جـامعـة قـاصـدي مـربـا
كلية الحقوق والعلوم ا
قسم الحقوق

تخصص: قانون جنائي

مذكرة مقدمة لنيل شهادة الماجستير

بعنوان

آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09

تاريخ المناقشة: 2013/04/23

إعداد الطالبة:

ـ أحمد مسعود مريم

إشراف الدكتور:

ـ قريشي محمد

لجنة المناقشة:

ـ الدكتور بن محمد محمد	أستاذ محاضر	جامعة ورقلة	رئيسا
ـ الدكتور قريشي محمد	أستاذ محاضر	جامعة ورقلة	مشرفا ومقررا
ـ الدكتور خلف بوبكر	أستاذ محاضر	جامعة ورقلة	مناقشا
ـ الدكتور بن مشري عبد الحليم	أستاذ محاضر	جامعة بسكرة	مناقشا

السنة الجامعية: 2013/2012

مقدمة

خلال السنوات القليلة الماضية انتشرت تكنولوجيات ا
بمنأى عن تأثيرها المباشر والمتواصل في حياة الأفراد والمجتم
الإنترنت حبيسة العالم الافتراضي ولكنها توسعت لتشمل كل مجالات حياتنا، لتتجاوزها غير المتناهية أصبحت اليوم بوسائلها الرقمية عامل مؤثر على سلوكيات الأفراد والمجتمعات، ومن كان ليعتقد ما فعلته مواقع عديدة وأهمها Facebook في التأثير على توجهات مجتمعات بأكملها، فالانترنت بعالمها الافتراضي أصبحت جزءً مؤثرا على توجهات الشعوب، وما يمكننا ملاحظته حول هذا الانتصار القوي للمعلوماتية هو ثلاث عناصر مهمة تتمثل في سرعة انتشارها وعالميتها وتعدد مهامها:

– سرعة الانتشار: لقد عمل الباحثون والعلماء في مجال تكنولوجيات الإعلام والاتصال لنحو أكثر من 50 سنة من تطور علم الإلكترونيك إلى زيادة متنامية لأفكار وأداءات وأسواق جديدة (الهواتف النقالة، الانترنت، الإعلام السمعي البصري عبر الفضائيات أو عبر شبكة الانترنت)

– 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 مُغوي 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 أدغالا حيث وحدهم المفترسون يزدهرون، ولا أن تقيد الحريات فيها إلى حد أن تكون كحديقة فرنسية تخنق فيها حيوية الحرية التي تعد المحرك الحقيقي لرائعة " كل شيء رقمي" والذي هو شعار التطور الذي تؤول إليه المجتمعات بعد انتشار تكنولوجيات الإعلام والاتصال وإنشاء الحكومات الرقمية لجعل كل شيء رقمي.

ولكن فن التوفيق بين الواقعة والحق كما نعرفه دائما صعب، حيث منذ 50 سنة 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 العمل المتزامن مع تنامي تكنولوجيات الاتصال والتطبيقات الق بالقانون العقابي السيبيري(المعلوماتي) وهو المرتبط بالجرائم المرتكبة عبر الانترنت وباستعمال التكنولوجيات الحديثة للإعلام والاتصال يُبرِز 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 آليات 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 تش
فقهاؤنا بالدراسة والتحليل الجديرين بها، وذلك لحداثة دخول هذ
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 مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في القانون 04/09 ؟

ويتبع هذا التساؤل مجوعة من الأسئلة يمكن طرحها وهي

– كيف يمكن لرجال القضاء من ضباط للشرطة القضائية بكل موضوعية وفهم للتحري والتحقيق ثم الحكم في دعاوى أطرافها (الضحايا أو المتهمين) ومواضيعها تتميز بالاستثنائية؟

– 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 تدّخل 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 ثلاث فصول على النحو التالي:

فصل تمهيدي: القانون الجزائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الأول: القانون الجزائي في مواجهة البيئة الرقمية

المبحث الثاني: الحماية الجزائية لنظم المعلوماتية والجرائم المرتكبة عبرها

الفصل الأول: هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

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

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

الفصل الثاني: آليات البحث والتحري للكشف عن 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

فصل تمهيدي:

القانون الجزائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

فصل تمهيدي: القانون الجزائي في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

في عام 1844 وعبر خط سلكي طوله حوالي 70 كيلومتر ربط بين مدينتي(بلتيمور و واشنطن) أرسلت أول رسالة تحملها وسيلة اتصال Télécommunication message أرسلها المخترع صامويل موريسSamuel morse وبدأ هذا الاختراع في الانتشار وتعددت الجهات التي وظفته كي تُسَهِل أعمالها واتصالاتها ومن ذلك السكك الحديدية والصحافة، ثم تم نقل الصوت عن طريق السلك من طرف الكسندر جراهام بل لأمتار قليلة وكان هذا الاختراع هو الهاتف بتاريخ 02 جوان 1875 وتوالت من بعده الانجازات التي واكبت عصر الاتصالات في القرن 20 فمن الهاتف السلكي أو ما نسميه الأرضي إلى الهاتف اللاسلكي وبعده تم اختراع شبكات التلفزيون والإذاعة وتطورت هذه الأجهزة لتستقبل موجاتها عبر الأقمار الصناعية، وتطور الهاتف ليصبح الفاكس والتيلكس ثم الهواتف المحمولة والنقالة وخلال هذه النهضة في تكنولوجيا الاتصالات كان هناك مخاض ولادة لثورة أخرى تلتها وهي ما تسمى بثورة المعلومات في الثلاثين سنة الأخيرة من القرن العشرين، وكان نتاجها شبكة الانترنت[1].

وما يجب ادراكه ان هذه التطورات المذهلة في تكنولوجيات الإعلام والاتصال واكبته جهود دولية للتعاون فيما بين الدول والمؤسسات لكي تتم الاتصالات الدولية بنجاح، مؤدية الأغراض الانسانية في المساعدة على خلق مجتمع دولي يسوده التفاهم وتنمو بين أطرافه روح الاحترام المتبادل، خاصة أن الشعوب تسعى لخلق العلاقات الودية والإنسانية بينها، بصرف النظر عن تكويناتها الإثنية واختلاف لغاتها، وتعدد عقائدها، والاتصالات عبر الحدود هو العامل المرجح لتحقيق هذه الأهداف.

ولهذه الاعتبارات تعاونت بلدان العالم في مجال الاتصالات حيث تم تأسيس "الاتحاد الدولي للاتصالات السلكية واللاسلكية" وقد كان يسمى في البداية "الاتحاد الدولي للتلغراف" وهذا الاتحاد هو الأول من نوعه الذي جمع كل دول العالم وشعوبها للاستفادة من الاختراعات العظيمة في مجال التلغراف والهاتف والراديو ووسائل الاتصال الحديثة.

وتعتبر منظمة اليونسكو UNESCO للتربية والثقافة، وهي إحدى الوكالات المتخصصة في الامم المتحدة التي لها باع طويل فيما يخص الأنشطة العالمية المتعلقة بالاتصالات وتقنية المعلومات، وتهتم إدارة الاتصال والثقافة في هذه المنظمة بتقنية المعلومات الدولية، وتقنية الاتصالات ، وثورة الاتصالات ، وكذلك ثورة المعلومات، ولذلك يطلق على المجتمع الدولي اليوم أنه مجتمع المعلومات أو مجتمع الاتصالات[2].

---

[1] عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيات الاتصالات الحديثة، الطبعة الأولى، 2009، دار النهضة العربية ، القاهرة، ص 7.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 11 و 12.

المبحث الأول: القانون الجزائي في مواجهة البيئة الرقمية

من المؤكد بأن القانون الجزائي هو في مواجهة لفضاء جديد المعلوماتي" والمصطلح الأجنبي الذي جاء منه هو« cyberespace »بدأت أول مرة الكاتب الروائي المختص في الخيال العلمي الأمريكي وليام جيبسون William Gibson في سنة 1984 في كتابه: Neuromancer فضاء عالمي بدون حدود، حيث أجهزة الإعلام الآلي مرتبطة فيما بينها عن طريق شبكات، وفي هذا العالم ستتطور الجريمة المعلوماتية «La cybercriminalité »[1] ويضعها بعض الكتاب العرب كما هي في كتاباتهم" الجريمة السيبيرية " وأنا لا أرى بأسا في ذلك لأن مصطلح "Cyber"[2] ليس له ترجمة حقيقية أو مقابل له في اللغة العربية، والإجرام المعلوماتي ترجمته الحرفية هي «La criminalité informatique »، ولا ضير في استعمال أحد المصطلحين فنحن نستعمل مصطلح التلفزيون والراديو وغيرها من المصطلحات الأجنبية التي دخلت في لغتنا، والأهم هو مواكبة التطور القانوني الذي تشهده الولايات المتحدة الأمريكية ودول أوربا في هذا الصعيد.

المطلب الأول: القانون الجزائي والجريمة المتصلة بتكنولوجيات الإعلام والاتصال

ونقوم فيه بتعريف الجرائم المتصلة بتكنولوجيات الاعلام والاتصال أولا، ثم نتناول خصائص الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ثانيا.

الفرع الأول: التعريف بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال

تُعرّف الجريمة عموما بأنها: « كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية"[3]

وعرفها البعض الآخر بأنها " عدوان على مصلحة يحميها القانون ويختص القانون الجنائي بالنص عليها وبيان أركانها والعقوبة المقررة لفاعلها »[4].

أما بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال باعتبار أن المشرع الجزائري قد اختار لها هذا الاسم بدلا من جرائم المعلوماتية، فإنه عرفها في المادة 2 فقرة أ من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بقوله « يقصد في مفهوم هذا القانون:

---

[1] في دراستنا هذه حول الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها سنستعمل العبارة التي جاء بها المشرع الجزائري وهي "**الجرائم المتصلة بتكنولوجيات الاعلام والاتصال**"، كما سنستعمل عبارة " **الجرائم المعلوماتية** " والتي لها نفس المعنى والعبارة أكثر تداولا عند الفقهاء القانونيون.

[2] مصطلح Cybercriminalité مأخوذ من cyber ويعني ***kubernan*** باليونانية ويعني يدير ويوجه ويحكم، أي المعالجة المعلوماتية وهي مرتبطة مع الاجرام الذي يستعمل الشبكات المعلوماتية ، أنظر في هذا :

Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, Droit pénal appliqué», 2010, ECONOMICA ,Paris France, page 7.

[3] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، الطبعة الخامسة، 2007 ، ص 21

[4] حسنين عبيد، الجريمة الدولية (دراسة تحليلية تطبيقية)، دار النهضة العربية ، سنة 1990، ص 45، مشار له لدى طارق إبراهيم الدسوقي عطية: الأمن المعلوماتي(النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 145.

الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: جرائم المساس بأ
العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظ
من هذا التعريف يمكن أن نحصي ثلاث أنواع من الجرائم التي
والاتصال وهي:

– جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات في المواد من 394 مكرر إلى 394 مكرر7 وهي أفعال الدخول أو البقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات، وكذلك فعل الإدخال أو الإزالة أو التعديل بطريق الغش لمعطيات في نظام للمعالجة الآلية؛

– الأشكال التقليدية المجرمة كالغش والنصب عن طريق شبكة الانترنت؛

– الجرائم المعروفة بالمحتوى كجرائم القذف والسب وتحريض القصر على الفسق والدعارة.

وتوجد عدة تعريفات للجرائم المتصلة بتكنولوجيات الاعلام والاتصال أوردها الفقهاء ولكنها تعد في أغلبها ضيقة لأنها تقتصر على الأنظمة المعلوماتية وخاصة منها المرتكبة عن طريق جهاز الحاسوب، غير مبرزين الأفعال التي ترتكب بواسطة أو ضد أنظمة الاتصالات، كجرائم القذف والسب باستعمال البريد الالكتروني أو غرف الدردشة في مواقع الانترنت وكلها تعد من تكنولوجيات الاتصالات، فالأنظمة المعلوماتية مرتبطة ببعض بواسطة شبكات الاتصال، هذه الشبكات تسمح لنظم المعلوماتية بمشاركة البرامج، والمعطيات والأجهزة التابعة لها، وفي دراستنا شبكات الاتصال هي أيضا مُنْظَمة في مجموعة واحدة مع شبكات المعلومات، وفي الوقت الحاضر شبكة الانترنت هي مثال عن نوع الشبكات المعلوماتية حيث تتصل أجهزة الحاسوب فيما بينها وتتم عملية تبادل المعطيات من خلالها.

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

– هي « كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية »[1]؛

– وهي « كل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت »[2]؛

– وهي« كل سلوك غير مشروع يتم بالتدخل في العمليات الالكترونية التي تمس امن النظم المعلوماتية والمعطيات التي تعالجها »[3]؛

– وهي « كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها » وهو تعريف لمجموعة من الخبراء في منظمة التعاون الاقتصادي والتنمية (OCDE)، ويؤخذ على هذا التعريف ابتعاده عن

---

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

[2] محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، طبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 152، مشار إليه لدى نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2008، ص 49.

[3] تعريف تبناه المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين بتاريخ 10-17 أفريل 2000 والمنعقد بفيينا، مشار إليه لدى Myriam QUÉMÉNER, Yves CHARPENEL ، مرجع سابق، ص 8.

مبدأ لا جريمة ولا عقوبة أو تدابير أمن إلا بقانون، أي هو يخال
السابقين له على هذا المبدأ الجنائي الهام، ويؤخذ على هذه التعاريف
العقوبات في حال ارتكاب الأفعال الضارة التي نص عليها قانون الع

– وهناك تعريف آخر للجرائم المعلوماتية للدكتور هلالي عبد اللاه أحمد بأنها: " عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، والتي يحميها قانون العقوبات ويفرض له عقابا"[1]

– وقد عرفها د. محمد شوقي بأنها:" كل فعل غير مشروع اقترن بالتواصل مع منظومات معلوماتية وشبكات الاتصالات، في حين يكون غياب هذا التواصل مانعا لارتكاب هذا الفعل غير المشروع "[2]، وبحسب الكاتب فإن هذا التعريف يحوي الوظائف الأربعة التي تلعبها النظم المعلوماتية في الأفعال غير المشروعة:

- **موضوع:** في الحالات المتعلقة بإتلاف المنظومة المعلوماتية، كذلك المعطيات أو البرامج التي تحويها، ففي هذه الحالة تكون المنظومة المعلوماتية هدفا وموضوعا للجريمة، ومن أوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية عندما تكون السرية (confidentialité) والسلامة (intégrité) والقدرة أو التوفر (disponibilité) هي التي يتم الاعتداء عليها[3]، بمعنى أن توجه هجمات الحاسوب إلى معلومات الحاسوب أو خدماته بقصد المساس بالسرية أو المساس بالسلامة والمحتوى أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها، وهدف هذا النمط الإجرامي هو نظام الحاسوب وبشكل خاص المعلومات المخزنة داخله بهدف السيطرة على النظام دون ترخيص ودون أن يدفع الشخص مقابل الخدمة، أو المساس بسلامة المعلومات وتعطيل القدرة لخدمات الحاسوب وغالبية هذه الأفعال تتضمن ابتداءً الدخول غير المصرح به إلى النظام الهدف.
- **دعامة:** المنظومة المعلوماتية تكون أحيانا موضعا أو دعامة لجريمة، وهو ما يسميها البعض بيئة للجريمة[4]، كما في تخزين البرامج المقرصنة فيه، أو في حالة استخدامه أداة تخزين أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونوعها.
- **أداة أو وسيلة:** إن قائمة الجرائم المرتكبة في الفضاء المعلوماتي تزيد يوما بعد يوم، تتضمن تصرفات تدخل في إطار الجرائم التقليدية، جرائم خاصة بقانون الأعمال، جرائم الاعتداء على الحقوق الفكرية والصناعية، تحويل الأموال، وكذلك جرائم المخدرات وجرائم الفساد التي ترتبط بتبييض الأموال وتمويل الإرهاب، فالانترنت قامت بإنماء العديد من

---

[1] مشار إليه لدى طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 158.

[2] Mohamed CHAWKI, Combattre la cybercriminalité, Edition de Saint Amans France, 2008, p 41.

[3] يوسف حسن يوسف، الجرائم الدولية للانترنت، المركز القومي للاصدارات القانونية، القاهرة، الطبعة الأولى، 2011، ص 33، وأنظر في ذلك أيضا محمد شوقي، المرجع السابق ص 40، في إشارة منه لتحديد مجال الجريمة المعلوماتية بقوله: =

« Tous les actes perpétrés contre l'assurance de la confidentialité, de l'intégrité, ou de la disponibilité des données ou des opération de traitement, sont commis dans un environnement électronique impliquant un réseau de télécommunication sont considérés comme une cybercriminalité ».

[4] يوسف حسن يوسف، المرجع نفسه، ص 35.

الجرائم المرتبطة بحركة المعلومات مثل الاعتداء على حقوق المؤل
السرية ، جرائم الإعلام والقذف[1]....

- **رمز**: النظام المعلوماتي يمكن استعماله مثل رمز للتهديد أو الخ
موجودة، هذه الحالات وُجدت في نوادي التعارف عبر مواقع الانترنت[2].

أمّا بالنسبة للتعريف الذي جاء به المشرع للجرائم المتصلة بتكنولوجيات الاعلام والاتصال بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية، فقد وُفق برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية، ولولا هذه النظم المعلوماتية وشبكات الاتصالات ما كان أن نصبغ صفة المعلوماتية على هذه الجرائم، وهو ما يوافق تماما التعريف الذي جاء به الدكتور محمد شوقي.

الفرع الثاني: خصائص الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

تمتاز الجرائم المعلوماتية بعدة خصائص تميزها عن الجرائم التقليدية هي:

أولا: أنها جريمة عابرة للحدود الوطنية: فالعالم الآن أصبح قرية، يمكن التجول في أنحائها بمجرد الضغط على فأرة الحاسوب المرتبط بشبكة الانترنت، فيمكن لشخص ما ان يرتكب جريمة ما في دولة ما وتكون آثارها في دولة أو دول عديدة أخرى وهذا ما نسميه تلاشي الحدود بين الدول في العالم الافتراضي، وخير مثال على ذلك القضية التي حدثت خلال سنة 1989 والمسماة مرض نقص المناعة المكتسب (الايدز) التي تتلخص وقائعها في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج التي تهدف في ظاهرها تقديم بعض النصائح المتعلقة بمرض نقص المناعة المكتسب، غير أن هذا البرنامج يحوي فيروسا يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل وتظهر عبارة على الشاشة يطلب فيها الفاعل مبلغ مالي يرسل على عنوان معين لِقاء حصول المتضرر على مضاد للفيروس، وبتاريخ 03 فيفري 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتم تسليمه للمملكة المتحدة بطلب من هذه الأخيرة باعتبار أن فعل الإرسال تم داخل إقليمها، وتم توجيه أحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية. وعلى الرغم من ذلك فإن للقضية أهمية لسببين:

الأول: تعد المرة الأولى التي يقدم فيها متهم للمحاكمة بتهمة إعداد برنامج خبيث (فيروس)،

الثاني: تعد المرة الأولى التي يتم فيها تسليم متهم في جريمة مرتبطة بتكنولوجيات الإعلام والاتصال.

وبسبب تزايد هذا النوع من الإجرام الذي انتشر في الكثير من الدول ولم تعد هناك دولة بمنأى عنه تعالت الأصوات من أجل التصدي لهذه الظاهرة وذلك في إطار تعاون دولي، بمقتضاه يتم توحيد القواعد القانونية إلى حد معين (مع احترام سيادة الدول في سن قوانينها التي تتناسب ومبادئها) والتي تجرم التصرفات التي يتم بها الاعتداء على النظم المعلوماتية وشبكات الاتصال المختلفة حتى لا يفلت مجرمو المعلوماتية من قبضة القانون، وكذلك إرساء

[1] محمد شوقي، المرجع السابق ص: 39

[2] محمد شوقي، المرجع نفسه ص: 42

قواعد إجرائية فعالة تسمح للمتحريين والمحققين في هذا النوع من
مرتكبيها إلى القضاء، وقد نادى بعض الفقهاء بوجوب إرساء قانو
الموضوعي والإجرائي، وذلك بأن تسن كل دولة قوانينها وفقا لهذا الا

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

ثالثا: صعوبة اكتشافها ونسبتها لشخص معين: لأن الجرائم المعلوماتية ترتكب بهدوء فإن اكتشافها يكون في كثير من الأحيان بمحض الصدفة، ولأن مستعملي تكنولوجيا الاعلام والاتصال غير مجبرين على الكشف عن هويتهم (l'anonymat) عند استعمالهم لهذه التكنولوجيات وخاصة عند تواصلهم بشبكة الانترنت يكون من الصعب التوصل إليهم والكثير من مرتكبي الأفعال الضارة والمجرمة لا ينالون جزاءهم لعدم امكانية التوصل إليهم[2]، وخاصة في الدول التي لا تملك التقنية والمهارات اللازمة في مؤسساتها الأمنية أو خلال التحقيق في تلك الجرائم من طرف سلطاتها القضائية.

رابعا: صعوبة إثباتها: إن التحقيق في الجرائم المعلوماتية يتطلب الإلمام بتقنيات تكنولوجيات الإعلام والاتصال، وليس فقط تعلمها بل مواكبة التطور السريع الذي يحدث كل يوم في هذا المجال، فيستحيل الإلمام بكل جوانب هذه التقنيات ولكن مسايرتها والتعاون فيما بين التقنيين قد يسهل استخلاص الدليل الالكتروني من بيئته الافتراضية والتحقق من سلامته، ويستلزم لذلك أن تقوم سلطات التحقيق بالتدريب والتأهيل اللازمين والاستعانة بذوي الخبرة الأكفاء حتى تكون أعمالهم في التحري والتحقيق على قدر من المهنية التي يمكن بها تقديم دليل الكتروني موثوق إلى القضاء.

مع العلم أن الدليل الالكتروني يترك دائما آثارا في حالة محوه أو تعديله والخبير فقط من يكتشف التلاعبات التي تحدث في النظم المعلوماتية التي يحدثها المجرمون لمحو آثار جرائمهم والآثار التي توصل إليهم، وسيكون في هذا الموضوع توضيحات أكثر عند التكلم في البحث والتحري عن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في الفصل الثاني من هذه الدراسة[3].

خامسا: إنها جريمة منظمة: في البداية اعتبرت الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كسلسلة متتابعة من الاعتداءات على الشبكات، ولكنها تلونت بصبغة المافيا أي الجريمة المنظمة، منشئة بذلك "سوق سوداء" حقيقية للمعلومات المقرصنة، ابتداء من التعدي على حقوق الملكية الفكرية والفنية، والغش في البطاقات البنكية، فأصبحت

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2008، ص 52-53.

[2] 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 Panthéon-Sorbonne paris I, disponible sur: www.univ-paris1.fr/.../2004_sept_OK_Brisset_ Giustinani_ Version_ ... . p 25

[3] 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-V5.1-pdf.

هناك صلات قوية بين الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المعلوماتية أكثر تنظيما يوما بعد يوم[1].

1- أصناف المجرمين مرتكبي الجرائم المتصلة بتكنولوجيات

إذا كان الانتقام أو الرغبة في التواجد هي الأسباب المتكررة لدى مجرمي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، فإن الحافز الأساسي يبقى مغريات الكسب المادي، ويعدّ الوسط الذي يمارس فيه هؤلاء المجرمون في كثير من الأحيان جد منظم وصارم بالنسبة لنشاطهم، كذلك بالنسبة لمستواهم المعرفي ولأهدافهم، وبعض الشباب لديهم سلوك فرضه إدمانهم على الانترنت حيث يتصرفون بانعزالية، مثل ذلك الشهير « Hacker croll »حيث مؤخرا استجوب وحوكم بعد قرصنته في 2009 حسابات Twitter خاصة حساب الرئيس الأمريكي Barack Obama[2]، قبض على الشاب من طرف قوات الشرطة لأجل النصب عبر الشبكة والذي تحصل بموجبها على 15 000 أورو، وحكم عليه بـ 5 أشهر حبس غير نافذة[3].

ولوحظ أن هناك في كثير من الأحيان علاقات طيبة تربط هؤلاء المجرمين فيما بينهم، كأن هذا النوع من الجرائم يحملهم على ابرام نوع من التحديات الضارة والمسلّية في نفس الوقت.

كما أن هناك صانعي للبرامج الضارة (كالفيروسات) يستعملها آخرون من أجل ارتكاب نشاطات مُجرمة، ومن الصعب وضع تصنيفا لهؤلاء المجرمين، حيث نلاحظ الآن منظمات إجرامية (المافيا) التي انتشرت في دول الشرق أو في أمريكا الجنوبية مع تراتبية منظمة بعدة مستويات تتصل فيما بينها، والقاعدة تتكون من مرمزين ـ مبرمجين(codeurs–programmeurs) ومثال ذلك شراء kit de phishing ثمنه 20 دولارا، و القيام بعملية فورية من نوع phishing ثمنها 60 دولارا، وثمار هذه العملية تكون سريعة ومباشرة، حتى ولو توجب القيام بملايين عمليات التجسس، فالجرائم المتصلة بتكنولوجيات الاعلام والاتصال أصبحت صناعة مع موزعي خدماتها، فيروساتها، وسطائها، مهندسي النظم، موزعي ملفات الخاصة بالبيانات البنكية أو البريد الالكتروني، وهذه الحالات مرئية كثيرا في دول الكتلة الشرقية كرومانيا وروسيا وأوكرانيا، والجدول التالي يبين تصنيفات مجرمي المعلوماتية ومهامهم[4].

نوع المجرم المعلوماتي	نوع النشاط الذي يمارسه
Script kiddles	شباب بين 15 و 20 سنة الذين يشكلون اليد العاملة
Drops	يحولون المال الافتراضي إلى نقود حقيقية
Mules	وسطاء يؤجرون حساباتهم للمجرمين المعلوماتيين
Crackers(black hat)	الدخول إلى الشبكات من أجل الإضرار
Hackers	قراصنة المعلوماتية، الجريمة المنظمة، المافيا
Spammeurs	طلبة أو إطار معلوماتي يبحثون عن موارد مالية إضافية

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p. 12.
[2] www.01net.com/editorial/514625/comment-hacker-croll-a-pirate-des-comptes-twitter/
[3] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.12.
[4] Ibid.p.13.

2- الاقتصاد الموازي:

المعطيات المجمعة من طرف القراصنة يمكن بيعها في المعاملات، فالأجر المطبق على رقم بطاقة ائتمان بدون PIN و[illegible] الالكترونية e-commerce يتراوح 25 دولار، وبطاقة ائتمان مع PIN مطابق تصل إلى 500 دولار، وبحسب نوعها فإن أحصنة طروادة(فيروس تجسس) يمكن تملكها بمبالغ قد تصل إلى المئات أو أكثر من الآلاف الدولارات.

فالمعلومات في الوقت الحالي تباع بأثمان زهيدة يوما بعد يوم، لأنه يمكن إيجادها وقرصنتها ببساطة، وبالنسبة للقراصنة المعلوماتيين فهم مَحميون من ناحية باستعمالهم أسماء مستعارة ومن ناحية أخرى بسبب ارتفاع عددهم، وهو فعلا ما يعد شبكات تحتية « underground » تتطور في أوربا الشرقية والولايات المتحدة والصين وألمانيا[1].

المطلب الثاني: التحديات المرتبطة بمكافحة الجرائم المعلوماتية

ونتناول فيه ما يلي:

الفرع الأول: اتساع ظاهرة جرائم تكنولوجيات الإعلام والاتصال وثمن خسائرها

تتميز جرائم تكنولوجيات الإعلام والاتصال بنوع من الغموض يتعلق باتساعها والحجم الحقيقي للاعتداءات التي يمكن أن تسببها، ومثل أي ظاهرة جنائية لا يمكن وضع معالم حقيقية لمداها، فبحسب مختصين في علم الاجرام قد لا يصل تسجيل الجرائم المعلوماتية المرتكبة سوى نسبة 15%، ومع ذلك توجد إحصاءات تساعد على تمييز مختلف الظواهر المتعلقة بجرائم تكنولوجيات الإعلام والاتصال، وتعمل على تجميع المعلومات بطريقة مماثلة لما يقوم به جهاز العدالة الجنائية، وبالرغم من تنوع هذه الإحصاءات، ولكل منها طريقة في قياس الأشياء، إلا أن الجميع يؤكد الزيادة السريعة لهذا النوع من الإجرام.

& 1- الصعوبات المنهجية في قياس حجم الجرائم المعلوماتية

بشكل عام توجد ثلاث صور للأرقام التي تمثل حجم الجريمة، « حقيقية »، « ظاهرة »، « قانونية »، فالأولى تحدد الرقم الحقيقي للجرائم المرتكبة (جنح وجنايات) خلال فترة زمنية معينة، وعدد معين من السكان داخل رقعة مكانية محددة المعالم، أما الثانية (الاجرام الظاهر) فتشمل مجموع الجرائم التي وصلت إلى علم مصالح الأمن والدرك الوطنيين، عن طريق إيداع الشكاوى، أو التبليغات، والجرائم الأقل خطورة لا تندرج ضمن مجموع الجرائم الظاهرية، إن الفرق بين الرقم الحقيقي للجريمة (الذي يمكن لأجهزة الأمن والدرك وضعه) والجريمة الظاهرة يسمى « الرقم الأسود »، وأخيرا السلطة القضائية تعرض الإحصاءات حول الحجم « القانوني » للجريمة، هذا الأخير يعادل عدد الدعاوى الجزائية المرفوعة أمام القضاء الجزائي، أي الجرائم التي وصلت إلى علم النيابة العامة، والتي تكون موضوعا للمتابعة الجزائية و موضوعا للإدانة، ومجموعهما يمثل « الرقم القانوني للجريمة »[2].

---

[1] Mohamed CHAWKI, op.cit.p.51.

وهذا التطور في سوق المعلومات المقرصنة لم يعد حكرا على هذه الدول فالكثيرون في الدول العربية أصبحت مهنتهم قرصنة البطاقات الرقمية بكل أنواعها وأكثرها انتشارا تلك الأرقام السرية المقرصنة من الانترنت لفتح القنوات المشفرة، وهي تجارة رائجة فعلا في أيامنا هذه.

[2] Mohamed CHAWKI, op.cit. p. 95.

الرقم الذي يمثل حجم الجرائم المتصلة بتكنولوجيات الإعلا
يجرنا إلى نتائج صحيحة مثلما هو رقم الحالات الحقيقي، فالحالات
على العراقيل التالية[1]:

- **أولا:** الطبيعة العامة لشبكة الانترنت والتي تسمح للمجرمين بإخفاء هوياتهم، بارتكاب جرائمهم و التواصل مع الغير عالميا، من أجل متابعتهم يجب حجز الاتصالات وما يتم نقله عبر الشبكات في الوقت الحقيقي خلال الاتصال الحقيقي، وهو ما يعد صعبا تقنيا بسبب أن العديد من الاتصالات لا يمكن متابعة مصدرها، فكثير من الأحيان يتلقى الضحية عنوان جهاز الحاسوب المتصل مباشرة عبر الانترنت، وليس عنوان الاتصال، حيث أن مصدر هذا العنوان يمكن أي يكون متلاعبا فيه، فبنية الانترنت لا توفر طريقة آلية لتحديد المصدر الصحيح للاتصالات، وبالتالي يكون المحققين بحاجة إلى الاتصال بكل مقدم لخدمات الانترنت على حده في هذه الدائرة الواسعة للاتصالات، وعندما تتجاوز هذه التحقيقات الحدود الوطنية، فهي تتجاوز غالبا حدود الوقت، وحتى في حالة اكتشاف الجرائم وتحديد المجرمين لا نجد تقارير مفصلة تسمح لنا بتحليل ، ومحاكمة، وتعيين هذه الجرائم.
- **ثانيا:** توجد صعوبات تتعلق بكشف الجرائم المعلوماتية وإقامة الدليل عليها، وبالنتيجة وفي حالة حدوث عطل معلوماتي توجد العديد من الأسباب التي قد تشرحه، ومثال ذلك الخطأ البشري بينما الدليل على سوء النية ليس سهلا إحرازه في الأوضاع التي يقوم فيها المجرمون بمحو كل أثر لفعلهم.
- **ثالثا:** غياب الرؤية في هذا الإجرام.
- **رابعا:** الكثير من الحالات المرفوعة أمام الأمن الوطني لا يتم متابعتها كلها، بسبب غياب التخصص ونقص الامكانات المالية .
- **خامسا:** في كثير من الحالات الجرائم المعلوماتية المرفوعة أمام السلطات القضائية عولِجت باعتبارها جرائم تقليدية(خيانة الأمانة، السرقة)، وبالنتيجة لا تحتسب خلال الإحصاءات واستطلاعات الرأي المتعلقة بالجرائم المعلوماتية.

وبناء على كل ما سبق، يمكن أن نأخذ مثالا على الاجرام المعلوماتي في فرنسا والولايات المتحدة الأمريكية (و م أ)، فمقابل 719 جنحة معلوماتية مسجلة عند مصالح المديرية المركزية للشرطة القضائية بفرنسا لسنة 1999، سجل مركز شكاوى الاحتيال عبر الانترنت (IFCC) في الولايات المتحدة الأمريكية 19490 جنحة معلوماتية خلال الفترة الممتدة من 8 ماي 2000 إلى 3 نوفمبر 2000، هذا الفرق يمكن تفسيره بأمرين: 1- مستعملي الانترنت في الولايات المتحدة الأمريكية أكثر عددا من الذين هم بفرنسا، حيث أن ثقافة فرنسا في الانترنت أقل تطورا؛ 2- الاحصاءات المنجزة من طرف المديرية المركزية للشرطة القضائية بفرنسا مرتكزة على الشكاوى المقدمة من طرف أشخاص محددي الهوية، بينما في الاحصاءات المنجزة في الولايات المتحدة الأمريكية يمكن أنها اعتمدت على شكاوى لم يحدد أصحابها، وأخيرا أساليب جمع المعطيات ليست موحدة على الصعيد الدولي، مما يشكل اختلاف في النتائج المحصل عليها، لذا يجب إدراج الشكاوى التي لم يعرف أصحابها ضمن الإحصاء إن ثبتت صحتها.

[1] Ibid.p. 96,97

§ 2- أدوات قياس الإجرام المعلوماتي

كما لاحظنا سابقا لا توجد إحصاءات كثيرة موثوق بها [illegible] المعلوماتي، وبالمقابل عدد الاعتداءات التي يتم كشفها تعكس مدى [illegible] الجرائم حيث يصعب تقديرها.

فمنذ سنة 2000 قدرت الخسائر المالية للمؤسسات التي تم الاعتداء عليها عبر العالم بـ 1600 مليار دولار طبقا للإحصاء السنوي الذي قامت به Information Week Research بالتعاون مع مكتب الاستشارات Waterhouse Coopers، وعلى الإجمال أضاعت هذه المؤسسات ما يقارب 3.3 % من وقتها بين البطالة التقنية و اصلاح الأنظمة المصابة.

الجرائم المعلوماتية سببت في خسارة مقدرة بـ 1000 مليار دولار في سنة 2008[1]، عن طريق سرقة المعطيات المعلوماتية من المؤسسات بحسب دراسة أجرتها شركة مختصة في الأمن المعلوماتي McAfee، ومن أجل أول دراسة على المستوى الدولي حول«أمن المعلومات الاقتصادية » قُدم في المنتدى الاقتصادي العالمي بدافوس (Davos-Suisse) عناصر جمعها أكثر من 800 مسؤول من اليابان، الصين، الهند، البرازيل، بريطانيا، دبي، ألمانيا، والولايات المتحدة الأمريكية مما يقدم تمثيلا أكيدا.

وبحسب تحليل لـ FBI (Federal Bureau of investigation) بالاشتراك مع iC3 (Crime Complaint Center) قدرت خسائر الاقتصاد الأمريكي من جراء الجرائم المعلوماتية في سنة 2009 بـ 559.7 مليون دولار بزيادة الضعف عن السنة التي سبقتها(264.6 مليون دولار)، وفي نفس الفترة الزمنية كان عدد الشكاوى لدى مكتب التحقيقات الأمريكي FBI من مستعملي الانترنت المتضررين بزيادة 22 % من 284 275 في سنة 2008 إلى 655 336 .[2]

هذه التقديرات للخسائر التي سببتها الجرائم المعلوماتية يجب أن تكون حاضرة عند رجال القضاء وأعوانه لمواجهة هذا الإجرام.

الفرع الثاني: الأمن المعلوماتي

إن أمن البنية المعلوماتية أصبح من الاهتمامات الكبرى للأشخاص والمؤسسات سواء العامة أو الخاصة لوضع حواجز تقنية و أخذ تدابير لمكافحة المحتويات غير المشروعة أو الضارة والمرتكبة عبر تكنولوجيات الإعلام والاتصال وخاصة منها الانترنت لحماية حقوق الملكية الفكرية والمعطيات الشخصية، وتقوية أمن النقل الالكتروني.

فالجرائم المعلوماتية تمثل في الغالب خطرا يسبب خسائر للاقتصاد وللمؤسسات التي تمثل البنية التحتية الحيوية للدول، وبالنتيجة الانترنت بالنسبة للمجرمين تعد أداة تضاعف مخالفاتهم التي تعد اعتداءات على أمن الشبكات في حد ذاتها وعلى مستعملي الانترنت ضحايا هذه الاعتداءات.

فالأمن المعلوماتي يعد أولوية استراتيجية أساسية لتطور المؤسسات، وتتم حماية النظم المعلوماتية والمعلومات التي تعالجها بوسيلتين:

الأولى: الحماية الفنية(التقنية) للنظم

---

[1] Resources.mcafee.com/content/NAUnsecuredEconomirsReport

[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p. .11

والثانية: الحماية القانونية لهذه النظم بسن التشريعات التي تنظم ال
كأداة لارتكاب جرائم أخرى.

§ 1- ماهية الأمن المعلوماتي: الأمن المعلوماتي هو « حماية أ
مشروعة، وهو أيضا أداة تتحكم في تنظيم العلاقات والاتصالات، وذلك دون أن يؤثر على قدرة مستخدمي هذا النظام على الأداء أو يعوق عملهم من حيث الكفاءة أو التوقيت »[1]، لا تعد الحماية المعلوماتية مانعة من اختراقات الأنظمة ولكنها تحد منها في حالة ما إذا كانت قوية وفاعلة ودقيقة، وفي حالة تحقق هذه الشروط وتم الاختراق فإنه يكون:

- مرهقا للقائم بالاختراق
- يستغرق وقتا طويلا
- يسهل اكتشافه قبل النجاح فيه أو بعده

§ 2- مجالات أمن المعلومات:

1- أمن المعلومات: وهو المرتبط بالمعلومات التي هي أساس أو هدف نظام المعلومات القائم

2- أمن الوصول إلى الأنظمة: ويشمل إجراءات تأمين عمليات التحكم في الدخول للنظام المعلوماتي ذاته، والتحكم في التطبيقات التي يعمل عليها نظام المعلومات بالمنشأة.

3- أمن برمجيات نظم المعلومات: وهو عملية حماية البرامج التي تشغل أو يقوم عليها نظام المعلومات ذاته.

4- أمن الاتصالات: وهو عملية تأمين وسائل الاتصال التي تعتمد عليها المنشأة في أعمالها الوظيفية[2].

§ 3- وسائل اختراق النظم المعلوماتية: يمكن تعريف الوسائل المعلوماتية التخريبية بأنها عبارة عن « برمجيات أو وسائط تقنية قابلة للتوظيف مع عتاد الحاسوب وبرمجياته لتحقيق الأهداف الرئيسة التالية:

1- مضايقة وإنهاك مستمر لموارد النظام المعلوماتي

2- تدمير قواعد البيانات والمعارف وموارد البرمجيات والنظم التطبيقية

3- إحداث ثغرات في النظام المعلوماتي ، أو التمهيد لها من خلال الكشف عن مواطنها »[3]

أهم وسائل اختراق نظم أمن المعلوماتية:

أولا: الفاحص Scanner

وهو عبارة عن برنامج تطبيقي أعد لغرض الكشف الآلي عن مواطن الضعف في المضيفات المحلية والنائية Local & Remote Hosts تعمد هذه البرمجيات إلى قرع أبواب الطرفيات TCP/IP والخدمات المصاحبة لها، وتباشر بعملية تسجيل ردود أفعالها من الموقع الهدف.

وبذلك توفر هذه الأدوات معلومات ثمينة تخص الهدف المضيف ومستوى الحماية الأمنية المعلوماتية التي يمتلكها، من أجل هذه تتبوأ هذه الأداة مكانة متميزة في ميدان أمن شبكة الانترنت، وتعتبر موردا ثريا لقراصنة المعلومات، حيث يمكنها الحصول على آلاف كلمات السر الشخصية.

---

[1] طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 515.

[2] طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 518

[3] طارق ابراهيم الدسوقي عطية، المرجع نفسه، ص 526

ثانيا: الشمّام Sniffer

يعرف الشمام بأنه عبارة عن أي جزء من عتاد الحاسوب أو
المرور المعلوماتي على الشبكة، لأغراض انتزاع أو اختطاف المعلو
البرتوكولات السائدة في الشبكات الحاسوبية مثل: IPX, TCP/IP, ETHERNET وغيرها من النظم حيث يباشر بوضع طرفية الشبكة Network interface، يتألف الشمام من جزأين أحدهما من عتاد الحاسوب، والآخر من برمجياته، تعتبر بطاقة الشبكة من نوع Ethernet Card المفتاح الأساسي لعتاد الحاسوب الذي يتكئ عليه الشمام بوصفه أداة ارتباط الحاسوب بالشبكات، ومحطات العمل، أما البرمجيات فيمكن توظيف البرمجيات الشائعة في ميدان تحليل الشبكات الحاسوبية شريطة أن تتوفر فيها خيارات متقدمة لعمليات الفحص، وتكمن التهديدات المعلوماتية التي تنشب عن أنظمة الشمام فيما يلي:

- القدرة على اقتناص كلمات المرور
- القدرة على اقتناص المعلومات الخاصة، والتي تمتاز بدرجة عالية من السرية
- امكانية استخدامها في خرق النظم الأمنية للشبكات الرقمية بشتى مستوياتها.

ثالثا: مصدّع كلمات المرور(كلمات السر) Cracker de mots passe

تشمل أداة مصدع كلمات المرور أي برنامج تطبيقي يمتلك القدرة على تجاوز عقبة شيفرة كلماتها، أو احباط آليات الحماية المصاحبة لها، وهو لا يلغي الشيفرة المستخدمة فيها، أو يظهرها على شكل نص مقروء، بل يتيح إمكانية تجاوز الجدار الامني الذي توفره لصاحبها في درء أي نشاط يسعى إلى تجاوز الحدود الشخصية لمملكة معلوماته الخاصة.

رابعا: حصان طروادة Cheval de Troie

يعتبر حصان طروادة من الأدوات الفاعلة في ميدان خرق الأمن المعلوماتي، وتوجد أكثر من خاصية برمجية تتصف بها النسخ المتوفرة بميدان المعلوماتية من هذه الأداة، بحيث نقول عنه إنه عبارة عن:

1- برنامج غير مرخص مُتضمن في برنامج شرعي، فيباشر البرنامج غير المرخص إجراء زمرة من المهام التي لا يريدها المستخدم،

2- برنامج شرعي تم تغييره بإدخال شيفرات غير مرخصة داخل هيكليته البرمجية، بحيث يقوم بجملة من الأنشطة غير المشروعة،

3- برنامج يوفر خدمة مفيدة أو مثيرة لاهتمام الآخرين، إلا أنه يقوم بأنشطة غير متوقعة، مثل سرقة كلمات المرور، او استنساخ ملفات، أو إلغاؤها دون علم المستخدم.

وتكمن الصعوبة في تشخيص هوية برنامج حصان طروادة في كون الأنشطة التي يقوم بها لا يمكن تمييزها عن بقية الأنشطة التقليدية السائدة في ميدان المعلوماتية، فلا توجد طريق تصلح كأساس للحكم على وجود حصان طروادة، إلا عن طريق المقارنة بين الأنشطة التي يقوم بها برنامج ما مع قائمة الأنشطة التي يتوقعها المستخدم لذلك البرنامج، وهذا أمر يصعب القيام به.

وتتنوع أشكال حصان طروادة بحسب وظيفتها:

– الأبواب المخفية Portes dérobées: وهي الأخطر والأكثر استـ
الانترنت الذي يمنع المستخدم من السيطرة على جهاز الحاسوب ا
بإدارة حاسوب المستخدم المشروعة، ولكن الباب المخفي مُثبت ويُشغ
الدخيل يتم به الاشراف على النظام المحلي للحاسوب، ولا يظهر إلا نادرا في سجل التطبيقات النشطة، حيث يمكنه إرسال أو استقبال أو تنفيذ أو حذف ملفات أو مجلدات، كذلك تشغيل الجهاز، فهدفه هو استعادة المعلومات السرية، تشغيل رمز خبيث، تدمير معطيات..إلخ.

– حصان طروادة من نوع PSW وهو يبحث عن ملفات النظام التي تحوي معلومات سرية (مثل كلمات المرور، تفاصيل النظام، عناوين IP ، ..) ثم يقوم بإرسال المعلومات المجمعة للشخص السيئ النية عبر البريد الالكتروني.

– حصان طروادة الجاسوس: وهو عبارة عن برنامج جوسسة وتسجيل للضربات على لوحة المفاتيح، فهو يراقب ويسجل أنشطة المستخدم في حاسوبه ثم يحول المعلومات (الضربات على لوحة المفاتيح، التقاط الصور عبر الشاشة، سجل التطبيقات النشطة..) إلى المُهاجم.

بالإضافة للعديد من أنواع احصنة طروادة التي لها مهام مختلفة، يمكنها ان تقوم بمهمة أو أكثر بحسب برنامجها[1].

خامسا:التصيّد (PHISHING)

هو محاولة الحصول على المعلومات الخاصة بمستخدمي الانترنت سواء أكانت معلومات شخصية أو مالية، عن طريق الرسائل الإلكترونية أو مواقع الانترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية وحكومية، كالبنوك الإلكترونية online banks[2].

أتت كلمة Phishing لأنّ محتالي الإنترنت (Internet Scammers) يستخدمون رسائل إلكترونية مغرية لاصطياد (fishing) كلمات السر والبيانات المالية من مستخدمي الإنترنت. كما وأن قراصنة الإنترنت Hackers يميلون لاستبدال حرف (f) بحرفيّ (ph) .

يقوم المتصيدون (phishers) بإرسال رسائل إلكترونية e-mails زائفة تطلب من مستخدمي الشبكة زيارة إحدى المواقع الإلكترونية بحيث يطلب من المستخدم إجراء تحديث على بياناته، مثل:اسم المستخدم، كلمة المرور، بطاقة الائتمان، الضمان الاجتماعي، رقم الحساب في البنك. هذه المواقع الإلكترونية هي مواقع زائفة، صمّمت فقط لسرقة معلومات المستخدم، ومن الأمثلة عليها موقع شبيه بـ (yahoo)،حيث يقوم المستخدم بإدخال اسم البريد وكلمة السر للدخول إلى بريده الإلكتروني، دون العلم أنه تم الاطلاع على تلك البيانات المدخلة.

ولكن هناك عوارض يمكن أن تكشف وجوده تتمثل في:

– أنشطة غير طبيعية للمودم(modem)، ولبطاقة الشبكة، ولنشاط القرص الصلب (تُحمل معطيات في غياب لأي نشاط من طرف المستخدم)

[1] Fr.wikipedia.org/wiki/cheval_de_troie_(informatique)
[2] ar.wikipedia.org/wiki/phishing

– ردود فعل غريبة للفأرة

– فتح برامج متكرر وارتجالي، كذلك فيما يتعلق بقارئ الأقراص المد

– تعطلات متكررة

– إعادة تشغيل متكرر للنظام.

سادسا: الفيروسات virus:

الفيروسات عبارة عن برامج خبيثة صممت لتنتشر إلى حواسيب أخرى، وهي تربط نفسها ببرامج شرعية أخرى تسمى « Hôtes »، يمكن للفيروسات تخريب بشكل كبير أو قليل وظائف الحاسوب المصاب، كما يمكنها الامتداد إلى جميع وسائل نقل المعطيات الرقمية كالشبكات المعلوماتية، الأقراص المدمجة، مفاتيح USB...

وتختلف الفيروسات عن أحصنة طروادة والديدان المعلوماتية، فهذه الأخيرة يمكنها الانتشار وتتناسخ بنفسها دون اللجوء إلى برامج Hôtes ولكنها تستعمل الشبكات لتتمكن من الانتشار في مجموعة من الحواسيب، أما حصان طروادة فهو برنامج لا يتناسخ ولكن ينقسم إلى عدة أصناف لها وظائف معينة كما تم تناوله سابقا، ولكن درج استعمال مصطلح الفيروسات على كل برنامج معلوماتي خبيث بما في ذلك أحصنة طروادة والدودة المعلوماتية وغيرها من البرامج .

وهناك العديد من التصنيفات للفيروسات ومنها:

– الفيروس التقليدي والذي يدمج داخل برنامج طبيعي، حيث في كل مرة يشغل المستخدم هذا البرنامج المصاب يقوم بتشغيل الفيروس الذي يقوم بدوره بالاندماج داخل برامج أخرى قابلة للتشغيل، كذلك في حالة وجود ضغط يمكنه بعد وقت معين أو في ظروف معينة تنفيذ إجراء محدد مسبقا، هذا الاجراء يكون عن طريق رسالة تافهة تؤدي إلى اتلاف بعض وظائف نظام التشغيل، أو اتلاف بعض الملفات أو تدمير كامل لجميع معطيات الحاسوب (يسمونها القنبلة المنطقية)[1].

– virus de boot فيروسات عدوى قاطع التحميل: تستقر هذه الفيروسات في الأماكن التي يقراها الكمبيوتر بالقرص الصلب عند اقلاعه (تشغيله) ليستقر في الذاكره وينفذ شفرته

–Macrovirus: فيروسات الماكرو: وهو أحدث أنواع الفيروسات وهو فيروس يكتب بلغة الورد Word ويصيب هذا الفيروس ملفات البيانات Macro. ويصيب ملفات Microsoft Office كملفات الوورد والإكسل(Word, Excel) .

وتظهر أعراض الاصابة بالفيروسات على النحو التالي:

- تكرار رسائل الخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع [نظام التشغيل] أو تنفيذ بعض التطبيقات، رفض بعض التطبيقات للتنفيذ.

[1] http://fr.wikipedia.org/wiki/Virus_informatique

§ 4- الحماية الفنية للمعلومات:

تتمثل الحماية الفنية في إيجاد أنظمة أمان لحماية نظم المع
من البرامج التي تحول دون قرصنة المعلومات ودخول القراصنة إلى النظم المعلوماتية ، كبرامج التقفيه للمعلومات وللمواقع، البرامج المضادة للفيروسات، الجدران النارية، وكذلك التشفير(Cryptologie) الذي يعد وسيلة هامة للحفاظ على سرية المعلومات والرسائل، والذي سنتناوله بالتفصيل نظرا لأهميته من الناحية القانونية:

التشفير Cryptologie:

ينقسم علم التشفير إلى Cryptographie الذي يشمل دراسة الآليات المخصصة لضمان السرية، وتحليل التشفير cryptanalyse، الذي يهدف إلى إبطال الحماية أو وضعها.

ويقصد بمجموع تقنيات التشفير والترميز تحويل المعطيات، والذي يهدف إلى سلامة التخزين أو النقل للمعطيات، وبالتالي يسمح بتأمين سريتها والتحقق من هوية الكيان صاحبه Authentification [1] ومراقبة سلامتها(المعطيات)[2]، فتحويل المعطيات يكون بجعلها غير مفهومة inintelligible للغير، فبعض مستخدمي الانترنت[3] يبتغون أن يتمكنوا – بواسطة برنامج خاص– من تشفير معلوماتهم قبل نقلها عبر الشبكة، على أن يتم فك رموزها ببرنامج مماثل عند استقبالها من جانب المرسل إليه[4].

يعتمد التشفير على أربع مبادئ، الأول خصوصية وسرية التبادل بجعل المعلومات غير مفهومة لكل الأشخاص ما عدى المعنيين بنقلها، من ناحية أخرى ينبغي على هذه الطريقة ضمان سلامة المعطيات التي لا يجب أن تتلف خلال المراسلة بطريقة عرضية أو مقصودة، كذلك يجب أن تسمح هذه الطريقة بالتعرف على هوية القائمين بها بالتحقق من هذه الهوية، أي يجب ضمان كل من المراسلين بأنهم أصحاب العملية التي يجب أن تكون، وأخيرا

---

[1] Authentification هو الإجراء الذي يرتكز من أجل نظام معلوماتي على التحقق من هوية كيان (شخص، جهاز الحاسوب..) لغرض الترخيص بالدخول لهذا الكيان إلى مصادر معينة (أنظمة، شبكات، تطبيقات..) فتأكيد الهوية يسمح بالتعرف على هوية الكيان و Authentification يسمح بالتحقق من هذه الهوية، ويتم ذلك بأربع طرق تقليدية للتأكد من هوية هذا الكيان(commettant) وهي:1- استخدام معلومة لا يعرفها إلا هذا الكيان، 2- استخدام معلومة واحدة يحوزها هذا الكيان فقط، 3- استخدام معلومة تميز الكيان في سياق معين، 4- استخدام معلومة وحده الكيان من يضعها.

أنظر في ذلك http://fr.wikipedia.org/wiki/Authentification .

[2] L'article 29 de la loi 2004-575 du 22 juin 2004 pour la confiance dans l'économie numérique «On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie». Disponible sur www.le

[3] وخاصة المؤسسات المالية كـ VISA card و Master card لاستعمال بطاقات الائتمان Crédit Card في التسوق عبر شبكة الانترنت

[4] طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 586.

يجب أن تسمح هذه الطريقة بأن كل من القائمين عليها(أص
التنصل(الإنكار)[1].

وبالرغم من المزايا التي يقدمها التشفير إلا أن له عواقب وخيمة فيما يتعلق باكتشاف الجرائم وخاصة منها الارهابية ومروجي الصور الاباحية والاتفاقات الاجرامية للمافيا التي تبرم عن طريق تكنولوجيات الاتصالات الحديثة، وما يعقب ذلك من موانع تحول دون اتمام التحريات والتحقيقات القضائية، فلا يمكن اقامة دليل على ارتكاب جريمة إذا كان هذا الدليل مشفراً، لذا عمدت الكثير من التشريعات للحد من التشفير وذلك بوجوب تقديم ترخيص خاص لمن يعمد إلى استعماله ولكن بشكل متفاوت من تشريع لآخر، كما أن المشرع الجزائري لم يتناوله مطلقا حتى في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أما بالنسبة للمشرع الفرنسي فقد حدّ سابقا من اللجوء إلى التشفير وذلك لضرورات الدفاع والأمن الوطنيين، إلى غاية 1990 حيث تم تحريره تدريجيا، وذلك بالاعتماد أولا على تصريح ورخصة مسبقة من هيئة مختصة، إلى غاية صدور القانون 96-659 المؤرخ في 26 جويلية 1996 حيث أن بعض الوسائل والخدمات المتعلقة بالتشفير أصبحت حرة تماما، كذلك الاستعمال الشخصي من طرف الشخص الطبيعي لوسائل التشفير من أجل سلامة الرسائل المنقولة لم يعد يخضع لأي تصريح أو ترخيص، ومثال ذلك حماية الأرقام السرية، رمز التعريف الشخصي أو معطيات التحقق من الهوية المستعملة لمراقبة الدخول إلى المعطيات، ثم تلاه القانون رقم 2004-575 المؤرخ في 21 جوان 2004 من أجل الثقة في الاقتصاد الرقمي(LCEN) في الباب الثالث المتعلق بالأمن في الاقتصاد الرقمي، حيث أكد المشرع الفرنسي على اللجوء إلى وسائل وخدمات التشفير، ففي فرنسا يقتضي نظام التشفير في قطاع تكنولوجيات الاتصال توفر خاصيتين، سواء لما تَضْمنه من سرية المعطيات أو في تحديد للهوية وسلامة المعطيات كالتوقيع الالكتروني، ولنظام التشفير في القانون الفرنسي أربع مقاصد: الاستيراد والتصدير والتزويد والاستعمال، فالمادة 30 من القانون السابق الذكر تحدد النظام القانوني للتشفير من خلال مقاصده الأربعة، فاستعمال وسائل التشفير وتوفيرها (عرضها) واستيرادها وتصديرها يكون بشكل حر إذا كان الغرض منها وعلى سبيل الحصر ضمان خاصية مراقبة سلامة المعطيات وتحديد الهوية، فإن كانت وسائل التشفير لا تضمن بشكل حصري هذه الوظائف فإنها يجب أن تخضع لترخيص أو تصريح من الوزير الأول، كذلك الأمر بالنسبة للمتخصصين في إصدار الشهادات الالكترونية يجب أن يصرحوا بنشاطهم في توفير خدمات التشفير إلى مصالح الوزير الأول وهم ملتزمون بالسر المهني، ومخالفة هذه الإجراءات تعرض مخالفيها إلى تطبيق جزاءات إدارية وفي نفس الوقت جنائية (جنح وجنايات) بحسب القانون الفرنسي[2].

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.82.
[2] Ibid. p. 84.

المبحث الثاني: الحماية الجزائية لنظم المعلوماتية والجرائم

تطورت تكنولوجيا الإعلام والاتصال خلال القرن الماضي [illegible] الوقت يمكن للجميع اقتنائها، ثم تطور الأمر فأصبحت هذه الوسائل [illegible] شبكات أهمها شبكة الانترنت، لكن هذا المظهر المتألق لهذه الحضارة الجديدة يقابله تطور في أشكال الجريمة المرتكبة عبر هذه التكنولوجيات فأصبح ما يسمى "عولمة الجريمة"[1]، فأصبحت تحديات الجريمة عابرة الحدود قضية تهدد الأمن الوطني والدولي في آن واحد، بما تقدمه من تسهيلات للأنشطة الإجرامية للأفراد أو للمنظمات(المافيا والجماعات الإرهابية)، وذلك بخلقها بيئة خصبة للأنشطة الإجرامية، ويطرح السؤال نفسه حول مدى كفاية آليات مكافحة هذه الجرائم، سواء من ناحية التقنية العلمية المستخدمة، أو من حيث تأهيل العناصر البشرية القادرة على اكتشاف الجريمة ذات الطبيعة التقنية المعقدة، والتحقيق فيها، والقدرة على التعامل مع مختلف القرائن والأدلة الرقمية ، ناهيك عن قصور التشريعات الوطنية في معظم الدول لمكافحة هذا الإجرام.

والأمر المهم الذي يجب تذكره أن الجريمة في مظهرها القديم لم تختفِ، بل اتسع نطاقها ليحتل العالم الافتراضي أي الانترنت وباقي تكنولوجيات الإعلام والاتصال(خاصة منها الهاتف المحمول المتعدد الوسائط)، وظهرت علاوة على ذلك أنماط من الجرائم المستحدثة زادت في حجم الضحايا والخسائر وفي كافة المستويات[2]، فنحن نشاهد بما لا جدال فيه تنامي هذا الإجرام لأن المجرمين يستوعبون بسرعة امتيازات الشبكات الرقمية التي تسمح لهم بارتكاب جرائم على أوسع نطاق بإمكانات مادية ضئيلة مع القليل من الخطر[3].

وبسبب هذا الحجم المتزايد للجرائم المتصلة بتكنولوجيات الاعلام والاتصال فضلنا دراستها وفقا للتقسيم الفقهي الغالب في كتب الفقه وما تم النص عليه في التشريع الجزائري مع دراسة مقارنة مع التشريع الفرنسي، والذي سيكون كالتالي:

المطلب الأول: أهم جرائم الاعتداء على الأشخاص والدولة باستعمال تكنولوجيات الاعلام والاتصال

ونتناول فيه مجموعة من الجرائم أهمها:

الفرع الأول: انتحال الشخصية:

انتحال الشخصية يرتكز على أخذ اسم الغير، من أجل التنكر أو إخفاء نفسه أو التهرب من مسؤولياته وبالتالي المتابعة الجزائية، ويمكن تعريفها عمليا بأنها "أيا كان يستعمل أو يستغل بعلم المعلومات الشخصية لشخص آخر لغاية غير مشروعة "[4]، والهدف الوحيد هو ارتكاب جريمة للحصول على امتياز مادي.

---

[1] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الالكترونية)، منشورات الحلبي القانونية، الطبعة الأولى، بيروت، 2007، ص 22.

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

[3] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.8

[4] Ibid. op.cit.p.89.

انتحال الشخصية هو سلوك تقليدي لمجرم، ولكنه ضا
والانترنت، فهذا التحايل عرف زيادة سنوية تصل إلى 40 % في
واتساع هذه الظاهرة سببه اللجوء للشبكات الرقمية لهدفين، من
باستعمال اسم مستعار، ومن جهة أخرى بهدف غير مشروع ولتحقيق مكاسب مالية.

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

1- انتحال اسم عائلة خلاف اسمه في محرر عمومي أو رسمي أو في وثيقة إدارية معدة لتقديمها للسلطة العمومية وذلك بموجب المادة 247 من قانون العقوبات، تقابلها المادة 433-19 من قانون العقوبات الفرنسي.

2- أحكام المادة 248 ق ع (تقابلها المادة 781 ق ع فرنسي) التي نصت على من تحصل على صحيفة السوابق القضائية باسم الغير، وذلك بانتحال اسما كاذبا أوصفة كاذبة.

3- انتحال اسم الغير في ظروف أدت إلى قيد حكم في صحيفة السوابق القضائية لهذا الغير أو كان من الجائز أن تؤدي إلى ذلك (المادة 249 ق ع وتقابلها المادة 434-23 ق ع فرنسي ولكن في حالة استعمال اسم الغير في ظروف أدت إلى متابعات جزائية، وقيد حكم في صحيفة السوابق القضائية لا يكون إلا بمتابعة جزائية تسبقه).

وفي تطبيق موسع لهذه المادة، اعتبرت محكمة النقض الفرنسية أن فعل استعمال عنوان الكتروني للغير الذي يتبعه خطر متابعات جزائية لهذا الغير يشكل جنحة انتحال للشخصية[1].

ويمكن للقاضي أن يعاقب أيضا على التصرفات الضارة في حالة النصب عبر الشبكة المنصوص والمعاقب عليها بموجب المادة 372 ق ع وتقابلها المادة 313-1 ق ع فرنسي والذي استعمل فيها المجرم أسماء أو صفات كاذبة.

وفي فرنسا تم تعديل بعض مواد قانون العقوبات حيث جرمت الأفعال التي من شأنها استعمال هوية الغير أو معطيات مهما كانت طبيعتها عبر شبكة الاتصالات الالكترونية، تسمح بتعكير هدوء هذا الغير أو آخرون.

الفرع الثاني: جرائم الاعتداء على حرمة الحياة الخاصة وصور الأشخاص

الحق في الحياة الخاصة هو أحد الحقوق اللصيقة بالشخصية التي تثبت للإنسان لمجرد كونه إنسانا، وهناك الكثير من التعريفات لهذا الحق نظرا لاختلاف نطاق الخصوصية من فرد لآخر، فهناك من يجعل حياته الخاصة كتابا مفتوحا وهناك من يجعلها سرا غامضا، كما يختلف مضمون الحياة الخاصة من مجتمع لآخر نتيجة لاختلاف القيم الأخلاقية والتقاليد والثقافة والدين، مع وجوب التأكيد على أن الخلاف ينصب على نطاق الحق في الحياة الخاصة لكنه لا يمتد إلى الحق في الخصوصية فهو حقيقة مؤكدة لجميع الأفراد في كل المجتمعات[2].

فقد عرفه الفقيه Allen Westin بأنه: « الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات في أن يحددوا لأنفسهم متى وكيف وبأي قدر يمكن ايصال المعلومات الخاصة بهم إلى غيرهم »[3].

---

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.92

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2008، ص 165.

[3] مشار إليه عند نهلا عبد القادر المومني، ص165.

أما الفقيه الفرنسي Ean Malherbe فقد عرفه بقوله: « الـ
يكونان متطابقين لأنهما يقرران حق الفرد في حماية اسمه ومراسلاته
وكل ما له تأثير على حياته الشخصية »[1].

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

و نص المادة 39: «لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة»

§ 1- القواعد العامة لحماية الحياة الخاصة

أما بالنسبة لقانون العقوبات فقد جرم أفعال تمس الحياة الخاصة للأشخاص كجريمة الوشاية الكاذبة (المادة 300 ق ع)، جريمة إفشاء السر المهني في غير الحالات المحددة قانونا (المادة 301 ق ع) كذلك جريمة اتلاف الرسائل أو المراسلات الموجهة للغير وفضها مع سوء النية (المادة 303 والمادة 137 ق ع)، جرائم القدف والسب التي تمس الاعتبار والشرف (المواد من 296 إلى 299 ق ع) وتقضي المادة 303 مكرر3 من ق ع على مسؤولية الشخص المعنوي عن الجرائم المرتكبة المذكورة آنفا.

وبالنسبة للقانون رقم 03/2000 المؤرخ في 5 أوت 2000 الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، فقد نصت المادة 127 منه في الفصل المتعلق بالأحكام الجزائية على ما يلي: « تطبق العقوبات المنصوص عليها في المادة 137 من قانون العقوبات على كل شخص مرخص له بتقديم خدمة البريد السريع الدولي أو كل عون يعمل لديه والذي في إطار ممارسة مهامه، يفتح أو يحول أو يخرب البريد أو ينتهك سرية المراسلات أو يساعد في ارتكاب هذه الأفعال.

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

يعاقب بالحبس من شهرين (2) إلى سنة وبغرامة مالية من 50.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل شخص، غير الأشخاص المذكورين في الفقرتين السابقتين، ارتكب الأفعال المعاقب عليها بموجب هاتين الفقرتين.

علاوة على العقوبات المنصوص عليها في الفقرات 1 و2 و3 المشار إليها أعلاه، يمنع المخالف من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية واللاسلكية أو قطاع البريد أو في قطاع ذي صلة بهذين القطاعين لمدة تتراوح بين سنة إلى خمس(5) سنوات»

[1] نهلا المومني، المرجع نفسه، ص 166.

§ 2 ـ التحديات المرتبطة بمكافحة الجرائم المتصلة بتكنولوجيات الـ
للأشخاص

إذا كانت الانترنت وسيلة للاتصالات فيمكنها أيضا ان تهدد
يقدم أبعاد جديدة لهذا التهديد، حيث يتم تشجيع مستعملي الانترنت بالتضحية بأنفسهم بالبوح بحياتهم الخاصة، والنتيجة هي دفعهم إلى الكشف عن أكثر العناصر الحميمية في حياتهم (صداقاتهم، أحبائهم، عائلاتهم، حياتهم المهنية...).

فالشبكات الاجتماعية تُكَوِن القواعد الأساسية للاتصالات عبر النت[1]، تسمح بمشاركة النفع العام، وهي الآن تشكل نجاحا منقطع النظير خاصة بين الشباب الذي يتراوح عمره بين 14 و35 سنة، وإذا كانت الأسباب وراء هذه المنافع المتزايدة كثيرة، فإن المخاطر كذلك ـ في مواجهة لحماية الحياة الخاصة.

وحتى في حالة عدم وجود أي قانون يمنع نشر الفرد لمكنونات حياته الخاصة، فهو لم يُنذر حتّى من أن هذا البوح هو تهديد طبيعي في أبعاد لا أحد يعلم حدودها لا الزمنية ولا المكانية، ومن ناحية أخرى هذا البوح الإرادي يفتح بكل تأكيد الطريق إلى سلوكيات سيئة من أشخاص لا يتهاونون عن الإضرار العمدي بالأشخاص.

كذلك فإنه من المؤكد أن تقديم لشخص عن طريق الانترنت مجموعة من الصور أو المعلومات عن الغير ولو كان من مجموعته المحيطة به (العائلة، حياته الخاصة والمهنية...) يخلق قناة ممتازة للاعتداءات على الحياة الخاصة أو الحق في الصورة وحتى القذف، ومثال ذلك حالة نشر صور للأصدقاء في بطاقته، هذا النشر العلني يمكن أن يشكل اعتداء على حق الصورة إذا لم يوافق الشخص صاحب الصورة على ذلك قبل النشر، وتقضي المادة 303 مكرر1 « يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.. » وتنص المادة 303 مكررعلى أنه: « يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

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

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

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية ».

إن تطور هذه المواقع يؤدي إلى خطر آخر مقلق لا تظهر نتائجه إلا بعد حين وهو فقدان جيل كامل لسلوكه في حماية حياته الخاصة ومعطياته الشخصية، والنتيجة مستعملي الانترنت الصغار يجدون أن الحد والتضييق الإرادي في حياتهم الخاصة يعد أمرا طبيعيا جدا عند اطلاعهم الآخرين ـ غالبا من أجل الترفيه والتسلية ـ على معلومات جد خاصة[2].

[1] النت هو اختصار لمصطلح الانترنت، يستعمل في حالة الاتصال بالانترنت مباشرة.

[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.16-17

هناك الملايين من مستعملي الشبكات الاجتماعية ينشرون أصدقائهم، وأحيانا معتقداتهم الدينية، مثل هذه الثورة في العقليات (ح الخاصة، وفي مواجهة لهذه الظاهرة من الأحسن قبل كل شيء تحس حياتهم الخاصة، لذا ندعو في هذه الدراسة قيام المؤسسات التربوية والتي تعنى بالطفولة والشباب بالتوعية والتحسيس حول خطورة هذا النوع من الشبكات.

كما نلاحظ غالبا ما يكون هناك غياب للترجمة العربية لشروط الاستعمال وللعناوين التي لا تسمح لمستعملي الانترنت وخاصة منهم الشباب تقدير النتائج المتعلقة باستعمال وإطلاع الآخرين على معطياتهم الشخصية في هذه المواقع.

وبالنسبة لاحتمالات الأضرار التي يمكن حدوثها للأشخاص في هذه المواقع فإن التصرفات القضائية المنفردة خلال الوقت الحالي يصعب إن لم نقل يستحيل العمل بها، لأن عدم التأكيد على نظام قانوني لمواقع الشبكات الاجتماعية فيما بين الناشرين ومقدمي خدمة الإيواء، يؤدي إلى التساؤل حول الطريقة المتبعة في حالة وجود نزاع معين، ومثال ذلك في حالة وجود صور مُذِلة لطفل في الرابعة عشرة من عمره نشرها أصدقاؤه في المدرسة في موقع للفايس بوك (Facebook)، أو تسجيل فيديو لفتاة متمدرسة في إقامتها الجامعية مع صديقاتها يتراقصن عبر YouTube، فهل يمكن اتخاذ إجراءات استعجاليه أمام المحكمة لسحب هذه المحتويات في الوقت القريب؟

في هذا الأمر حيث عدد ضحايا هذا النوع من الاعتداءات يتزايد ونتائجها يمكن أن تكون فعلا خطيرة، يبدو من الضروري طرح إجراءات بسيطة وسريعة متلائمة مع حالات كهذه.

§ 3- المؤسسة والحياة الخاصة للموظف[1]:

يمكن للعامل أو الموظف في مكان عمله ان يتنقل عبر النت والاتصال بآخر نقطة في العالم، واليوم أغلبية العمال يستغلون الأدوات المعلوماتية الموضوعة تحت أيديهم في أماكن عملهم من أجل تفحص بريدهم الالكتروني الخاص أو التنقل عبر مواقع مختلفة في الإنترنت، كذلك الأمر في حالة الاتصال بالانترنت بطريقة واضحة ومتكررة إلى حد الافراط في مكان العمل ومن أجل أغراض شخصية لا علاقة لها بالعمل ومن ثَم يقوم بمسح سجل الاتصالات، الاجتهاد الفرنسي عدّ هذه الحالة من الأخطاء الجسيمة التي لا يمكن بها للعامل الاستمرار في مؤسسته، فما هي حقوق وواجبات كل من الموظف ورب عمله في هذه الظروف الجديدة المرتبطة بظهور وتطور الشبكات الرقمية؟

فمسألة الحياة الخاصة للأجير في مقر عمله وإمكانية أرباب العمل فتح الملفات والبريد الالكتروني لموظفيهم تشكل جدال(على الأقل في العالم المتحضر تقنيا) في الوقت الحاضر.

إن مراقبة الأجير داخل مكان عمله ترتكز على أمرين، الأمر الأول يتعلق بمراقبة نشاطه بفضل وعن طريق الشبكات التكنولوجية للمعلوماتية وشبكات الاتصال، والأمر الثاني يتعلق بالتطورات الحاصلة المرتبطة بدراسة القواعد المتعلقة بمراقبة شروط استعمال أداة العمل التي يمثلها جهاز الحاسوب عند الموظف، فكيف ننظم استعمال الانترنت داخل المؤسسة وخاصة البريد الالكتروني والرسائل والملفات المعلوماتية؟

[1] لا يقصد بالموظف من يمارس عمله داخل مؤسسة عمومية فقط ولكن كل أجير يعمل داخل مؤسسة عامة أو خاصة .

إن المراقبة الالكترونية(cyber-vaillance) للموظف يجب التوازن بين سلطة الإدارة لرب العمل واحترام الحرية الشخصية للأ التحديات فيما يخص التزامه بالحفاظ على مسؤوليته عن الفعل الص العامل، الاجتهاد القضائي الفرنسي أقر مسؤولية رب العمل عن الاعمال الناتجة عن استعمال وسائل اتصالات الكترونية الخاصة بالمؤسسة من طرف العامل، وجعلت الملفات الورقية كالملفات الرقمية تعد وظيفية وليست شخصية مادامت موجودة في المؤسسة ولم يقم الدليل على أنها شخصية تخص العامل وبالتالي لا يجوز لرب العمل مراقبتها[1].

وتجوز مراقبة الملفات الورقية أو الالكترونية بحضور العامل أو في غيابه، ولا يستطيع هذا الأخير الاحتجاج على ذلك[2].

الفرع الثالث: الاعتداءات على القصر

عبر العالم هناك فئات كثيرة ومتزايدة ممن يفضلون التنقل عبر مواقع بذيئة بواسطة الشبكات الرقمية، وفي الواقع من السهل هذه الأيام أن يجد الشخص المواد (الأفلام والصور) الفاحشة عبر الانترنت حيث يكون، فالكل يستطيع زيارة هذه المواقع من أجل الطباعة ، تنزيل الملفات، ..، فالجنس والمنتجات التي تحوي الإباحية حاضرة وبكل قوة عبر الشبكة، فمنتجيها يميلون دائما لامتلاك التكنولوجيات الحديثة وخاصة منها الاجتماعية فهي تهيئ لهم استغلالها(الانترنت وكذلك الهواتف النقالة)، وهذه الصناعة تعد من أكبر الصناعات عبر الانترنت بجانب صناعة الألعاب[3]، أما المواقع الإباحية فلا تعد ولا تحصى والعشرات منها تظهر كل يوم، أشكال خدماتها تختلف من موقع لآخر، ولكن هذه المضامين تنتج على أنها « للكبار» غير أنه ليس كل مستعملي الانترنت كبارا ، فالقصر والأطفال يعدون من أكثر الشرائح استعمالا للانترنت، ودخولهم المواقع الإباحية أمر يحدث كثيرا، سواء بالمصادفة وأحيانا بالرغم منهم، وأحيانا أخرى بإيعاز من أصدقائهم على سبيل الفضول.

فالقصر يستعملون يوميا الانترنت بمعدلات عالية، 12% منهم يمضون أكثر من ثلاث ساعات في المراسلات الالكترونية، و 87% وقعوا في محتويات سيئة خلال تنقلهم عبر الانترنت، فالصور والأفلام الإباحية التي تتضمن أطفالا (pédopornographie) هي شكل خاص وخطير من الاستغلال الجنسي للأطفال والذي يتخذ مدى عالمي مع تطور استعمال الشبكات الرقمية[4]، فالانترنت تسهل نشر هذا النوع من العروض الاباحية في أكثر من 100 000 موقع.

كما أن هذه المواقع يسهل الوصول إليها من طرف البالغين المنحرفين وحتى الأشخاص العاديين ولكن التعود على مشاهدتها يؤدي في كثير من الأحيان إلى جرائم بشعة ضد الأطفال من أشخاص مقربين في محيطهم نتيجة للمشاهدة المفرطة للمواقع الاباحية بصفة عامة، فكيف هو الحال بالنسبة لهذه المواقع المتخصصة.

---

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.100-101.

[2] Cass.soc, n° 04647-400 et n°04648-025, du 18 octobre 2006.

[3] 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 III, (03/09/2012).

[4] ديباجة للقرار JAI/68/2004 لمجلس الاتحاد الأوربي في 23 ديسمبر 2003 متعلق بمكافحة الاستغلال الجنسي للأطفال و الأفلام أو الصور الإباحية التي تحوي أطفالا. أنظر

Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p. 103.

وعند النظر في الأسلحة القانونية التي وضعت لحماية الأ
القصر (المادة 342 ق ع) والمادتين 347 و333 مكرر من قانو
بالحياء قصد بيعها أو عرضها وهما نصان موجهان لحماية المج
المجتمع فعلا من الانتهاكات المستمرة عبر تكنولوجيات الاعلام والاتصال وخاصة منها الانترنت والهواتف النقالة؟ وهل هي قادرة على إيقاف المد المستمر الذي يستهدف بشكل مقصود الأطفال والمراهقين؟[1]

§ 1- مدى انطباق النصوص الخاصة في قانون العقوبات الجزائري على الانترنت:

تنص المادة 333 مكرر من قانون العقوبات على: « يعاقب بالحبس من شهرين(2) إلى سنتين(2) وبغرامة من 500 إلى 2.000 دج كل من صنع أو حاز أو استورد أو سعى في استيراد من أجل التجارة أو وزع أو أجر أو لصق أو أقام معرضا أو عرض أو شرع في العرض للجمهور أو باع أو شرع في البيع أو وزع أو شرع في التوزيع كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أصل الصورة أو قالبها أو أنتج أي شيء مخل بالحياء ».

وتنص المادة 347 فقرة 1 من ق ع على أنه: « يعاقب بالحبس من ستة (6) أشهر إلى سنتين(2) وبغرامة من 1.000 إلى 20.000 دج كل من قام علنا بإغراء أشخاص من أي من الجنسين بقصد تحريضهم على الفسق وذلك بالإشارة والأقوال أو الكتابات أو بأية وسيلة أخرى»

أما المادة 342 فقرة 1 من قانون العقوبات فتنص على أنه: « كل من حرض قصرا لم يكملوا التاسعة عشر (19) ذكورا أو إناثا على الفسق أو فساد الأخلاق أو تشجيعهم عليه أو تسهيله لهم وكل من ارتكب ذلك بصفة عرضية بالنسبة لقصر لم يكملوا السادسة عشرة (16) يعاقب بالحبس من خمس(5) سنوات إلى عشر (10) سنوات وبغرامة من 500 إلى 25.000 دج ».

باستقراء المادتين 333 مكرر و347 من قانون العقوبات نجد أن المشرع حرص على تجريم أية مادة بذيئة تؤدي إلى إفساد الأخلاق وذلك إذا تم بيعها أو احرازها بقصد البيع أو التوزيع أو العرض، ونلاحظ أن المشرع لا يعاقب على إحراز المواد البذيئة إلّا إذا اتجهت النية إلى بيعها، فمن حاز مواد اباحية مخلة بالحياء في بريده الالكتروني الخاص دون أن تتجه نيته لبيعها أو توزيعها فإنه لا يُعد مرتكبا لجريمة ضد الآداب والأخلاق العامة، وحتى تعد جريمة قائمة وفقا لنص المادة 333 مكرر يجب أن يتم بيع أو عرض أو توزيع هذه المادة أو حيازة هذه المادة من أجل عرضها أو توزيعها أو بيعها، وهذه الأفعال يمكن تصورها في نطاق شبكة الانترنت، أو باستعمال الهاتف النقال[2]

ويستوي لدى المشرع أن تكون تلك المواد مطبوعة أو مخطوطة، ولا يهم الدعامة التي تكون عليها لوحات زيتية أو صور شمسية أو شرائط ممغنطة فالمشرع وسع من نطاق التجريم بقوله: « أو أنتج أي شيء مخل بالحياء » حيث

---

[1] الآية القرآنية الكريمة ﴿ إِنَّ الذِينَ يُحِبُونَ أَنْ تَشِيعَ الفَاحِشَةُ فِي الذِينَ ءَامَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُنيا وَ الآخِرَةِ وَاللَّهُ يَعْلَمُ وَ أَنتُم لَا تَعلَمُونَ ﴾ سورة النور الآية 19، تعبر عن الخطر الكبير ممن يتاجرون بالأخلاق والحياء العام بحجة أن كل فرد حر في اختيار ما يشاهده ويستمع إليه، لكن الإباحية تعد توجها نحو انتشار المزيد من جرائم هتك العرض والاعتداء على القصر، وهو ما نقرأه دائما في جرائدنا عن النسب المتزايدة للجرائم التي ترتكب في حق القصر في هذا المجتمع.

[2] محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، الطبعة الأولى، 2007، ص 109.

شمل كل المواد المخلة بالحياء وطرق صنعها ونقلها، والانترنت وت
هذه المادة.

وكذلك الشراء أو الانتاج من أجل البيع أو التوزيع أو العر
كذلك، فعرض هذه المواد عن طريق الهواتف النقالة والانترنت وتوزيعها بشتى الطرق الحديثة تحقق الركن المادي للجريمة[1].

أما بالنسبة للمادة 347 ق ع فهي الخاصة بالإغراء العمومي Racolage public وتقوم هذه بتوافر ثلاث أركان: فعل الإغراء، العلنية، والقصد الجنائي.

ويقصد بالإغراء « كل دعوة موجهة إلى شخص، سواء كان ذكر أو أنثى، مجهولا أو معروفا لإتيان الفجور، وذلك مهما كانت الوسيلة المستعملة »[2]، ويجب أن يكون الإغراء في مكان عمومي، ولا يشترط القانون الاعتياد.

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

ويجب أن تتوافر النية لدى من يحرض على الفسق لقيام الجريمة[3].

أمّا المادة 342 ق ع وهي المادة التي تجرم فعل تحريض القصر على الفسق، فهي تحوي صورتين بحسب عُمر الضحية:

– الجريمة العرضية المرتكبة على قاصر لم يكمل 16 سنة،

– جريمة الاعتياد إذا كان الضحية قاصرا أكمل 16 سنة ولم يبلغ 19 سنة، ولم ينص المشرع على الاعتياد بصراحة ولكن يستشف ذلك من الفقرة الأولى للمادة في شطرها الثاني « وكل من ارتكب ذلك بصفة عرضية بالنسبة لقصر لم يكملوا السادسة عشرة (16).. »، وتكرار الفعل مرتين يكفي لقيام الاعتياد، ويمكن استخلاص الاعتياد من أفعال الفجور التي تم تكرارها في أوقات مختلفة، أو في وقت معين على شخص واحد، كما يمكن استخلاصها من أفعال متتالية تمارس على عدة أشخاص.

أما بالنسبة للعمل المادي فلا تقتضي الجريمة بصورتيها أن يؤدي إلى نتيجة معينة وفي القضاء الفرنسي أمثلة عن هذه الأفعال: قبول قصر في دور دعارة، أو التسهيلات التي توفر للبعض لإشباع رغباتهم مع الآخرين، القيام باتصالات جنسية أو بأي عمل من أعمال الفجور في حضور القصر، تنظيم لقاءات يكون فيها القصر تارة فاعلين، وتارة أخرى شهودا على المشهد، إلى غيرها من الصور المتعددة[4].

والملاحظ على هذه الأمثلة أنها تتطلب حضور القاصر المادي في هذه المشاهد، فهل عرض هذه المشاهد عن طريق تكنولوجيات الاعلام والاتصال الحديثة تضفي صفة الجريمة على هذه الأفعال؟ وكيف الأمر بالنسبة

---

[1] محمد أمين الشوابكة، المرجع السابق، ص 109.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الجزائر، الطبعة التاسعة، 2008، ص: 127.

[3] أحسن بوسقيعة، المرجع نفسه، ص 129.

[4] أحسن بوسقيعة، المرجع نفسه، ص 123–124.

للعروض التي تقدم عن طريق الانترنت من طرف بالغين على
القضاء في الجزائر أجوبة عن ذلك، ولكن ندعو وبشدة إدراج نص
والمجتمع ككل وتكون التكنولوجيات الحديثة للإعلام والاتصال وسيل
والمستمر والشديد على أخلاق واعتبار المجتمع ككل، فالعديد من التشريعات الأجنبية(بريطانيا، فرنسا، الولايات المتحدة الأمريكية...) سَنّت قوانين واضحة في هذا الشأن بسبب الخطر الداهم التي تمثله هذه الاعتداءات بارتكابها بواسطة الانترنت التي تعد طريق سريع للمعلومات وللاعتداءات المختلفة أيضا.

§ 2- موقف التشريع الفرنسي من الاعتداءات على القصر باستعمال الانترنت

القواعد الجزائية الفرنسية تطورت عبر الوقت مع تعديلات كثيرة لقانون العقوبات الفرنسي وذلك لتشمل مجموع الأفعال التي يجب العقاب عليها، فالقانون رقم 297/2007 المؤرخ في 5 مارس 2007 المتعلق بالوقاية من الإجرام الذي يهدف خصوصا إلى تقوية الحماية للقصر بتعديل من جهة القانون 468/98 المؤرخ في 17 جوان 1998 المتعلق بالوقاية وقمع الجرائم الجنسية وكذلك حماية القصر، ومن جهة أخرى قانون العقوبات الفرنسي، فهو يحوي أحكاما جديدة مقررة لقمع أفعال معينة مرتبطة باستعمال الانترنت للإضرار بالقصر.

أ- حماية القصر ضد الصور والأفلام التي تبرز الأطفال أو المراهقين في أوضاع جنسية[1]: بحسب المادة 227-23 الفقرة 1 و2 من ق ع الفرنسي[2] : « إن فعل التسجيل، التثبيت، أو النقل من أجل النشر لصورة قاصر أو الصورة التي تظهر حضوره إذا كانت هذه الصورة ذات طابع إباحي، يعاقب عليه ب 5 سنوات حبس وبغرامة 75.000 أورو.

أن القيام بتقديم، أو بجعلها متوفرة، أو استيرادها او تصديرها، أو محاولة الاستيراد أو محاولة التصدير،أو نشر مثل هذه الصورة أو التمثيل، بأي وسيلة مهما كانت، يعاقب عليه بنفس العقوبة ».

أما الفقرة 5 من هذه المادة فتنص:« إن فعل الاعتياد على الإطلاع على خدمة اتصالات عامة عبر الانترنت على مثل هذه الصورة أو التمثيل الذي تحتويه أو حيازتها بأية وسيلة يعاقب بسنتين(2) حبس وغرامة تقدر ب 30.000 أورو».

الفقرة الخامسة من المادة 227-23 عدلت بموجب القانون 2007/297 المتعلق بالوقاية من الإجرام وكانت قبل التعديل تنص على أنه « إن حيازة مثل هذه الصورة أو التمثيل يعاقب عليه بسنتين حبس وبغرامة 30.000 أورو ».

---

[1] وهي ما تسمى ب Pédopornographie

[2] Alinéa 1 : *« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.*

Alinéa 2 : *« Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines »*

Alinéa 5 : *« le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende ».*

نأخذ الآن شخص قام بالإطلاع على مواقع في الانترنت تح
بتسجيلها إراديا في ملف خاص على جهاز الحاسوب، وفي حال الإ
الموقع يتم تنزيلها وحفظها بشكل غير مرئي في فهرس نظام(stème
مؤقت مخفي للانترنت، هذه الطريقة تسمح لمستعمل الانترنت في وقت آخر الدخول بسرعة إلى الموقع نفسه أي أنها تسرع في عملية الدخول لنفس الموقع.

إذن من المهم معرفة إذا كانت هذه الصور غير القانونية المخزنة في هذا الفهرس المؤقت والمخفي للانترنت التي تلي الاطلاع على هذه المواقع غير المشروعة من طرف شخص تُشكل جريمة وفقا للمادة 227-23 الفقرة 5 قبل تعديلها؟

في الواقع وبقرار من محكمة الاستئناف ب Lyon[1] بفرنسا بتاريخ 1 أفريل 2004 أكدته محكمة النقض في 05 جانفي 2005 أعلنت براءة المتهم بحجة: « لا تعد حيازة، بمجرد الاطلاع على مواقع للاستغلال الجنسي للأطفال باستعمال جهاز الحاسوب يسجل تلقائيا في الذاكرة المؤقتة تلك الصور لقصر التي تحوي أوضاعا إباحية، وأن المتهم بالتأكيد لم يقم إلا بترك آثار لمروره إلى هذه المواقع باستعمال جهاز لا يملكه وأن القانون لم ينص على مجرد الاطلاع على مواقع إباحية تحوي مشاهد جنسية للأطفال»، وبالتالي فإن هذا القرار يحمي الشخص الذي يتصل بمواقع مجرمة عن طريق الصدفة، وحتى بالنسبة للأشخاص الذين اعتادوا زيارة هذه المواقع ولم يقوموا بتسجيل تلك الصور المجرَّمة، ولذلك فإن تعديل الفقرة الخامسة من المادة 227-23 من ق ع الفرنسي لتشمل الاعتياد على زيارة هذه المواقع المجرمة هو بهدف عقاب هؤلاء المنحرفين لاعتيادهم زيارة تلك المواقع دون أن يقوموا بتسجيل أو حيازة الصور المجرمة[2].

ولكي يمكن أن يتم الحكم على المتهم بقيامه بالإطلاع المتكرر على هذا النوع من المواقع يجب التدقيق في جهاز الحاسوب المستعمل في هذه الجريمة من أجل مراقبة عدة أمور هامة:

1- عنصر « التعود » في الاطلاع يجب إظهاره، فتكرار الزيارة للمواقع المجرمة يجب أن يظهر في دليل الإدانة وذلك بإقامة تحليل بين عدد الصور الموجودة في الذاكرة المؤقتة للحاسوب المستعمل و تواريخ آخر دخول للموقع، فيجب اثبات أن المتهم تعدد دخوله للموقع في فترات مختلفة .

2- عنصر الارادة في الاطلاع من طرف المعني يجب إظهاره، حيث توجد في بعض صفحات الانترنت أو الفيروسات التي تدخل عبر البريد الالكتروني يمكن أن تحوي رموز خبيثة تسمح بالاتصال عبر الانترنت بمواقع إباحية تحوي

---

[1] CA Lyon 4ème ch Arrêt du 01 avril 2004 Ministère public / Jean Luc B.,http://www.legalis.net /jurisprudence-decision.php3?id_article=1446

[2] 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 47. disponible sur www.univ-paris1.fr/.TYRODE_ MEMOIRE.pdf [03/09/2012].

صور جنسية لقصر بغير علم المعني، كذلك موقع لصور إباحية [illegible] المواقع المجرَّمة ، فهذا الاطلاع لا يعتد به.

3- يجب إثبات هوية الفاعل، فالتحليل التقني يجب أن يثبت أن جه[illegible] أو أن عنوانه IP لم يتم استعماله، بالإضافة إلى ذلك أن استعمال مقاهي الانترنت للاتصال بالمواقع المجرمة تزيد من صعوبة التعرف على هوية الفاعلين.

4- عدد الصور المكتشفة التي قد تصل إلى المئات أو حتى الآلاف توضح للقاضي الحالة النفسية للمعني[1].

ب- الجريمة الخاصة بدعوة جنسية لقاصر باستعمال وسيلة الكترونية للاتصالات: المادة 227-22-1 من ق ع الفرنسي تعاقب على العروض الجنسية التي يقدمها شخص بالغ لقاصر في الخامسة عشرة (15) سنة أو إلى شخص عرض نفسه على أنه كذلك مستعملا في ذلك الاتصالات الالكترونية، فهذه الجنحة تتعلق بصفة خاصة بالعروض التي ترسل إلى القُصَر عن طريق الانترنت أو الرسائل القصيرة SMS ويعاقب عليها بالحبس لسنتين وبغرامة 30.000 أورو، وهي تخص فقط الوسائل الالكترونية.

تشدد العقوبة في حالة أن الدعوة أو العرض المقدم ارتبط بتعارف (المادة 227-22-1 فقرة 2 من ق ع الفرنسي) لتصل العقوبة إلى 5 سنوات وغرامة 75.000 أورو، هذه الجنحة تخص الملاحقة الأفضل للبالغين الذين يملكون سلوكيات ضارية للتُقرب من الأطفال عن طريق حلقات الدردشة في الانترنت مثلا.

هذا التجريم من طرف المشرع الفرنسي في هذه المادة يُظهر حذر المشرع فيما يخص الانترنت، لأنه يقيم جريمة مستقلة لفعل تمهيدي أو محاولة للشروع في اعتداء جنسي[2]، كما تجدر الإشارة أن هذه المادة تعاقب على هذا النوع من التحريض بدون أن تشترط أن تكون هناك نتيجة[3].

ج - حماية القصر ضد المحتويات الضارة: المادة 227-24 من ق ع الفرنسي لا تجرم فقط نشر صورة إباحية لقاصر أو يكون القاصر فيها حاضرا، ولكنها تجرم أيضا الفعل الذي يكون برسالة إباحية يمكن لقاصر رؤيتها، هذه الأحكام تفرض على الناشر أو صاحب الموقع بوضع ترتيبات تمنع القصر من الدخول للموقع[4].

« القيام إما بإنتاج أو نقل أو نشر بأي وسيلة وعلى أي دعامة، رسالة توصف بأنها عنيفة أو إباحية أو ذات طبيعة تعد ماسة جدا بالكرامة الانسانية، أو لأجل التجارة بهذه الرسالة، إذا كان بالإمكان لقاصر رؤيتها » يعاقب الفاعل بالحبس لثلاث سنوات و بغرامة تقدر بـ 75.000 أورو، هذه المادة تسهر على ضمان التطور والتفتح العقلي والنفسي وحتى البدني للطفل، إن مجرد كون الصور يمكن أن يراها القاصر ينطبق فيها حكم المادة 227-22-1 حتى ولم يقم الدليل على أن قاصر قد رآها فعلا، كذلك لا يمكن التذرع بنوع الوسيلة التقنية التي تم بها النقل أو النشر كالانترنت مثلا في حالة ما إذا كان هناك امكانية دخولها من طرف القاصر.

إن تمثيل القاصر في صور إباحية تتضمن التركيب التقني للصور(montage) والرسوم التي بها عناصر تتضمن الاستغلال الجنسي للأطفال، وكذلك الصور الافتراضية كلية، كل هذه النماذج تعد مجرمة وفقا للقانون الفرنسي[1].

---

[1] Ibid..p.48-49.
[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.107.
[3] Jean-François TYRODE, op.cit.p.51.
[4] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.108.

د- التوسع المستمر للظروف المشددة في حالة اللجوء إلى شب

مشدد في حالة اللجوء إلى شبكة اتصالات كالانترنت في حالة إثب
الجريمة للإضرار بالقصر في العديد من مواد قانون العقوبات الفرنسي

ومثال ذلك جريمة إفساد قاصر (المادة 227-22 فقرة 1 من ق ع الفرنسي) يمكن تشديد العقوبة في حالة أن القاصر اتصل بالفاعل لقيام هذا الأخير بنشر رسالة لجمهور غير محدد عن طريق شبكة اتصالات الكترونية.

هذه مجموع الجرائم التي نظمها وعاقب عليها المشرع الفرنسي معتمدا على الخطر الذي تلحقه شبكات الاتصال الرقمية، في تطور وزيادة خطر الجرائم الجنسية على الأطفال ومن ثم المجتمع ككل، وعليه ندعو المشرع الجزائري بدق ناقوس الخطر واعتماد سياسة جنائية صارمة في هذا المجال، وعدم التساهل مع مجرمي الاعتداءات الجنسية على القصر.

الفرع الرابع: الارهاب المعلوماتي Cyberterrorisme

إن الإرهاب المعلوماتي هو نقطة التقاء الإرهاب التقليدي مع الشبكات الالكترونية بداية بالانترنت، فيمكن تعريفه بأنه النشاط المُتَعمد لتدمير، إتلاف أو تغيير في المعطيات أو في تدفق المعلومات أو النظم المعلوماتية الحيوية للدول أو المؤسسات الحيوية في الدولة، من أجل الإضرار و/أو التأثير لأبعد ما يمكن لأسباب سياسية أو دينية أو ايديولوجية، وهذه الأضرار قد تكون اقتصادية، اجتماعية، بيئية أو حتى خسائر أساسية للأفراد في بعض الحالات[2].

فمجرد افساد (défiguration) موقع الكتروني (Web) قليل الأهمية يشكل نوعا ما ارهاب معلوماتي، وهذا سيشكل فيما بعد سقوط لمواقع مهمة وخطيرة، أو بجعل البنى التحتية للدولة أو لمؤسسة ما غير فعالة، كما يمكن اعتبار افساد معطيات مهمة من الاعتداءات الارهابية، لأن الفوضى وغياب الثقة الناتجين عن هذا الاعتداء يضر بطبيعته المجتمع، فالإجرام المعلوماتي يستهدف: إدارة مرافق الاتصالات (المراكز الهاتفية، الشبكات السلكية واللاسلكية..)، مواقع توليد وتوزيع الطاقة، تنظيم مرافق النقل (المطارات، الموانئ، مراقبة الحركة الجوية والبحرية، السكك الحديدية، الطرق السريعة، نظم مراقبة إشارات المرور)، مرافق توزيع المنتجات البترولية، مرافق البريد، مواقع توزيع المياه، المؤسسات المالية والبنكية، الإدارات العمومية (الضمان الاجتماعي، المؤسسات الدستورية)، ووسائل الإعلام

في حالة هجوم إرهابي لمجموعة من هذه المواقع في وقت واحد قد يحدث آثار مدمرة لدول غير مهيأة، فقد يحدث توقف كامل لبعض النشاطات في الدولة، وقد تشكل خطرا في بعض الحالات على حياة الأشخاص[3].

كما لا ننسى الاستعمالات الرهيبة للهواتف النقالة كأزرار لتشغيل القنابل في هجمات تستهدف الأشخاص(شخصيات معروفة سياسية أو دينية أو منتمية لعرق أو طائفة معينة، أو فئات معينة من المجتمع كتعبير عن الحقد العنصري والطائفي، إلى غيرها من المبررات).

---

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit.p.109.

[2] Patrick CHAMBET, Le cyber-terrorisme, disponible sur www.chambet.com/publications/Cyberterrorisme. pdf [03/09/2012]

[3] Patrick CHAMBET, op.cit .

القانون الجزائري يجرم الإرهاب بكل صوره ومن بينها الارهـ
القانون العام تنطبق على الأفعال التخريبية التي تستخدم الشبكات و
العقوبات في القسم الخاص بالجرائم الموصوفة بأفعال إرهابية أو تخريبية.

المواد 394 مكرر و ما يليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، فعل الدخول والحذف أو التغيير داخل منظومة للمعالجة الآلية للمعلومات، أو فعل الادخال أو إزالة أو تعديل في محتوى يؤدي إلى تخريب نظام الاشتغال المنظومة، كذلك يجرم المشرع تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية كالفيروسات) يمكن أن ترتكب بها الجرائم السابقة الذكر، كذلك في حالة الاشتراك في مجموعة أو اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم التي تمس أنظمة المعالجة الآلية للمعلومات.

كذلك يمكن قيام فعل الاشتراك في جريمة حسب المادة 42 ق ع بتقديم المساعدة بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك، في هذا المقام تقديم وسائل معلوماتية، او المساعدة في الدخول إلى شبكة الانترنت تشكل فعل الاشتراك مادام الشخص يعلم بنهاية العمليات.

كذلك المادة 87 مكرر 5 التي تعاقب الفعل العمدي لطبع أو نشر الوثائق أو المطبوعات أو التسجيلات التي تُمَجِد الأفعال الارهابية والتخريبية، فالشبكات الرقمية تشكل بالنسبة للتنظيمات الإرهابية وسيلة لنشر أفكارهم و قبول أعضاء جدد، كذلك تمجيد و إقرار لنشاطاتهم الإجرامية، فالانترنت تعد وسيلة دعائية بسبب حرية تبادل الاتصالات المتوفرة في شبكات العالم بقصد نشر معتقداتهم المتعارضة بشكل واضح مع المبادئ الأساسية للديمقراطية[1].

المطلب الثاني: جرائم المساس بأنظمة المعالجة الآلية للمعطيات

Infractions aux systèmes de traitement automatisé de données (STAD)

الغش المعلوماتي يظهر كمجموعة أفعال مجرمة متصلة بأنظمة المعالجة الآلية للمعلومات، ويكون بذلك بين يدي قانون العقوبات.

جرم المشرع الجزائري في القسم السابع مكرر من قانون العقوبات الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، تم إدراج هذا القسم بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ليواجه المشرع الجرائم الحديثة المتصلة بتكنولوجيات الإعلام والاتصال، هذه الجرائم محددة بموجب المواد 394 مكرر إلى 394 مكرر6، أحكام هذه المواد تعاقب على الاختراقات غير المصرح بها داخل نظم المعالجة الآلية للمعطيات.

وقبل التطرق إلى هذه الجرائم يجب أولا التعريف بأنظمة المعالجة الآلية للمعطيات، حيث لم يقم المشرع بتعريفها على غرار المشرع الفرنسي، وقد عرفها الفقه في فرنسا بأنها: « كل مُرَكب يتكون من: وحدة أو مجموعة وحدات للمعالجة، ذاكرة، برامج، معطيات، أجهزة الادخال و الاخراج، أجهزة الربط، التي تعمل فيما بينها لتحقيق نتيجة محددة، هذا المركب يكون خاضعا لنظام حماية »[2] .

---

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit. p. 127 .
[2] Ibid.p 71.

وانظر كذلك آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الطبعة الثانية، 2007، الجزائر، ص 102.

الفرع الأول: الدخول أو البقاء عن طريق الغش داخل نظا

يفرق القانون في حالة ما إذا كان الدخول أو البقاء يؤدي أو

394 مكرر فقرة 1 من قانون العقوبات وتقابلها المادة 323-1 من [illegible] « يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك »، هذه المادة تسمح بعقاب الأشخاص الذين يريدون الدخول إلى معلومات حيث الدخول لهم ممنوع، هذا السلوك يجب أن يكون عمديا.

وفي ظل الاجتهاد القضائي الفرنسي، مفهوم الدخول إلى نظام للمعالجة الآلية للمعلومات يمكن تمييزه سواء عن طريق اختراق النظام، أو عن طريق التلاعب المعلوماتي باستعمال الاتصال أو استدعاء برنامج يعمل عن طريق الغش، أي بدون ترخيص من المؤسسة، ومثال ذلك الاستيلاء على رقم سري والاتصال في فضاء مخصص لنظام مفتوح للجمهور، إذا استعمل شخص ما مصدع لكلمات المرور عبر الانترنت بقصد اختراق الوصلات الإدارية لموقع بالانترنت يمكن أن يُعاقب على هذا الأساس، كذلك استعمال الشمام « sniffer » لاعتراض الملفات والايميل (البريد الالكتروني) عبر الشبكة يمكن أن يشكل هذه الجريمة أيضا، أما عنصر الغش فيمكن استنتاجه من إدخال ملف تجسس مثل حصان طروادة أو اتصال معين لفحص النظام عن بعد.

وتقوم الجريمة بمجرد اختراق الشخص لمنظومة معلوماتية بدون ترخيص، فالدخول عن طريق الغش هو جنحة آنية، ومثال ذلك استعمال قاعدة بيانات لا يمكن الدخول إليها إلا لأشخاص مرخص لهم بفضل رمز code وُضع خلال الفترة التجريبية يشكل جريمة البقاء عن طريق الغش في نظام للمعالجة الآلية للمعطيات حتى ولو كان الدخول إليها كان قانونيا خلال الفترة التجريبية.

إن تجريم البقاء عن طريق الغش يُكَمل الدخول عن طريق الغش، فهو يحدد الحالات حين يكون الدخول إلى انظمة المعالجة الآلية للمعطيات قانونيا ولكن البقاء لا يكون كذلك حيث يكون الفاعل غير مخول كلية للبقاء داخل النظام، فالبقاء عن طريق الغش يتميز بحالات مختلفة غير عادية، كالاتصالات أو جميع العمليات الموجهة ضد نظام معلوماتي، ففعل الدخول إلى خادم الويب ثم معالجة متغيراته [1]وتغيير لغة برمجية(Requête SQL) من أجل الدخول لمعلومات محفوظة يمكن تكييفه على أنه دخول عن طريق الغش[2].

إن الركن المادي يتكون فقط من الدخول أو البقاء بحد ذاته مستقلا عن النتيجة، فحتى في غياب الضرر، فإن الفاعل لهذا الدخول أو البقاء يمكن عقابه.

أما الركن المعنوي فيجب تحديده، بمعنى أن يكون المتهم على علم بالدخول أو البقاء غير القانوني وبدون وجه حق في النظام، والدخول والبقاء يشكلان جريمة عندما يرتكبان عن طريق الغش، فمصطلح « عن طريق الغش » يفترض أن الدخول أو البقاء كانا بإرادة الفاعل، وأن هذا الأخير كان على علم بارتكابه النشاط المجرم، ولكن لا يهم أي يكون الفاعل أراد الإضرار أو لا بالنظام المخترق، كما أن الركن المعنوي في هذه الجريمة يصعب إثباته في الواقع.

---

[1] المتغيرات في لغة المعلوماتية تشترك مع اسم (رمز) ولها قيمة أو موضوع، وهي جزء من تعريف لوغاريتمي، ويجب بالنتيجة إيجاد أسماء مختلفة لكلمات محفوظة فقط لكل لغة برمجية . أنظر في ذلك http://fr.wikipedia.org/wiki/Variable_(informatique) .

[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit. p. 73.

فالقضاء الفرنسي يعتبر أن القصد في الجريمة محدد عندما يكفي أن "صاحب النظام" عمد إلى حصر الدخول إلى الأشخاص [illegible] عدم الترخيص المصرح به من طرف صاحب المنظومة»، ويلاحظ [illegible] بوجود مجموعة من الدلائل، فصاحب النظام هو الشخص أو المصلحة المختصة بالترخيص في الدخول، ومثال ذلك تخصيص رموز الدخول إلى أشخاص محددين بقائمة، يُجسد حقهم في الدخول للنظام.

ليس من الضروري لقيام الجريمة أن يكون النظام محميا بنظام حماية (مثل الجدران النارية firewall)، كما أنه ليس من الضروري إظهار أن المتهم قد دخل بـ "القوة" للنظام، يكفي فقط أن يكون المستخدم (صاحب النظام) قد أوضح نيته الصريحة بحصر الدخول إلى أشخاص معينين فقط، ومن تطبيقات ذلك في القضاء الفرنسي قضية Kitetoa ضد Tati SA، في هذه القضية المسؤول عن موقع للصحافة المتخصصة في الحماية المعلوماتية والمدعو Kitetoa توبع من طرف الشركة Tati لدخوله المتكرر في قاعدة البيانات الخاصة بموقع Tati.fr مؤسسين دعواهم على الدخول عن طريق الغش لمنظومة المعالجة الآلية للمعطيات، والمتهم احتج بغياب الحماية للموقع، ومحكمة الجنح بباريس في حكمها بتاريخ 13 فيفري 2002 أكسبت القضية للشركة Tati معتبرة أن وجود عطل أو ضعف بالحماية لا يشكل « في أي حالة عذرا أو ذريعة للمتهم للدخول مدركا ومتعمدا لمعطيات لم تكن محمية والتي يمكن أن تشكل جريمة »[1]، ولكن في قرارها بتاريخ 30 أكتوبر 2002 محكمة الاستئناف لباريس ألغت الحكم المستند على أن فعل الدخول إلى معطيات اسمية مخزنة داخل موقع، يكون باستعمال ابسط متصفح للانترنت (كـ Google)، وبوجود العديد من الأعطال في الحماية، لا يشكل دخول و بقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات، المحكمة اعتبرت أنه لا يمكن لوم أحد مستعملي الانترنت للدخول أو البقاء في أجزاء من الموقع « الذي يمكن الاعتداء عليه باستعمال أبسط متصفح موضوع للجمهور»، وأضافت المحكمة ان هذه الأجزاء من الموقع لا تعد موضوعا للحماية من طرف المستخدم أو مقدمي الخدمة لهذا الموقع والذي يجب في هذا المقام اعتباره غير سري و غير خاص في غياب لأي إشارة تدل على خلاف ذلك[2]، ويمكن اعتبار أن القضاء وضع قرينة بسيطة، في حالة أن الدخول والبقاء في منظومة للمعالجة الآلية للمعطيات(فيما يتعلق بالمواقع عبر الانترنت) غير محمية تسمح أيضا بالدخول باستعمال أدوات مخصصة للجمهور(في هذه الحالة متصفح) لا يَكون معاقبا عليه لعدم توفر الغش الموجب للجريمة المنصوص عليها في المادة 394 مكرر فقرة 1 من قانون العقوبات.

كذلك قضت الغرفة الجنائية بمحكمة النقض بفرنسا في قرار لها بتاريخ 3 أكتوبر 2007[3] قيام الجنحة بموجب المادة 323-1 من ق ع الفرنسي والتي تقابلها المادة 394 مكرر من ق ع في حالة أن المسير السابق لمؤسسة تنشر معلومات تجارية عبر الانترنت، استمر باستعماله رمز تعريف للاتصال مجانا، هذا الرمز كان قد تحصل عليه خلال الفترة التجريبية، ولا يهم إن لم تحذفه الشركة بعدما غادرها المتهم.

المادة 394 مكرر من ق ع في الفقرتين 2 و 3 أقامت ظرف مشدد في حالة أن الدخول والبقاء بطريق الغش في منظومة للمعالجة الآلية للمعطيات أدّى إمّا إلى حذف أو تغيير في المعطيات داخل المنظومة أو إلى تخريب نظام

[1] TGI de Paris, 13 février 2002.
[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit. p.74
[3] Cqss. Crim., 3 octobre 2007, pourvoi n° 07-81.045.

اشتغال المنظومة، ويكفي لتوافر هذا الظرف وجود علاقة سببية بي
يشترط أن تكون تلك النتيجة مقصودة[1]. والعقوبة تكون بالحبس من
إذا كان الدخول والبقاء أدى إلى حذف وتغيير في معطيات المنظ
(تضاعف العقوبة بحسب الفقرة 2 من المادة 394 مكرر) ، وفي حالة تخريب نظام الاشتغال المنظومة (الفقرة 3 من المادة) فالغرامة هي من 50.000 دج إلى 150.000 دج.

الفرع الثاني: الاعتداء على سلامة المعطيات

§ 1- الاعتداء على سلامة المعطيات الموجودة داخل النظام:

بموجب المادة 394 مكرر 1 من قانون العقوبات[2] « يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ».

هذا النص يعاقب على كل تلاعب بمحو أو تعديل المعطيات داخل النظام، بغض النظر عن النتائج، وبالنسبة لتطبيقات هذا النص في فرنسا يطابق التجريم كل تعديل للمعطيات أو الملفات أو قواعد البيانات.

هذه المادة تحوي ثلاث صور:

1- **الإدخال:** وذلك بإضافة معطيات جديدة على الدعامة الخاصة بها، ويتحقق فعل الإدخال كذلك بإدخال برنامج غريب (فيروس، حصان طروادة...) ليضيف معطيات جديدة.

2- **المحو:** وذلك بإزالة جزء من المعطيات الموجودة داخل النظام.

3- **التعديل:** وذلك بتغيير المعطيات الموجودة سواء بطريق مباشر أو باستخدام برامج خبيثة كالفيروسات.

هذه الصور الثلاث وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غير هذه الأفعال، ولو تضمن اعتداء على المعطيات داخل النظام كفعل النسخ أو النقل[3].

ولا تقوم هذه الجريمة إلا إذا كانت هذه العمليات تمت مع قصد جنائي وخارج الاستعمال المرخص، يتكون القصد الجنائي في الوقت الذي يحدث فيه إدخال المعطيات بإرادة التغيير في النظام وبغض النظر عن النتائج التي تحدث فيه[4].

إن فعل التعديل أو المحو العمدي للمعطيات الموجودة في نظام للمعالجة الآلية للمعطيات يُحدد الجريمة، وليس بالضرورة أن تكون هذه التغييرات صدرت من شخص ليس له الحق في الدخول للنظام، ولا من الفاعل الذي حرك إرادته لإحداث الضرر.

---

[1] آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر،الطبعة الثانية، 2007، ص 114.

[2] تقابلها المادة 323-3 من قانون العقوبات الفرنسي.

[3] آمال قارة، المرجع السابق، ص 122.

[4] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit. p. 77.

§ 2- الاعتداء على سلامة المعطيات خارج النظام:

نصت المادة 394 مكرر2 ق ع في القسم الثاني منها « [illegible] سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم [illegible]

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

هذه المادة تهدف لحماية هذه المعطيات من استعمالها في أغراض غير مشروعة كالمنافسة غير المشروعة ، الإرهاب، التحريض على الفسق، الاعتداء على الحياة الخاصة للأشخاص...إلخ[1]، إن لم تشكل جرائم أشد فيعاقب مرتكبها بالعقوبة الأشد.

الفرع الثالث: تصميم، بحث، تجميع أو توفير أو نشر أو الاتجار بأدوات للاعتداء على نظم المعالجة الآلية للمعطيات

المادة 394 مكرر 2 من قانون العقوبات في قسمها الأول تنص على أنه « يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

تقابلها المادة 323-3-1 من ق ع الفرنسي[2] ولكن باختلاف في الصياغة وهي على النحو التالي: « إن فعل، من غير السبب الشرعي، الاستيراد، الحيازة، عرض، بيع أو توفير جهاز أو أداة، أو برنامج معلوماتي أو معطيات صممت، او خصصت لارتكاب جريمة أو عدة جرائم منصوص عليها في المواد 323-1 إلى 323-3، يعاقب عليه بالعقوبات المنصوص عليها عن الجريمة المراد ارتكابها أو عن الجريمة الأشد عقوبة ».

حيث يظهر الفرق بين الصياغتين فيما يتعلق استثناء المشرع الفرنسي لفعل الحيازة أو البحث الذي تكون منه الغاية مشروعة وهي مثلا الأبحاث العلمية، أمن (حماية) الشبكات، فنرجو من المشرع الجزائري استدراك هذا الاستثناء المهم.

تشير المادتين لعقاب الأشخاص الذين يوفرون الأدوات وخاصة منها الفيروسات المعلوماتية أو برامج للتحكم عن بعد تسمح بارتكاب الجرائم المعاقب عليها جنائيا، هاتين المادتين وُضعتا من أجل مكافحة التطور المهم للفيروسات عبر الشبكات الرقمية.

ومن التطبيقات القضائية المهمة لهذه المادة قيام محكمة الاستئناف بـ Montpellier[3] في مجال

---

[1] آمال قارة، المرجع السابق، ص 123.

[2] Art. 323-3-1 « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

[3] CA de Montpellier, 3ech., 12 mars 2009, jurisData n° 2009-004341.

الاعلام المتعلق بتعطل (ضعف) الحماية المعلوماتية، معتبرة بعدم و
إدانة مسير شركة متخصصة في التحكم بأخطار وضعف الحماية
الشركة عبر بوابتها في الانترنت مخطوطات تسمح باستغلال ضعف
من طرف الكل، وقد اعتبر قضاة الدرجة الأولى بعدم وجود تحريض على القرصنة وأن غرض المسير هو إعلام مستعملي البرامج المعلوماتية بالأخطار الموجودة.

أما محكمة النقض فأكدت على عدم مشروعية الإعلام العلني للجمهور بالنشر عبر موقع بالويب يمكن دخوله للجميع، كل برنامج معلوماتي أو رموز توصل للبرامج المعلوماتية التي تسمح باستغلال ضعف الحماية المعلوماتية للأنظمة، وعلى العكس من ذلك يمكن دائما إعلام الجمهور حول الأعطال أو ضعف الحماية المعلوماتية.

كذلك في قرار آخر للغرفة الجنائية بمحكمة النقض[1] بتاريخ 27 أكتوبر 2009 التي أكدت إدانة شخص قام بنشر عبر بوابة شركة مختصة بالنصائح حول الأمن المعلوماتي كتابات « واضحة عبر الموقع وقابلة للدخول من الجميع، تسمح باستغلال ضعف الحماية المعلوماتية » فقَصْدُه المُجَرَّم بعرضه المفصل لخبرته في الموضوع ونشره عن علم معلومات « تمثل خطرا باستعمالها لأغراض القرصنة من طرف أحدهم، يبحث خاصة عن هذا النوع من الانحراف »[2].

الفرع الرابع: الاشتراك في مجموعة أو في اتفاق تألف بغرض ارتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات

تعاقب المادة 394 مكرر5 الاشتراك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في المواد 394 مكرر إلى 394 مكرر2 من قانون العقوبات وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، هذه الجريمة يعاقب عليها بنفس العقوبة للجريمة المراد ارتكابها، أو بالعقوبة الأشد في حالة تعدد الجرائم.

الأفعال المادية تكون مثلا بتبادل معلومات مثل رموز الدخول(les codes d'accès)، ولتقوم الجريمة يجب تواجد مجموعة منظمة بغرض ارتكاب الجرائم المنصوص والمعاقب عليها في المواد 394 مكر إلى غاية 394 مكرر2، ولا يكفي الاتفاق وحده وإنما يجب أن يتبع بتحضير لجريمة أو أكثر، هذا التحضير لا يعاقب عليه إلا بتجسيده بعمل مادي أي بإتيان عمل إيجابي[3].

الفرع الخامس: القواعد المشتركة بين كل هذه الجرائم

1- أقامت المادة 394 مكرر 3 من قانون العقوبات ظرف مشدد في حالة ما إذا استهدفت جرائم المساس بأنظمة المعالجة الآلية للمعطيات الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، حيث تضاعف العقوبات، ودون الإخلال بتطبيق عقوبات أشد.

---

[1] Cass. Crim, 27 octobre 2009.
[2] Myriam QUÉMÉNER, Yves CHARPENEL, op.cit. p.78.
[3] آمال قارة، المرجع السابق، ص 131.

2- في كل هذه الجرائم الشروع يعاقب عليه طبقا لنص المادة 394 المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.»

3- كذلك يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم ال مكرر2 بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي (المادة 394 مكرر 4 من ق ع).

4- المصادرة مع الاحتفاظ بحقوق الغير حسن النية، حيث يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة، علاوة على إغلاق المحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم مالك المحل أو المكان[1].

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، دار هومة، الجزائر، الطبعة التاسعة، 2008، ص 448.

الفصل الأول:

هيئات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تمهيد:

على خلاف جرائم أخرى تمتاز الجرائم المتصلة بتكنولوجيا على وسائل الاتصال الحديثة وشبكة الانترنت المتوافرة في كل بقاع العالم، كما أنّ سرعة التنفيذ والأثر الذي تخلّفُه على المجتمعات يُعدّ 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 فإنَّ 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 أنَّ الكثير منها يتم دون متابعات جزائية، إمّا 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 يُعدُّ جزءً منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتي تكون من اختصاص هيئات قضائية متخصصة للفصل فيها (الأقطاب الجزائية).

كذلك فإنَّ السِّمات الدولية لهذه الجرائم باعتبارها عابرة للحدود في كثير من الأحيان تجعل من تطبيق القوانين الوطنية الجزائية للعديد من الدول لقمعها يُشكل 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 أمراً حتمياً، وإلاّ فإنَّ 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 فإنَّ دراستنا لآليات 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

يمكننا إدراج تساؤل تسمح لنا الإجابة عنه بتحديد عناصر هذ

– هل مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (الجرائم المعلوماتية) تتطلب سلطات أو هيئات أو أشخاص يتمتعون بقدر كافٍ من المعرفة التكنولوجية الحديثة لوسائل الإعلام والاتصال؟ أم أنَّه 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 أنَّه:

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

2- إنَّ الجرائم المعلوماتية تقف بِجنْب جرائم أخرى كثيرة متعددة ومتنوعة، ولكنها في النهاية تُعدّ من أهم الجرائم المستحدثة لأمر واحد وهو أنّ جميع الجرائم يمكن استعمال تكنولوجيات الإعلام والاتصال في ارتكابها، ومثال ذلك: جرائم تبييض الأموال، الإرهاب ، الجريمة المنظمة، جرائم الفساد، وحتّى الجرائم التقليدية كالسرقة والنصب والقتل. ومن خلال ذلك نرى أنّ 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: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها « تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم »، أما مهامها فقد أوردتها المادة 14 من نفس القانون.

الفرع الأول : تنظيم الهيئة

بالرغم من الأهمية المرجوة من هذه الهيئة إلاّ أنّه لـ
خاص بها يحدد تشكيلتها وتنظيمها وسيرها. وباستقراء نصوص القانون 04/09 فإنّ تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع لهذه الهيئة، وهو نفس الأمر لما هو في فرنسا إذ أُنشِأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال Office central de lutte contre la criminalité liée aux technologie de l'information et de la communication، وهي هيئة تابعة للمديرية العامة للشرطة الوطنية الفرنسية وخاضعة للمديرية المركزية للشرطة القضائية، نشأت سنة 2000 [1].

الفرع الثاني: مهام الهيئة

من خلال اسمها فإنَّ للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها:

1/ الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

إنَّ إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الالكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية..إلخ.

2/ مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

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

أ- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة ب من القانون 04/09، وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا فإن لها مهام أدرجها المرسوم رقم 2000- 405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة تتمثل في[2]:

- ✓ تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،

---

[1] www.secureteinfo.com/legal/OCLCTIC.shtml [13/07/2011]

[2] لقد أدرجنا هذه المهام لتوضيح وتفصيل مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المستقبلية وهي في رأينا جد مقبولة لتطبيقها. أنظر www.legifrance.gouv.fr/affichTexte.do?...

- ✓ القيام بإذن من السلطات القضائية بجميع إجراءات التحر
لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكب
والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون،
- ✓ تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح،
- ✓ التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون 04/09 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به.
- ✓ من أجل القيام بمهامها فلها تركيز، تحليل، استقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة)، وكذلك كل الإدارات والمصالح العامة للدولة المعنية للقيام بمهامها،
- ✓ يجب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما تسمح به القوانين– وخاصة منها ما يتعلق بالسر المهني– بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والاتصال.

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

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

إنَّ لسلطة الضبط القضائي دور فعال في ضبط أدلة الجرائم ومرتكبيها وكشف كل ما يتعلق بها حال وقوعها.

أما بالنسبة للجرائم المستحدثة فإنَّها تُلقي 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 تكنولوجي... التحقيقات قد يدمر الدليل بمحوه للقرص الصلب بخطأ منه أو بإه... مجال البحث عن أدلة إثبات الجريمة المعلوماتية، من حيث إعداد ضباط الشرطة القضائية وحتى قضاة النيابة العامة والتحقيق وقضاة الحكم[1].

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

فعلى مستوى الدرك الوطني الذي باشر منذ سنة 2004 في عمليات تكوين مستخدمين من أجل إنشاء مركز وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فبموجب هذا العمل فإنّ الكثير من إطارات الدرك الوطني استفادوا من تكوين خاص في جامعات سويسرا وأمريكا، كندا، سواء في المجال التقني (الإعلام الآلي) أو القانوني (الجرائم المتصلة بتكنولوجيات الإعلام والاتصال)، وكذلك تمَّ التكوين في مؤسسات وطنية مثل مركز الدراسات والبحوث في الإعلام العلمي والتقني Cerist الذي عرض تكوينا في الأمن المعلوماتي في إطار التكوين كل سنة.

هذا البرنامج التكويني يهدف إلى تطوير كفاءات سلك الدرك الوطني، حتّى تكون أكثر عملية في مجال مكافحة الجرائم المعلوماتية[2].

كما أنَّ 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[3] .

هذا ما استجد في الجزائر بينما في الأنظمة المقارنة فنجد أنَّه في فرنسا مثلا تمَّ تأسيس العديد من الهيئات التي تختص بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نذكر على سبيل المثال[4]:

– الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال السابق ذكرها، من أجل مكافحة أفضل ضد هذه الجرائم، وهذه المصلحة الخاصة بالشرطة القضائية لِما بين الوزارات تحوي أعوان الشرطة، وأعوان الدرك، الذين يشتركون باختصاصهم في مكافحة هذه الآفة،

---

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص 232.

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

[3] أنظر المرجع السابق.

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

- مديرية مراقبة الإقليم مختصة بتسريع عمليات التحريات الآلية للمؤسسات ذات التدابير الحصرية أو معطيات مصنفة للدفاع
- القسمة الوطنية لقمع الاعتداءات على الأشخاص والأموال La Division nationale de repression des atteintes aux personnes et aux biens التي أخذت على عاتقها منذ سنة 1997 دراسة الاعتداءات ضد الضحايا القصر، وجرائم الإعلام المتصلة بالعالم الافتراضي(Cyber space) .

كما أنَّ الدرك الوطني الفرنسي أنشأ منذ سنة 1998 إدارة مكافحة الجرائم المعلوماتية ضمن المصلحة التقنية للأبحاث القانونية والوثائقية، كل هذه الترسانة من الهيئات والمؤسسات لمكافحة الجرائم المعلوماتية بمختلف أشكالها ما هي إلاّ دليل على خطورة وتشعب هذا النوع الجديد من الإجرام، وهو ما يجب على السياسة الجنائية الجزائرية أن تتبِعْهُ، لأنَّه 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 فإنّ فاعلي هذه الجرائم يتمادون في ارتكاب جرائمهم بدون متابعات قضائية تحد من إجرامهم، لهذا فإنّ التدريب الجيد لعناصر الأمن والدرك الوطنيين والحملات التحسيسية للمواطنين ستحدّ من انتشار هذه الجرائم، وفي حالة وقوعها فإنّ المجرمين ينالون عقابهم لإمكانية الوصول إليهم عبر إجراءات قانونية تتسم بالشرعية.

المطلب الثالث: السلطة القضائية في مواجهة الجرائم المعلوماتية

إنَّ السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد اللّجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، 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[1].

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 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

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

وإطارات وزارة العدل في إطار التعاون الثنائي، ومنها: التعاون الأمريكي الذي تناول خاصة التكوين المتخصص في الملكية الفكرية ولا شك أنَّ تخصيص جهات القضاء وتخصص القضاة هما من السمات الحديثة البارزة للتنظيم القضائي الجزائري ، وقد جاء في اتفاقية التمويل الجزائرية الأوربية لمشروع دعم إصلاح العدالة في الجزائر أنَّ: هذا المشروع يهدف إلى دعم التخصص وتكوين القضاة داخل وخارج الوطن للاستجابة للمتطلبات المستجدة الناتجة عن التزايد المستمر للمنازعات التي يجب عليهم الفصل فيها، ونظرا لأهمية التخصص القضائي فقد عقد له عدة مؤتمرات دولية منها: مؤتمر روما سنة 1958، مؤتمر نيس سنة 1972، مؤتمر ريو دي جانيرو لسنة 1978، وقد أكدت هذه المؤتمرات أنَّ التخصص في مجال القضاء له أهمية كبيرة ودور فعّال في رفع مستوى العمل القضائي، ولنظام التخصص جانبين هما: تخصص القضاة، وتخصيص جهات القضاء[3].

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية(ق إ ج) على أنَّه 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 40 مكرر من ق إ ج على أنَّه « تُطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 40، 37، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه ».

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإنّ هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنَّه جعل المشرع الجزائري لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية[4]، فيتجنب إنشاء هيئات قضائية جديدة لكنّه 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 اختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أنَّ التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية.

---

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

[2] أنظر المنشور الصادر عن وزارة العدل حول فعاليات الندوة الوطنية لإصلاح العدالة –نادي الصنوبر 2005، ص23.

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

[4] عمار بوضياف، المرجع السابق، ص 229.

هذه الأقطاب الجزائية المتخصصة طبقا لنصوص المرسو
2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء
في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، ولأنَّ الجريمة المنظمة تشمل جرائم جِدُ متنوعة تتعلق بسلوكيات خطيرة لأنها تستهدف الأشخاص والممتلكات والدولة، وتُرتكب من طرف عدة أفراد يتصرفون بطريقة منظمة، تعدُّ الجرائم المعلوماتية بشكل من الأشكال جريمة منظمة ترتكب عن طريق الشبكات الرقمية، والتي يمكن معالجتها عن طريق الأقطاب الجزائية المتخصصة، وكما لاحظنا سابقا فإنّ الحركة المتزايدة والضرورية أدت إلى تركيز الاختصاص القضائي في إطار الاهتمام بجدوى وفاعلية الجهاز القضائي في مكافحة الجرائم المستحدثة[1].

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

المبحث الثاني: مكافحة الجرائم المتصلة بتكنولوجيات الإع

لا يمكن مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والا
الكامل فيما بينها، وهذا التعاون غالبا ما يكون في شكل اتفاقيات ثنائية أو متعددة الأطراف في المواد الجزائية ولكنّ 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 معلوماتية يثير عدد من المشاكل فكيف يتم تحديد أي من تلك الدول تمّ 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 أنّ 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 بُدّ 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 كُلِيةً، 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 و/ أو باقي المدعى عليهم من شركاء أو متدخلين أو محرضين، أم لجهة « المكان » حيث وقعت الجريمة »[3] وهو يُعدّ من النظام العام الذي يمكن إثارته في كل 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،

---

[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.

وعناصرها الدولية تجعلها السبب في صعوبات تتعلق بتحديد ال القضية[1].

الفرع الأول: التذكير بالقواعد

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

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

وعليه فإنَّ الفقه الفرنسي بناءً على هذه الاجتهادات القضائية يؤكد على أنَّ 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[4].

3 – تنص المادة 585 من ق إ ج والتي تقابلها المادة 113–5 من قانون العقوبات الفرنسي على أنَّه « كلّ 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 في كِلا القانونين الأجنبي والجزائري بشرط أن تكون تلك الواقعة الموصوفة بأنها جناية أو جنحة قد ثُبت 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[1]

---

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

[2] 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.

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

[4] Yann PADOVA, op. cit, p. 769.

هذا الحكم ينطبق على الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الخارج.

4 – أمّا 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:

– 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 584 ق إ ج)،

– يجب أن يعود المتهم إلى الجزائر،

– يجب ألاّ 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..) فإنّ المادة 583 من ق إ ج توقف تطبيق قانون العقوبات الجزائري على شكوى من الطرف المضرور أو بلاغ من سلطات القطر الذي ارتكبت فيه تلك الجريمة[2](وهي نفس الأحكام الواردة في المادة 113–6 من قانون العقوبات الفرنسي).

وفي الأخير فإنّ الجنايات والجنح المرتكبة ضد جزائريين في الخارج من طرف أجانب فلا ولاية للقضاء الجزائري عليها إلّا في حالة واحدة حددها المشرع بالمادة 591 ق 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[3].

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

---

[1] 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.

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

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

*إنه بمجرد أن تتوافر صورة من هذه الصور الثلاث تعتبر المحكمة صالحة للنظر في القضية، ولكن هل هناك أفضلية لمحكمة من هذه المحاكم الثلاث؟

6 – الجنايات والجنح الماسة بالمصالح الأساسية للجزائر: وهو م
القانون الجنائي الوطني على الجرائم التي ترتكب بالخارج بصرف ال
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 588 من ق إ ج والمادة 15 من 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 589 ق إ ج.

لكن وفي المقابل فإنّ المادة 15 من القانون 04/09 السالف ذكره قد وسعت من اختصاص القضاء الجزائري الجزائري ليشمل الجرائم المرتكبة من أجنبي في الخارج التي تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتجية للاقتصاد الوطني، وذلك لسهولة ارتكابها باستخدام تكنولوجيات الإعلام والاتصال ولعظيم أثرها وسرعة تنفيذها، ولهذا لم يدرج المشرع شرط تسليم المجرم أو القبض عليه في الجزائر ليمنح السلطات القضائية المختصة مجالا للبحث والتحقيق في هذه الجرائم المرتكبة عبر الانترنت ثمّ السعي للحصول على تسليم المجرم لإدانته، كلّ هذا طبعا في حال أنّ المجرم لم تتم إدانته في الخارج من أجل هذه الجرائم ولم يثبت أنّه قضى عقوبته أو تقادمت أو صدر عفو عنه (المادة 589 ق إ ج) تطبيقا لمبدأ عدم جواز معاقبة الشخص عن نفس الفعل مرتين.

الفرع الثاني: تكييف الاختصاص وفق المنازعات

إنَّ 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 أنَّ جزء من تلك الأفعال قد وقعت في مجال اختصاصها.

و الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في غالب الأحيان لها ميزات دولية، غير أنَّ التحقيقات فيها هي بحد ذاتها تعدُّ معطيات تُدَار وتُسَيَر بالقانون الوطني، وفي هذا الصدد فإنَّ تدفق المعلومات عبر تيار حر وهو الانترنت والتحقيق فيها من قِبل سلطات مخولة لذلك لا بدّ أن تكون مقيدة باختصاصها الإقليمي الوطني وبمبدأ السيادة[2].

ذهب بعض الفقه إلى القول بأنه تكون الأفضلية للمحكمة التي ترفع إليها الدعوى أولا، في حين اعتبر البعض الآخر أن لا ميزة مبدئية لمحكمة على أخرى والأفضلية تعود للمرجع الذي يؤمن سير العدالة بصورة عملية، أنظر في هذا الشأن عمر السعيد رمضان، المرجع السابق ص 545.

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

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

وفي غياب اتفاق دولي لتوسيع الاختصاص، وتشريع دقـ
المتصلة بتكنولوجيات الإعلام والاتصال فإنَّ الاجتهاد القضائي الفر
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 أنَّ النيابة العامة مختصة إقليميا أين تمّ نشر الخبر، وفي حالة أنَّ المحتوى صادر عن موقع أجنبي ومُحمل في فرنسا مثلا فإنَّ السلطات القضائية الفرنسية مختصة إجمالا، كما لو أنَّ الجريمة قد ارتكبت بالكامل في الإقليم الفرنسي.

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

2- جرائم التقليد عبر الانترنت: في مواد التقليد المعلوماتي* تكون مختصة إمّا محكمة المكان الذي تمَّ فيه فعل التقليد وإما مكان نشره.

وقد فصلت محكمة النقض الفرنسية في العديد من القضايا مسألة الاختصاص القضائي الفرنسي في مواد التقليد عبر الانترنت ومثال ذلك: عندما قبلت اختصاص محكمة فرنسية مستندة على قواعد القانون الدولي الخاص للنظر في إصلاح الضرر الناتج عن تقليد علامة تجارية في موقع اسباني بالانترنت ولكنه قابِل للوصول إليه من فرنسا، فاعتبرت في هذه القضية بأنّه « إنَّ محكمة الاستئناف التي وجدت بأنَّ هذا الموقع المُغَرَّم يمكن الوصول إليه في الأراضي الفرنسية، بِشكل أن الأضرار المدعى بها من الواقعة الوحيدة لهذا النشر لم تكن احتمالية ولا افتراضية، وقد بررت قانونا قرارها»[1].

وبالمقابل فإنَّ محكمة استئناف باريس[2] أعلنت أنَّ محكمة باريس غير مختصة في الفصل في دعوى تقليد علامة تجارية من موقع للانترنت على شركة لبنانية بالرغم من أنَّ الموقع يمكن الوصول إليه في فرنسا، وبخاصة أنَّ الموقع تتم إدارته في بريطانيا وهو غير موجه أبدا على الوجه المباشر أو غير المباشر إلى مستعملي الانترنت بفرنسا.

---

* لغياب الاجتهاد القضائي الجزائري في هذه القضايا المستحدثة.

* في مراجع عربية مختلفة تم ترجمة مصطلح Contrefaçon en ligne بالتزوير المعلوماتي وهو خطأ في الترجمة فاستنادا لكتاب الوجيز في القانون الجزائي الخاص الجزء الثاني للأستاذ أحسن بوسقيعة ، في موضوع جرائم التزوير فإنَّ هناك ثلاث أعمال مكونة لركنها المادي وهي التقليد contrefaçon التزوير falsification والتزييف altération ، الصفحة 311.

[1] Civ .1re, 9 dec.2003, legalis.net, art 1017, V. Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011

[2] 26 avr.2006, legalis.net,art.1653, V. Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011

هذا الرفض لتنظيم الاختصاص القضائي الفرنسي المستند على Google، لأنَّ محكمة الاستئناف بباريس وضعت معيار جديد للاختـ والأساسي بين هذه الوقائع والضرر المدعى به»[1].

وأخيرا قامت محكمة باريس بإصدار أمرين لها في 16 ماي 2008 باحتفاظ قاضي فرنسي باختصاصه في مواد تقليد العلامات التجارية عبر الانترنت مُستندةً على واقعة أنَّ الأفعال المجرمة التي يمكن الوصول إليها لها أثار اقتصادية على المجتمع الفرنسي « غير هام بأنَّ هذا الموقع يُدار في اسبانيا ويصعُب الوصول إليه بمحركات البحث في فرنسا»[2].

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

إنَّ الاجتهاد القضائي الفرنسي مثّل محل تنفيذ هذه الجرائم بمكان الموقع الالكتروني(web) أين أُتلف، أُنشأ، سُير، غُذي، رُوقب، مستقلا في ذلك عن موقع الخادم الضروري لقيامه بعمله[3].

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

ففي حالة أنَّ هناك عناصر مكونة لجريمة الدخول بطرق الغش لنظام معالجة المعطيات أو جريمة إتلاف المعطيات أو التلاعب بها (بالتعديل، المحو..) موجودة داخل الإقليم الوطني فإنَّ القانون الجزائي الوطني يطبق[4].

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

إنَّ الحاجة إلى تنسيق دولي وثيق في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تَرتبت قبل كل شيء عن الحركة الكبيرة للمعلومات في الأنظمة المعلوماتية، هذه الحركة سمحت بارتكاب جرائم عن طريق جهاز للإعلام الآلي (الكمبيوتر) في دولة ما في حين أنَّ نجاح الفعل الإجرامي يكون بتنفيذه في دولة أخرى. كما أنَّ هذا

[1] 06 juin 2007, legalis.net,art.1944, V. Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011, disponible sur: www.dalloz.fr
[2] TGI Paris, ord.16 mai 2008 legalis.net,art.2419. , V. Répertoire de droit pénal et de procédure pénale © Editions Dalloz 2011.
[3] Ca Paris,13e ch. Section A, 25 septembre2007.
[4] Myriam QUÉMÉNER, Yves CHARPENEL , op .cit. page 163,164.

النوع من الإجرام يتطلب تعاون دولي فعّال لمكافحته[1]، والذي هو م
العابرة للعديد من الدول، أضف إلى ذلك أنَّ تصدير البرامج المعلو
لحمايتها.

ونتيجة لذلك فإنَّ الانترنت بقدر ما هي فضاء مفتوح للاتصالات فإنَّها تخلصت من كل قيود الإقليمية، وتسمح بنشر كل أنواع المعلومات بدون عقبات جغرافية. وبالمقابل، القانون الجزائي هو تعبير عن سيادة الدول، وفي هذا السياق فإنَّه 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، فإنَّ هذه الأخيرة يمكن أن تعدُّ إمّا مشروعة أو غير مشروعة، يرجع هذا غالبا للوظيفة المتغيرة لمبادئ حرية التعبير واحترام الحياة الخاصة [2]، وخير مثال على ذلك قضية Yahoo حيث أنَّه 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 الإستعجالي أُرفق بتقرير كُتب من طرف مجموعة من الخبراء يُفصلون 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 القضائي لمقاطعة شمال كاليفورنيا بفحص الأمر أولا من حيث مطابقته للدستور الأمريكي الحامي لحرية التعبير، وفي حكمه بتاريخ 07 نوفمبر 2001 اعتبر القاضي جيرمي فوجيل Jeremy FOGEL أنَّ القرارات الفرنسية تكون« بوضوح غير متلائمة مع أول تعديل إذا هي أصبحت مطبقة في الولايات المتحدة الأمريكية من محكمة [...]، إنَّ فرنسا لها السيادة من أجل وضع الحدود لحرية التعبير في إقليمها، هذا المجلس لا يمكنه تنفيذ قرار أجنبي لا يحترم الدستور الأمريكي، إلاّ في حالة إلغاء حرية التعبير المحمية داخل حدودنا الإقليمية [...]، إنَّ المجلس ملتزم حتما ببعض الأحكام التي هي على قدر من المشاركة الجوهرية في الثوابت، وخاصة في فكرة أساسية وجوهرية للتعديل الأول، الذي بمقتضاه أنَّه من الأحسن

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، 2009، دار المعارف بالاسكندرية، ص 103.

[2] 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 Pantheon-Sorbonne paris I, disponible sur: www.univ-paris1.fr/.../2004_sept_OK_Brisset_ Giustinani_ Version_ ... .[06/06/2011].

السماح بتعبير غير عنيف لأراء مزعجة أفضل من وضع أفكار ح
بأنَّ الجهود نحو تعاون دولي لوحدها التغلب على خطر إزالة فاع
الفضاءات القانونية الوطنية[2]، ومن المهم ملاحظته أنَّ التشريعات الوطنية في مجال الجريمة المعلوماتية في مجملِها حديثة الصدور وبعض الفوارق يمكن إيجادها، خاصة في حالات تجريم القرصنة، فمثلا في الولايات المتحدة الأمريكية الدخول غير المشروع للنظام المعلوماتي لا يُعَدُّ مجرما إلاّ إذا وقع على أجهزة الكمبيوتر للمؤسسات العامة، وأمّا في اليابان فإنَّ هذه الجريمة لم توضع قواعد تجريمها إلاّ في سنة 1999[3]، وبالنسبة لنا فإنَّ أحكام المساس بأنظمة المعالجة الآلية للمعطيات ومن بينها الدخول غير المشروع للأنظمة المعلوماتية لم يتم تجريمه إلاّ في سنة 2004 بموجب تعديل قانون العقوبات بالقانون رقم: 15/04 المؤرخ في 10 نوفمبر 2004.

وللتعاون الدولي صور عديدة يهمنا منها التعاون القضائي الدولي الذي أدرجه القانون 04/09 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

يُعَدّ 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

إنَّ مكافحة أساليب الإجرام المعلوماتي لا يتحقق إلاّ 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.

فإنَّه يصعب على الدولة بمفردها القضاء على جرائم المعلوماتية العابرة للحدود، لأنَّ جهاز الأمن في هذه الدول أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة، ولذلك فإنَّ الحاجة مُلِّحة إلى تعاون

[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/. V. Yann PADOVA, op. cit, p. 775.
[2] . Ibid., p. 775.
[3] Anne BRISSET-GIUSTINIANI, source précédente.

أجهزة الأمن بين الدول وتنسيق العمل فيما بينها لضبط المجرمين حدود الدولة، وقد تبلور هذا النوع من التعاون الدولي في إنشاء المنظ

وتستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات الأمن في الدول الأطراف على نحو فعال يُحقق مكافحة الجريمة، وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المُنظَمة، وتبادل المعلومات والبيانات فيما بينها والتعاون في ضبط المجرمين بمساعدة أجهزة الأمن في الدول الأطراف، ومدها بالمعلومات المتوافرة لديها على إقليمها، أي أنَّ عضو الإنتربول لا يقوم بنفسه بإجراء القبض على المجرم، بل أنَّ هذا العمل منوط بجهاز الأمن الوطني في الدولة التي يتواجد المجرم على إقليمها، الأمر الذي يؤكد على احترام السيادة الوطنية.

ولذلك فإنَّه من الأهمية تدعيم التعاون بين أجهزة الشرطة في هذه الدول المختلفة بناءً على اتفاقيات دولية، ولهذا التعاون أهميته بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أنَّ إحدى الجرائم المعلوماتية قد تمّ ارتكابها عبر شبكة الانترنت من خلال موقع موجود في الخارج فإنَّها تقوم بالإبلاغ عن هذه الجريمة إلى سلطات الأمن بالدولة التي تمّ منها البث[2].

يجمع الإنتربول 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)[3]:

- 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 الجُرمية المتبعة في الإجرام المعلوماتي عن طريق الفِرَق العاملة الإقليمية وحلقات العمل التدريبية،
- إنماء شَرَاكات 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

---

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

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

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

كمبيوتر ضبطت خلال عملية لمكافحة المخدرات والإرهاب نفذت
لتحديد ما إذا كان جرى التلاعب بمضمون أي من المعدات بعد
للإنتربول دراسة فنية مستقلة وأصدر تقريرا خلُص لغياب أي دليل يشير إلى تعديل ملفات المستخدمين او تحريفها او 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 كوّن الإنتربول 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 شرطاً أساسياً لاستحداث منظومة الإنذار المبكر. وقد بادر أكثر من 120 مكتباً مركزياً إلى تعيين نقاط مرجعية مركزية وطنية.

كما استحدثت فرق للانتربول تعنى بجرائم تكنولوجيا المعلومات لتيسير إنماء الإستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجُرمية 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].

الفرع الثاني: المساعدة القضائية الدولية في المواد الجزائية

1- أشكال المساعدة القضائية الدولية:

لمّا كانت جرائم المعلوماتية ذات طابع عالمي وبالتالي يمكن أن تتعدى آثارها عدة دول، فإنَّ 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 حُول 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[2].

---

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

[2] طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي– النظام القانوني للحماية المعلوماتية– (مرجع سابق) ص: 597.

وتُعرَّف المساعدة القضائية الدولية بأنَّها« كل إجرا
المحاكمة في دولة أخرى بصدد جريمة من الجرائم »[1] ، كما يمكن
قضائية لدولة بتوجيه إنابة قضائية إلى سلطات قضائية مختصة في دول أخرى من أجل تنفيذ جيد لها» ، 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:

أ- **نقل إجراءات الردع Transmission des procédures répressives:** ويقصد به قيام دولة بناءً على اتفاقية باتخاذ إجراءات جزائية بصدد جريمة ارتكبت في دولة أخرى، وذلك إذا توافرت شروط معينة:

1. أن يكون الفعل المنسوب إلى الشخص يُشكل 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[3].

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

وخلاصة الاتفاق بينهما هو أنَّ 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[4]، وقد أقرَّ المجلس الأوربي اتفاقية نقل الإجراءات الجنائية، التي تعطي لإطراف المُنضمة 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 7 أكتوبر سنة 2002 (المرسوم الرئاسي رقم 23/04 مؤرخ في 7 فيفري 2004، الجريدة الرسمية عدد 08).

ب-**تبادل المعلومات:** وهو ما نصت عليه المادة 17 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نصت على أنَّه « يتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات

---

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

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

[3] طارق ابراهيم الدسوقي عطية، مرجع سابق، صفحة 599.

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

الدولية الثنائية ومبدأ المعاملة بالمثل»، فتبادل المعلومات يش
قضائية أجنبية بصدد جريمة ما، عن الاتهامات التي وُجهت
ضدهم، كما أنَّ 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، إلاّ أنَّ تدويل صحيفة السوابق القضائية لا يتم إلاّ 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 أنَّه « 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 في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[2]، وهو ما أبرزته المادتين 16 و 17 من القانون 04/09 السالف الذكر، والذي عبّرت عنه باتخاذ إجراءات تحفظية، ولا يكون ذلك إلاّ 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 فإنَّه 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، ولأنَّ الجريمة المعلوماتية لها ثلاث ميزات:

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

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

[2] بن محمد محمد، مرجع سابق، ص 156.

فإنَّ تلك الطريق لا يمكن اعتمادها دائما في مجال التح
والاتصال، ولهذا نجد أنَّ المشرع الجزائري أورد استثناءً في المادة 16
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 »

بناءً على ما أوردته الفقرة 2 من المادة 16 نجد أنَّ 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 رأينا 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 تُرفض 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- بِحسب نص المادة 16 فقرة 1 من القانون 04/09 أدرج المشرع مبدأ ازدواجية التجريم La double incrimination وإن لم يكن قد صرح به وتنص المادة على أنَّه « 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 تخُصُ أفعالا غير مُجرمة لديها، وعليه فإنَّه 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] .

وفي الواقع وحتى في حالة عدم استخدام قاعدة ازدواجية التجريم في كل حالات المساعدة القضائية، فإنَّ هذه القاعدة هي في الكثير من الأحيان ضرورية من أجل " إتمام أعمال التحقيق أو الوصول إلى أدلة الإدانة أو إلى الملفات أو الوثائق"[2].

---

* يتم فقد المعلومات في حالة أنَّ القانون الوطني لدولة ما تسمح لمقدمي الخدمات بحفظ المعطيات لمدة معينة (في الجزائر مدة الحفظ سنة واحدة وفي دول أخرى مدة الحفظ لا تتجاوز 6 أشهر) بعدها يتم محو تلك البيانات، أمّا بالنسبة لإتلاف المعلومات فيكون عمدا من طرف مرتكبي الجريمة.

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

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

لقد تم البحث في هذا الفصل عن دور السلطات بتكنولوجيات الإعلام والاتصال، وذلك بنص المشرع على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وإن 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.

ثمّ 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 أنَّ 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:

آليات البحث والتحري للكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تمهيد:

إنَّ إصدار المشرع للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قد أرسى قواعد إجرائية جديدة تخضع لها السلطة القضائية وأعوانها تطبيقا لمبدأ الشرعية الذي يعدُّ حجر الزاوية في الإجراءات القانونية للتحقيق في الجرائم المرتكبة ومتابعة فاعليها وتوقيع العقوبة المناسبة لهم[1]، هذه الإجراءات الجديدة التي يستطيع بها رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية التي أرساها قانون الإجراءات الجزائية، لذلك سيكون تقسيم هذا الفصل على نحو يسمح بالتعرف على الأدلة الرقمية وأساليب استخلاصها وفقا للمبحثين التاليين:

المبحث الأول: الدليل الرقمي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

المبحث الثاني: طرق التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

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

المبحث الأول: الدليل الرقمي في الجرائم المتصلة بتكنولوج

تقوم فكرة الإثبات عموماً على احترام حقوق الإنسان، فأ
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 آثاراً جزائية، 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 أنَّ 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 اتفاقها مع التقنية الحديثة يبدو غير ذي معنى إذ لم يكن مدعماً بتوفيق من قبل التقنية ذاتها مع كل ما يتم إثباته في هذا الشأن[3].

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[4]، وهذا فعلاً ما قام به المشرع الجزائري مُحتذياً بذلك بما قامت به التشريعات المقارنة، من تبني وسائل جديدة للبحث والتحري في هذه

---

[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 أعلاه، ص 582.

[3] فتحي محمد أنور عزت، المرجع أعلاه، ص 632.

[4] فتحي محمد أنور عزت، المرجع أعلاه ، ص 633 (أنظر الهامش).

الجرائم، فإضافة للوسائل التقليدية (التلبس، التفتيش، التسرب، اعترا
جديدة للتحري والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و
إلى تفتيش النظم المعلوماتية وكيفية حجز الدليل الإلكتروني جاعلاً من الدليل الرقمي بنفس قيمة الدليل التقليدي الذي يستند عليه في 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:

المطلب الأول: مفهوم الدليل الرقمي

يعرف الدليل في اللغة بأنه المرشد، وما به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات[1]، ويعرف الديل 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 إِلَى 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 الاقناعي 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:

الفرع الأول: تعريف الدليل الرقمي،

---

[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 السابق، ص 29.

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

الفرع الأول: تعريف الدليل الرقمي

يمكن تعريف الدليل الرقمي، بأنه الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات[1]، والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة باستعماله تكنولوجيات الإعلام والاتصال [2].

كما عرفته المنظمة العالمية لدليل الكمبيوتر في أكتوبر 2001 بأنه: المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية، وقبل ذلك عرفته في سنة 2000 بأنه: المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة[3]، ويؤخذ على هذين التعريفين ما يلي:

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

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

والتعريف الأكثر شمولاً في نظرنا هو الذي يعرف الدليل الرقمي بأنَّه « طريقة خاصة لإظهار الحقيقة والذي يتم فيه اللجوء إلى أحد الوسائل الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب Le Disque Dur ، والرسائل الإلكترونية المخزنة أو المنقولة رقمياً».[4]

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.

---

[1] فتحي محمد أنور عزت، المرجع أعلاه ، ص 635.

[2] فتحي محمد أنور عزت، المرجع أعلاه ، ص 635.

[3] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009، ص 213 (أنظر الهامش).

[4] 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 de justice en informatique et associées: www.cnejita.org/.../CNEJITA-ACTES-COLLOQUE13042010-A5-V5.1-pdf.[28/02/2011]

أولا: المعلومة الرقمية قبل الدليل:

تذكير بخصائص المعلومات الرقمية:

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

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

ب- غنية كمياً: لأنه يقدر بأنه 100 مليار 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 أحياناً، وأحيانا أخرى يكون صعبا استغلالها.

و- هذه المعلومة قابلة للمحو والحذف ولكن ليس بسهولة.

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

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، وأخيراً معيار الاستمرارية يعد كماليا ولكن لا يمكن إهماله وهو مرتبط بالحفظ الجيد للمعلومة.

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).

3- تسمح أيضاً بتنظيم أساليب صالحة للمعارضة أو الطعن في أدلة الطرف الآخر

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

وهو معيار ضروري جداً، والذي حتى بدون حق الوقوع في أو البراءة) فمثلاً: 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(Métadonnés) يمكن بسهولة تغييرها سواء عن طريق الخطأ أو عمداً، كذلك طلب بسيط لملف يغير من هذه البيانات التعريفية، وبالتالي تعد هذه البيانات متبخرة جداً، 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.[1]

2- 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 تماماً، 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 aprés: 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 فيزيائياً أي (bit à bit) وهو يسمح بالبحث عن بقايا محتملة لملفات محذوفة.[2]

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

[1]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-ACTES-COLLOQUE13042010-A5-V5.1-pdf.

[2]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 traçabilité

معيار التتبع هو معيار مرافق للمعيارين السابقين (أصالة السابقة ضرورة أن العمليات التي تتم يجب أن توصف بدقة، وهناك اساليب للتتبع سواء يدوية او الية، ومثال مبسط لذلك النسخ على قرص ليزر (Gravure d'un CD Rom) يسمح بتوضيح أهمية معيار التتبع:

1- قرص ليزر تم النسخ إليه بنجاح بواسطة Graveur de Windows 7 ؛

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

3- قرص ليزر تم النسخ إليه بواسطة Windows XP؛

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

إن الملف الذي تم نسخه إلى القرص أنشئ بتاريخ 1 جانفي، تم نسخه إلى الأقراص في 15 جانفي، 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 General 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 Windows XP	1er janvier	1er janvier	1er janvier	1er 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 المتوجب فإن عرض حالة إنشاء الملف سيكون خاطئاً. 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 و CD، إذ بمرور الوقت لا يمكن متابعة تسجيل فيديو على CD أو DVD مرت عليه

[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.

سنوات من الحفظ ليس بسبب البرنامج ولكن بسبب تلف الدعامة الم
لإمكانية استغلال الدليل إذ يجب أن يكون مقروءً و واضحا*.

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 الاشكالية: تحليل الدليل الرقمي (القرص الصلب، مفتاح USB، بطاقات الذاكرة...) لا يجب أن يتغير خلال العمليات التقنية، وهو يعد تحدٍ مهم لأن أطراف الدعوى بإمكانهم اعتباره معيبا لعدم حفظ سلامة الدليل الرقمي، أو للمتهم أن يفند التحقيق التقني للصور غير المشروعة التي وُجدت في جهازه في حالة أن بايت واحد (وحدة قياس في المعلوماتية) من الدليل الرقمي قد تغير.

فالتغيرات قد تكون غير عمدية: مثلا يكفي فقط تشغيل الحاسوب في محيط Windows ، حتى يتم تغيير العديد من ملفات النظام (تاريخ آخر تعديل مثلا)، وهو ما يدعى « أعراض القراءة 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.

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

* إذ أن بعض الملفات تكون إما غير مرئية أو مشفرة مثلا.

وفي الأخير يجب حساب البصمة الرقمية للنسخة المنجزة، وكذلك ح
عند انتهاء المعالجة، وتسمح المقارنة بين البصمات الثلاث (
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:

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 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 .

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 المتصليـ الصوتي).

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

الاستفادة من ذاكرة الهاتف المحمول تتم بتشغيل الهاتف ببطاقة SIM للاختبارات ويتم استعمال برنامج خاص بقراءة المعلومات الموجودة في الهاتف (الرسائل القصيرة، الصور، الأفلام...).

أما الاستفادة من الملفات المقدمة من طرف مقدمي خدمة الهاتف فيتم 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 القراءة (lecteurs)، تقوم مختلف أجهزة الأمن بجلبها أو حتى بصنعها لمساعدتها في مختلف التحقيقات.

[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.univ-paris1.fr/.TYRODE_ MEMOIRE.pdf [03/09/2012].

المطلب الثالث: المبادئ العامة للأدلة الرقمية

خلف التعقيد التقني الملازم للعالم الرقمي فإن التحريات الخ
المبادئ الرئيسة للأدلة الجنائية، وبانبثاق إجراءات خاصة 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 أحياناً 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.

وإذا كان تقديم الأدلة في المواد الجزائية حر بناءً على نص المادة 212 من قانون الإجراءات الجزائية فهي ليست أقل خضوعاً لمراعاة 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 قانوناً 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.

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 ـ في وقت الحاجة ـ "الحدود" بين وسائل 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 يُفرَض عليهم جمعها قانونياً، 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،

[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

ولأنه يخصه فقط، وبتطبيق المادة 927 ق إ ج قدر القاضي قيمته ا
محكمة الاستئناف قد بررت قرارها ».

جزاء الإخلاء بالمبدأ:

توضيحاً لما يتعلق بالمحافظة على مجال التحقيقات الرقمية واعتباراً 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 قراراً في 04 جوان 2008[1] انتقدت فيه إجراء تم فيه استغلال معلومات محصلة من طرف السلطات الأمريكية عن تواجد جرائم حبس صور تحوي مواد إباحية للأطفال عن طريق الانترنت (Cyber-pédopornographiques)، 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.

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 وفقاً: "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[2].

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

[1] Cass. Crim, 04 juin2008, bulletin criminel 2008, n° 141.
[2] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit.page.172.

المبحث الثاني: طرق التحقيق في الجرائم المتصلة بتكنولو

إن الجرائم المرتكبة عن طريق الشبكة المعلوماتية الانترن
بالتطور التكنولوجي.

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

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

– القانون رقم 04/09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، يحوي هذا القانون تدابير مهمة لتدعيم فعالية 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 اعتراض المراسلات، أوجد المشرع وسائل أخرى أكثر فعالية مثل: التفتيش المعلوماتي، حجز المعلومات، التفتيش عن بعد، أدرجها ضمن القانون 04/09 السالف ذكره، إن الروح العامة لهذه القوانين الإجرائية هي السماح بوضع الأدوات 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.

وعليه فإن تقسيمنا للمبحث يكون بالبحث:

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 .

كل حال فإنَّ التكنولوجيات الحديثة للمعلوماتية قدمت نطاقا جديدا لتطبيق الرقابة[1].

أمّا الاتصالات الالكترونية فقد عرَّفها المشرع بأنَّها 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 (Facebook, 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 1986 أصبح التعريف المذكور يتسع ليشمل الاتصالات الالكترونية الأخرى[2].

وقد وضع الفقه العديد من التعريفات لمراقبة الاتصالات الالكترونية منها:

1- ذهب رأي إلى تعريف المراقبة الالكترونية بأنها تعمد الانصات 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[3].

---

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

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

[3] عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية،1999، ص 404، مشار إليه لدى ياسر الأمير فاروق، المرجع السابق، ص 139.

2- وذهب رأي آخر إلى تعريفها بأنها تعني من ناحية التنصت ناحية أخرى تسجيلها enregistrement بأجهزة التسجيل ويكفي لمباش لقيام المراقبة[1].

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[2] .

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 غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع إلى الحديث، ومن ناحية أخرى حفظه بواسطة أجهزة مخصصة لذلك[3]. 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 الارهاب

---

[1] 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.

[2] 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.

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

واحتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام الوطني (القانون 04/09 المتضمن قواعد الوقاية من الجرائم المتصلة

5- ومراقبة الاتصالات الالكترونية هو إجراء خاص يتم بإشراف قضائي بحسب الحالات، وتعرف بأنها تقنية تقوم على تدخل وسطي لتحويل مسار في خط مشترِك بوسيلة ممغنطة، من أجل التسجيل والمحادثة، وهي تمثل فائدة أكيدة لفاعلية المتابعات الجزائية[1].

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 ـ أ من قانون 04/09) أو كإجراء تقتضيه التحريات والتحقيقات القضائية.

وهذا الإجراء ليس جديدا على المنظومة القانونية الإجرائية الجزائية، فقد نصَّ عليه المشرع قَبلا في قانون الإجراءات الجزائية في الفصل المتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور (المواد من 65 مكرر إلى غاية المادة 65 مكرر 10 من ق إ ج)، ولكنَّه قَصَرَ 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 فإنَّ المشرع قد أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني لاستكمال التحريات أو التحقيقات حتى في جرائم تقليدية إن صحَّ قول ذلك، ومثال ذلك: جريمة الزِنا المنصوص عليها في المادة 339 من قانون العقوبات حيث يمكن إثباتها حتّى برسالة الكترونية في بريد المتهم الالكتروني كإثبات تقبله المحكمة.

الفرع الثاني: حالات اللُّجوء إلى المراقبة الالكترونية

يمكن اللُّجوء إلى المراقبة الالكترونية إذا توافرت إحدى الحالات التالية:

أ ـ 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

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

* وهي تختلف عن التفتيش الوقائي الذي لا يعدّ 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

تهديد لأمن الدول، وتشمل البحث عن المعلومات السياسية، الا
الإجراء التقني ليس موضوع إجراءات قضائية، ولا يمكنه التمتع بح
الإجراءات الجزائية، فهذا الشخص ليس في أغلب الأحيان مشتبه فيه لارتكاب جريمة في مفهوم قانون العقوبات ولكن شخصه أو نشاطاته يُمكن أن تُمثِل خطرا على الأمن الداخلي[1]. وعليه فإنَّ هذه الجرائم لم ترتكب ولكن المشرع سمح في إطار الوقاية من هذه الجرائم بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات يُحتمل تورطهم مستقبلاً بالقيام بالأفعال الموصوفة جرائم إرهاب أو تخريب أو الجرائم الماسة بأمن الدولة، والاحتمال هنا ليس لدرجة توافر دلائل قوية تربط هؤلاء الأشخاص بارتكاب تلك الأفعال، وإنما مُجرد الشكوك ولو بسيطة، فالوقاية لا تفترض القيام بأعمال تحضيرية لارتكاب هذه الأفعال وإنما مُجرد تكهنات أو حتّى دلائل بسيطة قد توحي بأنَّ هؤلاء الأشخاص يُمكنهم ارتكاب تلك الأفعال.

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

ب ـ 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 يُعرف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال أنَّها صعبة الاكتشاف ولا يتم اكتشافها أحيانا إلاّ مُصادفة، فكيف عن هذا الاحتمال الوارد في نص المادة 4 فقرة ب من القانون 04/09، وإن كان هذا الأمر يدخل أيضا في إطار الوقاية من هذه الجرائم.

ج ـ لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللّجوء إلى مراقبة الاتصالات الالكترونية.

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

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، الاسكندرية، مصر، 2008، ص 670.

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

الفرع الثالث: العمليات الإجرائية

هناك نوعان من الإجراءات المُطبقة على مراقبة الاتصالا التي يتم مراقبة مرتكبيها:

I ـ **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 أنَّ 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 إلاّ بإذن مكتوب من السلطات القضائية، حيث أنَّ المادة 3 من قانون 04/09 صرّحت بأنَّه « مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يُمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، **وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية** وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها»، وعليه فإنَّ الحالات التي لم يَرِد بشأن تنظيمها، قواعد وإجراءات معَيَنة 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 ـ الجرائم التي يُطَبَق عليها الإجراء[1]:

← **1**ـ 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** ـ في الفقرات ب، ج ، د من المادة 4 من قانون 04/09 لم يُحدد 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 يُحدد المشرع نوع الجرائم التي يصعب الوصول في التحريات والتحقيقات القضائية الجارية في شأنها إلى نتيجة تهم هذه الأبحاث دون اللجوء إلى هذه المراقبة ، وبالتالي فإنَّ جميع جرائم القانون العام يمكن أن يَلجأ فيها المحقق لهذه المراقبة في حالة ضرورتها.

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

ونلاحظ تراجع المشرع عن حصر الجرائم التي يمكن اللجوء فيـ
المراسلات بكل أنواعها.

ب ـ **نوعية العملية أو الإجراء:** وتتمثل في: – 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 ـ 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 ـ 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: كلُّ الجرائم المذكورة ، وإذا اكتشفت جرائم أخرى غير تلك الوارد ذكرها في الإذن فلا تُبطَل الإجراءات العارضة.
- ← شكل الإذن ومدته: يُسلَّم مكتوبا ولمدة أربعة أشهر قابلة للتجديد عند الضرورة، ويسمح بالدخول للأماكن السكنية أو غير السكنية في أي مواعيد (خارج تلك المحددة في الشريعة العامة بموجب المادة 47 ق إ ج)، وبغير رضا أو علم أصحاب الأماكن خلافا للشريعة العامة.

ثالثا: الإجراءات

أ ـ **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 ـ **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 يُسَخِر كلُّ عون مؤهل لدى أي مصلحة عامة أو خاصة

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

(وحدة أو هيئة ..) مكلفة بالاتصالات السلكية أو اللاسلكية من أج
القيام بها.

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

ويوضع هذا المحضر بين أوراق ملف الدعوى أمام القاضي المكلف به (وكيل الجمهورية أو قاضي التحقيق)[1].

د ـ حدود استعمال المعطيات المتحصل عليها: إنَّ 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).

هـ ـ لا يُعدُّ اعتراضا للمراسلات بمفهوم المادة 65 مكرر 5 من قانون الإجراءات الجزائية واقعة الاتصال بالشبكة الرقمية وبدون اللُّجوء إلى تعديلات مسبقة في البرنامج المُراقب، قراءة ما يستطيع أي مستعمل قراءته.

II ـ 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 ـ الإذن: يُقدم الإذن بناءً على تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها، وتكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في هذه الحالة موجهة حصريا 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 ـ 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.

جـ ـ 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.

د ـ مدة الإذن: حددها المشرع ب ستة (6) أشهر قابلة للتجديد.

---

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

المطلب الثاني: تفتيش المنظومات المعلوماتية:

ونتناول فيه ما يلي:

الفرع الأول: المفاهيم الأولية

يقصد بالتفتيش Perquisition التقصي والبحث عن الأدلة سعياً 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.[(*)]

ولتيسير هذا المفهوم يجب أن نتطرق إيجازاً 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

---

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

[*] أوضحت المذكرة التفسيرية لاتفاقية بودابست أن المقصود بالنظام المعلوماتي: هو جهاز يتكون من مكونات مادية Matériel (Hard Ward)، 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 يكون منفرداً 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.

أ- وحدة النظام التي تحوي وحدة المعالج Processeur والذي به تنف
إما أن تكون أوامر رياضية كعمليات الجمع والطرح، والمعادلات ا
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).

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

* **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.

ثانيا: الشبكات التقنية الإلكترونية

وهي تلك الشبكات التي تربط الحواسيب فيما بينها وهي ثلاث أنواع: الانترنت، الاترانت، والإكسترانت؛ 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 الأترانت الأشخاص العاملين في نفس المؤسسة بالاتصال ببعضهم البعض والوصول

إلى المعلومات بطريقة أسرع وأفضل وأكثر كفاءة وأقل تكلفة من الأس
إنجاز الاجتماعات وتحضير المذكرات وإرسال البريد.

تعتبر الأنترانت نسخة مصغرة من الانترنت تعمل داخل المؤسسة ولا يمكن لأحد الوصول إليها إلا لمن يعمل داخل المؤسسة ولديه كلمة السر للدخول إلى الأنترانت 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... إلخ. ومن جهة أخرى تعد الانترنت شبكة مفتوحة ذات امتداد عالمي فضلاً 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؛
5- منتديات المحادثة؛
6- خدمات تبادل الأخبار والمناقشة؛
7- خدمة نقل الملفات.

[1] ا مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، مصر، الطبعة الأولى 2009 ، ص 75.
[2] فتحي محمد أنور عزت، الأدلة الالكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون، مصر، طبعة 2010، ص 33.

الفرع الثاني: حالات اللجوء إلى تفتيش النظم المعلوماتية و

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].

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

1- وقوع جناية أو جنحة؛

2- اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها؛

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

هذه القواعد لا يمكن أن تكون سبب لتفتيش نظم المعلوماتية لأنه طبقاً لنص المادة 05 فقرة 01 من قانون 04/09 أجازت التفتيش بقصد الوقاية من جرائم حددها المشرع لم ترتكب ولكن تعد أسلوبا وقائياً 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 اعتداءً فعليا على الحياة الخاصة للأفراد التي كفلها الدستور، ولا يمكن اللجوء إليه إلا في حالة الوقوع الفعلي للجريمة.

والحالتين الأخريين هما:

---

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

– حالة اللجوء إلى تفتيش نظم المعلوماتية لمقتضيات التحريات والت
إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى تفتيش هذه المنظوم

– وأخيراً 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 الأولية كما هو الحال بالنسبة لمراقبة 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 أوراقاً 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 44 إلى 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).

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 ل
والاتصال ومكافحتها على: « إمكانية الدخول بغرض 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 المادة 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 أياً 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- وجود دلائل أو أسباب تدعو للاعتقاد بأن الكشف عن المعطيات يكون بالبحث في المنظومة الثانية. 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 أراه 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 مسبقاً، 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 (تسجيل البيانات، الحفظ، تحويل...) وكأن المراقب يشاهد ما يشاهد 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 حصراً من طرف النائب العام لمجلس قضاء الجزائر العاصمة، وأعتقد أن هذا يعد ضماناً كافياً لحماية الحياة الخاصة للأشخاص لعدم التوسع في المراقبة: سواء من حيث الاختصاص أو من حيث السلطة التي تسمح بهذا الإجراء. 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 وقائياً وإنما يتم فقط كتحريات أو تحقيقات لجرائم معينة على درجة من الخطورة قد ارتكبت فعلاً أو لوجود دلائل أو احتمالات قوية تهدد الأمن الوطني.

جـ- حالة وجود معطيات مبحوث عنها يمكن الدخول إليها انطلاقاً 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 طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً 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.

ويجدر التنبيه أنه يمكن بناءً 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 ووفقاً لمبدأ المعاملة بالمثل بين أطراف الاتفاقية الدولية[2]، من أجل معرفة المعطيات الموجودة في خادم موجود

---

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit,.p182

[2] المادة 32 من 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

بالخارج؛ فإن فتح تحقيق قضائي يسمح بتحرير إنابة قضائية دولية عقبة وقتية للحصول عليها، وفي هذه الحال يمكن للمجرم المعلوماتي

د- **التسخير**: (المادة 05 فقرة 04 من قانون 04/09 والمادة 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: بناءً 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 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.

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

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، ص 206.

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[1].

ويترتب على هذا الارتباط بين التفتيش والضبط؛ أن الضبط لا يجوز أن يقع على شيء إلا وصفه دليلاً 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 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 أيضاً على الأشياء التي تفيد الحقيقة أياً كانت وإن أدت إلى تبرئة المتهم ».[2]

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.[3]

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

---

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

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

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

الحجز يشمل المعطيات التي يمكن الدخول إليها أثناء التفتيش في المعطيات يتم بوضع يد القضاء عليها سواء الدعائم المادية، وسو 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 نموذجية لجمع الأدلة الرقمية تسمح بحماية الإجراءات وذلك بتقليص خطر إبطالها إجرائياً.[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 تماماً 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... ».

وأخيراً 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.

---

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

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

ب- الحجز عن طريق منع الوصول إلى المعطيات: تناولت الم
الاستحالة التقنية لإجراء الحجز بنسخ المعطيات الرقمية محل البحث
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 مثلاً شعارات 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 خطراً على أمن الأشخاص أو الممتلكات، مثال ذلك: الصور الخاصة بالاعتداءات الجنسية على القصر.[1]

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

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، وإن توصيل الخدمات المتنوعة لهذه

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

التكنولوجيات إلى مستعمليها يتطلب توافر مجموعة من الفاعلين (الـ

وقد عرفهم في المادة 02 فقرة د من قانون 04/09 على أنهم: « د ـ

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

2– وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ».

إن المشرع في تعريفه لمقدمي الخدمات قد جمع ثلاثة أنواع من الوسطاء يسمح تدخلهم بتوصيل خدمات تكنولوجيات الإعلام والاتصال بأنواعها إلى مستعمليها، وهم 1- 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 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 كلاً 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/1 بأنهم: « أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/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].

[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 éléctroniques".

2- **متعهدي(مقدمي) خدمة الإيواء isseurs d'hébergement**

وهم بحسب القانون الفرنسي « كل الأشخاص الطبيعية أو الجمهور و بواسطة وسائل الاتصال عبر الانترنت للجمهور: 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 إلاّ 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 ثَمَّ 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: 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 09 فيفري 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 المُطَوَرة تصنف المؤسسات MySpace inc, 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

---

[1] L'article 6-1-2 de la loi n°2004-575 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. p .44.

استندوا على الرسالة نفسها للقانون المتعلق بالثقة في الاقتصاد الرقمي LCEN ـ numérique ـ فالمحكمة وبالنتيجة أشارت إلى أنه « ليس وضع المحتوى المجرم عبر الانترنت، التدخل بطرق معينة وأيا كانت في إنشائه» ، فالمعيار المحدد هو إذن التدخل في إنشاء المحتوى نفسه، كما يظهر في نص المادة 6- II 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.

المدونون مقدمي خدمات خاصين:

صاغ مصطلح Weblog جون بارغير John Barger في 17 ديسمبر 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[3].

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[4]، ليس هذا فحسب وإنما يقوم المدون الذي يستخدم دائما اسما مستعارا و أيضا المشاركون معه في المواقع بالتحدث بحرية مطلقة وانتقاد الأوضاع الموجودة في البلد الذي ينتمون إليه والبلاد الأخرى.[5]

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] Ibid. p 45.
[2] Ibid. p 45.
[3] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية ، مطابع الشرطة القاهرة، مصر الطبعة الأولى، 2009، ص 84.
[4] 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.
[5] مصطفى محمد موسى، المرجع السابق، ص: 86.

ويعد المدون كالناشر في خدمة الاتصالات للجمهور عبر مدونته، ويمكن إذن متابعته في حالة ارتكاب جريمة من طرفه، كما 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 10 نوفمبر 2009 التي رأت 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 يَقُم 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 المجرَّم 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 رافقت تطبيق هذه الالتزامات.

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

عرّف 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 11 من القانون 04/09 المتضمن 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

[1] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p 46.
[2] Myriam QUÉMÉNER, Yves CHARPENEL, op. cit. p 46.

القضائية أو في حالة طلب هذه الأخيرة لأجل التحريات أو المعاينات 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 فقرة1 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 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.

[1] Ibid. p .176.

وبالرجوع لالتزام مقدمي الخدمات بتقديم المساعدة للسلطا
تتعلق بقانون مكافحة الإرهاب رقم 2006/64 الصادر في 23 جانفي
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 11 من 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؛

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها؛

هـ- 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 10 فقرة 1 على مقدمي الخدمات (التوصيل والإيواء) أن يضعوا بين أيدي السلطات المكلفة بالتحريات القضائية المعطيات التي تم حفظها، ووفقا 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 18 مكرر من قانون العقوبات فإن: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي: 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.

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

2- الالتزام بتصفية المواقع وبيان نوعها:

نصت المادة 12 من القانون 04/09 المتضمن الوقاية من 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 وإخبار 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 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 التي يمكن من خلالها وبطلب من السلطة القضائية وقف هذه المضامين المجرمة، ونحن نرى أن هذا التقصير يُخلُّ فعلا بحقوق الأشخاص سواء الطبيعيين أو المعنويين في حالة انتهاك حقوقهم عبر الانترنت، فكان لزاما 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 6-1-3 من 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 إلاّ 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 فورا لسحب المعلومات أو بجعل الوصول إليها مستحيلا[1].

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

وبموجب المادة 6-5 من القانون 2004/06/21 من أجل ال
الإيواء لا يمكن أن تقوم إلاّ إذا لم يقم وبسرعة بعد إعلامه بسحب م
أن يقيم الدليل على سرعة سحبه للمحتوى المجرم.

أما بالنسبة للاجتهاد القضائي الفرنسي في مسألة قيام المسؤولية الجزائية لمقدمي خدمة الإيواء الذين لهم نشاط تخزين دائم ومستمر للمعلومات (المادة 2/د/2 من 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 سُمِح 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 06 جوان 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 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

---

[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 CHARPENEL المرجع السابق صفحة 35.

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

الأساليب التقنية، وكذلك وجوب أن توضع مباشرة آليات المراقبة ا
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 تُكَوِن جرائم في القانون العام.[1]

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.

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

خاتمة

إن إصدار المشرع الجزائري لقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قام بإرساء قواعد إجرائية جديدة تضمن من الإجرام وبما يتوافق وخصائصه، فقد شملت مواده الكثير من الآليات المستحدثة:

1- بنصه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وإن لم يتم تنصيبها إلى حد الساعة،

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

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 وإدخالها 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 دورا 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 بتكنولوجيا في القانون 04/09 أمر مهم يجب على السلطات المعنية الإسراع 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 04 من 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.

4- 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.

- تمت بعون من الله -

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.

- المحامي إلياس أبو عيد، نظرية الاختصاص في أصول المحاكمات المدنية والجزائية، منشورات زين الحقوقية، لبنان، 2004.

- حاتم حسن بكار، أصول الإجراءات الجنائية وفق أحدث التعديلات التشريعية والاجتهادات الفقهية والقضائية، منشأة المعارف بالإسكندرية، مصر، 2007.

- د. سليمان عبد المنعم، أصول الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الاسكندرية، مصر، 2008.

- د. طارق سرور: جرائم النشر والإعلام، الكتاب الأول الأحكام الموضوعية، دار النهضة العربية القاهرة، الطبعة الثانية، 2008.

- د. طالبي حليمة: محاضرات في مقياس قانون الإجراءات الجزائية المقدمة لطلاب السنة أولى ماجستير، دفعة 2009- 2010 كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة ورقلة.

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

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

- د. محمد حماد الهيثي، التحقيق الجنائي والأدلة الجرمية، دار المناهج للنشر والتوزيع، عمان الأردن، طبعة أولى، 2010.

- 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 الأو
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، الاسكندرية، 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 الالكـ
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، الاسكندرية، 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-administrations-

bonne paris I, disponible sur: www.univ-
ni_ Version_ … .

océdure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité en droit européen, mémoire de master droit de l'Internet-Administration-Entreprises, 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-V5.1-pdf.

- 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