

الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها .

بقلم الأستاذة : شيخي عائشة
الدكتور: عياشي بوزيان
جامعة سعيدة.

مقدمة :

يشهد العالم في العقود الأخير ثورة في مجال المعلوماتية ، إذ أضحت بذلك السبيل الأمثل نحو الرقي الحضاري والاقتصادي، ويعد الوصول إلى المعلومات رهانا كبيرا للإنسان نظرا لارتباطها بمختلف مجالات النشاط الإنساني وجوانب الحياة المعاصرة ، ذلك أن توفير المعلومات وحسن استغلالها من المقومات الضرورية لدفع عجلة تقدم الأمم وازدهارها وصار وجودها دعامة أساسية لجهود التنمية والرقي المعرفي .

وعلى الرغم من المزايا الهائلة التي تحققت وتحقق في مجال تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة (1) ، فإن هذه الثورة التكنولوجية المتنامية رافقتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها ، تجلّت في تفشي طائفة من الظواهر الإجرامية المستحدثة ، ألا وهي ظاهرة الجرائم المعلوماتية ، التي لم تعد تقتصر على

إقليم دولة واحدة ، بل تجاوزت حدود الدول ، وهي جرائم مبتكرة ومستحدثة تمثل إحدى صور الذكاء الإجرامي ، مما صعب من مهمة إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية ، كما كشفت عن عدم قدرة قواعد الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة ، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أو على صعيد الملاحقة الجنائية الدولية .

ولما كانت الجرائم المعلوماتية ظاهرة حديثة لارتباطها بتكنولوجيا الإعلام والاتصال فقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا من أجل الوصول إلى تعريف مناسب يتلائم مع طبيعتها لكن دون جدوى حتى قيل إن الجريمة المعلوماتية تقاوم التعريف (2) لذا اختلفت التعاريف التي تتناول هذه الظاهرة الإجرامية غير أنه ومع ذلك فإن كافة المحاولات لإيجاد تعريف جامع جاءت قاصرة على الإحاطة بكافة أوجه هذه الظاهرة، وفي المسعى ذاته تبنى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين تعريفا جامعا للجريمة المعلوماتية بأنها كجريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية.(3)

مما يقتضي بغية مجابقتها تطوير البنية التشريعية الجنائية الوطنية بذلك
تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب
وأبعاد تلك التقنيات الجديدة ، بما يضمن في الأحوال كافة احترام مبدأ
قانونية الجرائم والعقوبات من ناحية ، ومبدأ الشرعية الإجرائية من ناحية
أخرى ، وتتكامل فيه مع الأهداف التي تقرها المعاهدات الدولية في هذا
الشأن.

والواقع أن المشرع الجزائري على غرار باقي التشريعات العربية والغربية
وضع عديد القواعد الخاصة بالوقاية من الجرائم المتصلة بالجرائم المعلوماتية
ومكافحتها وتجلى ذلك من خلال ما احتواه التشريع العقابي وكذا القواعد
الإجرائية التي تتبع في مجال الكشف عنها هذا فضلا عن إصدار المشرع
الجزائري للقانون 09-04 المؤرخ في 05/09/2009 المتضمن للقواعد
الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
ومكافحتها وكذا استحدثه بموجب المرسوم الرئاسي 261/15 المؤرخ في
08/10/2015 للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات
الإعلام والاتصال ومكافحتها.

واستنادا لما تقدم فإن الغاية من هذه الورقة البحثية تبين مدى كفاية
النصوص والآليات التي وضعها المشرع الجزائري للوقاية من الجرائم المتصلة
بتكنولوجيا الإعلام والاتصال ومكافحتها؟

وللإجابة عن هذه الإشكالية عاجلنا هذا الموضوع في مبحثين نتطرق في المبحث الأول إلى صور الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والأساليب الإجرائية للكشف عنها. ونخصص الحديث في المبحث عن دور الهئية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وكذا دور التعاون الدولي في مكافحتها.

المبحث الأول : صور الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والأساليب الإجرائية للكشف عنها.

لعل ما يجب الإشارة إليه في البداية أن صور الجرائم التي نحن بصدد الحديث عنها هي "الجرائم المعلوماتية" وقد اختلفت المصطلحات الدالة عليها، فالبعض يطلق عليها جريمة "الغش المعلوماتي" والآخر يسميها "الجريمة المعلوماتية"، و ثالث يصفها بظاهرة "الاختلاس المعلوماتي"، وغيرهم يرمز لها ب "جنح المعلوماتية" مما يصعب معه التقرير بإمكان إيجاد تعريف موحد باعتبار أن هذه الظاهرة حديثة نسبيا مما يخشى معه حصرها في نطاق محدد(4).

فالاصطلاح احتيال أو غش الكمبيوتر وغيره من التسميات أطلقت على أفعال من بين أفعال جرائم الكمبيوتر وصورها وليس على الظاهرة برمتها. كما أن تعبير جرائم التقنية العالية أو جرائم تقنية المعلومات أو نحوه

تعبيرات - تحديدا في الفترة التي أطلقت فيها - كان يقصد من التعبير جرائم الكمبيوتر، حتى قبل اتساع استخدام الانترنت .

وتظل تعبيرات واسعة لدلالة تحيط بأكثر مما تحتوي ظاهرة جرائم الكمبيوتر والانترنت والأمر نفسه يقال بشأن اصطلاح جرائم المعلوماتية والذي وفقا لدلالة الكلمة بالفرنسية لمصطلح Informatique بمعناها المعالجة الآلية للبيانات (5).

وبالرجوع لأحكام التشريع العقابي الجزائري نجد أن هذا الأخير قد خصص لصور التجريم هاته أحكاما في الفصل السابع مكرر من قانون العقوبات تحت تسمية المساس بأنظمة المعالجة الآلية للمعطيات ففي ما تتجلى هذه الصور وما هي القواعد الإجرائية التي خصصها بها المشرع بغية إثباتها و الكشف عنها.

المطلب الأول : صور الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

والجزء المقرر لها:

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا على أنه تعبير متطور يخضع للتطورات السريعة و المتلاحقة في مجال فن الحاسبات الآلية⁶

ولذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه كل من الفقه و القضاء. فالاتفاقية الدولية للإجرام المعلوماتي قدمت تعريف للنظام المعلوماتي في مادتها الثانية على النحو التالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnecté ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement ou tonatisé de données. (7)

أما الفقه الفرنسي فقد عرفه كما يلي: بأنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمصطلحات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية .

بناء على التعريفات السابقة, نخلص إلى القول أن تعريف نظام المعالجة الآلية للمعطيات يعتمد على عنصرين:

- العنصر الأول: مركب يتكون من عناصر مادة ومعنوية مختلفة ترتبط بينهما نتيجة علاقات توحيدهما نحو تحقيق هدف محدد.

- العنصر الثاني: ضرورة خضوع النظام لحماية فنية.

وفي هذا الشأن أورد المشرع الجزائري في أحكام المواد 394 مكرر إلى المادة 394 مكرر 7 من قانون العقوبات (8) نماذج الأفعال المجرمة ،ومن استقراء هذه النصوص القانونية يتضح أن الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات تأخذ صورتين أساسيتين هما:

الفرع الأول: صور جرائم أنظمة المعالجة الآلية للمعطيات

أولا: الدخول في منظومة معلوماتية : ويشمل هذا الفعل المادي المجرم شكلين هما:

1-الدخول :يتسع هذا الوصف لينصرف إلى كل فنيات الدخول الإحتيالي في منظومة محمية كانت أو غير محمية ، كما يشمل استعمال من لا حق له في ذلك .

2-البقاء :يشمل هذا الفعل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم دفع أتاوة وتقوم الجريمة سواء حصل الدخول

مباشرة على حاسوب أو حصل عن بعد كما يجرم البقاء حتى ولو حصل الدخول بصفة عرضية .

ثانيا :المساس بمنظومة معلوماتية :تشير أحكام المادة 394مكرر1في هذا الصدد على أنه (كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها وعلى ذلك يأخذ الفعل المحرم صورتين:

- إدخال معطيات في نظام المعالجة الآلية غريبة عنه .
- تخريب المعطيات التي يتضمنها نظام المعالجة الآلية .(9)

وتهدف التشريعات الجزائية على اختلافها من وراء تجريم الصورتين إلى حماية المعطيات أو المعلومات ذاتها ،لذا يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الانترنت، فهم يسعون لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة تلك المتعلقة بالأعمال التجارية الرقمية .لذلك يمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ، وفي هذا الشأن يرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية .(10)

ومن التطبيقات القضائية لهذه الجريمة قضي في فرنسا بأنه يقع تحت طائلة نص المادة 323 من قانون العقوبات ويقابلها في القانون الجزائري نص المادة 394 مكرر 1 من قانون العقوبات تعتمد إدخال فيروس المعلوماتية في برنامج الغير وكذا الإمتناع عن إخبار الأخير بإدخال مثل هذا الفيروس ولو حصل ذلك بصفة عرضية كما يقع تحت طائلة النص السالف الذكر تعد تعديل أو إزالة المعطيات التي يتضمنها نظام المعالجة الآلية للمعطيات الآلية، والحكمة من وراء تجريم هذا الأفعال توفير حماية للعتاد الضروري لتشغيل المنظومة.

إن هذه الأحكام الجزائية التي أقرها التشريع العقابي الجزائري تم تعزيزها بصور القانون 09-04 الذي أشار في أحكام المادة الثانية منه إلى أن جرائم المساس بأنظمة المعالجة الآلية للمعطيات هي تلك المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الالكترونية (1)، ويستفاد من ظاهر النص أن تجريم هذه الأفعال قد يرد في قانون العقوبات كما قد يرد في النصوص الجزائية المكملة لقانون العقوبات، وغاية المشرع في ذلك في تقديرنا هو وضع قواعد تتلائم وطبيعة الجريمة وحدثاتها بإمكانها الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

الفرع الثاني: الجزاء عن جرائم أنظمة المعالجة الآلية للمعطيات.

يتضح من استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يفصح عن الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، لذا كانت لكل جريمة العقوبة المقررة لها غير أن ما يجب الإشارة إليه أن هذه الجرائم كلها تشترك في مجموعة من القواعد .

أولاً: العقوبة المقررة لكل جريمة :

أ- الدخول إلى منظومة معلوماتية أو البقاء فيها : تعاقب أحكام المادة 394 مكرر ق ع على هذا الفعل بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000 دج إلى 200.000 دج وتطبق العقوبات ذاتها على المحاولة وتضاعف العقوبات إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذا نتج عن تلك الأفعال إفساد نظام عمل المنظومة تكون العقوبة من 06 أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.000 دج .

ب- المساس بمنظومة معلوماتية: العقوبة المقررة للاعتداء العمدي في أحكام المادة 394 مكرر 1 على المعطيات الموجودة داخل المنظومة المعلوماتية هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 2.000.000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم

الماسة بالأنظمة المعلوماتية، فالعقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج .

ثانيا :القواعد المشتركة بين كل جرائم أنظمة المعالجة الآلية للمعطيات :تتشرك الجرائم المشار إليها أعلاه في مجموعة من القواعد تتمثل في مايلي:

1-مضاعفة لعقوبة :جاء في نص المادة 394مكرر 3 أن العقوبات المقررة لهذه الجرائم تضاعف وذلك متى كان من شأنها أن تمس الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

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

3-المصادرة :ورد النص في أحكام المادة 394مكرر6على أنه مع الإحتفاظ بحقوق الغير حسن النية فإنه يحكم بمصادرة الأجهزة والبرامج

والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها.

4-جزاء الشخص المعنوي: المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي الغرامة التي تساوي خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي .

5-الشروع: نصت المادة 394 مكرر 7 قانون العقوبات "يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القانون هي ذاتها المقررة للجنحة"،ويبدو من خلال هذا النص أن إرادة المشرع هي توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية.(12)

المطلب الثاني: الأساليب الإجرائية للكشف للجرائم المتصلة بتكنولوجيا

الإعلام والاتصال.

يقف الدارس لعملية التفتيش بخصوص الجرائم الإلكترونية على حقيقة مفادها أن لهذه الأخيرة ذات طبيعة خاصة تختلف عن التفتيش التقليدي للأشخاص والمنازل ، إلا أنه يخضع في إجراءاته للضوابط التي حددها قانون

الإجراءات الجزائية وما يستلزمه من شروط موضوعية كوقوع الجريمة واتهام شخص أو أشخاص معينين بارتكاب جريمة ، وأن تكون هناك دلائل أو قرائن على ما يفيد في كشف الحقيقة في أجهزة الحاسب الآلي والإنترنت خاصة بالمتهم أو غيره من الأشخاص ، وإذا ما توافرت تلك الشروط ، فإنه يجوز لسلطة التحقيق تفتيش جهاز الحاسب الآلي وملحقاته المكونة له المادية والمعنوية ، وذلك من أجل الحصول على دلائل بشأن الجريمة المرتكبة ، غير أن ما يجب الإشارة إليه أنه في هذا الشأن قد ثار جدلٌ فقهيٌ بين فقهاء القانون الجنائي ، حول مدى إمكانية تفتيش وضبط البيانات المخزنة أو المعالجة إلكترونياً بصورها وأشكالها المختلفة كالأقراص والأشرطة المغنطة بما في ذلك ذاكرة جهاز الحاسب الآلي وانقسموا في ذلك لاتجاهين :

الاتجاه الأول : يذهب جانب من الفقه الجنائي إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة للإثبات المادي ، يهدف لضبط أدلة مادية تتعلق بالجريمة وتفيد في كشف الحقيقة ، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي ، ويمثل هذا الرأي جانب من الفقه الفرنسي الذي يرى أن التفتيش أو الإشارات الإلكترونية المغنطة لا تعد من قبيل الأشياء المادية المحسوسة التي يمكن تفتيشها وضبطها.(13)

الاتجاه الثاني : يعتقد أنصار هذا الإتجاه أن المعلومات التي لا تعد شيئا ماديا وإنما ذات طبيعة معنوية ، الأصل ومجرد ذبذبات ونبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية ، إلا أنها قابلة لتخزينها في أوعية ووسائط مادية كالأقراص والأشرطة الممغنطة ، وبالتالي فهي ليست شيئا معنويا كالحقوق والآراء والأفكار ، بل هي أشياء مادية محسوسة لها وجود ملموس في العالم الخارجي ، ومن ثم يصح أن ينصب عليها التفتيش والضبط⁽¹⁴⁾.

ونعتقد أن التفتيش يظل محتفظا بصحته طالما أمكن من خلاله الوقوف على المعلومات والبيانات والحوار وكلمات السر وكان ثمة امكانية لتصفحها وتحليلها لاستظهار الدليل المعلوماتي منها على الرغم من وجود الحاسب الآلي المراد تفتيشه في منزل غير المتهم .

وفي هذا الصدد نجد أن المشرع الجزائري سار على مسار التشريعات الإجرائية الجزائية في العالم الغربي والعربي التي أقرت عديد القواعد التي جابهت بها هذه الجرائم، لذلك وضعت أحكام القانون 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا قانون الإجراءات الجزائية الجزائري مجموعة من الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

وفي سياق حرص المشرع على إقرار قواعد مرنة تتلائم مع ما تقتضيه ضرورة الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجده في هذا الشأن خرج عن القاعدة العامة في مجال قواعد الاختصاص التي تحكم عمل الهيئات القضائية وكذا عمل ضباط الشرطة القضائية ليمدد هذا الاختصاص إلى كامل التراب الوطني.

الفرع الأول: تمديد الاختصاص .

على خلاف القواعد العامة في مجال الاختصاص المحلي بشأن الجرائم الوارد النص عليها في التشريع العقابي يلاحظ أن المشرع قد خص بعض الجرائم يصفها البعض بالإجرام الخطير بإجراءات خاصة ومنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ،لذا نجد أن قواعد قانون الإجراءات الجزائية بموجب التعديل الذي أدخل على أحكام المادة 16 من ذات القانون بتاريخ 20/12/2006 ،جعل من اختصاص ضباط الشرطة القضائية يمتد إلى كامل التراب الوطني ،كما جعل أيضا من اختصاص وكيل الجمهورية بموجب أحكام نص المادة 37 من قانون الإجراءات الجزائية يمتد إلى اختصاص محاكم أخرى كلما تعلق بجرائم محددة على سبيل الحصر ومنها الجرائم التي نتناولها بهذا البحث.

وفي ذات السياق ورد النص في أحكام نص المادة 40 من قانون الإجراءات الجزائية على جواز تمديد الاختصاص لقاضي التحقيق إلى دائرة

اختصاص محاكم أخرى. عن طريق التنظيم في جرائم وردت على سبيل الحصر شملت أيضا الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.(15)

تناول أيضا قانون الإجراءات الجزائية الجزائري موضوع هذه الجرائم الافتراضية بإحداثه لمحاكم جزائية ذات الاختصاص الموسع، والتي أجاز لها تمديد اختصاصها في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهو ما أورده المشرع في نص المادة 329، والغاية التي يسعى إليها المشرع من وراء ذلك هو دعم وسائل مكافحتها . (16)

الفرع الثاني: تفتيش المنظومات المعلوماتية .

إذا كانت أحكام المادة 47 في فقرتها الثالثة من قانون الإجراءات الجزائية أتاحت لأجهزة المتابعة إمكانية إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص عندما يتعلق الجرائم وردت على سبيل الحصر ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك عبر كامل التراب الوطني(17) كما سبقت الإشارة إليه، فإن أحكام القانون 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جاءت بقواعد غير مألوفة في قانون الإجراءات الجزائية، ذلك أنها أجازت للسلطات القضائية وكذا لضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن

بعد إلى منظومة معلوماتية أو جزء منها وكذا إلى المعطيات المعلوماتية المخزنة فيها، وفي هذه الحالة إذا كانت هناك ما يفيد 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 إلى جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك، كما أجازت أيضاً لها إلى أية منظومة تخزين معلوماتية .

وما يمكن الإشارة إليه في هذا الصدد أن السلطات المكلفة بالتفتيش يمكنها تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

ولما كانت إجراءات التفتيش قد تكون ذات نتائج إيجابية كما هو الحال في الجرائم التقليدية، فإن النتيجة نفسها قد تتحقق في هذا النوع من الجرائم مما يتعين معه - إعمالاً لأحكام المادة السادسة وما يليها من القانون 04-09 - على السلطات التي تباشر التفتيش في منظومة معلوماتية مخزنة عندما تكتشف معطيات مفيدة للكشف عن الجرائم ومرتكيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقاً للقواعد المقررة في قانون الإجراءات الجزائية.

المبحث الثاني : جرائم تكنولوجيا الإعلام والاتصال التي تمس الجانب

الاقتصادي :

لقد أدت ثورة تكنولوجيا المعلومات إلى تنامي ظاهرة الجريمة الاقتصادية، حتى أصبح العالم اليوم يواجه إجراما اقتصاديا قد تسلح بأحدث وسائل تكنولوجيا الإعلام و الاتصال، وأصبح قادرا على تنفيذ أهدافه مع صعوبة إقتفاء أثره وملاحقته ، وبالتالي فحينما نتحدث عن الجريمة المعلوماتية الاقتصادية فإننا نقصد بها عالم الإقتصاد كبيئة خاصة لظهور ونمو الجريمة المعلوماتية أو بعبارة أخرى الجرائم المعلوماتية التي تتم في مجالات الإقتصاد و المال و الأعمال(18) ،وتعد الجريمة المعلوماتية الاقتصادية من أحدث و أخطر الجرائم الاقتصادية التي تمس الأفراد والمؤسسات إذ أصبح الفرد ينجز تعاملاته ويدير أعماله وبحوثه ويتواصل مع العالم الخارجي بواسطة استخدام الانترنت وبالتالي أصبح عرضة لذا النوع من الجرائم، وكذلك المؤسسات الاقتصادية أيضا، إذ أصبحت تدار الكترونيا وتتواجد على الشبكة الالكترونية لفتح قنوات تواصل جديدة مع الناس لتكميل جهودها والإعلان عن آخر أخبارها وتسهيل التواصل معها والتفاعل مع ما تقدمه من خدمات وعروض كل هذا دون الحاجة إلى الذهاب إليها ,فقط عن طريق الشبكة الإلكترونية , بهدف استقطاب شريحة أكبر من الناس و زيادة أرباحها .

المطلب الأول : الأشكال الاقتصادية لجرائم تكنولوجيا الإعلام و

الاتصال

تأخذ الأشكال الاقتصادية لجرائم تكنولوجيا الإعلام والاتصال مجموعة هامة من الصور يمكن أن نوردتها في مايلي:

1-التعدي على الأنظمة المعلوماتية : وهي تتضمن جرائم الولوج غير المشروع للأنظمة المعلوماتية من خلال الدخول كسرقة كلمات المرور للأنظمة أو اختراق هذه الأنظمة وزرع الفيروسات بهدف التجسس وسرقة المعلومات أو تخريب هذه الأنظمة كما تتضمن إعاقة الوصول إلى هذه الأنظمة المعلوماتية من طرف مستخدميها ، وذلك كاختراق موقع الكتروني لمؤسسة ما على الانترنت ومنع وصول مدير النظام إليه و استعادته ، أو اختراق منظومة إدارة مصرف ومنع الوصول إليها و بالتالي إيقاف العمل بها وهذا ما يجعل هذا الأخير يتحمل تكاليف وخسائر كبيرة

2-إساءة استعمال الأجهزة أو البرامج المعلوماتية: وهي تتضمن الجرائم المتعلقة بتقديم أو نشر أو بيع التجهيزات و البرمجيات بهدف اختراق أو التعدي على الأنظمة المعلوماتية كتصميم أو بيع أو الترويج للفيروسات وبرمجيات إختراق و تغيير كلمة السر للشبكات المعلوماتية و التطبيقات كما يمكن أن يتعلق هذا النوع من الجرائم بجرائم تشفير المعلومات حيث تعتمد بعض الجهات إلى توزيع أو نشر أو بيع أو تسويق أو تصدير أو استيراد

وسائل تشفير دون الحصول على ترخيص من الجهات الرسمية المختصة في الدولة(18)

3-تخريب المعلومات و إساءة استخدامها :يتم تخريب المعلومات عن طريق محو الملفات أو تدمير الوسائط التي تحتويها ، بينما يتم إساءة استخدام المعلومات عن طريق الأذى الذي يتم تحقيقه باستخدام هذه المعلومات وذلك مثل عدم تمكين المستفيد من الوصول إليها وهذا النوع من الجرائم يمس خاصة المؤسسات .(19)

4-التزيف حيث يتم تزيف الوثائق :تأخذ هذه الصورة عدة أشكال إجرامية منها تزيف الشبكات المصرفية و الأسهم والسندات .

5-تزوير البيانات و تزوير العلامات التجارية : يعتبر تزوير البيانات من أكثر الجرائم انتشارا ، وتتم بإدخال بيانات خاطئة أو متلاعب فيها إلى قواعد البيانات أو بتعديل البيانات الموجودة عمدا بهدف إرتكاب الجريمة ، أما فيما يخص تزوير العلامات التجارية فبعض المؤسسات المنتجة لشرائح المعالجات المركزية يتم تزوير علاماتها التجارية على شرائح ذات أداء منخفض ليتم بيعها على أنها شرائح ذات أداء أعلى وبأسعار مرتفعة مما يلحق أضرار بمصالح المؤسسة التي يتم تزوير علاماتها ، ويكون الدافع من ارتكاب هذه الجريمة السعي وراء الربح و البحث عن التفوق و المنافسة

6- جرائم السطو على أرقام البطاقات الائتمانية : مفاد هذه الصورة أنه تتم سرقة أرقام بطاقات الائتمان ثم القيام بإعادة بيعها مما يتسبب في إلحاق أضرار بالمستفيد و بالمؤسسات التي تصدر هذه البطاقات.(20)

7- جرائم السطو على أموال البنوك و المؤسسات الاقتصادية: لقد ساهم القطاع المصرفي في انتشار الخدمات الالكترونية بل وكان سباقا في تقديم الخدمات المالية و المصرفية عبر تكنولوجيات الإعلام و الاتصال ومن بين ذلك خدمة تحويل الأموال و خدمات التحويل الالكتروني ، على غرار استخدام بطاقات الائتمان المصرفية وذلك لتأمين وصول العملاء إلى الحسابات المصرفية عن طريق قنوات متعددة كالصراف الآلي الخ ، وهذا ما أدى إلى ظهور العديد من المتسللين للسطو على الأموال الإلكترونية وإجراء التحويلات المالية بطرق غير مشروعة حتى أصبحت البنوك والمصارف هدف لمحتربي شبكات الانترنت الذين يتلاعبون في كشف الحسابات الخاصة بالعملاء ويقومون بنقل الأرصدة من حساب لآخر وبالتالي فهم يقومون بسرقة أرقام الحسابات بصورة غير مشروعة بهدف إجراء عمليات التحويل الإلكتروني للأموال أو اختراق الأنظمة المصرفية وسحب أو تحويل الأموال بين الحسابات وتسمى هذه الجرائم أيضا بالجرائم المعلوماتية المالية أي التي تمس المؤسسات المالية

كما تتضمن جرائم السطو على الأموال جرائم سرقة واختلاس الأموال باستخدام الوسائل المعلوماتية وجرائم التسويق غير المرغوب فيه مثل

إنشاء مواقع تجارة إلكترونية أو خدمات تواصل على الإنترنت مدفوعة القيمة وهذا بهدف سرقة أموال الزبائن دون تقديم الخدمات المطلوبة أي بمعنى بيع السلع أو الخدمات الوهمية ، بالإضافة إلى هذا فهي تشمل على الجرائم المتعلقة بالترويج غير المشروع لأسعار العملات أو أسعار الأسهم وذلك بهدف التأثير في أسعار الصرف وسوق الأسهم و بالتالي التأثير في الاقتصاد .

8- جرائم النقود الإلكترونية : وتتمثل في إنشاء نقود إلكترونية وطرحها للتداول دون الحصول على التراخيص اللازمة مثل إنشاء حسابات مصرفية و إجراء عمليات بيع وشراء باستخدام هذه النقود وذلك دون الحصول على التراخيص اللازمة من المصرف المركزي للدولة .(21)

وعموما يمكن القول أن الجرائم المعلوماتية الاقتصادية و التي تطل الجانِب المالي بصفة خاصة هي كالتالي : سرقة أو نسخ البطاقات المصرفية ، سرقة أرقام الحسابات المصرفية عن طريق التجسس أو من خلال مواقع وهمية ، اختراق منظومة المصرف وإجراء التحويلات المالية ، الترويج والتسويق غير المشروع لأسعار العملات وأسعار سوق الأسهم المالية بهدف التلاعب بها ، القيام بأعمال التجارة الإلكترونية غير المرخصة ، الحصول على الأموال مقابل سلع وخدمات وهمية (دون تقديم الخدمات و المنتجات) ، تزوير العلامات التجارية ، التعدي على الأنظمة المعلوماتية للمؤسسات

الذي يؤدي إلى تعطيلها أو توقيف عملها ، غسيل الأموال عبر الأنترنت
.....الخ

المطلب الثاني: الأثر الاقتصادي للجرائم المعلوماتية :

لا توجد آليات واضحة لقياس الآثار الاقتصادية الناجمة عن الجرائم المعلوماتية ، رغم المحاولات العديدة من طرف المؤسسات العامة و الخاصة لقياس الآثار المباشرة وغير المباشرة حيث أنه ومن الصعب قياس الضرر الناجم عن استخدام البرمجيات الخبيثة على الأفراد و المؤسسات إلا أنه يمكن أن تكون الخسائر الاقتصادية للجرائم المعلوماتية مرتبطة بالضرر الاقتصادي المباشر المرتبط بقيمة التجهيزات و البرمجيات موضوع الجريمة ، أو بالأثر الاقتصادي الناجم عن توقف هذه المؤسسات عن العمل فمثلا اختراق و تعطيل العمل بمنظومة شركة طيران بالرغم من عدم وجود أثر مالي مباشر إلا أن توقف المنظومة عن العمل يؤدي إلى خسائر تقدر بآلاف الدولارات للساعة الواحدة ،ومثل ذلك تعطيل منظومة سوق الأوراق المالية لمدة دقائق قد ينجم عنه خسائر مالية تقدر بعشرات آلاف الدولارات ، ومثله أيضا في حالة القيام بسرقة الأموال الإلكترونية و استخدام تكنولوجيات الإعلام و الاتصال للإستيلاء على أموال المؤسسات و الأفراد (22).

إن هذا النوع من الجرائم التي باتت تطل المؤسسات و الأفراد تؤدي إلى إحداث ضرر يسبب تعطيل وخسائر, وهنالك الملايين من ضحايا الاحتيال وسرقة بطاقات الائتمان والابتزاز , كما يوجد الكثير من الشركات والمؤسسات التي انهارت أو تعرضت لنكسة مالية أو تعطلت بسبب هذه الجرائم , وحتى المؤسسات الحكومية تتكبد سنويا الملايين لإعادة تشغيل و إصلاح ما تعطل من الآلات والمصالح , إذ أنه وفي دراسة أجرتها شركة "نورتن" الرائدة في تطوير الحلول البرمجية الأمنية أن ثلثي مستخدمي الانترنت حول العالم تعرضوا لجرمة إلكترونية على الأقل مرة واحدة وقد تمثلت في هجمات فيروسية و تجسسية واحتيالية لسرقة بطاقات الائتمان وسرقة الهوية أو البيانات المصرفية والشخصية الحساسة. و بشكل دقيق لا يوجد حتى الآن دراسات إحصائية شاملة عن ظاهرة الجرائم الإلكترونية خاصة الماسة بالجانب الاقتصادي , كل ما يتوفر ليس أكثر من تقديرات تتباين دقتها حسب موضوعية وقدرة الجهات القائمة على إنجاز هذا النوع من الدراسات . أيضا الأرقام الموجودة في هذه الدراسات لا تعكس واقع الظاهرة, فقط تقدم صور عامة عنها لكن في الواقع فإن حجم الجرائم الإلكترونية ونطاقها وحجم الخسائر أكثر مما تقدمه هذه الدراسات,و السبب في ذلك يعود إلى أن أغلب المؤسسات تحاول إخفاء وكتم خسائرها الناتجة من تعرضها لهذا النوع من الجرائم حتى لا تفقد ثقة زبائنهم ولا تثير الشكوك في فعالية نظام الأمن الخاص بها .

المبحث الثالث : دور الهيئة الوطنية و التعاون الدولي في مكافحة الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال .

إن إنشاء هذه الهيئة نص عليه القانون رقم 09-04 المؤرخ في 5 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لذلك تُعنى هذه الهيئة بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، وضمان مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المتخصص .

ومن بين الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى تُرتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وبخصوص التعاون والمساعدة القضائية الدولية، أشار القانون إلى أن "المحاكم الجزائية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا، وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني. وفي تقديرنا أن إنشاء هذه الآلية الهامة يمكن من تزويد جهاز القضاء بالمزيد من الموارد البشرية المؤهلة،

ومراجعة الترسنة التشريعية، لا سيما في ذلك المجال الجزائي، من أجل تحسين حماية حقوق وحرية المواطنين.

المطلب الأول: طبيعة ومهام الهيئة الوطنية للوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال.

أشارت أحكام المادة 13 من القانون 04-09 على أن مسألة تفعيل هذا القانون يحتاج إلى إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وقد تجسد ذلك بصدور المرسوم الرئاسي رقم 261-15 المؤرخ في 08 أكتوبر 2015 الذي جاء ليحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، كما بين بوضوح الطبيعة القانونية للهيئة وكذا المهام التي أنيطت بها حتى يتسنى لها تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومد يد العون للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، وضمان مراقبة الاتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المتخصص.

الفرع الأول: الطبيعة القانونية للهيئة الوطنية للوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال.

إن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتي ورد النص على إنشاءها بموجب القانون 09-04 تعد سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل وفقا لما جاء في أحكام المادة الثانية من المرسوم الرئاسي 15-261 المؤرخ في 2015/10/08 وتضم الهيئة لجنة مديرة ومجموعة من المديريات ذات طابع تقني، وتعمل اللجنة المديرة على توجيه عمل الهيئة وإشراف عليه ومراقبته ويرأس هذه الأخيرة وزير العدل، وتضم وزيري الداخلية والبريد وتكنولوجيا الإعلام وكذا مسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعيّنهما المجلس الأعلى للقضاء.

وفضلا على دور هذه اللجنة في توجيه عمل الهيئة والإشراف عليه فإنها تتولى دراسة كل مسألة تخضع لمجال اختصاص الهيئة لا سيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة الرابعة من القانون 09-04 السالف الذكر، كما تتولى اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. (23)

الفرع الثاني : مهام الهيئة الوطنية للوقاية من الجرائم المتصلة

بتكنولوجيات الإعلام والاتصال.

إن خصوصية هذا النوع من الجرائم تتجلى في كون مرتكبها شخص يتميز بالذكاء والدهاء وذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، على خلاف مرتكبي الجرائم التقليدية ، لذلك كان من مهام الهيئة أن تتصدى لطائفة معينة من المجرمين من خلال تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. والقيام بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأنها ، وضمان مراقبة الاتصالات الإلكترونية أيضا قصد الكشف عن طائفة من الإجرام الخطير الذي من شأنه المساس بكيان الدولة وأمنها.

ومن المهام الملقاة على عاتق الهيئة في هذا الشأن أيضا تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية، وتعمل في ذات الوقت على تطوير مجال تعاونها مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، وهي في سبيل أداء مهامها مؤهلة بأن تطلب من أي جهاز أو مؤسسة أو مصلحة كل وثيقة أو معلومة ضرورية لإنجاز المهام المسندة إليها.

ولما كانت هذه الجرائم تقتربها طائفة معينة من المجرمين لهم حظ وافر من العلم والذكاء الأمر الذي يجعل كشف الجريمة وتحديد مرتكبها أمراً في

غاية الصعوبة ، فإن الهيئة يقع على عاتقها المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية ما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار .(24)

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

غني عن البيان أن هذا النوع من الجرائم ذو بعد دولي ، وبالتالي فهي عابرة للحدود ، ذلك أنها قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية هذه الأخيرة التي لا تعتد بسيادة الدولة التقليدية ويتحقق بذلك الفعل الإجرامي على الرغم من التباعد الجغرافي بين الجاني والجني عليه ، هذا النوع من الجرائم يشكل إذن صورة من صور العولمة على اعتبار أنها لا تعترف بالحدود القائمة بين الدول سواء الجغرافية أو السياسية هذا ما أدى إلى تصنيفها على أنها من قبيل الجرائم الدولية أي ذات البعد الدولي ذلك أن قوعها يمتد خارج الإقليم الذي قد ترتكب فيه مما يعني إمكانية خضوعها لأكثر من قانون جنائي ، وهو ما يثير تحديات ومشاكل قانونية وإدارية وفقهية منها فكرة المجرم المعلوماتي الذي بمقدوره استخدام وسائل التقنية الحديثة أن يتوصل إلى أنظمة الحاسب الآلي في أي مكان في العالم ، وكذلك فكرة المال المعلوماتي (غير المادي) المتمثل في

البرامج والمعلومات والبيانات أيا كان موضوعها , كل ذلك أدى إلى تعدد الجهود المبذولة سواء على الصعيد الدولي أو المستوى الإقليمي.

الفرع الأول : - تفعيل التعاون الدولي ودور المعاهدات .

إن المخاطر التي تتعرض لها البرامج والنظم المعلوماتية على حد سواء باتت تهدد مختلف الأنشطة والقطاعات الأمر الذي جعل المجتمع الدولي يدرك أهمية التعاون الدولي تأسيسا على أنه أمر محتّم " لا غنى عنه لتجاوز تحديات الجرائم المعلوماتية ، ما دفع الكثير من الدول إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه جرائم الكمبيوتر (25) في عام 1983 أجرت منظمة التعاون و الإنماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية و تكيف نصوصها لمواجهة تحديات الجرائم الالكترونية وسوء استخدامه ، و في عام 1985 أصدرت هذه المنظمة تقريراً تضمن قائمة بالحد الأدنى ورد فيها تعداد للأفعال التي تشكل سوء استخدام الحاسب الآلي التي يجب علي الدول أن تجرمها و تفرض لها عقوبات في قوانينها و من أمثلة هذه الأفعال : الغش أو التزوير في الحاسب الآلي ، تغيير برامج الحاسب الآلي أو المعلومات المخزنة فيه، سرقة الأسرار المدعمة في قواعد الحاسب الآلي ؛ تفعيل التعاون الدولي في مجال مكافحة الجريمة الالكترونية ، كما عاجلت اتفاقية فيينا لسنة 1988 الموضوع ذاته ، وحثت الكثير من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه

الجرائم وكذلك حث اللقاء التمهيدي الإقليمي لآسيا و الباسفيك المنعقد 1989 الممهد للمؤتمر الثامن للأمم المتحدة المنعقد في كوريا 1990 ضرورة النظر إلى نتائج التطور و التقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة ، والمؤتمر الأخير ناشد في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف إلى ضرورة تكثيف جهودها لمكافحة الجرائم الإلكترونية في عدة وجوه(26)،وعلى الصعيد الدولي أيضا عقدت الأمم المتحدة العديد من المؤتمرات لمواجهة الجرائم الإلكترونية وإصدار الكثير من التوصيات ، ففي المؤتمر السابع للأمم المتحدة الخاص بمكافحة الجريمة ومعاملة المجرمين أشار المؤتمر إلى جرائم الحاسب الآلي والصعوبات المتعلقة بها باعتبارها من الجرائم المتعدية الحدود ذات الطابع الاقتصادي ، وفي شهر أوت عام 1995 عقد المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين في هافانا وكانت الجريمة الإلكترونية والاهتمام بمكافحتها وملاحقتها أحد الموضوعات التي تم بحثها من خلال ندوة أقيمت لهذا الغرض ، كما دعت الوكالات والمؤسسات ذات الطابع الدولي إلى التدخل لحماية المعلومات وعدم الاعتداء عليها ، وفي مقدمة هذه الوكالات منظمة التنمية والتعاون الاقتصادي .

أما على مستوى المنظمات الإقليمية فقد حرص مجلس الاتحاد الأوروبي على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات بإصدار العديد من التوصيات والتوجيهات الملزمة والتي تمثل الحد

الأدنى الذي يتعين على دول الاتحاد الالتزام به عند سن تشريعاتها في هذا الخصوص ، وقد تجلّى هذا الحرص بشكل ملموس بإبرام اتفاقية بودابست التي تم التوقيع عليها عام 2001 المتعلقة بالإجرام المعلوماتي ، وخلال المؤتمر السادس للمنظمة الدولية للشرطة الجنائية "أنتربول" المنعقد بالقاهرة في الفترة الممتدة من 13-15 أبريل 2005 تم الوقوف فيها على المخاطر المحدقة بالهياكل الوطنية والدولية نتيجة تنامي الجرائم المعلوماتية بسرعة فائقة لذلك صدرت عن هذا المؤتمر مجموعة هامة من التوصيات تهدف إلى تحسيس الجهات المسؤولة عن العدالة والإدارات العمومية والمؤسسات الخاصة للعمل على دعم أنظمتها بما يضمن مواجهة هذه الجرائم.(27)

الفرع الثاني :إقرار التشريع الجزائري لمبدأ المساعدة القضائية المتبادلة

استجابت العديد من الدول لحتمية التعاون الدولي بأن وجهت سياستها التشريعية نحو مواجهة الجرائم الماسة بالمعالجة الآلية للمعطيات ، وذلك بمحاولة سن تشريعات جديدة ، أو تطوير التشريعات القائمة بتعديل بعض نصوصها بما يواكب التطور التقني ، ويتلاءم مع الطبيعة الخاصة للجريمة المعلوماتية ، فكانت البداية محاولة مشرّعي بعض الدول تتمثل في التدخل لوضع ضوابط لاستخدام الإنترنت ووضع القواعد المنظمة لمباشرة خدماته ، سواء ما يتعلق بواجبات القائم بهذه الخدمات أو ما يتعلق بحقوقه.

ويعد التشريع الجزائري من التشريعات التي حرصت من أجل مواجهة فعالة لهذا النوع من الجرائم على إصدار نصوص قانونية ومنها القانون 09-04، لا سيما في أحكام المادة 16 منه التي تتيح في إطار التحريات أو التحقيقات القضائية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، ويمكن في حالة الاستعجال وذلك مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل قبول طلبات المساعدة القضائية، و ما يجب الإشارة إليه في هذا الصدد أنه ثمة قيد على طلبات المساعدة القضائية الدولية تمنع الإستجابة لها وذلك إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام، غير أنه يمكن الإستجابة إلى طلبات المساعدة شريطة المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب. (28)

خاتمة:

تخطت جرائم تكنولوجيا الإعلام الإتصال حدود الدول وشكل تهديدها الحقيقي والسلي على الاقتصاد خطرا كبيرا ويعود السبب في ذلك عوامل عدة أهمها:

- جهل الأفراد بأنواع الجرائم الإلكترونية وطرق استدراج الضحايا، وثقتهم ببعض الأشخاص والمواقع والرسائل الإلكترونية دون التأكد

المصادقية

من

•تنوع طرق الجريمة الالكترونية وتعدد أساليبها مع تقدم الزمن وتطور التقنية الحديثة .

•عدم حرص المستخدم على وضع برامج حماية ضد الفيروسات والتجسس .

•عدم تحديث أنظمة الحماية المستخدمة.

•وجود نقص وضعف في التشريعات والقوانين الخاصة بهذا النوع من الجرائم مما أسهم في تمادي المجرمين .

إن هذا الوضع فرض جملة من التحديات القانونية على الصعيد الإجرائي تجسدت في المقام الأول في بعض المسائل القانونية التي تتعلق بإثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموساً ، كما هو الحال في الجرائم التقليدية ، مما يقتضي الاهتمام بوضع تشريعات تتلائم وطبيعة هذا النوع من الجرائم ، كما يتعين في ذات الوقت التأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار، وتستوجب أيضاً استحداث ضبطين قضائية متخصصة في مجال الجرائم المعلوماتية أسوة بالدول المتقدمة ،ذلك أن أخطارها البالغة من شأنها تهديد الكيان الاقتصادي للدول.

الهوامش

-1.V. dr. Mohammed Buzubar : "la Criminalite informatique sur L'internet", Journal of law, (Kwait University), No.1, Vol.26, March 2002, P. 21.

- جميل عبد الباقي الصغير ، القانون الجنائي والتكنولوجيا الحديثة ، الكتاب الأول : الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية . القاهرة ، 1992 ، ص 4 . 5 ، محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، الطبعة الثانية ، دار النهضة العربية . القاهرة ، 1998 ، ص 3
- 2- هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة أسبوط ، الطبعة الأولى 1994، ص 29.
- 3- أحمد المناعسة ، جرائم الحاسب الآلي والأنترنت، دار وائل للنشر والتوزيع ، عمان الطبعة الأولى 2001، ص 08.
- 4- عفيف كامل عفيفي "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون" منشورات الحلبي الحقوقية الطبعة الثانية 2007 ص 31.
- 5- هدى قشوش جرائم الحاسب الآلي في التشريع المقارن الطبعة الأولى دار النهضة العربية القاهرة 1992، ص 3.
- 6- أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة الطبعة الأولى 2006 ص 13.
- 7- أحكام المادة الأولى من الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ: 2001/11/08 من طرف المجلس الأوروبي و تم وضعها للتوقيع منذ تاريخ: 2001/11/23.
- 8- قانون العقوبات الجزائري.
- 9- أحسن بوسقيعة ، الوجيز في القانون الجزائي الخاص ، الجزء الأول، دار هومة ، الطبعة الخامسة عشر 2013 ص 494.
- 10- أمال قارة ، مرجع سابق ص 103.
- 11- أنظر أحكام المادة الثانية من القانون 09-04 المؤرخ في 2009/09/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإنترنت ومكافحتها.
- 12- أحسن بوسقيعة مرجع سابق ص 497.
- 13- عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، بدون ناشر ، طبعة مزيطة ومنقحة ، 2009 ، ص 380 .

- 14- هشام محمد فريد رستم ، الجوانب الإجرامية للجرائم المعلوماتية، مكتبة الآلات الحديثة، الطبعة الأولى 1994، ص 66-67.
- 15- أنظر أحكام المواد 16-37-40 من قانون الإجراءات الجزائية.
- 16- مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية ،وجرائم الفضاء الافتراضي،نشرة القضاة،العدد66، 2011،ص63.
- 17-أنظر أحكام المادة 47 من قانون الإجراءات الجزائية.
- 18-فاديا سليمان ، الجرائم المعلوماتية وأثرها على العمليات المالية و المصرفية -الجرائم الالكترونية أنواعها و أهدافها و آثارها - ، مجلة الدراسات المالية و المصرفية ، الاكاديمية العربية للعلوم المالية و المصرفية ،الأردن، العدد الأول ، مارس 2015 ص 8
- 19-حسن طاهر داود ،جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ، السعودية 2000 ص23
- 20-الجريمة الإلكترونية ، متاح على الموقع (www.ictmoi/elibrary/crime).
- 21-فاديا سليمان ، مرجع سابق ، ص 8
- 22-فاديا سليمان ، مرجع سابق ،ص10
- 22-أنظر أحكام المواد02-06-08من المرسوم الرئاسي 15-261المؤرخ في 2015/10/08 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- 23-أنظر أحكام المادة 04 من المرسوم الرئاسي 15-261المؤرخ في 2015/10/08.
- 24-محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في الفترة من 1 - 3 ماي 2000 بكلية الشريعة والقانون بدولة الإمارات ، ص78.
- 25- محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر) ، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة 25 - 28 أكتوبر ، 1993 ، ص 362
- 26- محمد عبد الله أبوبكر سلامة ، جرائم الكمبيوتر والإنترنت ، منشأة المعارف ، الإسكندرية ، الطبعة الأولى 2006 ، ص 120 .
- 27-محمد العسكري،خصوصيات الإثبات في الجرائم المعلوماتية،مجلة القضاء والتشريع،المغرب ،جويلية العدد07ص47.
- 28-أنظر أحكام المادة 16-17-18 من القانون 09-04المؤرخ في 2009/09/05المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.