جميع الحالات فإن حجز المعطيات يتم بوضع يد القضاء عليها سواء الدعائم المادية، وسواء نسخة عنها بحضور الأشخاص الحاضرين في التفتيش (المادة 84 فقرة 03 ق إ ج).

ومن المناسب كنتيجة، تنسيق إجراءات حجز واستغلال المعطيات المعلوماتية قصد جعلها مفهومة وقابلة للإدراك من طرف الأشخاص الذين ستطرح عليهم كدليل.

كما انه من الضروري توضيح أساليب جمع الأدلة الرقمية والحفاظ على سلامتها كل ذلك مع وجوب حماية هذا الإجراء (حجز الدليل) على الشبكة المعلوماتية، كمثال بروتوكولات

[1] فوستان هيلي – الجزء الثالث – فقرة 1257، ص 499، منقول عن مصطفى محمد موسى، المرجع السابق ص:209.

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

نموذجية لجمع الأدلة الرقمية تسمح بحماية الإجراءات وذلك بتقليص خطر إبطالها إجرائيا.[1]

3- أساليب حجز المعطيات المعلوماتية:

لقد اعتمد المشرع في حجز المعطيات المجرمة على أسلوبين متمثلين في نسخ المعطيات أو حجبها(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 المعلوماتية المستخرجة من نفس مكان التفتيش، أي بدل حجز القطع الصلبة التي تتضمن المواد الممنوعة، فيتم مثلاً 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[2] وهذا ما قضت به المادة 06 من قانون 04/09 بقولها: " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث... على دعامة تخزين إلكترونية تكون قابلة للحجز... ".

وأخيرا وفي 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 إلى المعطيات: تناولت المادة 07 من قانون04/09 هذا الأسلوب في حالة الاستحالة التقنية لإجراء الحجز بنسخ المعطيات الرقمية محل

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit..p .179

[2] فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، طبعة 2010، ص 636.

البحث وكذا المعطيات اللازمة لفهم أعلى دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز، فأوجب 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 تجب عليه المادة 07 من قانون 04/09.

4- المعطيات المحجوزة ذات المحتوى المجرم:

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

أما بالنسبة للقانون المقارن فنجد أن المشرع الفرنسي منح لوكيل الجمهورية أو لقاضي التحقيق حسب الحالة بإعطاء أوامر للقيام بحذف المعطيات نهائياً من الدعائم التي تم نسخها، والتي – المعطيات المعلوماتية – في حالة استعمالها أو حيازتها تكون مجرمة أو تشكل خطرا على أمن الأشخاص أو الممتلكات، مثال ذلك: الصور الخاصة بالاعتداءات الجنسية على القصر.[1]

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

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit..p .179.

المطلب الثالث: دور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن تكنولوجيات الإعلام والاتصال متنوعة فمنها ما هو متعلق بخدمات الاتصال السلكية واللاسلكية: الهواتف الأرضية والنقالة، كما أن هناك الشبكات الرقمية المتمثلة في الانترنت، و إن توصيل الخدمات المتنوعة لهذه التكنولوجيات إلى مستعمليها يتطلب توافر مجموعة من الفاعلين (العاملين)أطلق عليهم المشرع اسم مقدمي الخدمات،وقد عرفهم في المادة 02 فقرة د من قانون 04/09 على أنهم: " **د** مقدموا الخدمات:

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصال.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ".[1]

إن المشرع في تعريفه لمقدمي الخدمات قد جمع ثلاثة أنواع من الوسطاء يسمح تدخلهم بتوصيل خدمات تكنولوجيات الإعلام والاتصال بأنواعها إلى مستعمليها، وهم 1ـ مقدمي (متعهدي) خدمة التوصيل Fournisseur d'accès، 2 - متعهدي الإيواء Fournisseur d'hébergement، 3- مقدمي المضمون Fournisseur de contenu ou Editeur، هؤلاء الوسطاء في تقديم الخدمات نص عليهم المشرع الفرنسي وأعطى لكل واحد منهم تعريفه الخاص، ولكن المشرع الجزائري جمع هؤلاء المقدمين في اسم واحد وهم مقدمي الخدمات لأن جميعهم لديه الالتزامات نفسها ويتحمل المسؤولية الجنائية نفسها على عاتقه في حالة تقصيره أو مخالفته للأنظمة المقررة قانوناً وهذا ما احتواه قانون 04/09، وعليه فإن دراستنا لدور مقدمي الخدمات ستكون على شكل دراسة مقارنة بين النظامين القانونيين الجزائري والفرنسي وذلك لسبق التشريع الفرنسي في هذا

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit..p .180.

المجال، ولزيادة التوضيح، لأن الفصل بين هؤلاء مقدمي الخدمات من طرف المشرع الفرنسي ساعد في فهم عمل كل منهم وتحديد مسؤولياته بناء على نوع الخدمة التي يقدمها ومن ثم دوره في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كلا في حدود اختصاصه.

الفرع الأول: المفاهيم القانونية لمقدمي الخدمات بأنواعهم

1- مقدمي خدمة التوصيل (متعهدي التوصيل) Les fournisseurs d'accès:

يشارك متعهدي التوصيل بإرسال وتوجيه المعلومات عن طريق الشبكات بتقديم الأجهزة والخدمات التقنية لمستعمليها من أجل الاتصال بالشبكات (Les modems)،[1] وقد عرفهم المشرع في المادة 2 فقرة د/1بأنهم: " أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات "، جامعا بذلك نوعين من خدمات التوصيل: خدمات التوصيل بالانترنت وكذلك الأمر خدمات التوصيل بمنظومات الاتصال المختلفة ومنها شبكات الهاتف النقال والهاتف الأرضي، وبالنسبة للمشرع الفرنسي فإنه قد عرفهم بأنهم:

الأشخاص الذين يضمنون " نشاط خدمة التوصيل بشبكة اتصالات الكترونية"[2].

2- متعهدي(مقدمي) خدمة الإيواء Les fournisseurs d'hébergement:

وهم بحسب القانون الفرنسي " كل الأشخاص الطبيعية أو المعنوية التي توفر ولو مجانا بوضع تحت تصرف الجمهور و بواسطة وسائل الاتصال عبر الانترنت للجمهور:

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit.p38

[2]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit.p 38: Les fournisseurs d'accès sont définis par article L.33-3-3 du Code des postes et télécommunications comme des personnes assurant une activité de " fourniture d'accès à réseau de communications électroniques".

تخزين الرموز والكتابات والصور والأصوات أو الرسائل أيا كانت طبيعتها لفائدة مستعملي هذه الخدمات "[1].

أما المشرع الجزائري فقد عرف مقدمي خدمة الإيواء بأنهم: " أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها«المادة 02 فقرة 2/ د من القانون 09 /04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وعليه فإنه لا يستطيع أي شخص سواء أكان طبيعيا أو معنويا أن ينشئ موقعا خاصا إلا عن طريق متعهد إيواء المواقع، وبعبارة أخرى فإن هؤلاء الأشخاص يقومون باستضافة أو بإيواء المواقع المختلفة لجعلها في متناول مستخدمي الانترنت، وذلك بالسماح للغير بالإطلاع على محتوياتها في أي وقت.[2]

3-مقدمو المضمون (الناشرون) Les fournisseurs de contenus ou l'éditeurs :

مقدم المضمون أو الناشر هو الشخص الذي يحرر الرسالة ومن ثم يضعها على الانترنت أي ينشرها الكترونيا، فهو يستخدم خدمات الاتصالات المختلفة وخاصة منها الانترنت لنشرها على الجمهور[3].

إن الأحكام القضائية في القانون المقارن وفي دراستنا القانون الفرنسي . بدأت تدريجيا في تحديد دور الناشر عبر شبكات الاتصال وذلك بأخذ معيار المساهمة في إنشاء المضمون، ومثال ذلك حالة المواقع الجماعية مثل:

---

[1]L'article 6-1-2 de la loi nº2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique« les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de de signaux, d'écrits, d'images, de son ou de messages de toutes natures fournis par des destinataires de ces services »; voir Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p 40

[2]طارق سرور، جرائم النشر والإعلام، الكتاب الأول الأحكام الموضوعية، دار النهضة العربية، القاهرة، الطبعة الثانية، 2008، صفحة 203.

[3]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit.p44.

MySpace, Youtube بطريقة أن الملفات توضع للجمهور بناء على تصنيف يتم اختياره من طرف منشئ الموقع ولا تكسب هذا الأخير صفة الناشر خاصة إذا لم يحدد مضمون الملفات الموضوعة على النت.

كذلك فإن كاتب المحتوى المتنازع فيه يمكن بالنتيجة أن يؤمر بتنفيذ سحب المضمون.

وتطبيقا لذلك فإن محكمة باريس أعلنت في 09فيفري 2009 حول وضع الناشر وفي إطار قانون الثقة في الاقتصاد الرقمي في قضية متعلقة باغتصاب حق الصورة لعارض أزياء، حيث وقعت الجريمة على صفحات الانترنت من طرف شاب (DJ)، الحجة القضائية المطورة تصنف المؤسساتMySpaceinc, ZePeople, Universpodcast الآوين للصفحات المتنازع فيها كناشرين قصد التخلص من أسباب الإعفاء من المسؤولية المرتبطة بنظام مقدمي خدمة الإيواء، بالنسبة لهذا الأمر القضاة في فرنسا رفضوا هذا التصنيف، وتمسكوا لأول مرة بمعيار تعريف الناشر، حيث استندوا على الرسالة نفسها للقانون المتعلق بالثقة في الاقتصاد الرقمي la confiance dans la loi pour l'économie LCEN numérique فالمحكمة وبالنتيجة أشارت إلى أنه " ليس من الثابت أن الشركات المدعى عليها تستطيع قبل وضع المحتوى المجرم عبر الانترنت، التدخل بطرق معينة وأيا كانت في إنشائه"[1]، فالمعيار المحدد هو إذن التدخل في إنشاء المحتوى نفسه، كما يظهر في نص المادة 6 فقرة 1 من القانون المتعلق بالثقة في الاقتصاد الرقمي فيما يخص التعريف بمقدم المضمون بأنه " هو الذي يشارك في إنشاء المحتوى أو أحد عناصره[2] ".

وكما يوجد مقدمو خدمات المضمون محترفون مثل الناشرون، هناك آخرون غير محترفين مثل: منشئي المدونات أي Les blogueurs لأنه الآن وبتطور الانترنت أصبح لمشتركيها إنشاء مضامين خاصة بهم.

[1]Ibid. p 45.
[2]Ibid. p 45.

المدونون مقدمي خدمات خاصين:

صاغ مصطلح Weblog جون بارغير John Barger في 17ديسمبر 1997، ثم اختصره بيتر ميرهولز Peter Merholz إلى Blog بمعنى Weblog ووضعه على المسطرة الجانبية لمدونته على الانترنت في أفريل / ماي 1999، وهكذا انتشر هذا المصطلح كاسم فعل Toblog أي تحرير المدونات وإرسالها[1].

والمدونة عبارة عن موقع على شبكة الانترنت ينشئه شخص يطلق عليه اسم المدون Blogueur يتناول فيه كل ما يخص الحياة في مجتمعه أو المجتمعات الأخرى، إلا أن المدونة تختلف عن الموقع Web site وتختلف عن المنتدى Forum كون المدونة تكون مجهولة لدى الجهة الرسمية المسؤولة عن الموافقة على إنشاء المواقع على شبكة الانترنت في البلد الذي أنشأ فيه المدون مدونته[2]، ليس هذا فحسب وإنما يقوم المدون الذي يستخدم دائما اسما مستعار و أيضا المشاركون معه في المواقع بالتحدث بحرية مطلقة وانتقاد الأوضاع الموجودة في البلد الذي ينتمون إليه والبلاد الأخرى.[3]

ومن وجهة نظر علم الاجتماع الانترنت يرى أن التدوين باعتباره وسيلة نشر عامة، التي أدت إلى زيادة دور الويب باعتباره وسيلة للتعبير والتواصل أكثر من أي وقت مضى، بالإضافة لكونه وسيلة للنشر والدعاية والترويج للمشروعات والحملات المختلفة، ويرى البعض أن المدونات إلى جانب البريد الالكتروني أهم خدمتين ظهرتا على الانترنت إطلاقا، خصوصا أن ناشري المدونات يتناولون في مدوناتهم مختلف أنواع الكتابة والتعبير من يوميات وخواطر وأفكار وإنتاج أدبي وسياسة ومتابعة الأخبار وتعليقات متنوعة.

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية ، مطابع الشرطة القاهرة، مصر الطبعة الأولى، 2009، ص 84.

[2] اللجنة الوطنية للمعلومات والحريات بفرنسا (CNIL) قررت في سنة 2005 إعفاء المدونات من الإعلام عنها، انظر في هذا الأمر

Myriam QUÉMÉNER, Yves CHARPENEL المرجع السابق، ص،: 46.

[3] مصطفى محمد موسى، المرجع السابق، ص: 86.

ويعد المدون كالناشر في خدمة الاتصالات للجمهور عبر الوسيلة الالكترونية متى كان مؤلف للمضمون في مدونته، ويمكن إذن متابعته في حالة ارتكاب جريمة من طرفه، كما يجب التفرقة بين وضع المدون ومقدم خدمة الإيواء للمدونة في المسؤولية لأن هذا الأخير ليس له أي دور في صدور المضامين المنشورة عبر المدونة فهو يقدم فقط الأرضية التقنية للمدون[1].

وفي قرار صادر عن الغرفة الجنائية بمحكمة النقض الفرنسية في 10نوفمبر 2009 التي أرت أن عبارات القذف الموضوعة في مدونة تابعة لجريدة La République de centre-ouest سمحت بإقامة المسؤولية الجزائية للناشر و لمدير النشرية لأن المدونة تعد جزء مكمل لكيان الجريدة، والتبرئة التي استفادت منها كانت لسبب واحد هو أن الدليل لم يقم على أن الناشر للعبارات المجرمة كان على علم بنشرها، فمحكمة النقض سوت بطريقة واضحة بين وضعية المدونة مع تلك المرتكزة على الإعلام التقليدي[2].

الفرع الثاني: التزامات مقدمو الخدمات

لقد أورد المشرع الجزائري كنظيره الفرنسي مجموعة من الالتزامات على عاتق مقدمي الخدمات تكاد تكون متماثلة على الرغم من أن المشرع الجزائري قد أغفل الدور الذي يلعبه مقدمو خدمات المضمون وأهميته في البحث والتحري للكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك لتحديد المسؤولية الجزائية المترتبة عن نشر المضمون المجرم عبر مختلف المواقع الاجتماعية الافتراضية، وعليه سنتناول الالتزامات المفروضة على نوعين من مقدمي الخدمات وهم مقدمي خدمة التوصيل ومقدمي خدمة الإيواء مع دراسة مقارنة بالقانون الفرنسي والاجتهادات القضائية التي أرفقت تطبيق هذه الالتزامات.

1- الالتزام بحفظ المعطيات المتعلقة بحركة السير ومساعدة السلطات القضائية:

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .64.
[2]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .64.

عرف المشرع الجزائري المعطيات المتعلقة بحركة السير في المادة 2 فقرة هـ بأنها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة "، إن الالتزام بحفظ المعطيات منصوص عليها في المادة 11من القانون 04/09المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي أوجبت على عاتق مقدمي الخدمات بنوعيهما – التي نص عليها المشرع بدون تحديد صنفيهما وهما مقدمي خدمات التوصيل بالانترنت أو منظومة اتصال ومقدمي خدمة الإيواء الخاصة بالانترنت– حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنت (المدونات، الصفحات الخاصة، والإعلانات في مواقع البيع عن طريق المزاد...) وذلك من أجل التبليغات المحتملة للسلطات القضائية أو في حالة طلب هذه الأخيرة لأجل التحريات أو المعاينات أو المتابعات القضائية لجرائم مرتكبة (المادة10 من القانون 09 (04/

وبحسب القانون فإن مقدمي الخدمات غير ملزمين بوضع ملفات اسمية لمستعملي الخدمات، كما لا يمكنهم الاحتفاظ بالمعلومات المتعلقة بمضمون الاتصالات: نصوص الرسائل القصيرة(SMS) أو مواضيع البريد الالكتروني Email[1]، كذلك حدد المشرع مدة حفظ هذه المعطيات لمدة لا تزيد عن سنة واحدة ابتداء من تاريخ التسجيل.

إلا أنه بالنظر لنص المادة 10 فقرة 1 من القانون 04/09 فإن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصال ولكن بشرط أن يكون في حينه، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلقة بمحتوى اتصالات أيا كانت (مكالمات صوتية هاتفية أو مكالمات فيديو عبر مواقع الانترنت، SMS, Email MMS،) ولكن لم يحدد المشرع الجزائري على

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .176.

عكس المشرع الفرنسي مدة تسجيل هذه الاتصالات وتركها مفتوحة، كما لم يحدد الأشخاص المكلفين بتسخير مقدمي الخدمات للقيام بهذا الإجراء الخطير، بينما المشرع الفرنسي سمح لضباط الشرطة القضائية بتسخير من وكيل الجمهورية مع ترخيص مسبق من طرف قاضي الحريات والحبس، بتسخير مقدمي الاتصالات للجمهور عبر الانترنت للقيام بكل الإجراءات التي تؤمن الحفظ لمدة لا تزيد عن سنة واحدة لمحتويات معلوماتية التي تتم من طرف أشخاص مستعملين للخدمات التي يؤمنها مقدمو الخدمات المعنيون (المادة 60-2 فقرة 2 من قانون الإجراءات الجزائية الفرنسي).

هذه الأحكام المختلفة بين القانونين والتي تهدف إلى نفس النتيجة وهي حفظ معطيات تتعلق بتسجيل وجمع محتوى اتصالات في حينها تختلف من حيث:

1- الأشخاص الذين يحق لهم تقديم طلب المساعدة: (والتي نص عليها المشرع الفرنسي بلفظ التسخير) يكون طلب المساعدة في التشريع الجزائري للسلطات المكلفة بالتحريات القضائية، بما فيهم ضباط الشرطة القضائية، فهل يستوجب على هؤلاء طلب إذن من وكيل الجمهورية أو قاضي التحقيق بحسب الحالة للقيام بطلب المساعدة من مقدمي الخدمات؟ وهذا عكس المشرع الفرنسي الذي قدم ضمانات قانونية تكفل حماية الحياة الخاصة للأشخاص وذلك عندما نص على أن طلب المساعدة يكون بتسخير من وكيل الجمهورية والذي بدوره لا يمكنه منح هذا التسخير إلا بوجود ترخيص مسبق من قاضي الحريات والحبس، هذه الإجراءات نرى أنها تحد من التجاوزات التي يمكن لأعوان الضبط القضائي ممارستها في حالة التحريات عن جرائم متصلة بتكنولوجيات الإعلام والاتصال.

2- من حيث مدة حفظ هذه المحتويات الخاصة بالاتصالات الآنية: إن تحديد مدة الحفظ يسمح بتعجيل إجراءات المتابعة الجزائية إن كان لها محل، وهو ما قدره المشرع الفرنسي (سنة واحدة لحفظ المكالمات) وما نراه أمرا مهما جدا يجب على المشرع تداركه.

وبالرجوع لالتزام مقدمي الخدمات بتقديم المساعدة للسلطات القضائية جاء المشرع الفرنسي بأحكام خاصة تتعلق بقانون مكافحة الإرهاب رقم 2006/64 الصادر في 23 جانفي2006 حيث وسع هذه الالتزامات بحفظ المعطيات لمدة سنة لمسيري مقاهي الانترنت وللأشخاص الذين يعرضون لزبائنهم مثل الفنادق أو شركات الطيران أو للجمهور الاتصال بشبكة اتصالات الكترونية بمقابل أو مجانا[1].

أصناف المعطيات الواجب حفظها:

لقد أوضحت المادة 11من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أصناف المعطيات التي يجب على مقدمي الخدمات حفظها وهي:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة (مثال ذلك عنوان IP، رقم الهاتف، عنوان البريد الالكتروني)؛

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال؛

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال؛

و- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها؛

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

وبالنسبة لمقدمي خدمات الهاتف فهم ملزمون بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة (الفقرة أ من المادة 11) وكذلك بحفظ المعطيات التي تسمح بالتعرف على مصدر الاتصال ومكانه.

جزاء الإخلال بالتزام حفظ المعطيات:

لقد أوجب المشرع في المادة 10فقرة 1على مقدمي الخدمات (التوصيل والإيواء) أن يضعوا بين أيدي السلطات المكلفة بالتحريات القضائية المعطيات التي تم حفظها، ووفقا

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .176.

للمادة 11 فقرة 3 وفي حالة عدم التزامهم بحفظ هذه المعطيات فإن مسؤوليتهم الجزائية تقوم عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية.

فيعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، وبالنسبة للشخص المعنوي فيعاقب بالغرامة وفقا لقواعد قانون العقوبات، بحسب نص المادة 18مكرر من قانون العقوبات فإن: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:[1]

1- الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة "، وتطبيقا لذلك يعاقب الشخص المعنوي المخالف لالتزاماته المقررة قانونا والتي أدت إلى عرقلة حسن سير التحريات القضائية بغرامة من 500.000 دج إلى 2.500.000 دج.

2 - **الالتزام بتصفية المواقع وبيان نوعها:**

نصت المادة 12من القانون 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه " زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه يتعين على مقدمي خدمات الانترنت ما يأتي:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام والآداب العامة و إخبار المشتركين لديهم بوجودها "

1- بالنسبة للتدخل الفوري لسحب المحتويات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن، هذا الالتزام الذي فرضه المشرع على مقدمي الخدمات لم يفرض فيه مسؤولية جزائية في حال عدم تنفيذه، مما يؤدي ذلك إلى القول بأن هذا الالتزام التزام أدبي من

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .177.

طرف مقدمي الخدمات، لأن المشرع لم يفرض عقوبة رادعة في حالة مخالفة مقدمي الخدمات لهذا الالتزام وفي هذا الحال لا يمكن مطالبة مقدمي الخدمات المتقاعسين عن أداء واجبهم في حذف المضامين المجرمة والمخالفة للقوانين بتعويضات مدنية في حالة حدوث أضرار نتيجة عرض المضامين المجرمة عبر الانترنت دون رقيب في انتظار تحريك الدعوى العمومية[1] التي يمكن من خلالها وبطلب من السلطة القضائية وقف هذه المضامين المجرمة، ونحن نرى أن هذا التقصير يخل فعلا بحقوق الأشخاص سواء الطبيعيين أو المعنويين في حالة انتهاك حقوقهم عبر الانترنت، فكان لازما على المشرع أن يفرض عقوبات رادعة لمقدمي الخدمات وخاصة منهم مقدمي خدمة الإيواء في حالة امتناعهم عن حذف هذه المحتويات في الوقت المناسب، وهذا خلافا للمشرع الفرنسي الذي فرض مسؤولية مدنية وجزائية على مقدمي خدمة الإيواء الذين يرفضون أو يتقاعسون عن القيام بالتزامهم المتمثل في سحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن وهو ما نصت عليه المادة 6-1-2 والمادة 6-1- 3من القانون 2004/575 الصادر في 21 جوان 2004 من أجل الثقة في الاقتصاد الرقمي (LCEN) حيث نصتا على أن المسئولية المدنية أو الجزائية لمقدم خدمة الإيواء لا يمكن أن تقوم إلا في حالة العلم الحقيقي بالوقائع أو الظروف التي بموجبها يكون النشاط أو المعلومة مجرمة، وفيما يتعلق بالمطالبة بالتعويضات فلا تقوم إلا مع وجود العلم بأن الوقائع أو الظروف بحسب النشاط أو المعلومة تكون مجرمة ولم يتصرف مقدم خدمة الإيواء فوار لسحب المعلومات أو بجعل الوصول إليها مستحيلا[2].

وبموجب المادة 6-5 من القانون 2004/06/21من أجل الثقة في الاقتصاد الرقمي فإن مسؤولية مقدم خدمة الإيواء لا يمكن أن تقوم إلا إذا لم يقم وبسرعة بعد إعلامه بسحب محتوى واضح أنه غير مشروع، وعلى متعهد الإيواء أن يقيم الدليل على سرعة سحبه للمحتوى المجرم.

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .177.
[2]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .41.

أما بالنسبة للاجتهاد القضائي الفرنسي في مسألة قيام المسؤولية الجزائية لمقدمي خدمة الإيواء الذين لهم نشاط تخزين دائم ومستمر للمعلومات (المادة 2/د/2من القانون 04/09) فلمحكمة النقض الفرنسية قرار صادر بتاريخ 2010/01/14 قامت فيه بإعادة النقاش حول النظام الذي يحكم مقدمي خدمة الإيواء. وعكس الاجتهاد القضائي الذي طبق وبشكل موسع نظام المسؤولية المخففة لمقدمي خدمة الإيواء على مواقع الويب (Web 2.0)[1]، فقد رفضت المحكمة العليا في فرنسا هذا التطبيق على مسؤولية مقدمي خدمة الإيواء لصفحات شخصية بموقع Tiscali، وهي واقعة تقديم العروض للمعلنين التجاريين في أماكن وضعت في صفحات شخصية سمح لمستعملي الانترنت بإنشائها، وذلك بوضع فضاءات للإعلانات مدفوعة الثمن عبر هذه الصفحات قد تجاوزت " بساطة الوظيفة التقنية للتخزين ".

هذا القرار يؤكد الأحكام التي تبنتها محكمة الاستئناف لباريس في حكمها بتاريخ 06جوان 2007، فقد أثارت اضطرابا عند مقدمي خدمة الإيواء لصفحات شخصية الذين جنوا أرباحا بسبب الإعلانات، فقد اعتبرت أن Tiscali التي تعرض هذا النوع من الإيواء تتمتع بصفة الناشر، وبالنتيجة تكون مسؤولة عن الإنتاج غير المشروع للأشرطة (Les bandes) المصورة على الموقع www.chez.com/bdz والتي لم يكن بالإمكان معرفة صاحبها[2].

2- أما بالنسبة لبيان نوع المواقع التي تحوي معلومات مخالفة للنظام العام والآداب العامة، فإن المشرع في المادة 12- ب من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فقد ألزم مقدمي الخدمات بوضع ترتيبات تقنية تسمح لمستعملي الانترنت بالتعرف وبسهولة على نوع هذه

[1] يعد Web 2.0 الإصدار الثاني للانترنت الذي يتسم بإمكانية التعاون بين مستعملي الانترنت، والشبكات الاجتماعية هي قاعدة الاتصالات عبر الانترنت التي تسمح بإنشاء شبكات لمستعملي الانترنت يتشاركون فيها الفوائد والمنافع العامة والأكثر شهرة من بين هذه المواقع: Facebook, MySpace, twiter ، أنظر في هذا الشأن، Myriam QUÉMÉNER, Yves CHARPENE، المرجع السابق، صفحة35.

[2]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .41.

المواقع وبالطبع يجب أن تكون واضحة يمكن لمن أراد أن يدخل لموقع معين معرفة أنه موقع مخالف للنظام العام والآداب العامة قبل الدخول إليه.

كما يجب لهذه التقنيات أن تُعلم لمن يستعملها بوجود وسائل تقنية تسمح بحصر الدخول إلى هذه المواقع كالمراقبة الأبوية التي تمنع القصر من دخول هذه المواقع باستعمال برامج وقائية تتطلب كلمة سر معينة.

أما بالنسبة للمشرع الفرنسي فقد فرض على مقدمي الخدمات أن يعلموا مستخدمي الانترنت بوجود تقنيات تسمح بحصر الوصول إلى مواقع معينة أو بتحديدها مع وجوب أن يعرضوا على مستخدمي الانترنت واحدة من هذه الأساليب التقنية، وكذلك وجوب أن توضع مباشرة آليات المراقبة الأبوية (المادة6-I- 1 من القانون لأجل الثقة في الاقتصاد الرقمي).

وأضافت المادة 6- I- 7 بوجوب التبليغ السريع للسلطات القضائية عن النشاطات المجرمة الموجودة في الانترنت والتي أعلنت عنها لمستعمليها بأنها مواقع تحوي مضامين مخالفة للقانون.

كما يجب على مقدمي الخدمات أن يقدموا للجمهور (مستعملي الانترنت) الوسائل المكرسة لمكافحة الانحرافات التي تكون جرائم في القانون العام[1].

[1]Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p .38.

خلاصة الفصل الثاني:

تناولنا في هذا الفصل مجموع الآليات الإجرائية التي اعتمدها المشرع في التحقيق والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

إذ تناولنا في المبحث الأول القواعد العامة للبحث والتحري عن الدليل الرقمي والمبادئ العامة التي يجب أن يخضع لها الدليل الرقمي حتى يمكنه أن يكون مقبولا أمام القضاء كدليل للإدانة أو لبراءة المتهم.

أما في المبحث الثاني فتناولنا الأساليب التقنية التي تتوافق والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فقد قدم المشرع مجموعة من الأساليب تتمثل في المراقبة الالكترونية والتي تحوي أسلوبي الوقاية والمكافحة للجرائم التي ترصدها، وكذلك إجراءات التفتيش في النظم المعلوماتية و أساليب حجز الدليل الرقمي(المعطيات المعلوماتية)، كذلك الأمر بالنسبة لدور مقدمي الخدمات والذي هو دور مهم جدا في مكافحة الجرائم المعلوماتية وفي التحقيق والتحري حول هذه الجرائم، بتقديم المساعدة التي فرضها المشرع الجزائي للسلطات القضائية المكلفة بالتحريات حول هذا النوع من الإجرام، فإننا نرى أن يقوم المشرع بتفعيل المسؤولية الجزائية والمدنية لمقدمي الخدمات لسحب المحتوى المجرم أو جعل الوصول إليه غير ممكن وذلك بإدراج عقوبات جزائية رادعة.

خاتمة

إذا كنا قد تطرقنا في بحثنا هذا لتفاصيل جرائم الاعتداء على النظام المعلوماتي لأهم إشكال الجرائم المتعلقة بتكنولوجيات الاتصال والمعلومات وإذا كانت خطورة تلك الجرائم له اثر على الدول صاحبة التكنولوجية الآن الخطورة لم تسلم منها حتى الدول النامية ولمسايرة هذه الممارسات قامت العديد من الدول بسن قوانين خاصة لمواجهة هذه الجرائم الجديدة وقام المشرع الجزائري بإصدار قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والقوانين اللاحقة عليه كالقانون 03/15 والقانون 04/15 المتعلقين بالتصديق والتوقيع الالكترونيين مما قام بإرساء قواعد إجرائية جديدة تضمنت حكما جيدا في أساليب مكافحة هذا النوع الجديد من الإجرام وبما يتوافق وخصائصه، فقد شملت مواده الكثير من الآليات المستحدثة:

1- حيث أن المشرع الجزائري جرم الاعتداء على النظم المعالجة الآلية في قسم خاص في قانون العقوبات وهو القسم السابع مكرر *المساس بأنظمة المعالجة الآلية للمعطيات * وبنصه على إنشاء هيئة وطنية للوقاية.

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و إن لم يتم تنصيبها إلى حد الساعة تماشيا مع الرؤية التشريعية الفرنسية.

2- كذلك القواعد المتعلقة بالاختصاص الإقليمي للقانون الجزائي الجزائري حيث تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد 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 أجانب، أيضا فإن عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من اختصاص القانون الجزائي لأكثر من دولة مما قد ينجر عنه تنازع في الاختصاص أو رفض له، مما قد ينشأ للمجرمين أماكن لا قانون فيها فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعال 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- إبرام اتفاقيات ومعاهدات دولية في مجال التعاون الدولي التي تهدف من تقريب القوانين الجزائية الوطنية والقوانين الدولية في إطار مكافحة الجرائم العالمية ومنها جرائم المتصلة بتكنولوجية الإعلام والاتصال .

4- أيضا فإن لطرق التحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ميزاتها والتي تبناها المشرع في القانون 04/09، فالمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية أعطى لها القانون صفة الشرعية القانونية بتقنينها و إدخالها ضمن الترسانة الإجرائية الجزائية في القانون الجزائري، تسمح للمتحريين عن الجرائم والمحققين فيها فسحة قانونية لتقديم الأدلة اللازمة لإدانة المتهم أو تبرئته.

5- كما يلعب مقدمو الخدمات بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للإعلام والاتصال دوار مهما في مكافحة هذا النوع من الإجرام وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن الجرائم المرتكبة بواسطة أو ضد هذه التكنولوجيات، وأيضا الالتزام 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 والاتصال ومكافحتها المنصوص عليها في القانون 04/09 أمر مهم يجب على السلطات المعنية الإسراع به لما يمكن لهذه الهيئة القيام به للوقاية من هذا النوع من الإجرام ومكافحته، وكذلك تقديم المساعدة للسلطات القضائية في التحقيقات الجارية حول هذه الجرائم.

2- تعد مراقبة الاتصالات الالكترونية وتفتيش النظم المعلوماتية من أهم وأخطر الإجراءات التي جاء بها قانون 04/09 فهذين الإجراءين خلفا صراعا كبيرا في كثير من

الدول الأوربية فسويسرا وألمانيا مثلا لم تسمحا بالقيام بالمراقبة الالكترونية والتفتيش في المنظومات المعلوماتية إلا إذا وقعت الجريمة فعلا، وليس كتدبير وقائي من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهذا لأن هذين الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد، فكان جديرا بالمشرع وضع قيود قانونية لتبرير اللجوء إلى هذين الإجراءين كما هو الحال بالنسبة للحالة أ من المادة 04من القانون 04/09.

3- لاحظنا كذلك بالنسبة لالتزامات 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 أو جعل الدخول إليها غير ممكن، ولم يدرج المشرع أي مسؤولية على عاتقهم في حالة امتناعهم عن القيام بهذا الالتزام على عكس نظيره المشرع الفرنسي، لهذا كان حريا بالمشرع إدراج عقوبات جزائية على مقدمي الخدمات المقصرين في أداء واجبهم القانوني.

وأخيرا إن صدور القانون 04/09 يعد تحديا فعليا للسلطات القضائية وأعوانها (سلطات الضبط القضائي، وكذلك المحامين) من أجل تطبيقه نظرا لخصوصية الإجراءات التي جاء بها، فيكون لزاما عليها أن تساير التقدم التكنولوجي الحاصل على مستوى الإعلام والاتصال من تكوين جيد يسمح بفهم وتطبيق هذه التقنيات حتى تكون عمليات البحث والتحري أكثر فاعلية، وكذلك الحكم والقضاء في الدعاوى الجزائية المتعلقة بهذه الجرائم مبنيان على فهم جيد للوقائع خاصة إذا كانت مرتبطة بجرائم تقنية بحتة، بل لا بد من إيجاد استراتيجيات الفني والتقني والقضائي على مستوى التعاون القضائي الدولي وتسليم المجرمين .

قائمة المراجع

قائمة المراجع باللغة العربية:

المراجع العامة

– د.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، الطبعة الخامسة 2007.

– د. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، دار هومة، الجزائر، الطبعة التاسعة، 2008.

– د. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1981.

– د. عمار بوضياف، النظام القضائي الجزائري، دار ريحانة، الجزائر، طبعة 2003.

ـ د.عمر السعيد رمضان، أصول المحاكمات الجزائية في التشريع اللبناني، منشورات الدار المصرية للطباعة والنشر،الطبعة الأولى، 1971.

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

– د. مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الأول(النظرية العامة للإثبات الجنائي)، دار هومة، الجزائر، 2007.

– د. منصور عمر المعايطة، الأدلة الجنائية والتحقيق الجنائي، دار الثقافة للنشر والتوزيع ، عمان الأردن، الطبعة الأولى ، 2009.

المراجع المتخصصة

– آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، 2007.

– د. خالد ممدوح إبراهيم: فن التحقيق في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

– د. طارق إبراهيم الدسوقي عطية: الأمن المعلوماتي(النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

– د. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، دار النهضة العربية، القاهرة، الطبعة الأولى، 2007.

– د. عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار المعارف، الإسكندرية، مصر، 2009.

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

– عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية)، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2007.

– د. فتحي محمد أنور عزت: الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، المنصورة مصر، الطبعة الأولى، 2010.

– محمد أمين الشوابكة، جرائم الحاسب والانترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2007.

– د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، الطبعة الثانية، 1998.

– د. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، الطبعة الأولى، 2009.

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

– د. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، مصر، الطبعة الأولى 2009.

– د. يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى،

.2011

المجلات والدوريات العلمية والمنشورات المختلفة

– د. بن محمد محمد، تنازع الاختصاص في الجرائم الالكترونية، مجلة دفاتر السياسة والقانون، صادرة عن كلية

الحقوق والعلوم السياسية، جامعة قاصدي مرباح بورقلة، العدد الثاني جانفي 2010.

– منشور صادر عن وزارة العدل حول فعاليات الندوة الوطنية لإصلاح العدالة – نادي الصنوبر 2005 .

قائمة المراجع الأجنبية الكتب الأجنبية

- Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, Droit pénal appliqué», 2010, ECONOMICA ,Paris France.
- Mohamed CHAWKI, Combattre la cybercriminalité, Edition de Saint Amans France, 2008.

الرسائل الجامعية

- Adélaïde TROUSSELARD, La protection des mineurs et le sexe en ligne, Mémoire
réalisé dans le cadre du Master 2,Faculté de droit et de science politique, Université Paul Cézanne Aix-Marseille II, [03/09/2012].
- Anne BRISSET-GIUSTINIANI, Aspects juridiques de l'émergence d'une sécurité européenne des réseaux et des systèmes d'information, Mémoire D.E.S.S. Droit de l'Internet-administrationsentreprises, Université Panthéon-Sorbonne paris I, disponible sur: www.univparis1.fr/.../2004_sept_OK_Brisset_ Giustinani_ Version_ ... .
- Jean-François TYRODE,Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit

européen, mémoire de master droit de l'Internet-AdministrationEntreprises, Université PARIS 1-PANTHEON-SORBONNE, année universitaire 2006-2007, disponible sur www.univ-paris1.fr/.TYRODE_ MEMOIRE.pdf[03/09/2012].

الدوريات باللغة الأجنبية

- Yann PADOVA, Un aperçu de la lutte contre la cybercriminalité en France, Revue de science criminelle, octobre-décembre 2002, Dalloz, France, 764 et s.
- Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011, disponible sur: www.dalloz.fr

مواقع الكترونية

- Colloque du 13/04/2010. La preuve numérique à l'épreuve du litige. Les acteurs du litige à la preuve numérique(l'information numérique fait la preuve), Site de Compagnie nationale des experts de justice en informatique et associées: www.cnejita.org/.../CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1pdf.
- Hadjira BOUDER: Orientations de la politique pénale de prévention et de lutte contre la criminalité liée aux TIC en Algérie, centre de recherche sue l'information scientifique et technique, CERIST,03 Rue des frères Aissiou, Benknoun, Alger, Algérie, www.alexalaw.com.
- Patrick CHAMBET, Le cyber-terrorisme, disponible sur www.chambet.com/publications/Cyberterrorisme. pdf [03/09/2012].
- Suisse« Nouvelles technologies et droit », voir l'article " La surveillance préventive en Suisse: les moyens techniques", http://ntdroit.wordpress.com
- Thiery BRETON ,Chantier sur la lutte contre la cybercriminalité, Rapport remis à Monsieur le ministre de l'Intérieur, de la sécurité intérieure et des Libertés Locales, le 25 février 2005, www.4law.co.il

- www.secureteinfo.com/legal/OCLCTIC.shtml, le cite de Office central de lutte contre la criminalité liée aux technologie de l'information et de la communication
- www.legifrance.gouv.fr/affichTexte.do
- www.interpol.int
- http://fr.wikipedia.org

الفهرس

مقدمة.....أ

الفصل الأول: هيئات مكافحة الجرائم المتصلة بتكنلوجيات الإعلام والاتصال.....08

المبحث الأول: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الوطني.....09

المطلب الأول: الهيئات الوطنية للوقاية والمكافحة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....10

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 10

الفرع الثاني: السلطة الوطنية للتصديق الالكتروني.....11

الفرع الثالث : السلطة الحكومية لتصديق الالكتروني 12

الفرع الرابع : سلطة الاقتصادية للتصديق الالكتروني 12

المطلب الثاني: دور الضبطية القضائية في إجراءات مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....13

المطلب الثالث: السلطة القضائية في مواجهة الجرائم المعلوماتية.....15

المبحث الثاني: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الصعيد الدولي.....17

المطلب الأول: مبدأ الإقليمية في مواجهة جرائم المعلوماتية.....18

الفرع الأول: التذكير بالقواعد.....19

الفرع الثاني: تكييف الاختصاص وفق المنازعات.....22

المطلب الثاني: ضرورة التعاون الدولي في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....24

المطلب الثالث: وسائل التعاون القضائي على الصعيد الدولي.....27
الفرع الأول: التعاون الأمني الدولي.....27
الفرع الثاني: المساعدة القضائية الدولية في المواد الجزائية.....30
الفصل الثاني: الدليل وطرق التحقيق في الجرائم المتصلة بتكنلوجيات الإعلام والاتصال.....38
المبحث الأول: الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ...39
المطلب الأول: مفهوم الدليل الرقمي..... 41
الفرع الأول: تعريف الدليل الرقمي.....42
الفرع الثاني: معايير تقدير الأدلة الرقمية (صحة وخطأ الأدلة الرقمية).....43
أولا: المعلومة الرقمية قبل الدليل.....43
ثانيا: من معلومة رقمية إلى دليل رقمي.....44
المطلب الثاني: الطرق التقنية للتحقيق في جرائم تكنولوجيات الإعلام والاتصال.....47
الفرع الأول: تقنيات التحقيق.....47
الفرع الثاني: أدوات التحقيق.....51
المطلب الثالث: المبادئ العامة للأدلة الرقمية.....51
المبحث الثاني: طرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال..54
المطلب الأول: مراقبة الاتصالات الالكترونية.....56
الفرع الأول: مفهوم مراقبة الاتصالات الالكترونية 56
الفرع الثاني: حالات اللجوء إلى المراقبة الالكترونية.....59
الفرع الثالث: العمليات الإجرائية.....61
الأحكام العامة.....61
أولا: الجرائم المعنية والعمليات الإجرائية.....62
ثانيا: الإذن.....63

ثالثا: الإجراءات.....64
حكم المادة 4 فقرة 3 من القانون 04/09.....65
المطلب الثاني: تفتيش المنظومات المعلوماتية.....66
الفرع الأول: المفاهيم الأولية.....66
الفرع الثاني: حالات اللجوء إلى تفتيش النظم المعلوماتية و إجراءات تفتيشها.....70
أولا: حالات تفتيش النظم المعلوماتية.....70
ثانيا: إجراءات تفتيش نظم المعلوماتية.....71
الفرع الثالث: حجز المعطيات المعلوماتية.....77
1- تعريف حجز (ضبط) الدليل الإلكتروني.....77
2- إجراءات حجز المعطيات المعلوماتية.....78
3- أساليب حجز المعطيات المعلوماتية.....78
4- المعطيات المحجوزة ذات المحتوى المجرم.....80
المطلب الثالث: دور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....82
الفرع الأول: المفاهيم القانونية لمقدمي الخدمات بأنواعهم.....86
الفرع الثاني: التزامات مقدمي لخدمات.....86
1- الالتزام بحفظ المعطيات المتعلقة بحركة السير ومساعدة السلطات القضائية.....86
2- الالتزام بتصفية المواقع وبيان نوعها.....90
خاتمة.....96
قائمة المراجع.....100
الفهرس.....106