جامعة د . مولاي الطاهر – سعيدة –

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري

مذكرة تخرج لنيل شهادة ماستر في الحقوق تخصص :

القانون الجنائي والعلوم الجنائية

إعداد الطالب :

– فليح نور الدين

إشراف الأستاذ :

– د . حمامي ميلود

أعضاء لجنة المناقشة

– د. حمامي ميلود .....مشرفا ومقرراً

– د.عياشي بوزيان .....رئيساً

– د. عثماني عبد الرحمن .....عضواً مناقشاً

– د.الشيخ قويدر ..... عضواً مناقشاً

السنة الجامعية: 2018م / 2019م

((رَبَّنَآ ءَاتِنَا مِن لَّدُنكَ رَحْمَةً وَهَيِّئْ لَنَا مِنْ أَمْرِنَا رَشَدًا))

صدق الله العظيم

إهداء

أهدي ثمرة الجهد هذا إلى :

- روح جدتي رحمها الله التي لم تبخل علي بعطفها وحنانها ورعايتها وحبها ،جدتي ،مقلتي.

- والداي العزيزان اللذان بفضلهما بعد الله سبحانه وتعالى وصلت إلى هذا المقام ،أبي الذي كد في تربيتي ، أمي ثم أمي ثم أمي بل وطني ، محياي ومماتي، الحبيبة التي ليس قبلها ولا بعدها حبيبة والمواسية التي أنارت دروبي ، الشاحن الذي أشحن به عزيمتي واستمد منه قوتي .

- زوجتي،رفيقتي وصاحبتي التي دعمتني وأعانتني وتحملتني.

- أولادي (أسامة عبد المعز،براء محمد طه،خليل الرحمان إبراهيم) ثمرة الفؤاد وجميع الوداد ،فاللهم كما اخترت أسمائهم فاجعل لهم نصيبا من أسمائهم وأنبتهم نباتا حسنا ترضاه وعلمهم من علمك وأحفظهم بحفظك .

- إخوتي أنصافي

- أصدقائي كلهم عملا ودراسة وخارجها.

شكر وتقدير

إلى من زرع هذه الشجرة ، شجرة العلم والمعرفة اهديهم ثمارها، أساتذتي المبجلين ومعلمي الفاضلين .

كل من علمني حرفا ونصح لي نصحا.

الأستاذ المشرف : حمامي ميلود صاحب هذا العمل في الحقيقة الذي يعود له الفضل في إخراج هذا البحث إلى النور عبر توقيع شهادة ميلاده ،أشكرك أستاذي على كل التوجيهات القيمة التي كانت عونا لنا في إتمام هذا العمل وصبرك وتحملك .

أستاذي الفاضل : عثماني عبد الرحمان.

أستاذي الفاضل وأخي : فليح كمال محمد عبد المجيد.

أستاذي الفاضل : عياشي بوزيان.

أستاذي الفاضل : شيخ قويدر.

والى كل من لم تسعني الكتابة ولا الصفحة لأذكره.

اذكركم في قلبي قبل ذاكرتي.

- شكرا لـكم -

المقدمة

مقدمة :

العالم يشهد تطورا مذهلا لم يسبق له مثيلا والجريمة باعتبارها ظاهرة اجتماعية كان لا بد لها أن تتطور بتطور المجتمعات وتنمو لتأخذ أبعادا خطيرة ومتشبعة لم تكن تخطر على البال ، فهي لم تعد منحصرة في مفهومها أو شكلها التقليدي بل تعدت إلى أن تصبح تنظيما تولد من نسيج تخطيط وتدبير يجسد في لنهاية بناءا منظما، تحكمه قواعد وسلوكات بات من الصعب احتوائها أو التحكم بها، إذ يشهد العالم من منتصف القرن العشرين ثورة جديدة، اصطلح على تسميتها بالثورة المعلوماتية وذلك بإشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، قد أمست قوة لا يستهان بها في أيدي الدول والأفراد، وكان التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة.

ومما لاشك فيه أن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت أثارا ايجابية وشكلت قفزة حضارية نوعية في حياة الأفراد والدول، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات. وتخزينها ومعالجتها ومن ثمة نقلها وتبادلها بين الأفراد والجهات و الشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، كما أصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية والاقتصادية،

كذلك أمست مستودعا لأسرار الدول الحربية والصناعية والاقتصادية التي تعتبر على قدر من الأهمية والسرية.

الا أن هذا الجانب الايجابي المشرق لعصر المعلوماتية لا ينفي الانعكاسات السلبية التي أفرزتها هذه التقنية العالية والمتمثلة في إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبصورة تضر بمصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع كله، حيث أدى هذا التطور المماثل إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميتها بالجرائم المعلوماتية أو الجرائم الالكترونية، هذا النوع الحديث من السلوكات الإجرامية الماسة بأمن وسلامة النظم المعلوماتية وبحقوق الغير تشكل خطرا بالغا وذلك لتعدد أوصافها الإجرامية ، كجرائم مسوقة المعلومات المخزنة أو تخزينها، أو جرائم التحويل غير المشروع للأموال، أو جرائم النقدي على الغير عبر الشبكات، أو جرائم الاستغلال الجنسي للقصر .....الخ من جرائم مستحدثة تتسم بطابعها المعنوي الخالص وتخلو في بعض الأحيان من الطابع المادي المميز بالأغلب الجرائم التقليدية.

إذا كان القانون هو وليد فكر المجتمع فهو يتطور بتطوره من اجل ذلك استوجب على التشريعات المختلفة للدول أن تواكب هذا التطور من خلال سن قوانين تتماشى وما تفرضه التطلعات من اجل إيجاد سبل واليات للحد من استعمال ظاهرة الجريمة الالكترونية وتبعاتها والحث على انتهاج سياسية جنائية تتكفل بمثل هاته السلوكات الإجرامية من تجريم وعقاب يخضع لها أفراد المجتمعات خاصة المجتمع الجزائري الذي هو محل الدراسة.

حيث انه بالنظر للتزايد المستمر للنشاط الإجرامي عبر النظم المعلوماتية، وتزايد درجة خطورة هذا النشاط وارتفاع مستوى التهديدات التي يشكلها على الآمن في ظل الاعتماد المطلق على تكنولوجيا المعلومات في المجتمع ، إضافة إلى أن الجرائم المعلوماتية من بين أهم المواضيع المطروحة للنقاش الدولي والوطني، فهي تشغل حيزا مهما من جهود الباحثين كذلك الفقه والتشريع لأجل وضع استراتيجيات قانونية وعملية آنية ومستقبلية، تضمن عدم فقدان السيطرة على التقنية المعلوماتية، وتحولها من تقنية تساعد على تطور المجتمعات من خلال تبادل المعارف والمعلومات إلى تقنية هدامة.

ولعل من أهم الأسباب التي دفعتها لاختبار هذا الموضوع هو الرغبة الملحة إلى تعرية الجريمة الالكترونية لتحليل مختلف جوانبها والتعرف عليها من خلال دراستها بتمعن وابرازها. من خلال إبراز خطورتها على المجتمع كذلك محاولة التحليل بالدراسة لموقف المشرع الجزائري من هذه الجرائم الحديثة والغريبة على المجتمع الجزائري والتي أصبحت تنهش القيم الاجتماعية والاقتصادية للبلد، ومعرفة كيفية معالجة المشرع الوطني لمختلف هاته الجرائم من خلال النصوص التشريعية العقابية وكذا التجريمية لما ثم استقراؤه من نصوص قانون العقوبات الجزائري وبالتالي إظهار مختلف السبل والآليات المستحدثة للحد من هذه الظاهرة والآليات لمكافحتها.

وككل موضوع يعني بالبحث والدراسة نجده لا يخلو من بعض الصعوبات ولعل أبرزها صعوبة الوصول إلى وضع خطة متوازنة ومعالجة فعالة ودقيقة لموضوع البحث بالنظر إلى طبيعة الموضوع المزدوجة القانونية والفنية والتي تشكل تحديا بالغ الصعوبة نظرا لما يميز الموضوع من دقة

المصطلحات والمفاهيم العلمية منها، والقانونية والتي يصعب التحكم فيها وتوظيفها بشكل متناسب ومتلازم.

شح المصادر المتخصصة إذ أن معظم المصادر التي تم العثور عليها هي مصادر لمشارقة تعني بدراسة قوانين الدول العربية الشقيقة كالقانون المغربي والقانون الأردني والقانون السعودي، والمصري.....الخ. حيث أن المصادر التي تعالج الظاهرة من منظور التشريع الجزائري قليلة إن لم نقل نادرة.

وقد تم الاعتماد في الدراسة موضوع البحث على منهجين أولينا أولهما إلى المنهج الوصفي، للجانب الفني من الدراسة مع الاستعانة بالمنهج التحليلي في بعض مراحل البحث لمختلف القواعد والسنن القانونية والتشريعية المرتبطة بعناصر البحث.

وبعد البحث والقراءة لمختلف جوانب الدراسة تراءت لنا إشكالية عامة تتمثل في :

إلى أي مدى وفق المشرع الجزائري في الحد من ظاهرة الجريمة الالكترونية ؟

وهاته الإشكالية العامة التي بدورها تتفرع عنها إشكاليات فرعية أو تساؤلات نذكر منها:

كيف عالج المشرع الجزائري ظاهرة الجريمة الالكترونية ؟

ماهي مختلف الوسائل والسبل والآليات التي وضعها المشرع للحيلولة دون استفحال ظاهرة الجريمة الالكترونية ؟

ومن أجل الكشف عن مختلف خطايا الموضوع وكذا إيجاد أجوبة لكل التساؤلات المطروحة عبر الإشكال العام.

ثم تقسيم الدراسات إلى فصلين أولهما عني بدراسة الجوانب الفنية والإطار المفاهيمي للجريمة الالكترونية ثم تقسيمه بدوره إلى مبحثين اثنين أولي أولهما إلى مفهوم الجريمة الالكترونية حيث تم التطرق عبر مطالبه الاثنان إلى تعريفها و أنواع الجرائم الالكترونية أما المبحث الثاني فقد خصص إلى دراسة مختلف الجرائم الالكترونية وفق ما جاء به قانون العقوبات الجزائري والتي تطرق إليها المشرع وعددها .الذي قسم على غير العادة إلى ثلاث مطالب وذلك للضرورة التي فرضتها المادة المعلوماتية أولينا أولهم إلى جرائم الاعتداء والنقدي على الأنظمة الآلية لمعالجة المعطيات والثاني تطرقنا فيه إلى الجرائم الالكترونية الواقعة على الأموال والثالث الذي أفردناه إلى جرائم النقدي على الأشخاص.

بالنسبة للفصل الثاني تمت دراسة الجانب القانوني من خلال استعراض آليات مكافحة الجريمة الالكترونية والحد منها في التشريع الجزائري الذي قسم إلى مبحثين اثنين بالاعتماد على خطة ثنائية بسيطة أولينا أول مبحث إلى القواعد الموضوعية لمكافحة الجريمة الالكترونية قسمناه بدوره إلى مطلبين تعرضنا في أولهما إلى الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات وأوردنا في الثاني الحماية الجزائية للمعلوماتية من خلال القوانين والتنظيمات الأخرى.

وانتهينا إلى المبحث الثاني الذي أظهرنا من خلاله مختلف القواعد الإجرائية لمكافحة الجريمة الالكترونية الذي تمت دراستها من خلال مطلبين أولهما يتمحور حول القواعد المنصوص عليها في قانون الإجراءات الجزائية والثاني تطرقنا فيه إلى الحماية الجزائية للمعلوماتية من خلال القانون 04/09.

الفصل الأول

أحاط بالجريمة المعلوماتية ،شأنها في ذلك شأن كل ظاهرة جديدة ،الكثير من التساؤلات التي تتعلق بتحديد مفهومها وخصائصها والتمييز بينها وبين ما يقترب منها من ظواهر ،وبتحديد حجم هذه الظاهرة ومعرفة أشكالها وتصنيفاتها والعوامل المختلفة التي تتدخل في هذا التحديد،والحقيقة أن تحديد مفهوم الجريمة الالكترونية وتحديد حجمها هو خطوة أولى للتعرف على هذه الظاهرة من جميع جوانبها القانونية ،الشيء الذي تم التطرق إليه في هذا الفصل بتسليط الضوء على تعريف الجريمة الإلكترونية وخصائصها ومختلف أشكالها وتصنيفاتها كمبحث أول وفي المبحث الثاني تم تخصيصه إلى أنواع وصور الجرائم الالكترونية التي عددها المشرع الجزائري في قانون العقوبات .

المبحث الأول: مفهوم الجريمة الإلكترونية

المطلب الأول: تعريف الجريمة الإلكترونية

تعددت تعريفات الجريمة الإلكترونية وتباينت مضامينها ضيقا واتساعا وقد أسفر ذلك عن تعذر إيجاد فهم مشترك لظاهرة الجريمة الإلكترونية وما يتبع ذلك من تسهيل التوصل إلى الحلول المناسبة لمواجهتها[1].

الفرع الأول: تعريف الجريمة الإلكترونية

استقطب مفهوم الجريمة الإلكترونية اهتمام الفقهاء القانونيين والمختصين في مجال المعلوماتية، من اجل وضع تعريف شامل للجريمة المعلوماتية ،فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم من عرفها تعريف ضيقا وقال بأنها :" الجرائم المرتبطة بالحاسوب والتي تشكل انتهاك القانون الجنائي" ، ومنهم من قال بأنها " تلك الجريمة التي يستخدم فيها الحاسوب" وهو تعريف واسع جدا" [2].

1- التعريف القانوني :

من الناحية القانونية فلا يوجد مصطلح قانوني موحد للدلالة على الجرائم الشائعة عن سوء استغلال النظم المعلوماتية أو إساءة استخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتي.

---

[1]- خالد داودي : **الجريمة المعلوماتية** ،دار الإعصار العلمي ،الطبعة الأولى ، ص21.

[2]- مخلوف عكاشة: **دور الشرطة القضائية في مكافحة الجريمة الإلكترونية**،رسالة لنيل شهادة ماستر جامعة سعيدة، السنة الجامعية 2016-2017 ، الصفحة 19.

وهناك من يطلق عليها وصف جريمة الإفلاس المعلوماتي وهناك من يصفها بجرائم الاحتيال المعلوماتي ،غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية.

وقد ورد تعريف الجريمة المعلوماتية بحسب ما قدمه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي انعقد بغينيا سنة 2000 بأنها " كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام الحاسوب وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية ومن التعاريف التي تم التوسع فيها تعريف الخبير الأمريكي (بـاركـر Parker) الذي حاول إعطائها مفهوما واسعا يحيط بكل أشكال التعسف في مجال استخدام النظم المعلوماتية ،فهي من وجهة نظره " كل فعل إجرامي متعمد،أي كانت صلته بالمعلوماتية ينشأ خسارة تلحق بالمجني عليه ،أو كسب يحققه الفاعل " [1].

2- التعريف الفقهي:

في إطار مساهمة الفقه في تعريف الجريمة الإلكترونية انقسم هذا الأخير إلى اتجاهين أساسيين أحدهما اعتمد التضييق والآخر التوسع في إطار وضع تعريف الجريمة المعلوماتية .

أولا: الاتجاه الفقهي الذي يعرفها بشكل ضيق: زعم هذا الاتجاه(ميروي) من خلال وضعه تعريفا مضمونه:" أن الجريمة المعلوماتية هي ذلك الفعل غير المشروع الذي يتورط في إرتكابه الحاسب" [2].

[1]- مخلوف عكاشة: المرجع السابق، ص 20.

[2]- محمد أمين الشوايكة: **جرائم الحاسوب والانترنت(الجريمة المعلوماتية)**،دار الثقافة للنشر والتوزيع،عمان الأردن،2009،ص08.

كما عرفها روزبلات بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه ".

كما عرفها روزبلات بأنها " نشاط غير مشروع موجه لنسخ أو تفسير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقة" .

أما (بمولرين) فعرفها بأنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " [1].

ثانيا: الاتجاه الفقهي الموسع للجريمة المعلوماتية بهدف تفادي النقص الظاهر على التعاريف السابقة فعرفت بأنها : " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية " .

كما عرفت بأنها" كل سلوك سلبي كان أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها باي صورة كانت " [2].وقد عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02 الفقرة 1 من القانون 09-04 الصادر في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي:

[1]- محمد سيد سلطان، **قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية** ،دار ناشري للنشر الإلكتروني، الكويت،2012،ص62.

[2]- تركي بن عبد الرحمان المويشري، **بناء نموذج امني لمكافحة الجرائم الإلكترونية وقياس فعاليته**، رسالة شهادة دكتوراه ،قسم العلوم الشرطية ،جامعة نايف للعلوم الأمنية ،السعودية الرياض، ص 15.

" الجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية [1].

3- الطبيعة القانونية للجريمة الإلكترونية:

بالنظر إلى التعاريف التي وردت بمفهوم الجريمة المعلوماتية وجملة الخصائص والسمات التي تتميز بها فإنه وبدون شك ستتبادر في أذهاننا فكرة التساؤل حول الطبيعة القانونية كالجريمة المعلوماتية فهي في ظاهرها جريمة غير مادية أي بدون أثر مادي ملموس فمجالها البيئة الإلكترونية مما يجعلها مختلفة كليا عن الجرائم الأخرى التي يرى التشريع الجنائي أنها تهدد مصلحة الغير العامة والخاصة ،في هذا الصدد بالنظر إلى تقاطع المفهوم الجريمة التقليدية والمعلوماتية بالمصالح المحمية قانونا فقد انقسم الفقه حول تكييف طبيعة هذه الجريمة بين الوصف الخاص والعلم لها.

أولا: الاتجاه الفقهي الذي يرى بان الجريمة المعلوماتية جريمة من نوع خاص .

يستند هذا الاتجاه على فكرة أن مجال الحماية القانونية هو المعلومة في حد ذاتها باعتبارها السند الأساسي للنظم المعلوماتية وانطلاقا من أن وصفا "التسمية" يضفي على الأشياء المادية القابلة للاستحواذ دون تلك المعنوية التي لا يمكن الاستحواذ عليها.

[1]- القانون 04/09 ،الصادر بتاريخ16-08-2009 ، الجريدة الرسمية رقم :74 ص 05.

فإن مجال الحماية المقررة لها هو في ضوء حقوق الملكية الفكرية فقط، ولعل أن فكر هذا لاتجاه الفقهي يتعارض والمفاهيم الحديثة للقانون الجنائي الذي يقر بأحقية توفير الحماية القانونية للمعلوم باعتبارها تكتسب صفة المال وهو ما تبناه أنصار المذهب الثاني[1].

ثانيا: الاتجاه الفقهي الذي يرى بان الجريمة المعلوماتية جريمة مستحدثة.

يتخذ هذا الاتجاه موقفا صريحا مفاده أن الجريمة المعلوماتية وباعتبارها جريمة تستهدف المعلومات وباعتبار هذه الأخيرة مجموعة مستحدثة من القيم باعتبارها قابلة للاستحواذ عليها بعيدا عن داعمتها المادية ،كما أنها قابلة للتقويم بحسب سعر السوق متى كانت غير محظورة تجاريا أنها نتاج مؤلفها وتجمع بينها علاقة وهو الرأي الذي جاء به الأستاذ (فيفانتي-**vivanti**) بقوله أن " فكرة الشيء أو القيمة لها صورة معنوية وان نوع الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي وان تكون جديرة بحماية القانون ومتى كانت المعلومات والبرامج المعالجة آليا ذات قيمة اقتصادية فإنه يجب معاملتها معاملة المال"[2].

إذا فالبيانات والمعلومات الموجودة داخل ذاكرة الحاسوب تعتبر من الأموال ولها قيمة مادية ، فهي قابلة للنقل من حاسوب لآخر أو القرص المضغوط أو البريد الإلكتروني فهي بالتالي مال منقول وإذا نقلت من دون رضا صاحبها فيطبق عليها قانون العقوبات .

[1]- مخلوف عكاشة: المرجع السابق،ص22.

[2]- محمد علي العريان: **الجرائم المعلوماتية** ،دار الجامعة الجديدة، الإسكندرية،مصر، 2004 ،ص51.

ولقد استقر الرأي الراجح حتى الفقه على أن البرامج والمعلومات تخضع لمبدأ الحماية الجنائية والبرامج والمعلومات ملك لصاحبها إذا سرقة دعامتها من الغير هي سرقة المعلومات في حد ذاتها لأنه لا يمكن الفصل بين الدعامة والمعلومة محل السرقة [1].

الفرع الثاني: خصائص الجريمة الإلكترونية

تتميز الجرائم الإلكترونية بخصائص تختلف إلى حد ما عن الجريمة العادية ذلك نتيجة ارتباطها بتقينة المعلومات والحاسب الآلي مع ما يتمتع به من تقنيات عالية،وقد أضفت الحقائق على هذا النوع من الجرائم عدد من السمات والتي انعكست بدورها على مرتكب هذه الجريمة والي أضحى يعرف بالمجرم المعلوماتي.

أولا: جريمة عابرة للحدود (الدول)

إن تعبير "جرائم عابرة للدول" أو جرائم عابرة للحدود هي تلك الجرائم التي تقع بين أكثر من دولة بمعنى أنها لا تعترف بالحدود الجغرافية للدول كجرائم تبيض الأموال ،المخذرات وغيرها .

وفي عصر الحاسب الآلي ومع انتشار شبكة الانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال فيما بينها أمرا سهلا طالما

[1] – خالد عباد الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت** ، الطبعة الأولى ،دار الثقافة للنشر ولتوزيع،عمان،الأردن، 2001،ص 57.

حدد عنوان المرسل غليه أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة[1].

في هذه البيئة يمكن أن توصف الجرائم الإلكترونية بأنها جرائم عابرة للدول إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه ،وعليه تعتبر الجرائم المعلوماتية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية اعتبار الجرائم الجرائم المعلوماتية جرائم عابرة الدول يظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها [2].

ثانيا : جريمة صعبة الإثبات

ذكرنا أنا جرائم التقنية تمتاز بالتباعد الجغرافي بين الجاني والمجني عليه،يستخدم الجاني فيها وسائل فنية وتقنية معقدة في كثير من الأحيان كما يتمثل السلوك المجرم المكون للركن المادي فيها من عمل سريع قد لا يستغرق أكثر من بضع ثواني بالإضافة إلى سهولة محو الدليل والتلاعب فيه.

أمام هذا كله تبرز صعوبة الإثبات في الجرائم المعلوماتية خصوصا مع الانتقال إلى الدليل المادي التقليدي (دم،شهر،بصمة...)[3].

[1]- القاضي: أسامة أحمد المناعسة،القاضي : جلال محمد الزغبي ،**جرائم تقنية نظم المعلومات الإلكترونية**،دراسة مقارنة،دار الثقافة للنشر والتوزيع ،عمان ،الأردن،2014،ص95.

[2]- نفسه،ص95.

[3]- نفسه،ص96.

مما يزيد الأمر صعوبة ضعف خبرة الشرطة ومعرفتهم الفنية بأجور الحاسب الآلي سواء تمثل ذلك الضعف في تحديد الدليل المعتبر أو في انتشال ذلك الدليل والمحافظة عليه.

بالإضافة إلى عدم تمثيل القضاء إلى غاية الآن بكثير من صور الجريمة الإلكترونية وإمكانية إثباتها بطرق جديدة ،ولا تزال الجرائم المعلوماتية تعامل وفق المفهوم التقليدي للجريمة العادية.

ويتفرع عن هذه الخاصية أن الجريمة المستحدثة وفي العديد من صورها تكتشف بالصدفة[1].

ثالثا: السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح ،سواء كان هذا التمييز في السمات العامة لها أو كان في البحث على تنفيذها أو في طريقة هذا التنفيذ ذاته كما تتميز بطابعها الأولي في أغلب الأحيان حيث تخطى آثار هذه الجريمة حدود الدولة الواحدة [2].

1- خصوصية الجريمة المعلوماتية:

تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها ويرجع ذلك إلى عدة أسباب من بينها:

*وسيلة تنفيذها إلى تمييز في اغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة فهي سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي

[1]- القاضي،أسامة أحمد المناعسة،القاضي جلال محمد الزغبي ،المرجع السابق، ص96.

[2]- خالد داودي،المرجع السابق،ص27.

1200 جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و18900 جريمة تندرج تحت وصف جرائم الآداب و3 مليون جريمة ضد الأموال وفي أحدث تقارير مركز شكاوي احتيال الانترنت (IFFC) الأمريكي أظهر التحليل الشامل للشكاوي التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكوى من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الانترنت و814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي[1] مع الإشارة إلى أن هذه الحالات هي نقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي .

*وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية ترتفع الإشارة الناجمة عن الجرائم فعلى سبيل المثال كانت الخسارة الناجمة عن 8000حالة سرقة بالإكراه في فرنسا عام 1986 حوالي 561 مليونا من الفرنكات الفرنسية FF.

في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها بنسبة 8 مرات عن حالات السرقة بالإكراه وفي الولايات المتحدة الأمريكية توصل مكتب التحقيقات FBI إلى أن متوسط الخسائر التي تحققها الجريمة المعلوماتية يبلغ حوالي 500.000دولار حين لا تزيد الخسائر التي تخلفها جرائم السرقة العادية عن 3500 .

*وفي المقابل فإنه وعلى غرار الآراء التي تتجه إلى القول بان الجريمة المعلوماتية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها أو انه لا يوجد شعور عام بعدم أخلاقية هذه الأفعال: فإننا لا

[1]– خالد داودي: المرجع السابق ،ص28.

نتفق مع هاته الآراء إذ أن الجريمة المعلوماتية لا تختلف عن غيرها من جرائم من حيث اعتدائها على مصالح لها أهميتها لدى أفراد المجتمع ومن ثم تستحق الحماية القانونية كون أن مساس هذه الأفعال بهذه المصالح هو الذي يبرز تجريمها[1].

رابعا: السمات الخاصة بالمجرم المعلوماتي:

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، و إنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين و لقد اختلف الباحثون عن تحرير هذه السمات، و يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة و بالمجرم المعلوماتي بصفة خاصة، إلى انه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه، فكل ما في الأمر انه ينتمي إلى طائفة خاصة من المجرمين[2] تقترب في سماتها من جرائم ذوي الياقات البيضاء وإن كانت- في رأيه- لا تتطابق معها.

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما انه على درجة من العلم والمعرفة (وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي كما هو الحال في جرائم ذوي الياقات البيضاء).

[1]- خالد دواري: المرجع السابق،ص28.

[2]- نفسه،ص28.

ويتميز المجرم المعلوماتي ذلك بمجموعة من الخصائص التي تتميز بصفة عامة عن غيره من المجرمين ويرمز غليها الأستاذ Parker بكلمة S.K.R.A.M وهي تعني [1]:

أ/ المهـارة Skills :

وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي ،والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال ،أو عن طريق الخبرة المكتسبة مع الآخرين إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال بل إن الواقع العلمي قد أثبت أن بعض أنجح المجرمين المعلوماتيون لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[2].

ب/المعـرفة knowledge:

والمعرفة تتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته كون المسرح الذي تمارس فيه هذه الجريمة هو نظام الحاسب الآلي فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها ذلك قبل تنفيذ الجريمة .

[1]- خالد دوادي : المرجع السابق،ص33.

[2]- سعيدي سليمة،**جرائم المعلومات والشبكات في العصر الرقمي** ،درا الفكر الجامعي ،الإسكندرية ،مصر،2017، ص33 .

ج/الوسيــلة Ressources:

أما الدراسة فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فان الوسائل المتطلبة للتلاعب بأنظمة الحواسب الآتية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها[1].

د/السلــطة Auttorrty:

أما السلطة فقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته نقد تتمثل هذه السلة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات أو المحو أو التعديل فيها، أو مجرد قراءتها أو كتابتها ،وقد تتمثل هذه السلطة في الحق في استكمال الحاسب الآلي أو إجراء بعض التعاملات وقد تكون هذه السلطة غير حقيقية كما في حالة واستخدام شفرة الدخول الخاصة بشخص آخر.

هـ/ البـــاعث Motives:

وأخيرا يأتي الباحث وراء ارتكاب الجريمة الذي قد لا تختلف في كثير من الأحيان من الباحث لارتكاب غيرها من الجرائم الأخرى فالرغبة في تحقيق الربح المادي بطر يق غير مشروع يظل الباحث الأول وراء ارتكاب الجريمة المعلوماتية ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله،وأخيرا الانتقام من رب العمل أو احد الزملاء [2].

[1]- خالد دوادي،المرجع السابق، ص84

[2]- خالد دوادي،المرجع السابق ، ص 74.

المطلب الثاني: تصنيفات وأنواع الجرائم الإلكترونية

يصنف الفقهاء والدارسون الجرائم المعلوماتية ضمن فئات متعددة،تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني ،فبعضم يقسمها إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته،وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة وآخرون يستندون إلى الباعث أو الدافع لارتكاب الجريمة،وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء وكذا تعدد الحق المعتدى عليه فتوزع الجرائم المعلوماتية وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الأشخاص أو بمعنى أصح على الحياة الخاصة.

الفرع الأول: تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة.

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات ،وهو التصنيف الذي يعكس أيضا التطور التاريخي لظاهرة الجرائم المعلوماتية ،ونجده التصنيف السائد في مختلف مؤلفات الفقيه الريش سيبر والمؤلفات المتأثرة به ولهذا نجد أن جرائم المعلوماتية بالاستناد إلى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية [1]:

أولا: الجرائم الماسة بقيمة معطيات الحاسوب

وتشمل هذه الطائفة فئتين:

أ- الجرائم الواقعة على ذات المعطيات،كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة الفيروسات .

ب- الجرائم الواقعة على ما تمثله المعطيات آليا ،من أموال أو أصول ،كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات ،وجرائم التحويل والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آليا واستخدامها)[2] .

[1]- خالد الدوادي ،المرجع السابق، ص44.

[2]- نفسه ،ص45.

ثانيا: الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة وجرائم قرصنة البرمجيات.

وتشتمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة، وكذا نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص والاعتداء على العلامة التجارية وبراءة الاختراع.

وبإمعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق، إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على امن المعطيات، لكن الفرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله، والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) ، لكنها تتميز عن الطوائف الأخرى بان محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.[1]

هذا من جهة، ومن جهة أخرى نجد أن الجنائية للمعلومات في نطاق القانون المقارن وفي إطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه، اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة وحماية المعطيات بالنظر لقيمتها. أو ما تمثله والذي عرف بحماية الأموال كل في ميدان

[1] – خالد داودي، الجريمة المعلوماتية،ص45.

وموقع مستقل، وهو في الحقيقة تمييز ليس مطلقا بين حماية قيمة المعطيات،وأمنها، والحقوق الملكية الفكرية ولا بد لنا من الإشارة أن حماية امن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرام الطائفة الأولى الماسة بقيمة المعطيات بالنظر إلى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من قبل الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم[1] .

الفرع الثاني: تصنيف الجرائم تبعا لدور الكومبيوتر في الجريمة

عرضنا فيما تقدم لدور الكومبيوتر في الجريمة، فقد يكون هدف الاعتداء، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبدلة بواسطة الكمبيوتر والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق، (جرائم الحاسوب) وقد يكون الكومبيوتر وسيلة ارتكاب جريمة أخرى في إطار مفهوم (الجرائم المرتبطة بالكمبيوتر)، وقد يكون الكمبيوتر أخيرا بيئة الجريمة أو وسطها أو مخزنا للمادة الجرمية، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن الدور الأول جرائم التخزين، ويقصد بها تخزين المواد الجرمية أو المستخدمة في ارتكاب الجريمة أو الناشئة عنها، والثاني، جرائم المحتوى أو ما يعبر عنها بالمحتوى غير المشروع أو غير القانوني، والاصطلاح الأخير استخدم في ضوء تطور إشكال الجريمة مع استخدام الانترنت، وأصبح محتوى غير القانوني يرمز إلى

[1]– خالد داودي، الجريدة المعلوماتية، ص 46.

جرائم المقامرة ونشر المواد الإباحية والفسيل الالكتروني للأموال وغيرها باعتبار أن مواقع الانترنت تتصل بشكل رئيسي بهذه الأنشطة، [1] والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة في نفس الوقت كوسيلة لارتكابها وهذا التقسيم شائع الجزء منه (وهو تقسيم الجرائم إلى جرائم هدف و وسيلة) لدى الفقه المصري والفرنسي، وتبعا له تنقسم الجرائم المعلوماتية إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر، أما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه، العالمي الجديد في ضوء تطور التدابير التشريعية في أوروبا تحديدا [2]،وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية، جرائم الكمبيوتر والانترنت عام 2001، ذلك أن العمل منذ مطلع عام 2000 يتجه إلى وضع إطار عام لتضيف جرائم المعلوماتية وعلى الأقل وضع قائمة الحد الأدنى محل التعاون الدولي في حقل مكافحة هذه الجرائم.

وهو جهد تقوده دول أوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا، وضمن هذا المفهوم نجد الاتفاقية المشار إليها تقسم الجرائم المعلوماتية إلى الطوائف التالية:

الأولى:

الجرائم التي تستهدف عناصر "السرية والسلامة" المعطيات والنظم وتظم:

- الاعتراض غير القانوني.
- تدمير المعطيات.

[1]- خالد داودي، المرجع السابق، ص46.

[2]- خالد داودي، المرجع السابق، ص47.

- اعتراض النظم.

- إساءة استخدام الأجهزة.

الثانية : الجرائم المرتبطة بالكمبيوتر وتظم:

- التزوير المرتبط بالحاسوب .

- الاحتيال المرتبط بالحاسوب.

الثالثة: الجرائم المرتبطة بالمحتوى ونظم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة الاباجية و اللاأخلاقية .

الرابعة : الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة-قرصنة البرمجيات-

الجزائري.

المبحث الثاني: الجرائم الالكترونية وفق ما جاء به المشروع الجزائري

يبدو أن المشرع الجزائري سارع إلى احتواء هذا التطور التكنولوجي بالتشريع الجنائي وأحاط الجريمة الالكترونية بإطار قانوني أدرج فيه تصورا مواكبا بمراحل هذه الجريمة وتشكيلاتها وأهدافها من خلال القانون رقم 4-15 المؤرخ في 10 نوفمبر 2004 والمتضمن قانون العقوبات المعدل والمتمم [1]، كما سوف يتأتى ويمكن القول بان الجرائم الالكترونية تختلف باختلاف طرق ووسائل اقتراضها أو أهدافها وسواء كانت فردية أو جماعية، فانه يمكن تصنيفها حسب نوعها أو حسب الأهداف، أو حسب الوسائل التي تستخدم فيها كالبريد الالكتروني واستعمال الهاتف الخلوي

[1]- خالد داودي، المرجع السابق، ص48.

ناهيك عن شبكة الانترنت ويبدو أن المشرع الجزائري خطا خطوات عامة وسريعة في هذا المجال وذلك بالتكفل بتحريم صور الاعتداء على شبكة الانترنت والمساس بالبيانات المعالجة أليا كما سوف نرى.

المطلب الأول: جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات

يتعين أن نعرف بان نظام المعالجة الآلية البيانات أو المعطيات هو علم قائم بذاته وبالمختصر فان كلمة معلوماتية هي مزج مختصر لكلمتين معلومة : Informatique وكلمة آلية Automatique ومعناها المعالجة الآلية للمعلومة ويفهم من المعطيات الفكرية المعالجة أليا هي عمل البرامج والبيانات الموجودة في الكمبيوتر وعلى شبكة الانترنت سواء كانت فنية أو أدبية أو علمية أو تجارية أو صناعية، فهي تصنف كإنتاج ذهني لأصحابها ومعلوم أن حقوق الملكية الفكرية تعد إحدى أغلى السلع في العالم ومن هنا فهي تصبح محل حماية قانونية في مواجهة الانتهاكات التي تتم من جراء الدخول غير المشروع في أنظمة المعالجة الآلية للمعطيات أو البقاء فيها.[1]

الفرع الأول: جرائم الدخول والبقاء غير المشروع لأنظمة المعالجة الآلية للمعطيات

أولا: جريمة الدخول غير المشروع في المنظومة المعلوماتية:

يعتبر قانون العقوبات الجزائري من القوانين العربية السابقة إلى هذا الموضوع، بل انه من التشريعات المواكبة للتشريعات الغربية. هدى التشريع الأمريكي والانجليزي والفرنسي، خطا المشرع

[1]- تهميش الجريدة الرسمية الخاصة بقانون العقوبات 2015.

الجزائري هذه الخطوة بالمبادرة إلى تعديل قانون العقوبات ، بإدراج القسم السابع المكرر بمحتوى المادة 394 مكرر إلى 394 مكرر 7، وقد نصت المادة 394 مكرر منه على مايلي:

(يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50000 دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك).[1]

يلاحظ أن المشرع الجزائري جرم فعل الدخول بطريقة غير شرعية إلى المنظومة المعلوماتية واعتبر هذا التصرف في حد ذاته بشكل جريمة أن يستخلص لأول وهلة أن مجرد اختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية بعد انتهاك للنظام المعلوماتي بطريقة غير مشروعة، ويمكن حسب مفهوم النص أن الجريمة تحقق بالصور التالية:

* أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه و واضح من نص المادة 394 مكرر ق ع ج أن جريمى الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك، أي أضرار بالمعلومات ودون تحديد للزمن ذلك أن جريدة الدخول غير المشروع هي جريمة وفنية كما نرى على عكس جريمة البقاء في المنظومة التي تعد من الجرائم المستمرة.[2]

ثانيا: جريمة البقاء في المنظومة المعلوماتية

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

[1]- زيبدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار المهدي عين مليلة، الجزائر 2011، ص46.

[2]- زيبدة زيدان، المرجع نفسه، ص48.

ويمكننا إيعاز ذلك إلى سبب بسيط يبرر هذه التفرقة وهو انه وان كان الدخول عن طريق الخطأ ينتقي معه الجرم فان البقاء عن قصد بشكل جرم قائم بذاته يتم عن إرادة الجاني في الإضرار بالغير.[1]

ونؤكد توافر القصد الجنائي أو الباعث لديه، لكنه ومع ذلك يظل الغموض قائما حول مدة البقاء داخل المنظومة يطرح صعوبة حول تحديد زمن البقاء، ويجب التفرقة هنا بين البقاء الحاصل عن جريمة الدخول غير المشروع وبين البقاء الناتج عن الدخول المسموح به يكون الجاني رفض الخروج بعد استيفاء الوقت المسموح له بالدخول فيه للنظام وفي كل الحالات يتضح أن المشرع ربط البقاء كتصرف إرادي من قبل الجاني، بسوء النية أي عن طريق الغش ويستوي في ذلك أن يكون الدخول أو البقاء في النظام كله أو حتى في جزء منه ذلك أن الاعتداء قد يستهدف جهاز الحاسوب نفسه بكيانة المنطقي (Logical).

الفرع الثاني: جرائم المساس بالأنظمة الآلية لمعالجة المعطيات

الملاحظ أن المشرع الجزائري شدد في العقوبة وجعلها مضاعفة. بنص المادة 394 مكرر ق ع ج إذ ترتب عن الدخول أو البقاء في النظام حذف، أو تفسير لمعطيات المنظومة إذ نص في الفقرة 2 من المادة المشار إليها على مايلي:

(تضاعف التقوية إذا ترتب على ذلك حذف أو تفسير لمعطيات المنظومة). ويتضح من هنا أن الحرص على حماية نظام المعلوماتية لم يتوقف عند تجريم الدخول إليه أو البقاء فيه، بل في

[1]- زبيدة زيدان، المرجع نفسه، ص 49.

مواجهة ما هو اخطر من ذلك وهو المساس بالمنظومة المعلوماتية من حذف أو تفسير أو تخريب أو زيادة أو نشر الخ.

أولا: جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها بطرق تدليسية:

نصت المادة 394 مكرر 1 من قانون العقوبات الجزائري على مايلي:

(يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500000دج إلى 2000000دج، كل من ادخل بطريق الغش معطيا في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها).[1]

والمقصود بإدخال معطيات في المنظومة هو إدراج برنامج ما ،والذي هو عبارة عن تعليمات بلغة ما توجه إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة هي بمثابة هدف الجاني لذلك فان البرنامج الجديد أما أن يكون برنامجا وهميا يهدف إلى التمويه أو التضليل في ارتكاب الجريمة وتغيير الحقيقة.[2]

فقد يعمد المجرم الالكتروني إلى إدخال بيانات جديدة على فاتورة الهاتف قبل طبعها وإرسالها أو بيانا متعلقة بحساب بنكي ومن الأمثلة الواقعية قيام طالب بتغيير درجاته المسجلة على الحاسوب أو القيام بالتسجيل الالكتروني متأن طالب أخر في الجامعة بواسطة اقتناص البيانات.

ويلاحظ بان المشرع من خلال نص المادة 394 مكرر 1 اعتبر كذلك إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملا مجرما أيضا فلا يتوقف الآمر على إدخال معطيات جديدة

[1]- زبيدة زيدان، المرجع نفسه، ص 50.

[2]- زبيدة زيدان، المرجع نفسه، ص53.

في النظام بل قد يعمد المجرم بعد الدخول غير المشروع إلى إتلاف البيانات المخزنة أو المتبادلة عبر شبكة الانترنت أو تعطيلها.

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

ثانيا: جريمة تجميع أو توفير بيانات مخزنة أو معالجة آليا

يلاحظ أن المشرع الجزائري وفي نص المادة 394 مكرر 2 ومع نطاق الحماية لما اسماه المعالجة الآلية للمعطيات إذ بسط هذه الحماية لتشمل المجال المتصل بالمعلومات أو البيانات، ففضلا عن تجريمه للدخول غير المشروع في المنظومة أو في جزء منها أو البقاء فيها فانه وتحسبا لما يترتب عن هذا الدخول أو البقاء من سلوكات إجرامية.

فقد اعتبر المشرع الجزائري عملية تجميع أو التقاط البيانات بغرض استغلالها أو نشرها أو الانجاز فيها من الجرائم التي يعاقب القانون فكما سبق توضيح مفهوم الجرم التصميم والبحث في المعطيات أو البيانات فان المشرع جرم كذلك التقاط البيانات اثر الوصول إليها بعد اقتحام المنظومة واعتبره عملا غير مشروع وسواء تم جمع هذه البيانات عن طريق أخذها من قاعدة التخزين أو أثناء تبادلها عبر شبكة الانترنت.[1]

[1]– زبيدة زيدان ، المرجع نفسه، ص63.

ويستوي في ذلك أن يحقق الجاني هدفا شخصيا أو مصلحة الغير والذي قد يكون مالك أو صاحب النظام المعلوماتي نفسه أو أي شخص مستأجر أو منتفع به وفي الخلاصة كل من له ، مصلحة في تلك البيانات والملاحظ أن المشرع الجزائري وفي المادة :2/394 لم يشترط بان تكون المعلومات أو المعطيات أو البيانات مخزنة داخل النظام المعلوماتي نفسه مما يعني أن الحماية القانونية تشمل كذلك المعلومات المعالجة آليا المخزنة بواسطة الأنشطة أو أقراص ويستوي في ذلك أن يتم التقاط المعلومات والوصول إليها عن طريق التجسس المعلوماتي أو بطرق الاحتيال وتكتسي عمليات التجسس خطورة كبيرة سيما حال استهدافها بيانات سرية تجارية أو عسكرية أو غيرها، والتي تعتبر ظرفا مشددا في نظر المشرع الجزائري .

ثالثا: جريمة نشر المعطيات وأحشائها:

نص المشرع الجزائري في المادة 394 مكرر 2 فقرة 1 من قانون العقوبات على مايلي:

يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1000000دج إلى 5000000دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

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

[1]- زبيدة زيدان ، المرجع نفسه، ص63.

رابعا: جريمة إعاقة سير المعلومات المرسلة عن طريق منظومة معلوماتية:

وهي ضمن الجرائم المنصوص عليها والمتضمنة بأحكام المادة 394 مكرر2من قانون العقوبات والتي يمكن استخلاصها من استقراء هذه المادة هي إعاقة أو اعتراض طريق نظام المعلومات أو المعطيات المرسلة عن طريق نظام المعلوماتية بغرض قرصنتها والانجاز فيها.

ومن الملاحظ أن المشرع الجزائري لم يقتصر على تجريم أفعال الدخول إلى النظام المعلوماتي أو البقاء فيه كما سبقت الإشارة بل مدد الحماية الجنائية. وبسطها حتى على تلك المعلومات المرسلة عن طريق منظومة معلوماتية وسواء تعلق الأمر بإعادة سير هذه المعلومة أو قرصنتها والاستحواذ عليها بغرض حيازتها أو الانجاز فيها ومعلوم أن تبادل المعلومات الكترونيا عن طريق الحواسيب أضحى مشاعا،بل أن الثورة الرقمية فتحت مجالات واسعة لتسخير الفضاء الكوني لربط الاتصال وبسرعة فائقة بما يسمى بالتبادل الالكتروني للمعلومات أو البيانات وذلك بنقلها من جهاز حاسوب إلى أخر يكون متصلا بشبكة الانترنت بواسطة جهاز موديم عبر خطوط الهاتف طرفية مرتبطة بشبكة الانترنت مما يسهل وييسر تبادل المعلومات بين المتراسلين بمختلف وسائل نقل هذه البيانات ومنها:

- الكابلات المحورية.
- الميكوريف.
- الأقمار الصناعية.
- أشعة الليزر والألياف الضوئية.

- البريد الالكتروني.

خامسا: جريمة حيازة البيانات أو المعطيات

يلاحظ أن المشرع الجزائري وكما سبقت الإشارة إليه تدرج في تصور المراحل التي يتوخاها المجرم المعلوماتي ضمن الدخول أو البقاء في النظام المعلوماتي عن طريق الغش إلى تخريب نظام أشغال المنظومة أو إدخال معطيات أو بيانات جديدة أو إزالة البيانات ليصل مرحلة أخرى. [1]

وهي حيازة البيانات بغرض استعمالها ويبدو أن الاستعمال يعد مجرما حتى أن تم بغرض سليم ومشروع طالما أن المعطيات نفسها متحصلة من الجرائم المنصوص عليها في المادة 394 ق ع أي عن طريق الدخول غير المشروع في كل أو جزء من منظومة متعلقة بالمعالجة الآلية للمعلومات وذلك عن طريق الغش.

المطلب الثاني : الجـرائم الالكتـــرونية الواقعـــة عـــلى الأمـوال

يمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه " كل مال الكتروني قابل للنقل والتملك " أو بأنه " المال الموجود على الحاسوب، سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية ، فهو بذلك كل المدخلات الالكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية " [2].

[1]- زبيدة زيدان، المرجع السابق، ص 72.

[2]- زبيدة زيدان، المرجع السابق، ص73.

الفرع الأول: جرائم التحويل غير المشروع للأموال أو جرائم الاحتيال الالكتروني

يعرف النصب أو الاحتيال على انه من جرائم الاعتداء على ملكية مال منقول يلجا فيها الجاني بواسطة إحدى وسائل الاحتيال المعنية قانونا إلى حمل المجني عليه على تسليم المال المنقول.

أولا: الركن المادي:

يقوم الركن المادي لفعل الاحتيال على فعل التظاهر والإيحاء، الذي يكون صالحا للإيقاع بالمجني عليه في الغلط،بطريقة تؤدي إلى الاقتناع المباشر بالمظهر الخارجي، والاحتيال لا يقع على الشخص الطبيعي فقط بل المعنوي أيضا، فالشركات والمؤسسات العامة والخاصة هي من الأشخاص هي من الأشخاص الاعتبارية في نظر القانون، وحيث أن الحاسوب وشبكات الاتصال الداخلية والخارجية تعد من فروع ومكونات الشركة أو المؤسسة فإنها تكون صالحة لوقوع فعل الخداع والتحايل عليها، وقد اعتبر الفقه ممارسة أفعال الاحتيال من خلال التلاعب بالبرامج والبيانات وما يترتب على ذلك من إيهام للمجني عليه بصحتها من أساليب الاحتيال، وحسب هذا الاتجاه فان الحاسوب ليس سوى وسيلة للتحايل.

ويشترط ليتحقق الركن المادي لجريمة الاحتيال تحقق الأفعال التالية:

1- فعل النصب:

أي تنفيذ فعل التلاعب بمدخلات النظام المعلوماتي أي تغذيته ببيانات غير صحيحة أو من خلال التلاعب ببرامجه، إضافة إلى فعل الإدخال والإتلاف والمحو والطمس التي سبق تفصيل

معناها،وقد قدم مكتب التحقيقات الفيدرالي الأمريكي مجموعة من النصائح لمستعملي الانترنت لأجل وقاية مستعمليها من الوقوع ضحايا جرائم الاحتيال وهي:

- تجنب المشاركة في المزايدات على شبكة الانترنت إلا بعد التأكد من صحتها ودور البائع والمزايد فيها.

- عدم تقديم أرقام الضمان الاجتماعي في مجال البيع بالمزايدة على الانترنت.

- عدم تقديم أرقام بطاقات الائتمان إلا بعد التأكد من تامين الموقع.[1]

2- استعمال الطرق الاحتيالية:

يستعين مرتكبو جرائم الاحتيال المعلوماتي بشبكة الانترنت أساسا، من اجل تحصيل مبتغاهم وذلك من خلال اعتماد أسلوب إرسال الرسائل الالكترونية لضحاياهم، في شكل رسائل صادرة عن مؤسسات موثوق فيها، يطلب فيها من الضحايا المحتلمين تقديم معلومات شخصية خاصة بهم، وهو ما يسمح لهؤلاء يتبع ضحاياهم والعمل على الإيقاع بهم، ولعل الأسلوب الأحدث هو الاحتيال على الطريقة النيجيرية التي تعتمد على إرسال رسائل بريدية الكترونية مفادها طلب المساعدة على تحويل العشرات من الملايين الدولارات من قبل الضحايا، بدعوى أن المرسل يعاني من مشاكل سياسية في بلده الأصلي، وانه مستعد لتقديم ما قيمته 10 إلى 15% من قيمة الأموال المحولة بشرط فتح حساب وتدعيمه بقيمة أولية لأجل إتمام العملية.[2]

---

[1]- ناير نبيل عمر، **الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة ، مصر 2012، ص32.

[2]- مخلوف عكاشة، المرجع نفسه، ص 44.

يكتمل الركن المادي بهذه الجرائم إذا ما سبب بصفة مباشرة للغير ضررا اقتصاديا أو ماديا أي أن يكون الجاني قد فقد جريمته بغية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، ومصطلح الضرر الاقتصادي أو المادي واسع جدا بمفهومه فهو يشمل النقود والأشياء المادية وغير المادية ذات القيمة الاقتصادية .

الفرع الثاني: جرائم الاستخدام غير المشروع لأدوات الدفع الالكتروني

تعتبر تقنية الدفع الالكتروني للأموال من أهم التطبيقات الحديثة للمعلوماتية، فقد كسرت حاجز التعامل بالنقود وكذلك عوائق المبادلات المالية، فأصبحت تتم بسهولة وسيولة كبيرة ولا تستغرق من الزمن سوى لحظات، غير أنها وبقدر تطعينات المؤسسات المالية بمدى أمنها، إلا أنها تبقى الهدف الأول لمجرمي المعلوماتية، نظرا كما تدركه من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة وماجاورها.

توفر البطاقات الخاصة بالدفع الالكتروني خاصية التعامل بالأموال في شكلها الالكتروني دون عناء التنقل لتسليمها أو تسلمها في سبيل إتمام المعاملات ، وهو ما عزز نطاق المعاملات التجارية حول العالم ، وتتخذ البطاقات الخاصة بالدفع الالكتروني أشكالا وأنواعا عديدة وذلك كنتيجة لشيوع استعمالها .

أولا: أنواع بطاقات الدفع الالكتروني

1- بطاقات الوفاء.

2- بطاقات الائتمان.

3- بطاقات الصرف الآلي.

4- بطاقات ضمان الشبكات.

ثانيا: صور الاستخدام غير المشروع لبطاقات الدفع الالكتروني

فتمثل جرائم الاستخدام التعسفي لبطاقات الدفع الالكتروني، أشهر الجرائم التي تستهدف الأموال المتداولة وتتمثل صور هذه الاستخدام عبر النظم المعلوماتية وخصوصا مع تنامي التجارة الالكترونية، الاستعمال التعسفي الذي يشكل الجريمة يتمثل في ذلك الاستعمال غير الشرعي من قبل الغير، أي من غير عامل البطاقة، لان الجرائم التي يرتكبها حاملها يمكن أن تصنف على أنها جريمة خيانة أمانة، ويقصد بالجرائم هنا والمرتكبة من قبل الغير بأنها تلك الجرائم التي يرتكبها طائفة تهتم بمجال المعلوماتية، وتستهدف أمنها وامن مرتكبها، فتلاكز جهودها على التقاط وقرصنة البيانات المالية الشخصية للأفراد أو المؤسسات البنكية من اجل إعادة استخدامها. بدون وجه حق ولأجل اقتناء سلع وخدمات وتحمل النبر مسؤولية دفع مقابلها، وتكون بطاقة الدفع الالكتروني من مكونين:(البطاقة نفسها، البيانات السرية الخاصة بحاملها).[1]

وقد يقع فعل الاعتداء أما على البطاقة نفسها أو على مكوناتها المعنوية في إحدى الأشكال التالية:

[1]- عكاشة مخلوف، المرجع السابق،ص 46.

1-في حالة سرقة البطاقة أو ضياعها:

تتخذ البطاقة الخاصة بالدفع الالكتروني شكلا خاصا مصنوعا من مادة البلاستيك، مطبوع عليها بعض المعلومات المتعلقة بحاملها، مع شريط ممغنط يحتوي على بيانات غير مقروءة تتعلق بالبنك والعميل، فإذا ما سرقت أو ضاعت هذه البطاقة من حاملها فعليه إبلاغ البنك الذي أصدرها فورا لمنع استعمالها من قبل الغير أو إلغائها، وهو ما ينطبق أيضا على رقمها السري، وتصبح الجهة التي سحبت منها المبالغ بعد الأخطار هي المسؤولة ويتحمل الشخص الذي عثر أو سرق هذه البطاقة مسؤولية فعل سحب المبالغ من رصيدها .

2-في حالة سرقة أو ضياع بيانات البطاقة:

جرت العادة أن لا يمنح البنك الرقم السري الخاص بالبطاقة إلا لحاملها، حتى لا يكون عرضة للسرقة أو الاحتيال من قبل الغير وبالتالي تنحصر مسؤولية الإدلاء بأرقام البطاقة البنكية عبر شبكة الانترنت على حاملها، كما يمكن أن يتعرض إلى سرقة رقمه السري وبيانات بطاقته من خلال ملئه لنموذج الشراء الالكتروني على شبكة الانترنت.

كما يمكن أن يتعرض لسرقة بياناته السرية من خلال بعض الأساليب التي يعتمدها لصوص التجارة الالكترونية هي :

* إنشاء موقع الكتروني وهمي على الشبكة مطابق لموقع بعض الشركات الكبرى واستعماله في الحصول على البيانات السرية للمتعاملين.

* التسلل إلى مواقع الشركات التجارية والمالية والحصول على معلومات عملائها ،أي إغراق الموقع المستهدف بالرسائل البريدية وبالتالي تحميله.

* استعمال تقنية (Mail Bombing) ما لا يستوعب من معلومات مما يؤدي إلى انفجاره عبر الشبكة، وبعثرة المعلومات المخزنة فيه ومنها البيانات السرية الخاصة بالعملاء.[1]

3- حالة تزوير بيانات بطاقة الائتمان:

يتم تزوير بطاقات الدفع الالكتروني على نطاق شبكة الانترنت، من خلال تشكيل أرقام بطاقات خاصة ببنك معين، وذلك بعد تزويد الحاسوب بالرقم الخاص بالبنك مصدر البطاقة عن طريق برامج تشغيل خاصة، ومن تم استخدام البطاقة المزورة بها، مستخدم أصلي، والقيام بعمليات الشراء بواسطتها مما يعرض العملاء الحقيقيين لمشكلات مع البنوك بسبب استخدام بطاقاتهم، أو بطاقات مطابقة لبطاقاتهم، وهو ما يفسر اكتشاف البنوك لاعتراضات من حاملي بطاقات الدفع الالكتروني، على عمليات لم يقوموا بها .

الفرع الثالث: جرائم الاعتداء على الملكية الفكرية

نظر الفقه في مدة الحماية التي يعطيها القانون للمصنفات ضمن حقوق الملكية الصناعية ومنها الاختراعات عموما ،فرأى فيها مددا طويلة جدا لا تتناسب مع برامج الحاسب الآلي ،من حيث إخضاعها لهذه المدة ،ذلك أن الفكر الإنساني والحاجة لديه لا تتناسب مع مدد الحماية الطويلة ،فيما يتعلق ببرامج الحاسب الآلي خاصة ،إذ لا تقبل منطقيا أن توضع برامج الحاسب

[1]- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع ، عمان، 2008، ص 186.

الآلي ضمن مدد الحماية الطويلة ،وإيقاف المد الفكري التطويري حولها، خصوصا مع ازدياد الحاجات الشبه اليومية لبرامج حاسب آلي جديدة متطورة ،ضمن فئات ونواح حياتية صناعية ،تجارية وثقافية متعددة ،فكان أثر ذلك الانحراف بالحماية الجزائية لبرامج الحاسب الآلي من قوانين الملكية الصناعية والدخول بها حيز قوانين حق المؤلف[1].

مع تقدم عصر الثورة الرقمية ،طفت إلى السطح تحديات تتناسب مع هذا التطور فقد برزت مشاكل التعامل مع نوع جديد من أنواع الملكية الفكرية يمكن وصفها بالملكية الرقمية ،وهي تلك الملكية التي تنصب على برامج الحاسوب وبيانتها والمصنفات الرقمية المنشورة على شبكة الانترنت التي بذل في إنتاجها وجمعها وإظهارها جهد فكري إبداعي جعل من الواجب حمايتها، كحق ملكية فردية وجماعية أن مسيرة التحول نحو مجتمع المعلومات تقضي السماح للأفراد بالنفاذ إلى هذه المعلومات مع كفالة حماية حقوق المؤلفين بمظاهر حماية حديثة تشمل الملكية الرقمية.

أولا: تعريف المصنفات الرقمية:

يعرف المصنف الرقمي بأنه كل : "مصنف إبداعي،عقلي، ينتمي إلى بيئة تقنية المعلومات". فبرنامج الحاسوب مصنف رقمي، وكذلك قاعدة البيانات وطوبوغرافيا الدوائر المتكاملة باعتبار لها نتائج تطور علم الحاسوب، بخلاف أسماء وعناوين الانترنت والبريد الالكتروني التي تعتبر من المصنفات التي ارتبط ظهورها بشبكة الانترنت.

[1]- القاضي: أسامة احمد المناعسة، القاضي: جلال محمد الزعبي، المرجع السابق،ص197.

وتصنف المصنفات عموما بطابع الأصالة أما من حيث الإنشاء أو التعبير أي انه نتاج ذهني بطابع معين يبرز شخصية صاحبه سواء في مضمون و جوهر الفكرة أو في مجدد طريقة عرضها.

ثانيا: صور الجرائم المعلوماتية الواقعة على المصنفات الرقمية:

اهتمت غالب التشريعات بوضع نصوص تجرم المساس بالحقوق المعنوية والفكرية للغير وبالتالي تضمن للمصنفات الحماية القانونية اللازمة، ومنها المصنفات الرقمية من كافة أنواع الاعتداء وهو ما تكلفت به وعلى نحو مفصل ودقيق اتفاقية بودابست لمكافحة الجريمة المعلوماتية، وهو ما دعمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.[1]

وهي الجهود التي توجها المشرع الجزائري حيث أشار إلى مفهوم المصنفات الرقمية في الأمر 08/03 المؤرخ في 2013/07/19 في نصوص المواد 02-03-04-05.[2]، إضافة إلى نص المادة 03 والمادة 27 من الأمر 05/03 المؤرخ في 2003/07/19.[3]، أن كل هذه النصوص يجسد مفاهيم جرائم النقدي على المصنفات الرقمية.

فجرائم المعلوماتية هي أكثر الجرائم مساسا بحق المؤلف من خلال ما يعرف بجرائم التقليد (La Contrefaçon) مثل جرائم التحميل غير المشروع عبر شبكة الانترنت، فملايين المتصفحين لشبكة الانترنت اعتادوه على تحميل الأفلام والموسيقى دون شرائها من مصدرها

[1]- القاضي: أسامة احمد المناعسة، القلاعي: جلال محمد الزعبي، المرجع السابق،ص197.

[2]- الامر08/03، المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة بتاريخ 2003/07/23، الجريدة الرسمية رقم 36،ص44.

[3]- الأمر 05/03 المتعلق بحقوق المؤلف الحقوق المجاورة ،بتاريخ 2003/07/23، الجريدة الرسمية رقم 44، ص04 إلى 07.

الأساسي، مستقلين في ذلك برامج متخصصة في فك شفرات الحماية، وذلك أما بغرض استعمالها الشخصي أو بغرض إعادة نشرها، وطرحها، للغير على شبكة الانترنت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة.

المطلب الثالث: جرائم التعدي على الأشخاص:

قابل الوجه المشرف لتقنية المعلوماتية، وجه مبلي يشكل خطرا وتهديدا على الحياة العامة والخاصة والحريات الفردية، وهو موضوع مستحدث شغل مؤخرا حيزا مهما من اهتمامات العام والخاص، خصوصا بعد ازدياد الطلب على المعلومات الشخصية من قبل مؤسسات الدولة أو المؤسسات الخاصة بل حتى من قبل الأفراد أنفسهم في ظل الاتجاه نحو مجتمع المعلومات.

ويتمثل الخطر خصوصا في غايات استعمالها هذه التكنولوجيات سواءا كانت بصفة آلية أو دورية، أو بشكل ظاهر أو خفي، مباشر أو غير مباشر من خلال تنفيذ عمليات تتمثل في جمع وتخزين ومعالجة ونشر معطيات تتعلق بأشخاص طبيعيين، في شكل كتابات أو صور أو أصوات، وتوفير الإمكانيات التقنية للتصرف فيها، أما على حالتها الأصلية أو بم معالجتها وبالتالي التحكم في الخليات المستوحاة منها.

الفرع الأول: الجرائم الماسة بالحريات العامة

ولعلها تعرف بالجرائم المعلوماتية الماسة بالآداب العامة تتلخص عموما هذه الجرائم في تلك السلوكيات الماسة بالأخلاق ولو أن التعرض لجرائم الأخلاق ليس بالأمر الهين، بالنظر إلى تباين القيم الاجتماعية من مجتمع الأخر، بل وحتى بين طبقات المجتمع نفسه، فما يعد انحلال خلقيا في

مجتمع ربما يكون غير ذلك في مجتمع آخر، وجرائم الأخلاق هي تلك التي تتضمن العدوان على القيم الاجتماعية والأخلاقية المتعارف عليها في النظم الاجتماعية. [1]

يشترط في القانون في غالبية القول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستوفي جملة من الشروط الأساسية وهي أن تكون علنية أي أن تترتب نتائج يعترف بها القانون ويرتب عليها أثاره، إضافة إلى أن تكون معروضة على الجمهور.

وقد تعرض المشرع الجزائري لمفهوم هذه الجرائم في بعض نصوص قانون العقوبات دون أن يحدد نطاقها المتصل بتقنية المعلوماتية، إلا انه يمكن لنا إعمال هذه النصوص على جرائم المعلوماتية بالنظر إلى عمومية وشمولية النصوص، فنجد نص المادة 333من قانون العقوبات الجزائري ، تشير إلى عقاب كل شخص ارتكب فعلا، مخلا بالحياء بصفة علنية وذلك بالحبس من شهرين (02) إلى سنتين (02) وبغرامة من 500دج إلى 2000دج إضافة إلى نص المادة 333 مكرر والتي تنص على نفس المقدار من العقاب في حق كل من صنع، أو حاز أو استورد أو سعى إلى ذلك، أو وزع ا واجد أو الصق أو أقام معارض أو عرض أو شرع في ذلك أو باع أو شرع في البيع أو وزع أو شرع في ذلك، كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زينيه أو صور فوتوغرافية أو أنتج أي شيء مخل بالحياء[2].

[1] د. عادل عبد العال إبراهيم حزامي، **إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، دار الجامعة الجديدة، –الإسكندرية،مصر،2015.

[2] القاضي: أسامة احمد المناعسة، القلاعي: جلال محمد الزعبي، المرجع السابق،ص197.

من خلال استقراء نصوص المواد السالفة الذكر نجد أن المشرع الجزائري لم يذكر بالتخصيص الجرائم التي تقع بواسطة النظم المعلوماتية والتي تستهدف المساس بالآداب العامة، وإنما يمكن تطبيق نصوص هذه المواد على الجريمة المعلوماتية باعتبارها وفي الوقت الراهن من أبرز الوسائل الإجرامية المستعملة من قبل مجرمي المعلوماتية الذين وجدوا في هذه التقنية وسلية ذات كفاءة عالية لأجل نشر إعلاناتهم الإلكترونية التي تمس بالآداب العامة ،والأفعال المجرمة حسب نص المادة تشمل: الصناعة أو الحيازة أو الاستيراد أو العرض ،الشروع في العرض للجمهور ،البيع أو التوزيع أو الشروع فيهما ،فيمكن تصنيع وتركيب الأفلام والصور بواسطة الحاسوب وكذلك تخزينها وكذلك تعديلها ونشرها إما على شبكة المعلومات أو على وسائط التخزين الخارجية،كالأقراص المضغوطة ،وبالتالي إتاحتها للجمهور والتأثير على قيمهم الاجتماعية ،خصوصا بالنسبة للمجتمعات العربية والإسلامية وهو الأمر الذي شددت عليه الاتفاقية العربية لمحاربة جرائم التقنية المعلوماتية [1].

الفرع الثاني: جرائم الاعتداء على حرمة الحياة الخاصة:

تعد الحياة الخاصة قطعة غالية من كيان الإنسان لا يمكن انتزاعها منه، وإلا تحول إلى أداة صماء خالية من القدرة على الإبداع الإنساني، فالإنسان بحكم طبيعته له أسراره الشخصية ومشاعره الذاتية وصلاته الخاصة وخصائصه المتميزة ولا يمكنه إن يتمتع بهذه الملامح إلا في إطار مغلق، يحفظها ويهيأ لها سبل البقاء وتقتضي جرمه هذه الحياة إن يكون للإنسان الحق في إضفاء

[1] عكاشة مخلوف، المرجع السابق،ص 53.

السرية على مظاهرها. وفي إطار المعلوماتية فبرز خطورة التهديد المعلوماتي للحياة الخاصة إساءة استخدام المعلومات والبيانات المتعلقة بالإفراد.

وصور الاعتداء على الحياة الخاصة يصعب حصرها ، لأنها متطورة نتيجة تطور تكنولوجيا المعلومات باستمرار إلا إننا يمكن إن نشير إلى ابرز الانتهاكات التي قد تطال حق الإفراد في حرمة حياتهم الخاصة نتيجة لاستخدام الأنظمة المعلوماتية.[1]

أولا: جرائم القذف والتشهير عبر الانترنت:

للشخص الحق في الشرف الذي يكفل له احترام سمعته وشرفه، واعتباره وكرامته من التعدي والإيذاء، ويقصد بالشرف مجموع القيم التي يضيفها الشخص على نفسه وتشكل سمعته التي ستتبع تقدير الناس له، ويتمثل الإخلال بالشرف في الحط من مكانة الإنسان وتعريضه للاحتقار والازدراء من قبل الغير عن طريق الأقوال والتشهير أو نسب الأفعال.

وتعد جرائم الذم والقدح والتحقير من أكثر الجرائم شيوعا في نطاق شبكة الانترنت، إذا اسيء استخدامها يهدف النيل من شرف الغير وكرامته واعتباره، ففي إطار مجتمع المعلومات الالكترونية يجد العابثون الحرية في نشر وبث رسائل تحتوي عبارات الذم والقدح والتحفيز اتجاه آخرين مستهدفين بذاتهم، بصفة وجاهية أو غيابية أو بواسطة الوسائط الالكترونية السمعية أو السمعية البصرية [2].

[1] نهلا عبد القادر المومني، المرجع السابق، ص 174.

[2] عكاشة محلوف، المرجع السابق، ص 55.

وغالبا ما تقع هذه الجرائم بوصفها الحديث الالكتروني تحت سلطة النصوص التقليدية مما يخلق إشكالا في أمر إثباتها وهو ما ينطبق على أحكام التشريع العقابي الجزائري، بحيث يخلو من نصوص تتعلق بتجريم الاعتداءات على شرف واعتبار الأشخاص ذات الطبيعة الالكترونية، وتبقى المادة 296، 297 من قانون العقوبات الجزائري مجرد نصوص توضيح الفعل المادي المكون لجريمة القذف والسب والقدح والتحفيز، إضافة إلى العقوبات المقرر لها بدون أي ربط مباشر مع تقنية المعلوماتية بالرغم من إقرار القانون رقم 04/15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لنصوص قانون العقوبات، وهو على عكس المشرع السعودي الذي تكفل في نصوص مكافحة الجرائم المعلوماتية بإيضاح هذا النوع من الجرائم بالتفصيل كما هو نص الفقرة من المادة 03 من نفس القانون وذلك تفسير لما ورد في نص المادة أربعة عشر (14) من مضمون الاتفاقية الفردية لمكافحة جرائم تقنية المعلوماتية [1]، ويمكن حصر هذه الجرائم في الأنماط والسلوكيات التالية:

1-استهداف شخص معين بذاته بالذم والتحقير والتشهير:

يكون ذلك إما باستخدام البريد الالكتروني بحيث يعمد الجاني من خلاله، إسناد مادة معينة إلى شخص ما قد يكون معنيا بذاته بحيث ينال من شرفه أو كرامته وتعرضه إلى بغض الناس واحتقارهم، خصوصا إذا ما اعتمد الجاني في ذلك على توزيع مضمون الرسالة الالكترونية إلى عدد غير محدد من المتعاملين مع الانترنت عن طريق رسائل البريد الالكتروني وقد يجد الجاني في شبكة الويب (web) العالمية وسيلة في إسناد مادة كتابية أو صوتية أو مرئية مسيئة لشخص ما ،

[1] - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة بمقر جامعة الدول العربية، مصر بتاريخ 21-12-2010.

فتنال عن شرفه وكرامته وتعرضه للاحتقار والذم من قبل الغير، كما أنها قد ترتكب عن طريق مواقع التواصل الاجتماعي (**Facebook**)أو (**Twitter**)أو (**Chatrooms**) أو (**Skype**).

2- استهداف مجموعة من الأفراد وحث الغير على كراهيتهم:

ويمكن أن تستهدف هذه الجرائم مجموعة من الأفراد جملة واحدة من خلال انتماءاتهم الدينية أو العقائدية أو العرقية، وهي النقطة الأساسية التي شكلت موضوع البروتوكول الإضافي لاتفاقية الجريمة الالكترونية بشان تجريم الأفعال ذات الطبيعة العنصرية، والتي تحرض على كراهية الأجانب والتي يرتكب عن طريق أنظمة الكمبيوتر المؤرخة في 28-01-2008 بستراسورغ بفرنسا والتي جاءت بفصلين الأول تضمن الأحكام العامة التي تبين الغرض الأساسي من هذا البروتوكول والثاني تكفل ببيان هذه الجرائم المعلوماتية وحصرها في السلوكات التالية:

- نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أنظمة الحاسوب.

-التهديد الذي تحركه دوافع التمييز العنصري وكراهية الأجانب.

- الاهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب.

-الانكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية.

ثانيا: جرائم التعدي على البيانات الشخصية:

إن احترام الحق في الحياة الخاصة يعد من المبادئ الدستورية الثابتة، بحيث يعد الدستور بان لحياة المواطنين الخاصة حرمة يحميها القانون فلكل شخص الحق في أن تظل أسرار حياته الخاصة محجوبة عن العلنية ومضمونة من تدخل الغير واستطلاعه، وتشكل الجريمة المعلوماتية مظهرا حديثا، يهدد بخطر محدق على البيانات الشخصية للأفراد من عدة زوايا تتمثل فيما يلي:

1- تجميع البيانات وتخزينها على نحو غير مشروع:

يتمثل فعل انتهاك الحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة منهم ولكن على نحو غير مشروع، ويستمد هذه الصفة غير المشروعة من الأساليب المستخدمة لأجل الحصول على هذه البيانات أو من حيث طبيعة هذه البيانات.[1]

أما من حيث الأساليب فقد يعمد الجاني على أسلوب التقاط ارتجاجات الجدران وترجمتها إلى عبارات وكلمات وذلك بواسطة معدات خاصة تغذي الحاسوب المزود ببرنامج خاص لترجمة كل ذلك، أو من خلال اعتراض الرسائل الالكترونية أو اختراق النظام المعلوماتي للضحية.

أما من حيث طبيعة البيانات فان البيانات الاسمية الخاصة يجب أن يحظر جمعها وتخزينها ومعالجتها داخل الحاسوب من قبل الغير، إضافة إلى المعلومات المتعلقة بالسجل القضائي التي لا يحق إلا للسلطة القضائية جمعها وتخزينها حفاظا على سمعة الشخص.

[1] نهلا عبد القادر المومني، المرجع السابق، ص174.

2- إساءة استعمال البيانات والمعلومات الاسمية (انتحال الشخصية):

ترتكز جريمة انتحال الشخصية على مبدأ النقدي على البيانات الاسمية للغير من اجل التخفي والتهرب من المسؤولية، أي الإفلات من المتابعة الجزائية، أي هي استخدام بيانات شخصية للغير من اجل الوصول إلى هدف غير مشروع يتمثل في جريمة تحقق الربح المادي لمفترقها، دون أن يكون هو المتابع بشأنها، وقد أشارت الإحصائيات السنوية لسنة 2009 أن حوالي 210000 شخص في فرنسا قد وقعوا ضحايا هذا النوع من الإجرام عبر الانترنت، يقدر معدل نموها على مستوى الدول الغربية بـ40 % وتشكل هذه الجريمة جزءا من جرائم لاحتيال المعلوماتي،[1] فالفرد أصبح معرضا أكثر من أي وقت مضى لمخاطر انتحال هويته من قبل الغير بسبب اعتماده المطلق أو الشبه الدائم على تقنية المعلوماتية وشبكة الانترنت خصوصا،ضف إلى ذلك أن وسائل التحقق من الشخصية عبر الانترنت هي غير تلك المتبعة أمام الجهات الرسمية.

3- إفشاء الأسرار والبيانات والمعلومات الاسمية:

إن هذا النوع من السلوكات الإجرامية قد يكون نتيجة حتمية الجرائم السابق ذكرها، بان البيانات الخاصة قد انتقلت من السر إلى العلانية، بمجرد تخزينها بعد تجميعها على نحو غير مشروع أو حتى بصفة مشروعة وبالتالي فإنها تكون عرضة للاطلاع عليها من قبل عدد غير محدد العدد من الأشخاص في حال عرضها على شبكة الانترنت أو على الأقل من قبل عدد محدد متمثل في الأشخاص العاملين في فضاء المعلوماتية.

[1] القاضي: أسامة احمد المناعسة، القلاعي: جلال محمد الزعبي، المرجع السابق،ص260.

الفرع الثالث: جرائم الاستغلال الجنسي للأطفال عبر الانترنت

امتدت نوازع البشر ومظاهر الإجرام الإلكتروني لتطال فئة عمرية تحظى أصلا بالحماية والرعاية الخاصة إن كان على المستوى الاجتماعي أو القانوني نظرا لحداثة السن وقلة الخبرة ،وهذه الفئة هي فئة القصر في المجتمع ونحن إذ نذكر لفظ المجتمع نقصدها أي مجتمع نظرا لاتحاد الصفة والغاية والحاجة والحماية بالرعاية.

ويندرج ضمن مفهوم القاصر من وجهة نظر القانون كل من لم يصل سن البلوغ وهو تسعة عشر سنة كاملة ذكورا وإناثا وفقا لأحكام القانون على أن تراعى المفروقات بتحديد سن البلوغ لدى بعض التشريعات المقارنة.

فمع اتساع نطاق بيئة الانترنت وتنوع الأنشطة والمهارات المتعلقة بها،ودخول فئات عمرية حديثة مجالات واسعة لتقنية نظم المعلومات ،سيما للاستفادة من خدمات هذه التقنية،خصوصا منها تقنية الانترنت ،واعتمادهم عليها،وبغياب وعي الأهل والبيئة المحيطة وقلة المراقبة فقد أصبح القاصرون موضوع اعتداءات متكررة،آخذه بالاتساع بإتباع تقنية نظم المعلومات واستخداماتها المختلفة [1].

استهداف القاصرين عبر الانترنت يتزايد مع مرور الزمان ،دون رادع أو زاجر حقيقي ،وهو يأخذ على العموم مظاهر الاستغلال الجنسي بمختلف صوره وأشكاله.

[1]– القاضي،أسامة أحمد المناعسة،القاضي جلال محمد الزغبي ،المرجع السابق، ص26.

توفر تقنية الانترنت ومواقع مشبوهة بواقة ذات جذب عليها ومنتدياتها المواد الأساسية التي تصيد عناوين البريد الإلكتروني الخاصة بمرتاديها من الأطفال القاصرين ،والتي تلعب دورا رئيسيا في اتساع نسبة استغلال القصر جنسيا عبر الانترنت حيث يأخذ الصور التالية.

أولا– تحريض القاصرين على الأعمال الجنسية

هناك مواقع على شبكة الانترنت للكافة،متخصصة بالجنس ذات بوابات ونوافذ مغرية للقاصرين،يتم الوصول إليها مباشرة عبر إدخال العنوان الإلكتروني في شريط العناوين ،حيث يبدأ الموقع بعرض مواده تلقائيا والخطير أن معظم هكذا مواقع مجانية يمكن الدخول إليها بمطلق السهولة ودون تكلفة مادية تذكر.

النافذة الأخرى أكثر خطورة إذ تتيح تقنية تلك المواقع الدخول إليها أو عبر مواقع أخرى ،يصدق أن المتصفح يعمل عليها ،ذلك أثناء أو عبر الاشتراك باتصال مع مواقع أخرى،حيث لا يجد القاصر نفسه إلا وهو داخل موقع الإباحة الجنسية.

وهناك وحين يدخل القاصر إلى موقع ما يتعلق بمواد الإباحة الجنسية يجد نفسه فريسة سهلة لمروجي هذه التجارة،تعرض تلك المواقع فرص للاتصال الجنسي ،وتمهد له وتعرض مساعدات تقنية هاتفية وأخرى ذات علاقة بترتيب لقاءات وهمية مع الطرف الآخر،وذلك للقيام بعمل جنسي معين،وفق منظومة وصور ومقاطع فيديو نصف الحال،بهدف بصورة منفردة أو بصورة جماعية

،وغالبا ما تدفع تلك المواقع القاصرين لدخول مواقعها من خلال الوعد بجائزة أو مسابقة مغرية ونحو ذلك [1].

ثانيا: إنتاج صور فاضحة للقاصرين

تتنوع صور الإنتاج بحد ذاتها مستخدمه تقنية الانترنت والحاسب الآلي وتضع هذه التقنية بين يدي الفاعل منظومة غير محدد لسبيل إنتاج صور جنسية فاضحة للقاصرين ذكورا أو إناثا بعضها قد يكون حقيقيا حصل عليه الفاعل بطرق غير مشروعة ،بروجها كما هي ،وأخرى وهي الأكثر الأعم صور ومقاطع غير حقيقية تدخل منظومة تقنيات الدبلاج والتحوير نحو ذلك ثم يعاد استغلال المنتج مرة أخرى في الجريمة واستغلال القاصرين بها.

فإذا توافرت الصورة الفاضحة المعينة بطريق الإنتاج ،انتقل الفاعل إلى مظاهر الاستغلال المرتبطة بذلك فعملية الإنتاج ليست مقصودة بذاتها ،بقدر ما هي خطوة إلى تحقيق استغلال القاصرين هنا يكون بأحد أمرين.

الأمر الأول: أن يكون القاصر هو مادة الإنتاج الجنسي ،سواء تمثل ذلك بالصور الفوتوغرافية أو مقاطع الفيديو ثم إعادة ترويج تلك الصور أو مقاطع الفيديو إلى الأخذ عبر شبكات تقنية نظم المعلومات.

الأمر الثاني: أن يكون القاصر هو الهدف ومن الاستغلال ومادته في آن معا،فمخرجات الإنتاج صور كانت أو مقاطع فيديو توجه هنا إلى القصر عبر ما يستجمع لدى الفاعل من عناوين ومواقع

[1] – القاضي،أسامة أحمد المناعسة،القاضي جلال محمد الزغبي ،المرجع السابق، ص262.

إلكترونية مدعمة بتقنية إلكترونية معلوماتية كافية لتأكيد إيصال المنتج عبر المشروع إلى القاصر حيثما كان[1].

ثالثا: استغلال الأطفال القاصرين جنسيا

لابد ابتداء أن تتوافر حالة فاضحة لأحد القاصرين ذكرا كان أم أنثى بين يدي الفاعل فالشرط هنا أن تكون المادة الفاضحة ذات علاقة بالقاصر ،من حيث اعتباره موضوعا لها ،فهو محور بنائها مما يظهر لنا تعاظم الاستغلال غير المشروع للقاصرين عبر تقنية نظم المعلومات واعتبارهم وسيلة الاعتداء وموضوعة في آن معا:

ثم لابد من استغلال ذلك بإحدى الصور التالية:

- توزيع الصور الفاضحة عبر منظومة الانترنت.
- بيع وتداول الصور الفاضحة عبر منظومة الانترنت.
- نشر الصور الفاضحة عبر منظومة الانترنت.
- بث الصور الفاضحة عبر منظومة الانترنت.

ويستوي هنا أن يحصل الفاعل على الصور الفاضحة للقاصرين لمنفعته الخاصة وبغية استغلالها الشخصي أو لمنفعة الغير أو لاستغلال الغير الخاص، أو حق لغايات استثمارية،المهم إلا فقد في مفهومها للاستغلال إلا انه لايشمل كافة الصور خصوصا مع دخول تقنية نظم المعلومات وتطور

[1]- القاضي،أسامة أحمد المناعسة،القاضي جلال محمد الزغبي ،المرجع السابق، ص263.

وسائل الاتصالات التقنية المتعلقة بانتساب المعلومات والمواد المسجلة الكترونيا وبأتساع نطاق توزيعها عبر العالم[1].

رابـعا: أعمـــال الدعـــارة والتـــرويج لـها.

لا يقتصر استغلل القاصرين جنسيا عبر شبكة الانترنت على حالات إنتاج صور إباحية خاصة بهم ،ونشوتها أو بثها أو تداولها عبر الشبكة وإنما قد يتخذ الاستغلال صور ارتكاب القصر لأعمال الدعارة وإظهار ذلك من خلال صور أو أفلام مصورة تطهرهم بحالات القيام بأعمال جنسية مختلفة ،سواء مع بعضهم البعض أو مع بالغين ليس هذا وحسب بل قد تتخذ أعمال الدعارة هنا استهداف القاصرين بأفلام وصور جنسية للبالغين تمرر عبر وسيلة اتصال معنية ،أو عبر تقنية شبكة الانترنت للقاصرين ،بحث يضمن عملهم بها سواء اختراقات منظمة مسبقا في حال دخول القاصرين عبر مواقع أخرى معينة قد لا تكون موثوقة أو عبر اختراق البريد الإلكتروني الخاص بأحد القاصرين ،وإرسال ملفات ذات محتوى جنسي له.

ويتسع فعل الترويج ليطال سائر صور وأشكال العرض الالكتروني للصور ومقاطع الفيديو والنشر والتوزيع والطباعة والإنتاج والتوفير والشراء والبيع والاستيراد الذي محله مواد إباحية[2].

[1]- القاضي،أسامة أحمد المناعسة،القاضي جلال محمد الزغبي ،المرجع السابق، ص265.

[2]- نفـسه ،ص 265.

الفصل الثاني

تهدف هذه الدراسة إلى التعريف بالإطار القانوني للنظام المعلوماتي في الجزائر، إذ عرف نظام المعلوماتية تطورا بطيئا في الجزائر بالرغم من الإمكانيات الاقتصادية و المالية و البشرية التي يزخر بها مقارنة بالكثير من دول العالم الثالث، و خاصة بجيرانها من دول المغرب العربي، فلم يكن المشكل يكمن في مجال نقص العتاد المعلوماتي بقدر ما هو التخطيط العقلاني المساير للواقع، ناهيك عن تأخر صدور قوانين لتنظيم الشبكة المعلوماتية عكس الشبكة الاتصالية التي وضعت لها قوانين واكبت التطور.

و قد مرت الجزائر بعدة مراحل، من أواخر الستينات(1968) التي بدأ فيها استخدام أجهزة الكمبيوتر إلى سنة 2004 تميزت بفراغ قانوني في مجال المعلوماتية بصفة خاصة و تكنولوجيا الإعلام و الاتصال بصفة عامة، و لمسايرة التطور التكنولوجي كان لابد للجزائر على غرار الدول المتقدمة من إيجاد الإطار القانوني المناسب، بدءا بصدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات الذي نص على حماية جزائية لأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات (الدخول غيرا لمشروع لأنظمة المعلوماتية، تغيير أو إتلاف المعطيات...) و يليه القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها. بالإضافة إلى الاتفاقيات الدولية ذات الصلة التي صادقت عليها الجزائر، كل هذه النصوص تشكل المنظومة القانونية للمعلوماتية في الجزائر.

و كل هذا جاء من أجل وضع النصوص الملائمة لمختلف الاستعمالات المعلوماتية و تكنولوجيا الإعلام و الاتصال، و في نفس السياق تم وضع قوانين خاصة لمواجهة ما يسمى بالجرم المعلوماتي أو الجرائم الإلكترونية.

لكن يبقى التنظيم القانوني الخاص بنظام المعلوماتية بصفة خاصة و تكنولوجيات الإعلام و الاتصال بصفة عامة رهينا بالتصحيح المطلوب و بوضع سياسة رشيدة من خلال الممارسة و التطبيق في الميدان.

المبحث الأول: القواعد الموضوعية لمكافحة جريمة الالكترونية

إن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فانه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية .

فما هي التشريعات الوطنية والاتفاقيات التي كانت تطبق في مجال المعلوماتية ؟

في الواقع هناك تشريعات واتفاقيات عديدة ؛ منها الأمر رقم 66 -156المؤرخ في 8 يونيو والمتضمن قانون العقوبات المعدل والمتمم 1966 والأمر رقم66-155 المؤرخ في 8 يونيو 1966والمتضمن قانون الإجراءات الجزائية المعدل والمتمم. والأمر رقم 75 - 58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني المعدل والمتمم[1].

والقانون رقم 08 -09 المؤرخ في 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية .

[1]- الأمر رقم 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية 25 فبراير 1966، العدد 16، الصفحة 198

والقانون رقم 2000 – 03 المؤرخ في 5 غشت سنة 2000 الذي يتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية المعدل و المتمم. والأمر رقم 03 -05 المؤرخ في 19يوليو 2003 و المتعلق بحقوق المؤلف والحقوق المجاورة.

ثم هناك جملة من الاتفاقيات الدولية التي صادقت عليها الجزائر، أصبحت تعتبر من النظام القانوني الجزائري، طبقا للمادة 132 من دستور سنة 1989 المعدل، وطبقا لقرارات وآراء المجلس الدستوري، مما يجعل الاتفاقيات المصادق عليها نافذة في الجزائر .ومن أهم هذه الاتفاقيات الدولية نذكر : اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883[1] و المعدلة ، الاتفاقية العالمية لسنة 1952 حول حق المؤلف والمراجعة بباريس في 24 يوليو 1971[2] ، اتفاقية إنشاء المنظمة العالمية للملكية الفكرية الموقعة باستكهولم في 14 يوليو1967[3]، اتفاقية بارن (Berne) لحماية المصنفات الأدبية والفنية المؤرخة في 9 سبتمبر 1886[4] المتممة والمعدلة بالإضافة إلى الانضمام إلى كل التوصيات والبروتوكولات المتعلقة بتكنولوجيات الإعلام والاتصال كبروتوكولات ونظام إدارة الشبكة الدولية للانترنت ICANN ... وإن كان للجزائر مواقف

[1] -الأمر رقم 66-48 المؤرخ في 25 فبراير 1966 المتضمن انضمام الجزائر إلى اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 و المعدلة، الجريدة الرسمية 25 فبراير 1966، العدد 16، الصفحة 198

[2] – الأمر رقم73- 26المؤرخ في 5 يونيو 1973 المتعلق بانضمام الجزائر إلى الاتفاقية العالمية لسنة 1952 حول حق المؤلف والمراجعة بباريس في 24 يوليو1971 ، الجريدة الرسمية 3 يوليو1973 ، العدد53 ، الصفحة762 .

[3] – الأمر رقم75- 2 المؤرخ في 9 يناير 1975 المتضمن المصادقة على اتفاقية باريس لحماية الملكية الصناعية المبرمة في 20 مارس 1883 (و المعدلة)، الجريدة الرسمية 4 فبراير 1975، العدد 10، الصفحة 154.

[4] – المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997 المتضمن انضمام الجزائر، مع التحفظ، إلى اتفاقية بارن (Berne) لحماية المصنفات الأدبية و الفنية المؤرخة في 9 سبتمبر 1886 المتممة و المعدلة،الجريدة الرسمية 14 فبراير 1975،العدد 61، الصفحة 8.

من القانون الدولي ، فقد تحفظت بشأن العديد من الاتفاقيات الدولية ؛ ونشير هنا إلى عدم انضمام الجزائر إلى الاتفاقية الدولية لمحاربة الجرائم الإلكترونية لبودابيست2001 .

وفي الجزائر تم سد الفراغ القانوني الذي عرفه هذا المجال بصدور القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائية لأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات) الدخول غير المشروع لأنظمة المعلوماتية، تغيير أو إتلاف المعطيات (... ويأتي مشروع هذا القانون لتعزيز نفس هذه القواعد، من خلال وضع إطار قانوني أكثر ملاءمة مع خصوصية الجريمة الافتراضية ليسبقه في ذلك القانون رقم 2000-03 المتضمن القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية المعدل و المتمم.

وقد جاء قانون رقم 09-04 مؤرخ في 5 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، آخذًا بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة ، لذلك تم اختيار عنوان القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذه التكنولوجيا ، كما أن التركيز على مجالي الإعلام والاتصال يبين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه.

المطلب الأول: الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات الجزائري

لم تعرف الجزائر قوانين – قبل - 2004 تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيات الإعلام والاتصال، ما عدا شبكة الاتصالات السلكية واللاسلكية ووسائل الإعلام السمعية والبصرية.

فقد عرف نظام المعلوماتية تطورا بطيئا في الجزائر بالرغم من الإمكانيات الاقتصادية والمالية والبشرية التي تزخر بها مقارنة بجيرانها من دول المغرب العربي ، بخاصة المغرب وتونس ، ليس في مجال نقص العتاد المعلوماتي بقدر ما هو في وضع سياسة رشيدة في التطبيق، ناهيك عن تأخر صدور قوانين لتنظيم الشبكة المعلوماتية عكس الشبكة الاتصالية . وفي هذا الصدد، وبصدور أحكام تضمنت تعديل قانون العقوبات كل هذا يطرح جملة من العناصر تتمثل في تحديد بعض المفاهيم المتعلقة بالجريمة المعلوماتية، حيث سنركز في دراستنا على الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال و كذا تلك المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات[1].

الفرع الأول: الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال المقررة في قانون العقوبات الجزائري

إذا كانت الجريمة المعلوماتية ظاهرة مستحدثة لها جانب مادي معلوماتي فهل يستطيع القاضي الجزائي من خلال النصوص الحالية لجرائم الأموال تحقيق حماية جزائية معلوماتية دون

[1] - أمال قارة ، **الحماية الجزائية للمعلوماتية في التشريع الجزائري** ، دار هومة للطباعة والنشر ، الجزائر 2006،ص10.

الإطاحة بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي ؟ ولهذا الغرض ارتأينا تركيز دراستنا على نقطتين أساسيتين وهما :

1-مدى اعتبار المعلوماتية موضوع لجرائم الأموال.

2-مدى خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال.

أولا: مدى اعتبار المعلوماتية موضوعا لجرائم الأموال

لتحديد مدى إمكانية إخضاع الاعتداءات الواردة على أموال الإعلام الآلي للنصوص التقليدية لجرائم الأموال وجب :

أ- مدى انطباق وصف المال على المعلوماتية : يقصد بالمال ألمعلوماتي الحاسوب بكل مكوناته وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب وهو يتكون من كيانين كيان مادي وكيان معنوي.

و يضم الكيان المادي الأجهزة المادية المختلفة وهي جهاز الإدخال، جهاز الإخراج ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلومات وتخزينها و إخراجها. أما الكيان المعنوي فيشمل البرامج المختلفة التي تتحقق من خلالها قيام الحاسب بوظائفها المختلفة بالإضافة إلى المعلومات المطلوب معالجتها بالفعل [1].

فإذا كانت الأجهزة المادية للحاسبات لا تحتاج إلى نصوص خاصة لحمايتها جزائيا إذ تشملها نصوص الجرائم التقليدية ، فالأمر يختلف بصدد الكيان المعنوي لتلك الحاسبات لان

[1] - د. محمد فتحي عبد الهادي، **مقدمة في علم المعلومات**، مكتبة غريب، القاهرة 1984، ص 217.

جرائم الاعتداء على الأموال يشترط بشأنها عادة أن يكون موضوعها شيئا ماديا ، وطبيعة الكيان المعنوي ليس كذلك وعليه فالسؤال يطرح حول مدى اعتبار الكيان المعنوي للحاسوب مالا [1].

المال هو كل ما يصلح أن يكون محلا للحق ذو القيمة المالية والشيء هو محل الحق ،وتقسم الأشياء، إلى أشياء مادية وأشياء غير مادية أو معنوية، علما بان الأموال من وجهة النظر التقليدية لا ترد على أشياء مادية ولهذا كان تعريف المال بصدد جرائم الأموال بأنه " كل شيء مادي يصلح لان يكون محلا حق من الحقوق المالية" .

ولكن مع التطور ازدادت الأشياء المعنوية عددا وتفوق بعضها من حيث قيمتها على الأشياء المادية مما استدعى البحث عن معيار أخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي.

ومن هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الآلي –هذه البرامج تكون عادة مثبتة على دعامة أو حامل SUPPORT –مثل الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى أو أي مادة أخرى .

والبرنامج المستقل عن دعامته لا جدال في انه شيء معنوي وبالتالي لا يصدق عليه وصف المال طبقا للتحديد التقليدي للاموا ل الذي يشترط أن يكون محله شيئا ماديا، أما إذا سجل البرنامج أو نقش على دعامته فان تلك الدعامة بما عليها من برامج تصلح لان تكون محلا لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرنامج تعتبر ضئيلة القيمة إذا ما قيست بقيمة

[1] – أمال قارة ، المرجع السابق،ص12.

البرنامج وعلى الرغم أيضا من أن الاعتداء عليها ليس في غاية في ذاته، وإنما الباعث على ذلك هو البرنامج نفسه لا دعامته ومع ذلك لا تأثير لهذه البواعث في القانون الجنائي [1]

ويعتبر الاعتداء على الدعامة في هذه الحالة قد وقع على شيء مادي مما يصلح تكييفه حسب النشاط الإجرامي بإحدى جرائم الأموال التي يتطابق نموذجها مع هذا النشاط ، أما إذا وقع الاعتداء على البرنامج مستقلا عن دعامته ،فان الأمر يختلف حيث يكون قد وقع على شيء معنوي ،هذا الشيء المعنوي لابد وان تثبت له صفة المال أولا حتى يمكن البحث بعد ذلك في مدى إمكانية وقوع جرائم الأموال عليه .

و قد انقسم الفقه في هذا الصدد إلى اتجاهين:

- الإتجاه الأول: الفقه المؤيد لإضفاء وصف المال على البرنامج

يرى جانب من الفقه أن المعلومات صالحة لأن تكون محلا للاعتداء عليها طالما كانت هذه المعلومات تعكس الرأي الشخصي لصاحبها ولا تتوقف عند نطاق المعلومات العامة ، وذلك على أساس أن هذه المعلومات صادرة عن صاحبها أي أنها ترتبط بشخصيته وهو الذي فكر فيه ،أو هذا يعني أنها من الحقوق اللصيقة بشخصية صاحبها ،وهذه المعلومات ذاتها هي موضوع هذا الحق ومن خصائصها القابلية للانتقال وهذا يعني أن هناك طرفا أخر يستقبل هذه المعلومات ،ومن هنا تنشا علاقات إما بينها وبين صاحبها وأما بين صاحبها والغير، فالمعلومات باعتبارها نتاجا

[1] – د. علي عبد الله القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية للطباعة والنشر، بيروت، 1999، ص7.

ذهنيا لمن يعطيها شكل المعلومة فهي تعد محور العلاقات مثل تلك التي تنشا بين المالك وبين ما يملك فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها. ومن أمثلة هذه المعلومات برامج الحاسب الآلي ،إذ أن هذه البرامج ترتب حقوقا لصاحبها وتخول له إبرام عقود متعلقة بها مثل الإيجار والبيع والحفظ وأي صورة أخرى من صور الاستغلال، لان من خصائصها القابلية للانتقال

كل هذه التصرفات والحقوق هي التي دفعت جانبا من الفقه إلى القول بان المعلومات مال ليس فقط لوجود علاقة حق استئثار خاص عليها، وإنما أيضا لأنها تعتبر قيمة اقتصادية، فهي تطرح في السوق للتداول مثلها في ذلك مثل أي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادية .

وإذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال على أساس أنها غير مادية أي أن عدم مادية المعلومات هو الذي أدى إلى عدم الاعتراف لها بصفة المال فان الفقه الحديث يرى على العكس أن المعيار في اعتبار الشيء مالا، ليس على أساس ماله من كيان مادي وإنما على أساس قيمته الاقتصادية، وان القانون الذي يرفض إصباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع [1].

ومادامت البرامج في جوهرها معلومات معالجة بطريقة ما ولها قيمة اقتصادية فانه يجب معاملتها على أنها مال [2].ما يؤكد هذا المعنى أن المشرع الحديث يعترف لصاحب هذه المعلومات

[1] – أمال قارة، المرجع السابق، ص 18.

[2] – أمال قارة، المرجع السابق، ص 18.

بما يطلق عليه الحق في الملكية الفكرية ،ولولا أن المعلومات مالا ما كان المشرع ليستطيع التسليم لها بهذا الحق، وان كانت طبيعة هذه الملكية محل جدل فقهي [1] .فإنها على كل حال نوع من الملكية أو الحق الذي لصاحبه في القليل الحق في احتكار استغلال هذا المال غير المادي أي المعلومات والتي منها برامج الحاسب الآلي .

- الاتجاه الثاني: الفقه المعارض لإضفاء وصف المال على البرنامج

الجانب الأخر من الفقه يرى عدم صلاحية المعلومات لان تكون محلا للاعتداء عليها ، حيث ذهب جانب من الفقه في فرنسا إلى أن المعلومة في حالتها المجردة والفكرة في حد ذاتها لا تقبل التملك والاستئثار ،وان تداولها والانتفاع بها من حق الكافة دون تمييز ومن ثم لا يمكن أن تكون محلا للملكية الفكرية.

ويفرق البعض الأخر بين المعلومات والبيانات التي تمت معالجتها الكترونيا فيرون أن الأولى باعتبار أن عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها ، لها طبيعة غير مادية ولا سبيل من ثم إلى اختلاسها أما البيانات التي تمت معالجتها الكترونيا، فتتحدد في كيان مادي يتمثل في نبضات أو إشارات ممغنطة يمكن تخزينها على وسائط معينة ونقلها واستغلالها وإعادة إنتاجها فضلا عن إمكانية تقديرها كميا وقياسها فهي إذن ليست شيئا معنويا كالحقوق والآراء والأفكار بل شيئا له في العالم الخارجي المحسوس وجود مادي وفقا لهذا الرأي فان المعلومات إذا لم تعالج أليا عن طريق الحاسب لا تعتبر من قبيل الأموال الخاضعة للحماية الجنائية باعتبار أن هذه المعالجة تتم

[1] - د. عبد الرشيد مأمون، **الحق الأدبي للمؤلف، النظرية العامة وتطبيقاتها**، دار النهضة العربية، القاهرة 1978.

في صورة نبضات الكترونية ،مما يمكن القول معه بأنه لعملية المعالجة تلك تتحول من أموال معنوية إلى أموال مادية، الأمر الذي يخضعها للنصوص التقليدية لجرائم الأموال ،ويأخذ نفس حكمها البيانات المخزنة سواء في برامج الحاسب أو في ذاكرته وبالتالي تأخذ برامج وبيانات الحاسب وحكم الأموال عليه وبالتالي تتمتع بالحماية الجنائية المقررة لها .

إن اعتبار المعلومات مالا قابلا للتملك أو الاستغلال كما سبق أن وضحنا يزيل أمامنا عقبة كبيرة تسمى التملك. هذا النوع من الأموال إلى مجموعة الأموال التي يحميها القانون الجنائي والتي تتمثل في ضرورة أن يكون المال موضوع جرائم الاعتداء على الأموال شيئا منقولا مملوكا للغير، فانه يمكن إسباغ حماية النصوص التقليدية عليه وذلك على أساس أن هذه النصوص جاءت عامة ولم يشترط أن تقع جرائم الأموال على منقول مادي .وعليه يكون من المتصور أن تقع هذه الجرائم على مجال غير مادي طالما اعترف لها بصفة المال وقابلية التملك .وقد سايرت هذا الاتجاه محكمة النقض الفرنسية في العديد من أحكامها [1].

ب– مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال:

ذكرنا أنفا أن برامج الحاسب وفقا للفقه الراجح ينطبق عليها وصف المال فإذا كانت المعلومات شيئا منقولا لا مملوكا للغير إلا أنها شيء غير مادي فهل تدخل البرامج استنادا إلى هذه الصفة تحت مفهوم الشيء الذي يصلح محلا لجرائم الأموال ؟

[1] – د. علي عبد القادر القهوجي، **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية للطباعة والنشر ،بيروت،1999،ص 23.

أ–1 مدى اعتبار البرنامج مالا بصدد جريمة السرقة:

طبقا للمادة 350 من قانون العقوبات الجزائري فان "كل من اختلس شيئا غير مملوك له يعد سارقا " نص المادة 350 لم يشترط صراحة ضرورة أن يكون المال موضوع الجريمة ماديا مما يجعل وقوع جريمة السرقة على مال معنوي أمرا لا يصطدم بمبدأ شرعية الجرائم والعقوبات .

يجد هذا الرأي تسويغه في أن الشيء وهو محل السرقة حسبما يصفه نموذجها في التشريع الجزائري لا يقتصر لورود لفظه بغير نعت أو تخصيص على الأشياء المادية المجسمة فحسب بل يشمل الأشياء غير المادية كذلك، وهذا التفسير الراجح فقها ، ولكن يبقى اعتبار البرنامج كمحل للسرقة غير قطعي ومن باب الإمكان لا غير .

أ–2 مدى اعتبار البرنامج كمحل لجريمة النصب :

طبقا للمادة 372 من قانون العقوبات الجزائري فان "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل بالفوز بأي شيء أو في وقوع حاد أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 20000 إلى 100000 دج ".

نستنتج من نص المادة 372 بأنه ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي عددتها المادة 372 على سبيل الحصر.

تجدر الإشارة إلى أن النص على المنقول ورد دون تحديد لطبيعته ودون أن يقيده المشرع بان يكون ماديا مما يسمح بتفسير هذا النص على نحو يسمح بدخول برامج الحاسب ضمن الأشياء التي تقع عليها جريمة النصب إلا انه حتى وان أخذنا بهذا التفسير، نصطدم بعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام ،وحتى على فرض أن التسليم قد تم ،فان المجني عليه لا يحرم من حيازة البرنامج والبيانات التي تبقى تحت سيطرته التامة .

أ–3 مدى اعتبار البرنامج كمحل لجريمة خيانة الأمانة :

طبقا للمادة 376 من قانون العقوبات الجزائري " كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل بأجر أو بغير اجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين وذلك إضرارا بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة ...." .

يستنتج من نص المادة 376 إن الاختلاس يقع على مال منقول سلم إلى الجاني بمقتضى عقد من عقود الأمانة، وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية.

وقد حددت المادة 376 الأشياء التي تصلح محلا لهذه الجريمة وهي على سبيل الحصر أوراق تجارية ، نقود بضائع ،أوراق مالية ، مخالصات ،محررات تتضمن أو تثبت التزاما أو ابرء وعليه فان إخضاع الاعتداءات الواردة على المال ألمعلوماتي إلى نصوص خيانة الأمانة يثير بعض المشاكل القانونية نظرا للطبيعة غير المادية للقيم في حقل الجريمة المعلوماتية .

الحل الوحيد هو الاقتداء بما اخذ به القضاء الفرنسي باعتباره بعض القيم في المجال المعلوماتي من قبيل(البضائع) أي التوسع في مفهوم البضاعة، وعليه فان تطبيق نصوص خيانة الأمانة في مجال المعلوماتية يكون في نطاق محدود ومن باب الإمكان لا غير .

أ–4 مدى اعتبار البرنامج كمحل لجريمة الإتلاف :

طبقا للمادة 407 من قانون العقوبات الجزائري "كل من خرب أو اتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأية وسيلة أخرى كليا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20000 إلى 100000 دج".

كما تنص المادة 412 من قانون العقوبات الجزائري "كل من اتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة وذلك بواسطة مواد من شانها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة 20000 دج إلى 100000 دج".

بالرجوع إلى نص المادة 412 نجدها قد حددت الأشياء الخاضعة للإتلاف وبالتالي فإنها تشمل المكونات المادية للحاسوب سواء بوصفها أجهزة أو بضائع .كما أن الكيان المنطقي يمكن أن يخضع لهذا النص ألتجريمي باعتباره مالا بالنظر لما له من قيمة اقتصادية .

ثانيا: مدى خضوع المعلومات للنشاط الإجرامي لجرائم الأموال

إذا كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال فإننا سنحاول دراسة مدى خضوع برامج الحاسب الآلي أو المعلومات بصفة عامة للسلوك الإجرامي الذي يتحقق به الركن المادي في جرائم السرقة والنصب وخيانة الأمانة والإتلاف.

أ- مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة :

بالنسبة للنشاط الإجرامي المكون لجريمة السرقة وهو الاختلاس وبتطبيقه على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة ، نلاحظ أن الجاني وان كان يدخل في ذمته ما استولى عليه من برامج إلا انه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون انتقاص من محتواها ، كما يلاحظ إن الاستيلاء على البرامج باعتبارها معلومات لا يتصور من الوهلة الأولى إلا على انه انتقال لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة [1] وهذه عقبة ثانية ويلاحظ ثالثا أن المعلومات التي تحويها البرامج من طبيعة غير المادية أي أنها شيء معنوي فكيف يتصور أن يرد

[1]- د. علي عبد القادر القهوجي، المرجع السابق، ص 95.

فعل الاختلاس الذي هو من طبيعة مادية على شيء معنوي وهذه عقبة ثالثة. نتيجة لهذه العقبات فليس من السهل بسط أحكام السرقة على برامج الحاسب الآلي وخاصة في الحالات التالية :

أ-1 سرقة المعلومات عن طريق النسخ غير المشروع للبيانات المخزنة الكترونيا:

أي عن طريق إعادة إنتاج الوثيقة أو الدعامة التي تحتويها، لمحاولة بسط أحكام السرقة على حالات النسخ غير المشروع يمكننا اعتماد ما توصل إليه الاجتهاد القضائي الفرنسي في هذا الصدد بإعلانه صراحة أن المعلومات التي نسخت أو أعيد إنتاجها هي التي سرقت كما انه لم يخرج عن مبدأ الشرعية الجنائية وحافظ على مبدأ مادية الاختلاس وعلاوة على ذلك فان إقرار الحكم باختلاسه المعلومات عن طريق إعادة إنتاج المستند الذي يحويها يحمل في طياته ثروة مستترة ولكنها عميقة لأنها تسمح بالعقاب على إعادة الإنتاج الذي لا يمكن أن يقع تحت طائلة جريمة التقليد .

وتجدر الإشارة إلا انه لا يجب الخلط بين جريمة سرقة المعلومات عن طريق النسخ غير المشروع وبين جريمة التقليد لان السرقة تحوي البيانات في ذاتها، بينما تنصب الحماية التي يكفلها المشرع للمصنفات بتجريم تقليدها على طريقة التعبير عن أفكار المؤلف [1] .

أ-2 سرقة وقت الآلة :

يكيفها فقهاء القانون الجنائي على أنها سرقة استعمال ، وفي هذه الحالة ليس من السهل بسط أحكام جريمة السرقة على وقت الآلة لان المشرع الجزائري لا يأخذ بما يسمى سرقة الخدمة وعليه

[1] – أمال قارة، المرجع السابق، ص 26.

تتطلب تدخلا تشريعيا على غرار ما فعل المشرع الفرنسي بتجريمه البقاء غير المشروع في نظام المعالجة الآلية للمعطيات ، فإذا كانت هذه الجريمة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة إلا أنها تحقق أيضا وبصورة غير مباشرة حماية للمعلومات ذاتها .

أ–3 الالتقاط الذهني للبيانات :

كأن يقوم شخص بالتقاط معلومات ظهرت على شاشة الحاسب وقام بحفظها و اختزانها في ذاكرته ، هذا المسلك يمكن أن يكون اختلاسا رغم انه لم يرد على ذات مادة المستند وإنما اقتصر الشيء المختلس على مضمون المستند مع بقائه في حيازة صاحبه لان هذا المضمون شيء منقول مملوك للغير منحصر في منفعة المستند كجزء من حق صاحبه في ملكيته ، إلا إن المشرع الجزائري لا يأخذ بسرقة الاستعمال وعليه ضرورة تدخل تشريعي يشمل حالتي الالتقاط الذهني للبيانات وحالة سرقة المعطيات دون استنساخها ودون المساس بسلامتها أو أصالتها [1] .

أ–4 تكييف الالتقاط الهوائي للبيانات المعالجة أو المنقولة الكترونيا:

من المعلوم أن الطاقة والقوى الطبيعية أو الصناعية تعد من الأموال المنقولة وتصلح لان تكون محلا للسرقة إلا انه لا يمكننا أن نطبق أحكام سرقة الطاقة على الإشعاعات والموجات والنبضات المنبعثة من الحاسب الآلي أثناء تشغيله رغم أنها كهربائيا قابلة للقياس والتقدير الكمي وذات قيمة.

[1] – أمال قارة، المرجع السابق، ص 23.

ولهذا نخلص لعدم وقوع السرقة في الحالات السابقة لأن طبيعة البرامج والمعلومات تأبى تحقيق الأخذ أو الاختلاس بمعناه الدقيق المسلم به في جريمة السرقة والذي يعني الاستيلاء على الحيازة الكاملة للشيء بدون رضا مالكه أو حائزه السابق لأنه إذا تصورنا وقوع الاختلاس من خلال النسخ أو التصوير على المعلومات فان هذه المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته ، ولما كان قانون العقوبات الجزائري لا يجرم سرقة الاستعمال بصفة عامة ، فان المخرج الوحيد لا يكون إلا بتدخل صريح من المشرع، لتفادي الجدل حول سرقة المعلومات وسرقة وقت الآلة أو سرقة استعمال الأصل وتحقق حماية مباشرة للبرامج والمعلومات .

ب– مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم النصب وخيانة الأمانة والإتـلاف :

ب–1 بتطبيق النشاط الإجرامي لجريمة النصب في المجال المعلوماتي :

نجد أن لجوء الجاني إلى إحدى الطرق الاحتيالية وحمل المجني عليه على تسليمه دعامة مادية مثبتا عليها احد البرامج ثم استيلاء الجاني عليها فان النشاط الإجرامي في جريمة النصب يتحقق .لكن هل من المتصور أن يتحقق النشاط الإجرامي لجريمة النصب من خلال الطرق الاحتيالية التي يلجا إليها الجاني والتي يترتب عليها وقوع المجني عليه في غلط يدفعه إلى أن ينقل إليه شفويا أي عن طريق القول محتويات برنامجه الذي يلتقطه الجاني ويحفظه في ذاكرته ؟.

هل النقل من خلال القول يعادل التسليم بناء على غلط منصوص عليه في م 376 من قانون العقوبات؟ وهل التقاط أو سماع الجاني للمعلومات يعادل الاستيلاء ؟

لا يوجد نشاط مادي يتحقق به التسليم والاستلام في جريمة النصب ، وحتى لو فرضنا جدلا إمكانية وقوع التسليم والاستلام، فانه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته وهو أمر وان كان يتفق وطبيعة البرامج والمعلومات إلا انه لا يتفق و طبيعة النشاط الإجرامي في جريمة النصب وهذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب .

ب-2 بتطبيق النشاط الإجرامي لجريمة خيانة الأمانة في المجال المعلوماتي :

نجد انه تطبيق نسبي فلا جدال في وقوع جريمة خيانة الأمانة بالنسبة للدعامات المثبتة عليها البرامج والمعلومات وذلك في الحالة التي يقوم فيها الأمين بنسخ البرنامج لحسابه الخاص متجاوزا الاتفاق الذي يربطه بصاحب البرنامج إذ يتحقق بهذا النسخ فعل الاستعمال والذي يقصد به استخدام الأمين للمال استخداما يستنزف قيمته كلها أو بعضها مع بقاء مادته على حالها إلا انه من الصعب القول بقيام جريمة خيانة الأمانة في حالة البرامج والمعلومات المستقلة عن الدعامة وذلك لعدم إمكانية قيام النشاط الإجرامي للجريمة ألا وهو التسليم بناء على عقد من عقود الأمانة لعدم وجود نشاط مادي مجسم يتحقق به فعل الاستلام، مما يحول دون صلاحية البرامج والمعلومات للخضوع للنشاط الإجرامي في جريمة خيانة الأمانة [1].

[1] – أمال قارة، المرجع السابق، ص 45-60.

ب–3 بتطبيق النشاط الإجرامي لجريمة الإتلاف في المجال المعلوماتي:

نجد أن المشرع الجزائري لم يقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة إذ هي من الجرائم ذات القالب الحر ولهذا لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج الحاسب الآلي خاصة وان المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة وحيدة محددة لقيامها، فانه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرنامج والدعامة المسجل عليهما معا ،أو إلى البرنامج فقط دون الدعامة، وقد تقع الجريمة عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد .

و عليه فان جريمة الإتلاف المنصوص عليها في قانون العقوبات تحقق حماية جنائية كاملة لبرامج الحاسب على خلاف باقي جرائم الأموال التي توفر حماية نسبية فقط.

الفرع الثاني: الحماية الجزائية للجريمة الالكترونية من خلال النصوص المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات

- لما كانت الحاجة ملحة و ضرورية لحماية المال المعلوماتي، فقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض، و قد استجابت عدة دول لهذا الاتجاه منها الولايات المتحدة الأمريكية، كندا، ألمانيا، النرويج و فرنسا...الخ . وقد تدارك المشرع الجزائري مؤخرا – ولو نسبيا– الفراغ القانوني في مجال الإجرام لمعلوماتي و ذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 15/04المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات و أحدث بذلك القسم السابع مكرر والذي شمل المواد من 394

مكرر إلى 394 مكرر7، متتبعا في ذلك خطى التشريعات الغربية التي اتجهت في وقت متقدم إلى إصدار تلك النصوص المتعلقة بالجريمة المعلوماتية.وأهم تلك التشريعات نجد التشريع الفرنسي ولا ننسى أول اتفاقية حول الإجرام المعلوماتي التي أبرمت بتاريخ:2001/11/08 من طرف المجلس الأوروبي. لكن تجدر الإشارة إلى أن المشرع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية أو ما يعرف بالغش المعلوماتي، و أغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي و المتمثلة في التزوير المعلوماتي. و سنتطرق في هذا الفرع إلى أهم الأحكام الخاصة بالجرائم الماسة بالأنظمة المعلوماتية و المتعلقة محددين في ذلك كل من الركن المادي و المعنوي و كذا الجزاءات المقررة لها من خلال جرائم:

- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام[1].

أولا:الركن المادي

أ– الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

نصت عليه المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك

[1] - أمال قارة، المرجع السابق، ص 20.

حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 150000 دج" كما نصت عليه المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، و يكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

*** الصورة البسيطة:**

أ- فعل الدخول : لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و في نفس الاتجاه إلى جهاز الحاسب الآلي و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. و لم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، و لذلك تقع الجريمة بأية وسيلة أو طريقة و يستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[1] .

ب- فعل البقاء Le maintien[2] : قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام

[1] - د. علي عبد القادر القهوجي، المرجع السابق، ص 121.

[2] - د. علي عبد القادر القهوجي، المرجع السابق، ص 133.

المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام و قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. و يكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا.و من أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده و ينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. و يكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية و الإطلاع فقط و يتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، و التي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، و قد يجتمع الدخول غير المشروع و البقاء غير المشروع معا و ذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام [1]، و يدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، و يتحقق في هذا الفرض الاجتماع المادي للجرائم و إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة ، و ذلك بالنسبة للموظف أو العامل أو غيرهما حين

[1] آمال قارة، المرجع السابق، ص 111.

يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج[1].

كما يمكن أن تطبق على الاستخدام غير المشروع البطاقات الممغنطة إما لسرقتها أو التزوير ثم استخدامها أو حتى إذا استخدمها صاحبها في سحب مبالغ دون أن يكون لديه رصيد كاف، أو عند عدم وجود الرصيد و تكون الجريمة في هذه الحالة هي جريمة البقاء غير المشروع داخل النظام بشرط أن يكون صاحب البطاقة يعلم مقدما بأنه ليس له رصيد كاف و يمكن أيضا تطبيقها على التصنت على المحادثات الهاتفية طالما أن أرقام الهواتف معالجة آليا في نظام خاص بها. هذه الجريمة تعد جريمة سلوك مجرد، أي أنها تقع و تكتمل بمجرد الانتهاء من السلوك المكون لها و هو الدخول أو البقاء دون أن يطلب المشرع في نموذجها القانوني حسب نصوص التجريم أية نتيجة إجرامية.

*** الصورة المشددة:**

نصت المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 دج إلى 150000 دج".

نصت المادة 394 مكرر 3/2 قانون العقوبات على ظرفين تشدد بهما عقوبة جريمة الدخول و البقاء داخل النظام، و يتحقق هذان الظرفان عندما ينتج عن الدخول أو البقاء إما محو

[1] – آمال قارة، المرجع السابق، ص 112.

أو تعديل المعطيات التي يحتويها النظام و إما عدم صلاحية النظام لأداء وظائفه ، و يكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول ، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة، أي على سبيل الخطأ غير ألعمدي، فالظرف المشدد هنا ظرف مادي يكفي أن توجد بينه و بين الجريمة العمدية الأساسية و هي جريمة الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره إلا إذا أثبت الجاني انتفاء تلك العلاقة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام للقيام بوظائفه يرجع إلى القوة القاهرة أو الحادث المفاجئ.

ب– الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

نصت عليه المادتين 05 و 08 من الاتفاقية الدولية للإجرام المعلوماتي [1] لم يورد المشرع الجزائري نصا خاصا بالاعتداء العمدي على سير النظام و اكتفى بالنص على الاعتداء العمدي على المعطيات الموجودة بداخل النظام و ربما يجد ذلك تفسيره في أن الاعتداء على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه، و قد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات و الاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية. فإذا كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل يشكل جريمة الاعتداء ألعمدي على

[1] – آمال قارة، المرجع السابق، ص 114.

النظام، أما إذا كان الاعتداء الذي وقع على المعطيات غاية فإن الفعل يشكل جريمة الإعتداء العمدي على المعطيات.

سبق و أن ذكرنا أن الاعتداء على سير النظام الناجم عن الدخول أو البقاء غير المشروع لا يشترط أن يكون مقصودا، لكن الإشكال المطروح أن أفعال الاعتداء على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب خاصة مع عدم وجود نص خاص بالاعتداء العمدي على سير النظام.

يتمثل هذا السلوك المادي في فعل توقيف نظام المعالجة الآلية للمعطيات من أداء نشاطه العادي و المنتظر منه القيام به، و إما في فعل إفساد نشاط أو وظائف هذا النظام، و لا يشترط أن يقع فعل التعطيل أو فعل الإفساد على كل عناصر النظام جملة، بل يكفي أن يؤثر على أحد هذه العناصر فقط سواء المادية جهاز الحاسب الآلي نفسه، شبكات الاتصال، أجهزة النقل ...الخ، أما المعنوية مثل البرامج و المعطيات.

ج: **الإعتداءات العمدية على المعطيات:** نصت عليها المادة 08،04،03 من الاتفاقية الدولية للإجرام المعلوماتي ، كما نص المشرع الجزائري عليها في المادة 394 مكرر2 في قانون العقوبات «يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها».

- **الصورة الأولى**: الاعتداءات العمدية على المعطيات الموجودة داخل النظام النشاط الإجرامي في جريمة الاعتداء ألعمدي على المعطيات يتجسد في إحدى الصور الثلاث التالية[1]:

* الإدخال L'intrusion.

*المحوL'effacement.

*التعديل Modification.

لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي. و أفعال الإدخال و المحو و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل و هذا يعني أن النشاط الإجرامي في هذه الجريمة إنما يرد على محل أو موضوع محدد و هو المعطيات أو المعلومات التي تمت معالجتها آليا و التي أصبحت مجرد إشارات أو رموزا تمثل تلك المعلومات، و ليست المعلومات في ذاتها باعتبارها أحد عناصر المعرفة، كما أن محل هذا النشاط الإجرامي يقتصر على المعطيات الموجودة داخل النظام، أي التي يحتويها النظام و تشكل جزءا منه.

لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت، و لم يتخذ حيالها إجراءات المعالجة الآلية، أما تلك التي في طريقها إلى المعالجة حتى و لو لم تكن

[1] – آمال قارة، المرجع السابق، ص 120.

المعالجة قد بدأت بالفعل تتمتع بالحماية الجنائية، و يكون هناك مجال للقول بتوافر الجريمة التامة أو الشروع على حسب الأحوال.

تجدر الإشارة إلى أن الحماية الجنائية تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية، أي طالما كان يحتويها ذلك النظام و كانت تكون وحدة واحدة مع عناصره و يترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها و حتى ولو لفترة قصيرة، كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام، فالحماية الجنائية تقتصر على المعطيات التي توجد داخل النظام أو تلك التي في طريقها إلى الدخول إليه، أو تلك التي دخلت بعد خروجها، و لا يشترط أن تقع أفعال الإدخال و المحو و تعديل المعطيات بطريق مباشر بل يمكن أن يتحقق ذلك بطريق غير مباشر سواء عن بعد أم بواسطة شخص ثالث [1].

و عمومًا التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية :

– الإدخال L'intrusion: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، و يتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي و ذلك حين يستخدم رقمه الخاص و السري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، و كذلك الحامل الشرعي لبطاقة

[1]– محمد أمين شوابكة، المرجع السابق، ص 16.

الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له و بصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة .

– المحو L'effacement : يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة و الموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

– التعديل Modification: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام و استبدالها بمعطيات أخرى، و يتحقق فعل المحو و التعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها و ذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات و برنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة[1]، و هذه الأفعال المتمثلة في الإدخال و المحو و التعديل وردت على سبيل الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى و لو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لأن كل تلك الأفعال لا تنطوي لا على إدخال و لا على تعديل بالمعنى السابق.

[1] – آمال قارة، المرجع السابق، ص 122.

- **الصورة الثانية:** المساس العمدي بالمعطيات خارج النظام

وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكات التالية:

1-نص المادة 394 مكرر2 يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

2-نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة،الجوسسة، الإرهاب، التحريض على الفسق ...الخ.

ثانيا : الركن المعنوي

إن الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش.

أ/الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات: الولوج و التجول و البقاء داخل نظام المعالجة الآلية للمعطيات لا يجرمان إلا تما عمدا.

المادة 02 من الاتفاقية الدولية للإجرام ألمعلوماتي تسمح للدولة العضو أن تشترط بأن ترتكب الجريمة عن طريق خرق الحماية الفنية للنظام بهدف الحصول على المعطيات الموجودة بداخله.

جريمة الدخول أو البقاء داخل النظام جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه العلم و الإرادة.

فيلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام و البقاء فيه، و عليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى و لو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام [1] .

بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

[1] – د. علي عبد القادر القهوجي، المرجع السابق، ص 136-137.

في الحقيقة أن الدخول و البقاء بالغش لا يتضمن معنى خرق الجهاز الرقابي للنظام، إنما يظهر من خلال الولوج دون وجه حق إلى النظام إلاّ أن الجهاز الرقابي ما هو إلاّ وسيلة لإثبات أن الدخول للنظام غير مرخص به.

ب/ الإعتداءات على سير نظام المعالجة الآلية للمعطيات :

إن هذه الجريمة جريمة عمدية ، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة[1] .

ج/ الإعتداءات العمدية على المعطيات:

جريمة الإعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه ألجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذالك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته[2] .

[1] – . علي عبد القادر القهوجي، المرجع السابق ، ص142.

[2] – المرجع نفسه، ص145.

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذالك واتجاه الإرادة إليه ، وان كان الضرر قد يتحقق في الواقع نتيجة النشاط الإجرامي إلا انه ليس عنصرا في الجريمة .

ثالثا : الجزاءات المقررة

وسنتناول فيما يلي الجزاءات التي قررها المشرع الجزائري لهذا النوع من الإجرام الحديث .

طبقا للمادة 13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات مالية للحرية ، والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي ، كما توجد عقوبات تطبق على الشخص المعنوي بناءا على تبني مبدأ مسالة الشخص المعنوي الواردة في المادة 12من الاتفاقية.

1- العقوبات المطبقة على الشخص الطبيعي :

العقوبات الأصلية :

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات ،إذ نجد سلم خطورة يتضمن ثلاث درجات ،جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة،أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس ألعمدي بالمعطيات.

أ/ الدخول والبقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة (المادة 394 مكرر) .

ب/ الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة ،وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03) .

ج/ الاعتداء العمدي على المعطيات : طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 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، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج [1].

العقوبات التكميلية:

نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية و المتمثلة في:

[1]- أمال قارة، المرجع السابق، ص 21.

أ/ **المصادرة:** وهي عقوبة تكميلية تشمل الأجهزة والبرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

ب/ **إغلاق المواقع:** والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

ج/ إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها[1].

الظروف المشددة:

أ/ نصت المادة 394 مكرر /2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر ،و في الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج .

هذه الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول والبقاء غير المشروع علاقة سببية للقول بتوافره.

[1]- خالد دوادي، المرجع السابق، ص43.

ب/ نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام .

2- العقوبات المطبقة على الشخص المعنوي :

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من الاتفاقية الدولية للإجرام ألمعلوماتي ، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة[1] .

كما تجدر الإشارة إلى أن 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 :

أ/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

ب/واحدة أو أكثر من العقوبات الآتية:

[1]- القاضيان: أسامة احمد المناعسة،جلال محمد الزعبي ،المرجع السابق، ص 102.

- حل الشخص المعنوي
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ،وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته .

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

3- عقوبة الاتفاق الجنائي:

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم 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 لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية ،يعاقب بالعقوبات المقررة بالجريمة ذاتها".

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي يمكن استخلاصها من نص المادة 394 مكرر 5 م قانون العقوبات[1]، والتي هي:

- مجموعة أو اتفاق.
- بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.

[1] – القانون 23/06 المؤرخ في 2002/12/20 ،المعدل والمتمم للأمر156/66 المتضمن قانون العقوبات ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد84 .

- القصد الجنائي.

فبالنسبة لمجموعة أو الاتفاق يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، كما.يستوي. أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الأخر من قبل و لكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي ، المهم أن يتم الاتفاق بين شخصين على الأقل ، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

وتكاثف الجهود لا يكفي بل يجب أن يكون بهذه تحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه فإنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات .

الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

التحضير لا يكفي بل يتم تجسيده بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور mots de passe أو رمز الدخول code d'accès الخ.

فعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توافر فعل إيجابي للمشاركة.

توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة كل عضو أي تحقيق نشاط إجرامي معين وهو العمل التحضيري.

4- عقوبة الشروع في الجريمة :

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

نصت المادة 394 مكرر 7 قانون العقوبات:" يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "[1].

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة ،ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص

[1] – القانون 23/06 المؤرخ في 2002/12/20 ،المعدل والمتمم للأمر156/66 المتضمن قانون العقوبات ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد84 .

المادة 394 مكرر5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي .

بعض التشريعات المقارنة بما فيها التشريع الفرنسي أخرجت جنحة الاتفاق الجنائي لتحضير جرائم ماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي ،لأن التحضير للجرائم الذي يتم في إطار اتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع.

المطلب الثاني: الحماية الجزائية للمعلوماتية من خلال القوانين و التنظيمات الأخرى

نظرا لنسبية الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات الجزائري فقد نص المشرع على بعض القوانين و التنظيمات من شأنها إضفاء نوع من الحماية الجزائية للجريمة المعلوماتية، و هو ما سنفصله من خلال الفرعين الآتيين:

الفرع الأول :مواجهة الجريمة الالكترونية من خلال نصوص الملكية الفكرية

أولا:الحماية في إطار الملكية الصناعية

من خلال أحكام العلامات التجارية :

ينظمها الأمر 06/03 المؤرخ في : 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر 57/66 المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 223/67 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية و

العلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات ،ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام والآداب .

السؤال المطروح: هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية ؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به. فالحماية بأحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد .

من خلال أحكام براءة الاختراع :

عرفت المادة 02 من الأمر 07/03 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية. وبشان الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي:

شرط الابتكار، شرط الجدة ،القابلية للتطبيق الصناعي و المشروعية[1] .

في حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض

[1] – الأمر 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع المعدل للأمر 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع .

وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

السؤال المطروح هل تستفيد برامج الحاسب من الحماية بواسطة براءات الاختراع ؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد سببين أساسين هما:

- إما تجرد البرامج من أي طابع صناعي

- إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا ، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه.

و الجهة المكلفة بتقرير توافر شرط الجدة في الجزائر هي المعهد الجزائري لحماية الملكية الصناعية إذ يأخذ المشرع الجزائري بمبدأ الجدة المطلقة [1] الذي يتنافى مع وجود أية سابقة دون تحديد زماني أو مكاني، إنما يشرط أن تتوافر علانية هذه السابقة .

[1] - الأمر 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع المعدل للأمر 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع .

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع ، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل ، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه بمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة .

وتجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 07/03 المتضمن براءة الاختراع " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب ".

ثانيا: الحماية في إطار الملكية الأدبية و الفنية

نظم المشرع الجزائري قانون الملكية الأدبية والفنية بمقتضى الأمر 14/73 المؤرخ في 1973/04/03 المعدل والمتمم بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 المعدل والمتمم بموجب الأمر 05/03 المؤرخ في 2003/07/19 المتعلق بحق المؤلف والحقوق المجاورة.

لتحديد مدى خضوع برامج الحاسب الآلي للحماية المقررة بمقتضى قانون حق المؤلف الجزائري وجب مناقشة نقطتين أساسيتين :

أ- مدى اعتبار البرنامج كموضوع من موضوعات حق المؤلف الجزائري :

موضوع حق المؤلف هو" المصنف الأدبي والفني" وقد عرف المشرع الجزائري المصنف في المادة الأولى من الأمر 14/73 كما نصت المادة 2 من الأمر 14/73 على أن المصنفات التي تشملها حماية حق المؤلف هي كالتالي:

- الكتب والمنشورات وغيرها من المؤلفات الأدبية والعلمية والفنية
- المحاضرات والخطب والمواعظ والمؤلفات الأخرى المماثلة
- مؤلفات الدراسة والدراسات الموسيقية
- مؤلفات الألحان الإيقاعية والمسرحيات الإيمائية المعبر عنها كتابة أو بطريقة أخرى
- أعمال التصوير والرسم والهندسة والنحت والنقش والطباعة الحجرية .
- مؤلفات الفنون التطبيقية.
- الصور والخرائط الجغرافية والتصميمات والرسوم والأعمال التشكيلية الخاصة بالجغرافيا والهندسة المعمارية أو العلوم .
- المؤلفات الفلكلورية وبصفة عامة المؤلفات التي هي جزء من التراث الثقافي التقليدي الجزائري .

إذن فالمشرع الجزائري لم ينص صراحة من خلال الأمر 14/73 على حماية البرامج المعلوماتية في إطار حق المؤلف، لكن رغم عدم التنصيص فان بعض المختصين يرون إمكانية الحماية واردة بدليل الصياغة المرنة عند ذكر المصنفات المشمولة بالحماية.

أي يمكن إسباغ الحماية على برامج الحاسوب كمصنفات فكرية ضمن عمومية نص المادة 2 الواردة في شان المصنفات التقليدية المحمية .

فنص المادة 2 وان كان لم يذكر صراحة برامج الحاسوب ضمن المصنفات المحمية لحماية حق المؤلف إلا أن صياغتها قد جاءت في صورة عامة ، هذا التعداد ورد على سبيل المثال لا الحصر.

ومنعا لأي لبس ،كان من الأفضل النص على البرامج صراحة ضمن قائمة المصنفات المحمية، وهذا مافعله المشرع الجزائري في تعديل قانون حق المؤلف بمقتضى الأمرين 10/97 – 05/03 حيث ادمج برامج الإعلام الآلي ضمن المصنفات الأصلية [1].

من استقراء الأمرين 10/97-05/03 المعدل والمتمم للأمر 14/73 نستخلص مايلي :

- مجموعة المصنفات والأساليب والقواعد، كما يمكن أن يشمل الوثائق المتعلقة بسير ومعالجة المعطيات [2].

- إن مدة الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية "بارن" التي حددت كمدة للحماية 50 سنة .

[1] – المادة 04 الأمر 10/97 "تعتبر على الخصوص كمؤلفات أدبية أو فنية محمية ما يأتي المصنفات الأدبية المكتوبة مثل المحاولات الأدبية والبحوث العلمية والتقنية والروايات والقصص والقصائد الشعرية ومصنفات وقواعد البيانات ".

[2] –المادة 05 الأمر 10/97 "تعتبر أيضا مصنفات محمية الأعمال الآتية مجموعات المعلومات البسيطة التي تتأتى أصالتها من انتقاء مواردها أو تنسيقها أو ترتيبها ".

– تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية (المادة 151 الأمر 10/97) إذ كان في السابق التعدي على الملكية الفكرية يخضع للمواد 394/390 من قانون العقوبات لكنها أخرجت بموجب الأمر 10/97 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة .

تجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين 10/97 – 05/03 تعود لأسباب أهمها الانضمام إلى المنظمة العالمية للتجارة هو المصادقة على اتفاقية بارن وهو مافعلته الجزائر بموجب المرسوم الرئاسي 341/97 .

إضافة إلى تبني أحكام اتفاق جوانب الملكية الفكرية المتعلق بالتجارة وذلك نظرا لانعكاسات حقوق المؤلف على المستوى الإقتصادي ولضمان حماية المؤلفات الأجنبية في الخارج وقد ورد في نص المادة 8 من الاتفاق أن على الدول الأعضاء عند تعديل أو تبني قوانين اتخاذ التدابير المناسبة بشرط أن تكون متوافقة مع الاتفاق لتفادي الاستعمال المتعسف لحقوق الملكية الفكرية من طرف حائزي الحقوق واللجوء إلى تصرفات تمس بالتجارة أو تضر بعقود نقل التكنولوجيا .

ومن أهم ما ورد في اتفاق جوانب الملكية الفكرية المتعلقة بالتجارة هو ما ورد في نص المادة 10 أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو الصورة المنقوشة فهي محمية على أساس أنها مصنفات أدبية ،كما أن الاتفاقية حول الإجرام ألمعلوماتي نصت على تجريم

الاعتداءات على حق المؤلف والحقوق المجاورة تطبيقا لأحكام اتفاق جوانب الملكية إذا ارتكبت هذه الاعتداءات عن طريق نظام معلوماتي في نطاق تجاري.

مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي لجرائم التقليد في التشريع الجزائري :

قانون حق المؤلف يوفر الحماية الجزائية لمصنفات الإعلام الآلي بعد إدماجها صراحة ضمن المصنفات المحمية. في السابق كانت أفعال التعدي على حقوق الملكية الأدبية والفنية معاقب عليها في قانون العقوبات المواد من (390 إلى 394) غير أن هذه المواد ألغيت بمقتضى المادة 165 من الأمر 10/97.

الملاحظ أن الاعتداءات على حقوق المؤلف أخرجت بموجب الأمر 10/97 من تحت مظلة قانون العقوبات، حيث كان منصوصا عليها في القسم التاسع المعنون بجنح التعدي على الملكية الأدبية والفنية من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال. لكن حاليا أخرجت من نطاق قانون العقوبات وأصبح لها تجريم خاص في إطار قانون حق المؤلف [1].

وتجدر الإشارة إلى الأمر 10/97 فقد شدد في العقوبات المقررة للاعتداءات على حقوق المؤلف مقارنة بالعقوبات المنصوص عليها في قانون العقوبات (المادة 75 الأمر 14/73) تحيل إلى المادة 390 من قانون العقوبات تقرر الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة .

[1] – نهلا عبد القادر المومني ، المرجع السابق، ص176 .

نخلص إلى انه نظرا لقصر أحكام العلامات التجارية ونصوص براءة اختراع في مواجهة الجريمة المعلوماتية ، ونظرا لكون قانون الملكية الأدبية والفنية ورغم اعتراف المشرع الجزائري لبرامج الإعلام الآلي وقواعد البيانات بصفة المصنف المحمي إلا انه لا يخفى علينا أن الحماية الجزائية للبرامج من خلال حق المؤلف تنصب بصفة أساسية على شكل البرنامج أو مضمونه ألابتكاري فقط دون أن تغطي تلك الحماية كل مضمون البرنامج . لهذا السبب كان البحث عن نوع أخر ينضم إلى الحماية السابقة من الحماية الجزائية لهذه البرامج في مثل هذه الحالات ،ولذلك فلا مفر من ضرورة اللجوء إلى استحداث نصوص تجريمية خاصة بالمعلوماتية وذلك ما اعتمده المشرع الجزائري في مشروع تعديل قانون العقوبات الجزائري باستحداث فصل خاص بالاعتداءات على أنظمة المعالجة الآلية للمعطيات.

الفرع الثاني: الحماية الجزائية للمعلوماتية من خلال القانون 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية و اللاسلكية.[1]

تضمن القانون 2000-03 القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، و المعدل بموجب:

- القانون 03-22 الممضي في 28 ديسمبر 2003 (وزارة المالية)[2]

[1] الجريدة الرسمية رقم 48 مؤرخة في 06 أغسطس 2000، ص03.
[2] الجريدة الرسمية رقم 83 المؤرخة في 05 نوفمبر 2003، ص03.

- القانون 06-24 الممضي في 26 ديسمبر 2006 (وزارة المالية)[1]

و يتضمن هذا القانون 151 مادة أدرجت لتنظيم الاتصالات السلكية و اللاسلكية و كذا البريد، و قد خصصت المواد من 127 منه إلى المادة 144 للنص على العقوبات المقررة للجرائم المتعلقة بها. و من السلوكيات المجرمة بنص هذا القانون نذكر:

- كل من يفتح أو يحول أو يخرب محل المراسلات أو ينتهك سريتها أو يأمر أو يساعد في ذلك من غير الأشخاص المعهود إليهم بتأدية هذا النوع من الخدمات، يعاقب بالحبس من شهرين إلى سنة و بغرامة من 50.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، (المادة 127 فقرة 03 من القانون 00-03).
- يعاقب بالحبس من 03 أشهر إلى 05 سنوات و بغرامة من 100.000 دج إلى 1.000.000 دج كل شخص يقطع عمدا كابل بحريا أو يسبب له تلفا قد يوقف أو يعطل المواصلات السلكية و اللاسلكية كليا أو جزئيا، (المادة 130 من القانون 00-03)
- يعاقب بالحبس من سنة إلى سنتين و بغرامة من 100.000 دج إلى 500.000 دج أو بإحدى هاتين العقوبتين، كل من ينشئ أو يستغل شبكة عمومية للمواصلات السلكية و اللاسلكية دون الرخص المنصوص عليها.

[1] الجريدة الرسمية رقم 85 مؤرخة في 07 نوفمبر 2006، ص03.

و قدر أدرجت في هذا القانون عديد المفاهيم و التعريفات التي من شانها توضيح بعض المفاهيم المنصوص عليها في القانون رقم 09-04و ذلك في الفصل الثاني منه، القسم الأول المعنون بالاتصالات السلكية و اللاسلكية، المواد من 08 إلى 23.

المبحث الثاني: القواعد الإجرائية لمكافحة الجريمة الإلكترونية

نتيجة للتطور التكنولوجي لتقنية المعلومات والتقدم السريع والمتواصل لتطوير الأجهزة والبرامج واعتماد قطاعات كبيرة من المجتمع على المعلوماتية ونظرا لعدم اعتراف الإنترنت بالحدود الإقليمية و القارية فإنه أصبح لزاما على الدولة أن تحمي هذا الكيان الجديد وتوفر له وسائل الحماية و لاسيما القانونية في مواجهة الجرائم الناشئة عن استخدام المعلوماتية ، ولما كانت هذه الجرائم لها طبيعة خاصة فإن مواجهتها تتطلب تأهيل من نوع خاص لرجال الضبط القضائي وهذا التأهيل ينسحب على أعضاء النيابة العامة وقضاة الحكم و التحقيق خاصة مع استحداث الأقطاب القضائية .

إن الإشكال المطروح هو مدى تطابق قواعد الاختصاص ونصوص الضبط والتحري و الواردة في قانون الإجراءات الجزائية على الجريمة المعلوماتية.

المطلب الأول:القواعد الإجرائية المنصوص عليها في ظل قانون الإجراءات الجزائية

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، فيلزم على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن تنشأ قواعد إجرائية حديثة إلى

جانب القواعد الموضوعية، فلما كانت هذه الجرائم المعلوماتية تتميز بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات العملية الإجرائية التي جعلت القواعد الإجرائية التقليدية قاصرة عن مواجهة تلك المشاكل، ولهذا اتجهت بعض التشريعات كالتشريع الانجليزي والأمريكي والجزائري إلى تعديل بعض قواعدها الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية كتلك المتعلقة بالاختصاص المحلي، وإجراءات البحث و التحري.

الفرع الأول:قواعد الاختصاص المحلي

عالج المشرع الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه، وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه،لكن لما كانت الجريمة المعلوماتية جرائم عابرة للإقليم،إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه، لهذا فإن المشرع الجزائري أجرى بعض التعديلات المتعلقة بالإختصاص المحلي في الجريمة المعلوماتية بموجب القانون 06/ 22المؤرخ في 20ديسمبر2006 المعدل والمتمم للأمر رقم155/66الموافق ل08يونيو1966والمتضمن قانون الإجراءات الجزائية، لهذا سنتطرق لتلك القواعد على النحو الآتي:

أولا:الاختصاص المحلي للنيابة العامة:

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة37من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ومحل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي في دائرته تم القبض على هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر.

وبالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو بمكان القبض على هؤلاء الأشخاص حتى ولو تم لسبب أخر لكن لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر فإن المشرع الجزائري بموجب المادة37فقرة2من قانون الإجراءات الجزائية أجاز تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة الاختصاص المحاكم الأخرى إلا أنه ترك كيفية تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص.

ويتعين على ضابط الشرطة القضائية طبقا للمادة40مكرر1من قانون الإجراءات الجزائية الجزائري أن يخبروا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل ونسختين من إجراءات البحث ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة،والذي يطالب طبقا للمادة40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة40مكرر من هذا القانون، وهذه الإجراءات تتعلق بتحريك الدعوى العمومية أو مباشرتها أو رفعها بمجرد أن يتبين للنائب العام أن الجريمة تدخل ضمن المحكمة المختصة التابعة لها وهذا ما نصت عليه المادة40مكرر3.

ثانيا:الاختصاص المحلي لقاضي التحقيق ومحاكم الجنح

أ- الاختصاص المحلي لقاضي التحقيق

يقصد بالإختصاص المحلي لقاضي التحقيق المجال الذي يباشر فيه قاضي التحقيق مهامه و الذي يتحدد طبقا للمادة40 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر إلا أن المشرع ألغى في التعديل الجديد الفقرة2و3من المادة40، وأصبحت تنص الفقرة2 على انه يجوز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ،وبالتالي فإن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى لكنه ترك تحديد كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر لاحقا.

ب- الاختصاص المحلي لمحاكم الجنح. يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة 329من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة،أو بمحل إقامة احد الأشخاص المتهمين،أو شركائهم،أو بمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر، غير أن المشرع في التعديل الصادر بموجب القانون 14/04أضاف فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم.

إذن فإن المشرع أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد اختصاص وكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح ولكنه ترك ذلك للتنظيم الذي سيصدر لاحقا والذي يحدد تلك المحاكم التي يمتد إليها الاختصاص،وقرر في المادة40مكرر أيضا تطبيق القواعد المتعلقة بالدعوى العمومية والتحقيق والمحاكم أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد37،40،329من قانون الإجراءات الجزائية.

والحقيقة أن مشكلة الاختصاص القضائي في الجريمة المعلوماتية تعد من المشكلات العويصة التي تعرقل الحصول على الدليل،ذلك أن هذه الجريمة قد ترتكب في مكان معين وتنتج أثارها في مكان أخر داخل الدولة أو خارجها وإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة فأي مكان في هذه الأماكن ينعقد الإختصاص الجنائي لسلطات التحقيق والمحاكمة في الجريمة المعلوماتية، لكن على المستوى الدولي فان الأمر بحاجة إلى اتفاقيات دولية ثنائية أو جماعية،ولقد شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسوب الآلي،إلا أن ذلك لم يحقق تقدما في معالجة الاختصاص القضائي،فلذلك فالحاجة ماسة إلى قوانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في كل المجالات.[1]

[1] ينظر محمد الأمين البشري، **التحقيق في جرائم الحاسب الآلي والانترنت**، المجلة العربية للدراسات الأمنية والتدريب، العدد30 نوفمبر2000، ص373.

الفرع الثاني:إجراءات البحث و التحري.

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الإتهام الموجه من طرف النيابة العامة بشأن واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك،والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم،وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جمع الإجراءات الضرورية للكشف عن الحقيقة.[1]

يهدف التحقيق الابتدائي إلى الكشف الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل،وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الأخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الإحتياطية ضد المتهم كالقبض والحبس المؤقت.

وسوف تقتصر دراستنا على إجراءات جمع الأدلة المادية التي يكون منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل والمنطق، فهي أقوى مفعولا في الإقتناع من الأدلة القولية على أن نخص بالدراسة التفتيش وضبط الأشياء باعتبارهما أهم التحديات الإجرائية لجرائم الكمبيوتر.

أولا:التفتيش في مجال الجريمة المعلوماتية

[1] ينظر عبد الله أوهابية،**محاضرات في قانون الإجراءات الجزائية**،ألقيت على طلبة سنة ثانية حقوق،جامعة الجزائر،الموسم الجامعي2010/2009.

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا للإجراءات القانونية المقررة،وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة. وإذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية،فما مدى خضوع البرامج والمعلومات كمكونات معنوية للحاسوب للتفتيش؟وماهي ضوابط تفتيش نظم الحاسوب؟

الفقرة الأولى:مدى قابلية نظم الحاسوب للتفتيش:

أشرنا سابقا إلى أن الحاسوب يتكون من مكونات مادية ومكونات معنوية،ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة،بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش،فإذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله وبنفس الضمانات المقررة قانونا في التشريعات المختلفة، وبالنسبة للأماكن العامة سواء كانت بطبيعتها

كالطرق العامة والشوارع أو كانت بالتخصيص كالمقاهي والمطاعم والسيارات العامة فان الشخص إذ وجد في هذه الأماكن وهو يحمل مكونات مادية للحاسوب أو كان مسيطرا أو حائزا لها فان التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد.[1]

أما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية،كبرامج لحاسوب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض،حيث يذهب رأي انه إذا كانت الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البرامج والبيانات.وقد لجأ الفقه في العديد من لدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعطيات ،وابرز مثال لذلك الفقه الكندي عندما وسع من تفسير المادة487من قانون العقوبات الكندي التي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعو للإعتقاد بأن الجريمة قد وقعت أو يشتبه فيل وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو انه سيتيح دليلا على ارتكاب الجريمة.وهكذا فإن هذا النص يفسر على أنه يسمح بضبط وبتفتيش البيانات وبرامج الحاسب الآلي.[2]

[1] – عبد الله هلالي، **تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات**، دراسة مقارنة، الطبعة الأولى، القاهرة، دار النهضة العربية1997، ص74.

[2] –كامل عفيفي، **جرائم الكمبيوتر**، لبنان، منشورات الحلبي، الحقوقية، 2003، ص366.

وفي هذا المعنى نجد المادة251 من قانون الإجراءات الجزائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل،ويفسر الفقه اليوناني أن عبارة أي شيء تشمل تفتيش البرامج والبيانات المعالجة الالكترونية.

وعلى النقيض يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على برامج وبيانات الحاسب الآلي غير محسوسة،ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (مواد معالجة الكترونية)،ولذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة أو أي مادة معالجة بواسطة الحاسب الآلي. والحقيقة أن الحاجة ماسة لتدخل تشريعي لتقرير الضوابط القانونية الكفيلة لتغلب على الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة المعلوماتية،ففي الولايات المتحدة الأمريكية تم تعديل المادة34من قانون الإجراءات الجنائية الفيدرالية عام1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الالكترونية،كما نص المشرع الانجليزي في القسم الثاني من قانون إساءة استخدام الكمبيوتر الصادر عام 1990 على تفتيش نظم الحاسب الآلي جرائم الولوج غير المصرح به على أنظمة الحاسب الآلي،والتعديل غير المرخص به في نظام الحاسب الآلي بدون إذن طالما كان هدف هذا الدخول ارتكاب أفعال غير مشروعة عن قصد،أما إذا كان الدخول مجرد دون نية لارتكاب أفعال غير مشروعة فإن التفتيش ممكن ولكن دون إذن قضائي.

كما قرر المشرع الجزائري بموجب المادة45 من القانون رقم 22/06المؤرخ في 20ديسمبر 2006، التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقرر له بعض الضوابط والقواعد سنراها لاحقا.

زيادة على ذلك فإن المشرع في بعض الدول الأخرى لجأ إلى تقرير بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة المعلوماتية،وشاركه في ذلك الفقه،ومن تلك التشريعات التشريع الهولندي الذي أجاز في المادة25/أ منه للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق وهذا لتذليل الصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في منزل أخر غير منزل المتهم،كما أجاز بموجب المادة25منه إلزام غير المتهم كالشاهد والشخص القائم بالتشغيل القائم بالتشغيل بتقديم كافة البيانات والمعلومات اللازمة لدخول نظام الحاسب الآلي والتعامل مع سلطة التحقيق في هذا الصدد،وأيضا اتجه المشرع الجزائري بموجب القانون السالف الذكر إلى وضع ضوابط للتفتيش في الجرائم المعلوماتية.

الفقرة الثانية:ضوابط تفتيش نظم الحاسب الآلي

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات،بيد أن تحقيق تلك الغاية لا يكون بأي ثمن،ففي كل الحالات فإن الغاية لا تبرر الوسيلة،فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد،بل إن ذلك يخضع لضوابط معينة،ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية:

أولا:الضوابط الموضوعية

تنحصر هذه الضوابط فيما يلي:

أ- وقوع جريمة معلوماتية:والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة،وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29يونيو1990،وفي فرنسا صدر قانون رقم19/88في 5يناير1988وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.

ب/اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها: فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية،سواء بصفته فاعلا أو شريكا،بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة،وهذا ما تؤكده المادة 163من قانون الإجراءات الجزائية الجزائري والمادة177من قانون الإجراءات الجزائية الفرنسي.

و في مجال المعلوماتية يمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا.

ج/توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة:

فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة،ويستو أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

وهكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.

د/إجراء التفتيش لنظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق:

يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق،وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق،أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس ،أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.

ثانيا:الضوابط الشكلية

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي،توجد ضمانات شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة وهي كالتالي:

أ- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظم الحاسوب الآلي:

والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط، وقد استوجب المشرع الجزائري في المادة 1/45أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش وكذلك المشرع الفرنسي استوجب في الفقرة الأولى من المادة57من قانون الإجراءات الجنائية حضور صاحب المسكن الذي يجري فيه التفتيش وعدم حضوره يترتب عليه البطلان للتفتيش.

غير أن المشرع الجزائري بموجب المادة45من القانون رقم23/06 المؤرخ في 20ديسمبر2006 استثنى إجراء الحضور لبعض الأشخاص[1]،إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،لكنه اوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات،لكن إذا تعلق التفتيش بمسكن موقوف صاحبه للنظر أو محبوس في

[1] - القانون 23/06 المؤرخ في 2006/12/20 ،المعدل والمتمم للأمر156/66 المتضمن قانون العقوبات ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد84 .

مكان أخر أوجب المشرع بموجب المادة 47 حضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش[1].

ب/محضر تفتيش نظم الحاسب الآلي :

فإن التفتيش من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش،وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.[2]

ج/الميقات الزمني لإجراء تفتيش نظم الحاسوب الآلي:

فحرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية وحرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل وما في حكمها في وقت معين،فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساءا،ولقد أخذت بعض التشريعات العربية بمبدأ عدم جواز تفتيش المنازل ليلا كقانون التونسي والجزائري،أما بالنسبة لتشريعات الدول الانجلوساكسونية كالقانون الانجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين.

[1] - عبد الله الهلالي، **تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات**، دراسة مقارنة، الطبعة الأولى، القاهرة، دار النهضة العربية،ص 116.

[2] – عبد الله الهلالي، المرجع السابق،ص 116.

لكن المشرع الجزائري بموجب المادة47 من قانون الإجراءات الجزائية الجزائري قرر إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات الليل والنهار أو الليل وفي كل محل سكني غير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص، إلا أنه أوجب الحفاظ على السر المهني.

د/أن يتم التفتيش بناءا على إذن مكتوب:إذا نصت المادة 44 من قانون الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناءا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان والشروع في تفتيش نظم الحاسوب الآلي.

فإن التفتيش لنظم الحاسوب الآلي يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر،فإجراء التفتيش دون تلك المذكرة مسالة تثير الكثير من المعارضة خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد.ويجب أن تكون المذكرة واضحة في تحديد النظام محل التفتيش.

ثانيا:الضبط في مجال الجريمة المعلوماتية

منح المشرع في المادة 63 صلاحية القيام بالتحقيقات الابتدائية لأعوان الضبطية القضائية بشرط أن تكون تحت رقابة ضباط الشرطة القضائية

الفقرة الأولى:فيما يخص التوقيف للنظر:إن التحقيق الابتدائي في الجرائم الخطيرة المذكورة في المادة16 من قانون الإجراءات الجزائية أصبح عسيرا و صعبا،خاصة وأن مرتكبي هذه الجرائم أصبحوا يستعملون أساليب متعددة،وحديثة و معقدة.

وأصبحت مدة الوضع تحت النظر لا تتماشى ومتطلبات التحقيق الأولي،مما جعل المشرع الجزائري يعدلها بالمادة51 والتي نصت على انه:

«يمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص:

-مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات.»

نلاحظ أن المشرع ربط تحديد مدة التوقيف للنظر بطبيعة الجريمة موضوع التحري واشترط أن يكون تمديد المدة بإذن مكتوب من وكيل الجمهورية وأثناء التحقيق الابتدائي كثيرا ما يقوم ضباط الشرطة القضائية باستدعاء أشخاص لإجراء التحقيق،إلا أنهم لا يمتثلون للإستدعاءات الواردة إليهم مما يقلص من فعالية وسرعة التحقيق لذا استوجب ترخيص رجال الضبطية القضائية استعمال القوة لإحضارهم.

الفقرة الثانية:استعمال القوة لإحضار الأشخاص.

جاء بالمادة 65الفقرة1 أنه يجوز لضباط الشرطة القضائية بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أن يستخدم القوة العمومية لإحضار الأشخاص الذين لم يستجيبوا لاستدعائين للمثول.

هذه المادة تتيح استعمال القوة لإحضار الأشخاص أمام الضبطية القضائية لأخذ أقوالهم بشرط أن يكون إحضارهم بترخيص من وكيل الجمهورية المختص،ولا يمكن إبقاؤهم في حالة التوقيف إلا للمدة اللازمة لأخذ أقوالهم بشرط أن يكون قد تم استدعائهم مرتين على الأقل ولم يمتثلوا.

حتى يحقق التفتيش غايته في جمع الأدلة الإجرامية لا بد من وسيلة التقاط تلك الأدلة،وهذه الوسيلة هي الضبط،والضبط في معظم الأحيان يكون هو غرض التفتيش و إن لم يكن هو السبب الأوحد له فقد يأتي الضبط لأسباب أخرى غير التفتيش مثل المعاينة.

ويقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث الطبيعة القانونية من إجراءات الاستدلال أو التحقيق،وتتحدد طبيعته بحسب الطريقة التي تم فيها وضع اليد على الشيء المضبوط،فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة استدلال.

وإذا كانت الجرائم الواقعة على المكونات المادية للحاسوب الآلي لا يثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها،ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء مادية،إلا أن الأمر بالنسبة للجرائم الواقعة على المكونات المعنوية للحاسوب الآلي،يثير مشاكل بالنسبة لضبط أدلتها.وقد اختلف الفقهاء بين مؤيد وعارض.ونجد المشرع الجزائري قد أجاز بموجب المادة 47الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي ساعة من مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية.

ومن اجل ضبط أدلة الجريمة فإن المشرع الجزائري بموجب مواد65مكررالى 65مكرر 10اجاز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور،إذا اقتضت ذلك ضرورة التحقيق الابتدائي

بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد،وتنفذ العمليات المأذون بها تحت مراقبة مباشرة لقاضي التحقيق،وتتم العمليات المحددة دون المساس بالسر المهني المنصوص عليه في المادة45.

ويبقى أن نتساءل عما إذا كان يجوز لضباط الشرطة القضائية الاطلاع على محتويات الحاسوب الآلي التي يتم ضبطها.

أجاب القسم 110من قانون الإجراءات الجنائية الألماني على هذا التساؤل بقوله إن سلطة الاطلاع على مطبوعات الحاسوب الآلي وحاملات البيانات الأخرى تقتصر على المدعي العام فقط ولا يكون لضباط الشرطة القضائية الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى ملفات البيانات المخزونة دون إذن الشخص الذي له حق نقل هذه البيانات لكل ما لهم هو مجرد فحص حاملات البيانات والبرامج دون استخدام أية مساعدات فنية.

وإذا كان الأمر يبدو محسوما من الناحية النظرية في بعض التشريعات التي قالت بصلاحية البرامج ومعلومات وبيانات الحاسوب الآلي للضبط،إلا أن المسالة عند التطبيق تأخذ بعد أخر،إذ لا يمكن ضبط مكونات الحاسوب الآلي المعنوية بعد تفتيشها إلا إذا نقلت من صورتها المعنوية إلى صورتها المادية،فلا بد من حصرها وجمعها في حيز مادي،ويتم ذلك بإخراجها على الورق أو بأخذ تسجيل منها أو جمعها على أقراص مرنة أو ممغنطة.

إلا أن السؤال الذي يطرح نفسه بشدة، إلى أي حد يمكن اعتبار هذه المخرجات بصورتها المختلفة مستندات تصلح أن تكون أدلة إثبات مقبولة أمام القضاء؟

القاعدة في الدعاوى الجزائية هي جواز الإثبات بكافة طرق الإثبات القانونية، والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الالكترونية خاصة مع احتمال ظهور أنشطة إجرامية عديدة.

والمعلومات إن كانت قيمتها تتجاوز شيئا فشيئا الموجودات والطاقة فإنها ليست من الماديات لتقبل بينة في الإثبات إلا أن الاتجاه الحديث لم يعد يقف عند المفهوم المحدود للمستندات، بل تطور بحيث أصبح يقبل بمخرجات الحاسوب الآلي سواء كانت على شكل مخرجات ورقية أو صور أو تسجيلات كدليل إثبات،إذ اعترف الفقه والقضاء الجنائيين في فرنسا بمخرجات الحاسوب الآلي سواء كانت مخرجات ورقية أو الكترونية كالأشرطة المغنطيسية وغيرها من الأشكال الالكترونية الأخرى بأن لها قيمة دلائل الإثبات،وبالتالي تصلح كأدلة إثبات أمام القضاء الجنائي،لاسيما و أن التعديل المدخل على قانون العقوبات الفرنسي بمقتضى القانون08يناير 1988 لم يتضمن ما يخالف وجهة النظر هذه.[1]

المطلب الثاني :الحماية الجزائية للمعلوماتية من خلال القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها

مراعاة من الجزائر لما شهده ويشهده العالم في الفترة الأخيرة من الألفية الثانية وبداية الألفية الثالثة تطورا كبيرا في مجال تكنولوجيات الإعلام والاتصال – كما سبق الذكر – تقوم بشكل أكبر

[1] – حجازي عبد الفتاح بيومي،**الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**،مصر–دار المحلة الكبرى:دار الكتب القانونية،2004،ص164.

على الاختراعات الجديدة في مجالي الإلكترونيك والمعلوماتية (أنظمة الوسائط المتعددة ، الاتصال المعلوماتي، الرقمنة ، الانترنت ....) وكان لظهور الانترنت دور لا مثيل له في وجود ما يسمى بالفضاء الافتراضي(Cyberespace) .

ولمسايرة هذا التطور التكنولوجي، كان لا بد للدول من إيجاد الإطار القانوني المناسب؛ " بوضع النصوص الملائمة لمختلف استعمالات الإعلام الآلي (التجارة الافتراضية، التوقيع الإلكتروني، حماية المعطيات الشخصية...)وفي نفس السياق تم وضع قوانين خاصة لمواجهة ما يسمى بالإجرام المعلوماتي أو الجرائم الإلكترونية (Cybercrimeأو Cybercriminalité).

نستعرض فيما يلي :أسباب صدور القانون رقم09 – 04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها و كذا مضمونه، ثم نتطرق إلى أهم الإجراءات المستحدثة في ظله.

الفرع الأول: أسباب صدور القانون رقم 04/09 و مضمونه

أ- أسباب صدور القانون رقم09 –04

إن الثورة في مجال تكنولوجيات الإعلام والاتصال – كما سبقت الإشارة إلى ذلك –أدت بالجزائر إلى محاولة الإقتداء بأغلب دول العالم في هذا المجال.

فكان لزاما سد الفراغ القانوني الذي عرفه هذا المجال بصدور القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائية لأنظمة

المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات)الدخول غير المشروع لأنظمة المعلوماتية ،تغيير أو إتلاف المعطي ويأتي هذا القانون لتعزيز نفس هذه القواعد، من خلال وضع إطار قانوني أكثر ملائمة مع خصوصية الجريمة الافتراضية.كما تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها.

وقد أخذ المشرع بعين الاعتبار الصعوبات التي تثيرها المصطلحات القانونية المتعلقة بهذه المادة ، لذلك تم اختيار عنوان " القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها " حتى لا يكون النص مرتبطا بتقنيات تشهد تطورا مستمرا بقدر ما يرتبط بالأهداف والغايات التي ترمي إليها هذا لتكنولوجيا، كما أن التركيز على مجالي الإعلام والاتصال بين مقاصد النص الذي يهدف إلى جعل المتعاملين في مجال الاتصالات السلكية واللاسلكية شركاء في مكافحة هذا الشكل من الإجرام والوقاية منه.

ب- مضمون القانون رقم 04/09

تضمن القانون رقم 09 -04 تسعة عشر مادة (19) مقسمة على ستة فصول نلخصها فيما يلي: نص الفصل الأول على الأحكام العامة التي تبين الأهداف المتوخاة من القانون وتحدد مفهوم مصطلح التقنية الواردة فيه وكذا مجال تطبيق أحكامه[1].

[1]- القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

و في الفصل الثاني نص القانون على مراقبة الاتصالات اللكترونية حيث خصها بأحكام خاصة بمراقبة الاتصالات الالكترونية، وقد روعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية.

و الفصل الثالث تضمن القواعد الإجرائية ؛ بمعنى النص على قواعد إجرائية خاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن ومع مراعاة ما تضمنه قانون الإجراءات الجزائية من مبادئ عامة.

و الفصل الرابع تطرق إلى التزامات المتعاملين في مجال الاتصالات الالكترونية، وذلك من خلال تحديد الالتزامات التي تقع على عاتق المتعاملين في الاتصالات الالكترونية لاسيما إلزامية حفظ المعطيات المتعلقة بحركة السير والتي من شأنها المساعدة في الكشف عن الجرائم ومرتكبيها ، يهدف هذا القانون إلى إعطاء مقدمي الخدمات دورا إيجابيا ومساعدا للسلطات العمومية في مواجهة الجرائم وكشف مرتكبيها.

و الفصل الخامس أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته ؛ إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفيات تنظيم هذه الهيئة.

و أما الفصل السادس فنص على التعاون والمساعدة القضائية الدولية؛ إذ تناول قواعد الاختصاص القضائي والتعاون الدولي بوجه عام:

-ففيما يخص الاختصاص القضائي فهو فضلا عن قواعد الاختصاص العادية فقد تم توسيع اختصاص المحاكم الجزائرية للنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي ترتكب من طرف الرعايا الأجانب عندما تكون المصالح الإستراتيجية للجزائر مستهدفة.

-وأما فيما يتعلق بالتعاون الدولي يقوم على مجموعة من المبادئ العامة في مجال التعاون الدولي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خاصة ما يتعلق منها بالمساعدة وتبادل المعلومات، حيث تم اعتماد مبدأ التعاون على أساس المعاملة بالمثل.

الفرع الثاني: الإجراءات المستحدثة بموجب القانون 04/09

لقد نص المشرع من خلال نصوص القانون 04/09 على إجراءات من شأنها التسهيل في عملية محاربة الجريمة المعلوماتية و هذا بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية.إذ نص في القانون على إجراء مراقبة الاتصالات الإلكترونية و حدد بنص المادة الرابعة منه الحالات التي تسمح باللجوء لهذا الإجراء كالآتي:

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج- لمقتضيات التحريات و التحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

و تضيف ذات المادة أنه لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية المختصة. وعندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة أ من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر العاصمة بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من القانون 04/09، إذن لمدة 06 أشهر قابلة للتجديد و ذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعلمة [1]و الأغراض الموجهة لها. وتكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في المادة "ا" موجهة حصريا لتجميع و تسجيل معطيات ذات صلة بالوقاية من الافعال الإرهابية و الإعتداءات على أمن الدولة و مكافحتهما، و ذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

كما نص القانون على فصل ثالث تناول المشرع من خلاله على القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية (المادة 5) إذ يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 ، الدخول، بغرض التفتيش، و لو عن بعد، إلى:

أ- منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية

[1] - القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

في الحالة المنصوص عليها في الفقرة "ا" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و آن هذه المعطيات يمكن الدخول إليها، انطلاقا، من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

و إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة و وفقا لمبدأ المعاملة بالمثل.

و يمكن للسلطة المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لإنجاز مهمته.

و نصت المادة 6 من القانون 04/09 على إجراء حجز المعطيات المعلوماتية عندما تكتشف السلطات القضائية التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و انه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

و يجب في كل الأحوال على السلطات التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية. غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات. وتضيف المادة 7 أنه إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

أما بالنسبة للمعطيات المحجوزة ذات المحتوى المجرم فإنه طبقا لنص المادة 8 فإنه يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذاك. إذ لا يجوز استعمال المعلومات المتحصل عليها عن طريق عملية المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية و إلا تقع تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به (المادة 9).

كما نصت المواد 10،11 و 12 على إلتزامات مقدمي الخدمات و كذا الجزاءات المقررة المترتبة على عدم احترام هاته الإلتزامات.

و قد أحدث ذات القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته على أن تحدد تشكيلتها و تنظيمها و كيفيات سيرها عن طريق التنظيم (المادة 13) و نصت المادة 14 على المهام المسندة لها.

وتناول المشرع الجزائري موضوع التعاون و المساعدة القضائية الدولية ضمن الفصل السادس بالنص على قواعد الإختصاص القضائي في المادة 15 أين يعود الإختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبي و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.و كذا المساعدة القضائية الدولية المتبادلة (المادة 16) وتبادل المعلومات و اتخاذ الإجراءات التحفظية (المادة17) و القيود الواردة على طلبات المساعد القضائية الدولية (المادة 18).

الخاتمة

خاتمة:

ما من شك أن من يغوص في عالم الشبكة العنكبوتية سوف يصاب بذهول كبير و تتملكه الدهشة إزاء هذا العلم الجديد الذي لا يعترف بالحدود الإقليمية والجغرافية فهو عالم افتراضي ومفتوح فالعام كله أضحى قرية صغيرة جراء الثورة المعلوماتية.

إن هذا التطور الذي ابهر العالم لم يكن بمنأى عن الأخطار المهددة لأمن الإنسان واستقرار المجتمعات ذلك أن عالم الانترنت ولد إلى جانب مزاياه ظاهرة جديدة وخطيرة تسمى بالجريمة الالكترونية أو الجريمة المعلوماتية أخذت في النمو والتزايد، وبشكل مذهل وخطير للغاية وبأنماط جديدة فالمجرم الالكتروني الآن يوجد في عالم افتراضي لا يعرف الحدود وهو ذكي ويتسم بقدر عالي من الكفاءة العلمية والتقنية يتولى الولوج إلى عمق الأنظمة المعلوماتية دون أن يكلف نفسه عناء التنقل يضاف إلى ذلك انه من الصعوبة بمكان ملاحقة هؤلاء المجرمين وضبط الأدلة دون الحديث عما يطرح أمام ذلك من تحديات بخصوص الاختصاص القضائي والمحاكمة العادلة، وبهذا الصدد حاولنا إبراز الجهود المبذولة من اجل مواكبة التطور التكنولوجي بتطور تشريعي وأكدت بأنه من واجب القانون أن يحتوي المسار الصحيح للتوسع التكنولوجي وتبادل المعلومات.

والمشرع الجزائري لم يقف عند هذا الحد بل سارع إلى تعديل قانون العقوبات وافرد بابا خاصا بالجرائم الالكترونية وهو الباب السابع مكرر وبالموازاة مع ذلك وسع من اختصاص ضباط

الشرطة القضائية و وكلاء الجمهورية وقضاة التحقيق بنية ملاحقة جرائم المعلوماتية المستحدثة وإنشاء ما يسمى بالأقطاب القضائية.

بالإضافة إلى بعض النصوص الخاصة والتي عنيت بمسالة تجريم الأفعال المادية المكونة للجرائم المعلوماتية مثل : القانون 03/2000 المتعلق بالبريد والمواصلات ولعل ابرز قانون أنتجه المشرع الجزائري في مجال مكافحة الجرائم المعلوماتية هو القانون رقم 04/09 المؤرخ في 05-08-2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي جاء بتقنيات جديدة ومعالم أخرى توضح القواعد الإجرائية في مجال تحريك الدعوى العمومية وتقفي أثار مجرمي المعلوماتية من خلال الترتيبات التقنية لمراقبة الاتصالات الالكترونية ورصدها وكيفية تفتيش المنظومة المعلوماتية عن بعد ثم إجراءات حجز المعطيات المعلوماتية، ولعل ابرز النتائج المتوصل إليها بموجب الموضوع محل الدراسة والبحث.

– أن التقنية المعلوماتية أصبحت من أساسيات حياة الدول والشعوب ولا يمكن تصور فكرة التخلي عنها، نظرا لتزايد مجالات استعمالها، في كافة الميادين، وذلك بالرغم من كافة التهديدات التي تشكلها الجريمة الالكترونية على امن وسلامة نظمها ومستعمليها.

– ظهور فئة جديدة من المجرمين والضحايا تحت وصفي "مجرمي المعلوماتية" و " ضحايا الإجرام المعلوماتي"، فالفئة الأولى أهم ما يميزها هو الذكاء والعلم والمعرفة، والخطورة الإجرامية في مجال المعلوماتية، وذلك بالرغم من خلو ملامحهم الشخصية من ملامح المجرمين لمتعارف عليها في

أصول علم الإجرام، وهو ما يزيد من درجة خطورتهم وتهديدهم نظرا لكونهم خارج مجال الشك والريبة مما يعزز ثقتهم في أنفسهم على مواصلة نشاطهم الإجرامي والسعي إلى تطوير أساليبهم الإجرامية، أما الفئة الثانية فعادة ما يميزها قلة المعرفة والتقدير بمجال المعلوماتية وهو ما يجعل منها أهدافا سهلة لمجرمي المعلوماتية.

– صعوبة اكتشاف الجريمة الالكترونية وكذا صعوبة التعرف على فاعليها وما يطرحه مشكل الإثبات في هذا الصدد.

– عدم كفاية النصوص القانونية المتوصل إليها من طرق المشرع الجزائري بمناسبة التجريم والعقوبة في مادة الجريمة الالكترونية وذلك لتعدد الأوصاف والكيفيات التي تتخذها الجريمة المعلوماتية في ظل التطور المذهل والمتسارع مما يلزم المشرع على أن يتماشى وما تفرضه المتمنيات المستقبلية لوضع آليات للتصدي لمثل هذه الجرائم.

– تكييف العقوبة لتصل إلى الجزاء المقرر على الفعل المعنوي وليس فقط الفعل المادي في الجرائم المعلوماتية.

من خلال كل العناصر السالفة الذكر خلصنا إلى اقتراح بعض لتوصيات التي من شانها. إثراء المنظومة الجزائية لمواجهة هذه الظاهرة وهي الجرائم الالكترونية والتي تجلى في :

– استحداث نصوص خاصة بمختلف الجرائم المعلوماتية إذ لا يجوز القياس في مسالة التجريم والعقاب.

قائمة المصادر والمراجع

قائمة المراجـــع:

أولا : المصادر القانونية :

أ/ الاتفاقيات الدولية :

– اتفاقية بودابست لمكافحة الجرائم المعلوماتية ،المنبثقة عن اجتماع المجلس الأوروبي بودابست ،المجر ،رقم 185 بتاريخ:2001/11/21.

– الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنبثقة عن اجتماع مجلس الوزراء الداخلية والعدل العرب بصفة مشتركة بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة مصر بتاريخ:2010/12/21 .

ب/ القوانـــين:

– الأمر 02/15 المؤرخ في 23-07-2015 الجريدة الرسمية للجمهورية الجزائرية الشعبية العدد40 المتضمن تعديل قانون الإجراءات الجزائية .

- الأمر 07/03 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع المعدل للأمر 17/93 المؤرخ في 1993/12/07 المتعلق بحماية الاختراعات المعدل للأمر 54/66 في 1963/03/03 المتعلق بشهادات المخترعين وإجازات الاختراع .

– القانون رقم 04/09 المؤرخ 2009/08/05 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد47،الصادرة في 16-08-2009.

– الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد44،الصادرة في 23-07-2003.

– القانون 2000/03 المؤرخ في 2000/08/05 ،المحدد للقواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد48 الصادرة في 06-08-2000.

– القانون 23/06 المؤرخ في 2002/12/20 ،المعدل والمتمم للأمر156/66 المتضمن قانون العقوبات ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد84 .

ثانيا: المراجـــــع:

أ): الكـــــتب:

-كامل عفيفي، جرائم الكمبيوتر، لبنان، منشورات الحلبي، الحقوقية، 2003.

– السعيدي سليمة،حجاز بلال ،جرائم المعلومات والشبكات في العصر الرقمي ، دار الفكر الجامعي، الطبعة الأولى،الإسكندرية، مصر، 2017.

– القاضي: أسامة احمد المناعسة، القاضي: جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة،الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان،الاردن،2014.

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

– أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت،الطبعة الأولى،دار الإعصار العلمي للنشر والتوزيع،عمان،الأردن، 2008.

– جميل عبد الباقي الصغير ،جرائم التكنولوجيا الحديثة ،دار النهضة العربية ،مصر.

– حجازي عبد الفتاح بيومي ،الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ،دار المحلة الكبرى، دار الكتب القانونية ،مصر،2004.

– خالد دوادي ،الجريمة المعلوماتية،الطبعة الأولى،دار الإعصار العلمي للنشر والتوزيع،عمان،الأردن،2008.

– زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدي عين مليلة، الجزائر 2011 .

– عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، –الإسكندرية،مصر،2015.

– عبد الرشيد مامون ،الحق الأدبي للمؤلف ،النظرية العامة وتطبيقاتها،دار النهضة العربية، القاهرة،مصر،1978.

– عبد الله أوهابية،محاضرات في قانون الإجراءات الجزائية ألقيت على طلبة السنة الثانية حقوق ،جامعة الجزائر، الموسم الجامعي 2010/2009 .

– عبد الله هلالي،تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات ،الطبعة الأولى ، دار النهضة العربية، القاهرة ،مصر،1997.

– علي عبد الله قهواجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر ،بيروت،1999.

– لينا محمد الأسدي ،مدى فاعلية القانون الجنائي في مكافحة الجريمة المعلوماتية ،دراسة مقارنة ،دار الحامد للنشر والتوزيع، الطبعة الأولى،عمان، الأردن، 2015.

– محمد الأمين البشري،التحقيق في جرائم الحاسب الآلي والانترنت،المجلة العربية للدراسات الأمنية والتدريب،العدد30،بتاريخ نوفمبر2000.

– محمد أمين الشوايكة: جرائم الحاسوب والانترنت(الجريمة المعلوماتية)،دار الثقافة للنشر والتوزيع،عمان الأردن،2009،ص08.

– محمد فتحي عبد الهادي ،مقدمة في علم المعلومات، مكتبة غريب، القاهرة، 1984.

– ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة ، مصر 2012.

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

– هشام فريد رستم ،قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 1995.

ب– الدراسات والبحوث:

– مخلوف عكاشة ،دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق ،تخصص قانون جنائي وعلوم جنائية ، جامعة د طاهر مولاي ، سعيدة،الجزائر،الموسم الجامعي 2017/2016.

فهرس الموضوعات

فهرس الموضوعات

الإهداء

شكر وتقدير

المقدمة **01**

الفصل الأول: ماهية الجريمة الالكترونية **07**

المبحث الأول: مفهوم الجريمة الإلكترونية..... **08**

المطلب الأول: تعريف الجريمة الإلكترونية..... **08**

الفرع الأول: تعريف الجريمة الإلكـترونية **08**

الفرع الثاني: خصائص الجريمة الإلكترونية..... **13**

المطلب الثاني: تصنيفات وأنواع الجرائم الإلكترونية..... **20**

الفرع الأول: تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة..... **21**

الفرع الثاني: تصنيف الجرائم تبعا لدور الكومبيوتر في الجريمة..... **23**

المبحث الثاني: الجرائم الالكترونية وفق ما جاء به المشروع الجزائري..... **25**

المطلب الأول: جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات..... **26**

الفرع الأول: جرائم الدخول والبقاء غير المشروع لأنظمة المعالجة الآلية للمعطيات..... **26**

الفرع الثاني: جرائم المساس بالأنظمة الآلية لمعالجة المعطيات..... **28**

المطلب الثاني : الجرائم الالكترونية الواقعة على الأموال..... **33**

الفرع الأول: جرائم التحويل غير المشروع للأموال أو جرائم الاحتيال الالكتروني..... **34**

الفرع الثاني: جرائم الاستخدام غير المشروع لأدوات الدفع الالكتروني..... **36**

الفرع الثالث: جرائم الاعتداء على الملكية الفكرية..... **39**

المطلب الثالث: جرائم التعدي على الأشخاص..... **42**

الفرع الأول: الجرائم الماسة بالحريات العامة..... **42**

الفرع الثاني: جرائم الاعتداء على حرمة الحياة الخاصة..... **44**

الفرع الثالث: جرائم الاستغلال الجنسي للأطفال عبر الانترنت **50**

الفصل الثاني: آليات مكافحة الجريمة الالكترونية والحد منها في التشريع الجزائري.....**56**

المبحث الأول: القواعد الموضوعية لمكافحة جريمة الالكترونية.....**58**

المطلب الأول: الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات الجزائري.....**61**

الفرع الأول: الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال المقررة في قانون العقوبات الجزائري **61**

الفرع الثاني: الحماية الجزائية للجريمة الالكترونية من خلال النصوص المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات **76**

المطلب الثاني: الحماية الجزائية للمعلوماتية من خلال القوانين و التنظيمات الأخرى **97**

الفرع الأول: مواجهة الجريمة الالكترونية من خلال نصوص الملكية الفكرية.....**97**

الفرع الثاني: الحماية الجزائية للمعلوماتية من خلال القانون 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية و اللاسلكية **105**

المبحث الثاني: القواعد الإجرائية لمكافحة الجريمة الإلكترونية.....**107**

المطلب الأول:القواعد الإجرائية المنصوص عليها في ظل قانون الإجراءات الجزائية.....**107**

الفرع الأول:قواعد الاختصاص المحلي.....**108**

الفرع الثاني:إجراءات البحث و التحري.....**112**

المطلب الثاني: الحماية الجزائية للمعلوماتية من خلال القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.....**125**

الفرع الأول: أسباب صدور القانون رقم 04/09 و مضمونه **126**

الفرع الثاني: الإجراءات المستحدثة بموجب القانون 09/ 04 .....**129**

الخاتمة **135**

قائمة المصادر والمراجع **139**