الإشكالات القانونية في تجريم الإعتداء على أنظمة المعلومات

أ- عباوي نجاة أستاذ مساعد أ
كلية الحقوق و العلوم
جامعة محمد الطاهري بشار (الجزائر)

الملخص:

يعد الوقوف على الإشكالات التي تواجه تجريم الإعتداء على أنظمة المعلوماتية من الموضوعات الهامة التي باتت الحاجة إلى دراستها دراسة دقيقة ومتأنية من الضرورات الملحة، لا سيما وأن الجزائر كغيرها من الدول النامية لا تزال تتدرج في النهل من هذه الأنظمة تخوفا من الإنفتاح على شبكات عالمية رافقها إجرام بلغ أوج تطوره في حين لا يزال استعداد الدول النامية التقني والقانوني في بداياته .

وقد حاولنا من خلال هذه المداخلة أن نقف على بعض الإشكالات التي صاحبت وضع نصوص جزائية لمكافحة جـرائم الإعتداء على أنظمة المعلوماتية وتلك التي تعترض تطبيقها أو تجعلها بدون فحوى سواء ما تعلق منها بالتـداخل بـين الأفعـال المرتكبة أو بغياب النصوص المتسعة للأفعال التي أغفلت وبقيت محل اختلاف قضائي ، بعض يبيحها وآخر يدرجها ضمن أحكام نصوص عامة، عاملين من خلال ذلك كله على استخلاص موقف المشرع الجزائري من بين النصوص التي جرم فيها المسـاس بأنظمة المعلوماتية.

الكلمات المفتاحية: جرائم المعلوماتية – أنظمة المعلومات – الدخول – البقاء – الإعتراض – التلاعب.

Abstract

To stand on the issues facing the criminalization of violating IT systems is one of the most important topics that require a thorough and careful study. And like other developing countries, Algeria is still cautious about these systems for fear of openness to global networks and criminality related to it which has reached the peak, while the thechnical and legal readiness of the developing countries is still in its beginnings.

In this paper we tryied to adress some issues that arise while making penal provisions to fight crimes of violating IT systems or hinder their application, and the cases where no provision can be found, both those related to the overlap between the acts committed or the lack of provisions that makes the criminal act a topic of judicial controversy, some permit it while others include it within the rules of general provisions , working through all this to draw the position of the Algerian legislator through these provisions .

Keywords: cybercrime - Information Systems - Access - stay - Intercept – manipulation

مقدمـــة

كان لربط الحاسبات الآلية بوسائل الإتصال وما حققته من تدفق للمعلومات وانسيابها بشكل كفل الإستفادة منهـــا الأثر الأكبر في زيادة أهميتها و الإعتماد عليها إذ غزت مختلف الأنشطة والأعمال سعيا مـــن القـــائمين عليهـــا إلـــى استغلال أمثل لفوائدها.غير أن هذا الإنتشار الواسع لهذه التقنيات وأهمية ما قد يجنى من وراء الإعتداء عليها وســـهولة ارتكابها شكلت اغراءات للمجرمين استفحلت في ظلها الجرائم الماسة بأنظمة المعلومات، وقد شهد استفار المســـاعي لمكافحة جرائم المعلوماتية تضاربا في أحكام القضاء ومواقف الفقهاء واختلافا في النصوص التشريعية الجزائية بشـــكل غير مسبوق بحكم الحداثة النسبية لهذه الظاهرة والتطورات المتلاحقة لها الناجمة عن اتصالها بتقنيات عالية ومتســـارعة استخدمت في شتى المجالات.

فلا تخلو المحاولات المبذولة لتجريم أشكال هذا الإجرام من الإشكالات المثارة بشأنه، والتي تتجلى أساسا في ما يثار من الإختلافات التشريعية المحددة لشروط تجريمها في خضم تعدد التشريعات وتنوع الشروط التي من شأنها عرقلة توحيد شروط قيام الجريمة باعتبارها عاملا ضروريا لتعزيز جهود التعاون لمكافحتها. وهي من المسائل التي تحتاج إلى الضبط والفصل فيها كخطوة مهمة في مسار التصدي لجرائم المعلوماتية لما تحمله من صعوبات ترافق موجات التشريع في ميدان تقنيات المعلومات و تعيق تطبيق نصوصه.

إرتأينا أن نستهل هذه الدراسة بمطلب أول نبحث فيه إشكالية الركن الشـــرعي فـــي الجـــرائم الماســـة بأنظمـــة المعلومات، ونتبعه بمطلب ثان يتضمن صعوبات تحديد الفعل المجرم، لنتطرق لأهم العوائق المحيطة بتحديد مجـــالات التلاعب بالمعطيات في مطلب ثالث.

المطلب الأول: إشكالية الركن الشرعي في الجرائم الماسة بأنظمة المعلومات:

أثارت حداثة جرائم أنظمة المعلومات مشكلة اعتماد مصطلحات تقنية غير معهود التعامـــل بهـــا، فضـــلا عـــن الإختلافات التشريعية حول أنماط صياغة النصوص التجريمية للأفعال المكونة لها.

الفرع الأول: إشكالية المصطلحات.

تطرح الجريمة المتخذة من النظام أو معطياته محلا لها - نظرا لطابعهـــا التقنـــي الحـــديث- مشـــكلة تضـــمن النصوص المجرمة لها مصطلحات غامضة المفهوم قد تقف عائقا أمام فهم النصوص.

يختلف موقف التشريعات إزاء تعريف المصطلحات الخاصة بهذه الجرائم ، فهناك تشريعات تعمد إلـــى وضـــع تعريفات في صلب القانون مثل بعض التشريعات الأمريكية، وهناك تشريعات أخـــرى توكـــل مهمـــة تحديـــد معـــاني المصطلحات للفقه والقضاء مثلما فعل التشريع الفرنسي.

أورد القانون العربي النموذجي تعريفات للمصطلحات الواردة بنصوص التجريم، فخطى بـــذلك خطـــوة مهمـــة جديرة بالإقتداء نظرا لكثرة المصطلحات التقنية المتعلقة بالإجرام في مجـــال تقنيـــة الحاســـبات والإتصـــالات وبحكـــم غموضها وحداثتها, وقد تضمن القانون العربي النموذجي تعريفات لمصطلحات عدة منعا لأي التباس في فهم النصوص فعرف الوسيط الإلكتروني، والتحليل، والشفرة، تعطل النظام، البيانات، البريد الإلكتروني،الشبكة، كلمـــة الســـر، اللغـــة المبرمجة، برامج الحاسب، الإلتقاط، الكتابة، نظام المعالجة الآلية للبيانات، إتلاف البرامج، التجارة الإلكترونية، التوقيـــع الإلكتروني، التشفير، الموقع، والإختراق.[1]

وقد انتهج المشرع الجزائري نهج المشرع الفرنسي إذ لم يقم بشرح المصطلحات الواردة في نصـــوص تجـــريم المساس بأنظمة المعلومات باعتبارها ألفاظ حديثة وذات طابع تقني وإن كان قد اعتمد نهـــج شـــرح الألفـــاظ الخاصـــة بمجالات معينة والواردة في العديد من القوانين التي وضعها سواء قبل أو بعد صدور تعديل قانون العقوبـــات بموجـــب

القانون المجرم للإعتداء على أنظمة المعلومات ولعل التفسير الأنسب لموقف المشرع الجزائري وغيره من المشرعين هو انعدام الإجماع على المقصود ببعض العبارات والصعوبة التي تكتنف توحيدها بسبب تطوراتها المتسارعة.[2]

الفرع الثاني: أنواع الصياغات التشريعية.

هناك عدة أنماط تشريعية قد يلجأ إليها المشرع لصياغة نصوص الحماية الجزائية لنظم المعلومات مع إمكانية الجمع بينها، نوجزها فيما يلي:

1. الإضافة: تضيف بعض الدول إلى النصوص القائمة بالفعل تلك الحالات التي يرتكب فيها الجاني النشاط الإجرامي الوارد بها عن طريق أنظمة المعلوماتية، ومن هذا القبيل ما نصت عليه المادة الثامنة من القانون الخاص بجرائم التزوير والتزييف لعام 1981 في بريطانيا، كما قد تضيف إلى محل السلوك الإجرامي الوارد بالنصوص القائمة المعلومات التي يحتوي عليها نظام المعلوماتية، مثل اعتبارها محلا للإستيلاء عليها في نصوص جريمة السرقة[3].
2. وضع نصوص جديدة قياسا على نصوص تقليدية بالفعل: في هذه الحالة يصاغ نص جديد يتفق مع أحد الأشكال التقليدية للسلوك الإجرامي وقد اتجهت العديد من الدول للعمل بهذه الطريقة.
3. قامت بعض الدول بوضع نص رئيسي واحد يستطيع التعامل مع الأوجه المختلفة للجريمة المعلوماتية، وقد قامت بذلك الولايات المتحدة الأمريكية.[4] كما قد يتم تجميع كل ما يتعلق بالجريمة المعلوماتية في قسم مستقل ملحق بالتشريع الجنائي أو في تشريع مستقل، وتوضح كل من هاتين الطريقتين الطبيعة الخاصة للجريمة المعلوماتية كما تسمح بوضع عقوبات خاصة لهذه الجريمة بحيث تتلاءم معها.

4. إن الجمع بين أكثر من نمط من هذه الأنماط أمر وارد، والحقيقة أن اختيار أي من هذه الطرق يتأثر بشكل كبير بالوقت الذي يتدخل فيه المشرع لمواجهة الجريمة المعلوماتية، وكذلك بطبيعة النظام القانوني في كل دولة. فعلى سبيل المثال تعد السويد واحدة من أولى الدول التي واجهت الجريمة المعلوماتية تشريعيا، فقد قامت بوضع نص عام يتعلق بالجريمة المعلوماتية في تشريع خاص، وبعد عدة أعوام أثناء تعديل قانون العقوبات قام المشرع بإضافة عدة نصوص تتعلق بالجريمة المعلوماتية قياسا على نصوص قائمة بالفعل في القانون، مع الإحتفاظ بالنص الأول المتعلق بهذه الجريمة.

ويرى البعض أن التعامل مع الجريمة المعلوماتية عن طريق اختيار نمط تشريعي واحد دون غيره يمكن أن يسفر عن فراغ تشريعي في كثير من الحالات، كما أن الجمع بين أكثر من أسلوب لا يخلو أيضا من المخاطر، فالإضافة إلى النصوص، وإضافة نصوص جديدة قياسا على نصوص قائمة بالفعل إذ لم يتم بكثير من الحذر فإن أكثر من نص قانوني يمكن أن ينطبق في الوقت ذاته على النشاط الإجرامي الواحد[5].

أما المشرع الجزائري فقد اتجه إلى خص جرائم المعلوماتية بقسم خاص من قانون العقوبات وهو القسم السابع مكرر المتضمن المساس بأنظمة المعالجة الآلية للمعطيات ،عند تعديله لقانون العقوبات بإضافة هذا القسم المشتمل على سبعة مواد تهتم بشتى أنواع الإعتداء على أنظمة المعلوماتية.[6] وإن كنا نرى عدم كفايتها إلا أن أسلوب خصها بنصوص تحكمها وحدها وعدم جعلها أجزاء من جرائم أخرى هو منهج سليم يتفق و الإعتراف بوجود ظاهرة جديدة بحاجة إلى التدخل التشريعي كما يستقيم وضرورة افراد عقوبات مناسبة لها، فضلا عن إمكانية إخضاعها للقواعد العامة في القانون الجزائي الجزائري.

المطلب الثاني: صعوبة تحديد الفعل المجرم.

شهدت التشريعات المجرمة لأفعال الدخول والبقاء غير المصرح بهما واعتراض أنظمة المعلومات اختلافات عدة وعرفت الآراء الفقهية بهذا الشأن تضاربا كبيرا، سنحاول في هذا المطلب الوقوف على أهمها.

الفرع الأول: الاختلافات القائمة حول تجريم الدخول غير المصرح به.

ثار بين الفقهاء جدل الواسع ما بين مؤيد ومعارض لتجريم الدخول غير المصرح به إلى أنظمة المعلوماتية، سنوضح فيما يلي طبيعة الإختلاف الفقهي بين الإتجاهين و موقف بعض التشريعات من هذا الجدل.

أولا: طبيعة الإختلاف الفقهي.

يرى الإتجاه المؤيد لتجريم الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات أن الدخول غير المصرح به إلى النظام سواء كان مقصودا في ذاته أو كان بغرض ارتكاب جريمة أخرى كالإتلاف أو الإفشاء أو السرقة، فإن له الكثير من الآثار السلبية التي تلحق صاحب النظام أو المعلومات.

بالإضافة إلى ذلك فإن قابلية المعلومات المبرمجة آليا للوصول غير المشروع إليها يفوق كثيرا ما كان عليه الحال قبل عصر تقنيات الحاسبات و الاتصالات، ذلك أن المعلومات الهامة والمدونة في أوراق وسجلات كان يتم حفظها في أماكن يصعب الوصول إليها، مما يجعلها بمنأى عن التلاعب بها والإطلاع عليها، وخاصة في مواجهة غير المتعاملين في المؤسسات المحفوظة بها، في حين أن المعلومات المبرمجة آليا والمتصلة فيما بينها عن طريق شبكات الإتصالات تكون أكثر عرضة للوصول غير المشروع إليها[7].

وتترتب في كثير من الحالات خسائر مادية كبيرة على مجرد محاولة وقف الدخول ولو لم تترتب عليه أضرار فعلية تلحق بالنظام وبالمعلومات التي يحتوي عليها[8].

هناك رأي يخالف ذلك ويرى أنه لا ضرورة لتجريم الدخول غير المصرح به إلى النظام لأنه لا توجد حاجة ملحة تستدعي هذا التجريم، حيث لم تبين الدراسات والإحصاءات المختلفة هذه الضرورة كما أن مجرد الدخول غير المصرح به إلى أنظمة المعلومات دون أن يكون لدى صاحبه نية ارتكاب جريمة لاحقة على هذا الدخول، لا يعدو أن يكون مجرد استعراض لبعض الملكات الذهنية والفنية التي يمتلكها، وهو ما لا يمكن أن يشكل جريمة يعاقب عليها.

فضلا عن ذلك فحالات الدخول غير المصرح به والتي لا يترتب عليها إتلاف للمعلومات أو استخدامها لغرض غير مشروع لا يمكن الكشف عنها حيث لا تترك أثرا يدل عليها، فالصعوبة العملية التي سوف تواجه جهات التحقيق في حالات الدخول غير المصرح به- نظرا لما تنطوي عليه من صعوبة فنية بالغة- ستكون عائقا دون تجريم هذا السلوك.

نؤيد ما ذهب إليه الإتجاه الأول الذي يرى ضرورة تجريم الدخول غير المصرح به، فإذا كانت الإحصائيات لا تبين بالفعل الحجم الحقيقي للدخول غير المصرح به فإن ذلك يرجع إلى عدم وجود تجريم لهذا الدخول في كثير من الدول، مما يؤدي بدوره إلى عدم الإبلاغ عن الحالات التي تقع بالفعل وبالتالي لا تظهر في الإحصائيات, وحتى في الدول التي تجرم قوانينها الدخول غير المصرح به، فإن المشاكل التي تواجه الجريمة المعلوماتية بشكل عام وتحول دون إحصاءها على نحو صحيح، تواجه الدخول غير المصرح به شأنه في ذلك شأن الجرائم المعلوماتية الأخرى.

و الدخول غير المصرح به وإن لم تصاحبه نية ارتكاب جريمة لاحقة عليه، فإن هذه النية قد تتولد فيما بعد، كما أن هذا الدخول في ذاته ينطوي على مساس بسرية المعلومات ولو لم يترتب على ذلك سلوك لاحق يتسم بعدم المشروعية, أما فيما يتعلق بصعوبة اكتشاف الدخول غير المصرح به فإن الواقع العملي يؤكد أنه قد تم بالفعل الكشف عن كثير من الحالات إما عن طريق الإجراءات الأمنية التي يحتوي عليها نظام المعلوماتية،[9] وإما عن طريق الفاعل نفسه[10]، أو عن طريق المعلومات التي تم التوصل إليها وتم استخدامها بأية صورة من الصور.

وفيما يخص الصعوبة الفنية التي ينطوي عليها التحقيق في هذه الجريمة، فهذه الصعوبة تواجه جرائم المعلوماتية جميعا بلا استثناء، وعلى الرغم من ذلك هناك اتجاه قوي يذهب إلى ضرورة تجريمها.

ثانيا: موقف التشريعات.

تم تجريم الدخول غير المصرح به إلى أنظمة المعلوماتية في العديد من الدول، وإن اختلفت فيما بينها من حيث الشروط المتطلبة لتطبيق نصوصه.[11]

أثار تحديد الهدف الذي يعقب عملية الدخول خلافا أظهرته النصوص القانونية المختلفة التي تناولت الجريمة، فالدخول غير المصرح به إلى نظام المعلوماتية يستمد عدم مشروعيته من كونه غير مصرح به أو كونه مخالف لأحكام القانون.غير أن هذا الدخول قد يكون مقصودا في ذاته كما قد يكون مقصودا باعتباره وسيلة لتحقيق غاية أخرى، سواء تمثلت هذه الغاية في الحصول على المعلومات لتحقيق غرض ما،أو كان الدخول إلى النظام ممرا يتم من خلاله الدخول إلى نظام آخر من الصعب على الفاعل الدخول إليه ابتداء[12].

وقد أسفر ذلك عن التساؤل حول مدى ملائمة تدخل المشرع الجنائي للعقاب على الدخول المجرد إلى نظام المعلوماتية، وتنازعت الإجابة عن هذا السؤال ثلاثة اتجاهات، يرى الأول أنه لا يمكن عقاب كل من يقرع باب النظام وإنما يجب أن يحاط التجريم بشروط محددة[13]،في حين يذهب اتجاه آخر إلى أن جريمة الدخول إلى الأنظمة المعلوماتية تقوم بمجرد فعل الدخول غير المصرح به بغض النظر عن النتيجة التي تعقب هذا الدخول[14]، بينما يذهب اتجاه ثالث إلى اعتبار جريمة الدخول غير المصرح به إلى الأنظمة الجريمة المعلوماتية الجريمة الأساسية، أما ما يعقب ذلك من أفعال فهي لا تشكل سوى ظروف مشددة[15].

وقد حدا المشرع الجزائري حدو المشرع الفرنسي في تجريمه لمجرد الدخول غير المصرح به في المادة 394 مكرر أيا كانت النتيجة التي تعقبه، وكان موفقا في اتجاهه كونه أحاط نظام المعالجة الآلية بضمانات فعالة تحميه من الإختراق.

الفرع الثاني: تمييز الدخول عن البقاء داخل الأنظمة

يرجع البعض الإختلاف القائم بين جريمتي الدخول و البقاء غير المصرح بهما إلى أن جريمة الدخول جريمة ايجابية تقتضي إتيان فعل الدخول، في حين تقوم جريمة البقاء بسلوك إجرامي سلبي، فرغم دخول الجاني صدفة أو خطأ، و رغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام و بمعنى آخر يمتنع عن الخروج، لذلك فالنشاط الإجرامي - حسب رأي هذا الجانب- يمثل في هذه الصورة سلوكا سلبيا من الجاني.[16]

إلا أن هناك جانب آخر- نؤيده- يرى أن الإمتناع عن الخروج من النظام الذي تم الدخول إليه ليس مناط التجريم، بل أن السلوك المجرم هو البقاء داخل هذا النظام بعد الدخول إليه مع العلم بأن هذا البقاء غير مصرح به وهو ما يشكل سلوكا ايجابيا.

ذهب بعض الفقه للقول بأن طبيعة البقاء هي طبيعة الدخول ذاتها و ينطبق عليه كل ما ينطبق على الدخول، لكن ما يميز بينهما هو وقوع الجريمة في وقت واحد أواستمرارها، [17]فيذهب رأي إلى اعتبار كل من جريمتي الدخول و البقاء من الجرائم المستمرة،بينما يرى رأي آخر اعتبار جريمة الدخول جريمة متتابعة الأفعال و جريمة البقاء مستمرة، ورأي ثالث يجد جريمة الدخول وقتية ذات أثر ممتد، وجريمة البقاء جريمة مستمرة.

لهذا التمييز أهمية في الإشكالات المطروحة حول هاتين الجريمتين والتي سنتناولها في العنصرين التاليين:

أولا: حدود كل من جريمتي البقاء والدخول غير المصرح بهما.

ذهب رأي فقهي إلى القول أن جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول فعلا إلى النظام، وإن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل ، وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام وتنتهي بانتهاء حالة البقاء.

ويؤخذ على هذا الرأي أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة، لهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، وأخذ على الرأي الثاني أيضا صعوبة إثبات علم المتدخل.

يرى رأي ثالث أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام، غير أن هذا الرأي وإن أمكن توفير تقنياته الفنية إلا أنه لن يكون متاحا إلا بالنسبة للشركات والمؤسسات الكبيرة فقط.[18]

ونرى أن الرأي الأصوب في مثل هذه الظروف هو اعتبار جريمة الدخول إلى النظام منتهية بمجرد إتيان الفاعل لسلوكه المجرم بدخول النظام كله أو إلى جزء منه غير مصرح له بالدخول إليه، أو بمجرد إنهاءه لفعله المنم عن تجاوز للتصريح الممنوح له ليجد نفسه أمام نظام أو جزء منه غير مسموح له بالدخول إليه، وتبدأ عندها مباشرة جريمة البقاء في نظام غير مصرح له أصلا بالدخول إليه والتي يكفي البقاء لتوافر الركن المادي بها ريمة ولا يشترط التقاط المعلومات أو أي شكل من أشكال الضرر.

ثانيا: تضمن تجريم الدخول لفعل البقاء غير المصرح به.

يجمع الفقه على أن البقاء غير المصرح به داخل نظام المعلوماتية جريمة مستمرة،نظرا لاستمرار الإعتداء على المصلحة التي يحميها القانون كلما استمر البقاء غير المصرح به، كما أن الدخول غير المصرح به مجرم بمجرد الدخول إلى النظام أو بالوصول إلى المعلومات التي يحتوي عليها، لأنه في كلتا الحالتين تتم الجريمة بمجرد الدخول إلى النظام أو بالوصول إلى المعلومات.[19]

يرى البعض أنه في حالة تجريم الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات دون أن يشير النص إلى تجريم البقاء غير المصرح به أو يتناوله بالتجريم نص آخر، فإن على القضاء أن يجيب على ما إذا كان البقاء غير المصرح به داخل النظام يأخذ ذات الأحكام التي تسري على الدخول غير المصرح به أم لا، ويذهب هذا الرأي إلى أن الإجابة عن هذا التساؤل تكمن في طبيعة كل جريمة.

فإذا كانت جريمة الدخول غير المصرح به وقتية، فإنها في بعض صورها تكون متتابعة الأفعال حيث تقوم على أفعال متعددة تجمع بينها وحدة الحق المعتدى عليه ووحدة الغرض الإجرامي المستهدف بها.

يتحقق ذلك في حالة النصوص التي تجرم الدخول غير المصرح به الذي يستهدف الوصول إلى المعلومات أو البرامج، أو تلك التي تجرم الدخول إلى كل جزء من النظام، ذلك أنه بعد دخول الفاعل إلى النظام يمكن القول من الناحية التقنية أن فعل الدخول يتكرر بالدخول إلى كل برنامج وكل جزء من النظام، فنكون أمام أفعال متماثلة يعد كل منها جريمة في ذاته لو اكتفى الجاني به لعوقب من أجله.

ينتهي أصحاب هذا الرأي إلى أنه في هذه الحالة يمكن العقاب على البقاء غير المصرح به، لأنه بعد اكتساب الدخول صفته غير المشروعة فإن الدخول يتحقق بالوصول إلى أية معلومة بعد ذلك أو أي جزء من النظام.

تثور الصعوبة في القوانين التي تتطلب لقيام جريمة الدخول غير المصرح به أن ينطوي الدخول على اختراق الإجراءات الأمنية الخاصة بالنظام، إذ يجب لإعتبار الجريمة متتابعة الأفعال في هذه الحالة أن يكون كل جزء من النظام تم الدخول إليه مشمولا بهذه الحماية.

أما في حالة النصوص التي تجرم مجرد الدخول إلى النظام، فإنه لا يمكن العقاب على البقاء غير المصرح به ما لم ينص على ذلك صراحة، [20]وهو ما فعله المشرع الفرنسي حيث نص صراحة على تجريم البقاء داخل النظام إثر تجريمه للدخول المجرد غير المصرح به[21] .

الواقع أنه وإن كانت ضرورة حماية أنظمة المعلوماتية تستدعي اعتبار جريمة الدخول غير المصرح به جريمة متتابعة الأفعال، الأمر الذي يجعل كل دخول إلى أي جزء من النظام يعتبر جريمة تتوجب العقاب بمجرد اكتساب فعل الدخول صفته غير المشروعة، ما يجعل البقاء داخل النظام مجرما، إلا أن مبدأ الشرعية في قانون العقوبات يتطلب تجريم البقاء غير المصرح به داخل أنظمة المعالجة الآلية للمعطيات صراحة، سواء كانت جريمة الدخول غير المصرح به تتم بمجرد الدخول إلى النظام، أو تشترط الوصول إلى ما يحتوي عليه من بيانات وبرامج لما يشكله فعل البقاء من تهديد لنظام المعلوماتية بمختلف محتوياته شأنه في ذلك شأن الدخول غير المصرح به.

وقد عمل المشرع الجزائري على ألا تفلت مثل هذه الحالات من العقاب، فقام بتجريم البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية للمعطيات مسايرا في ذلك ما ذهب إليه المشرع الفرنسي.

وباستثناء هذا الإشكال تبدو أهمية التفرقة بين الدخول والبقاء من حيث الاستمرارية ضئيلة.

الفرع الثالث: تجريم إعتراض أنظمة المعلومات

يرى الفقه أن الوصول غير المصرح به للمعلومات داخل أنظمة المعلوماتية قد يتم مباشرة عن طريق الدخول غير المشروع إلى النظام، أو بوسيلة غير مباشرة باعتراض النظام.[22]

يتمثل السلوك المادي لهذه الجريمة في قيام الفاعل بالتدخل غير المشروع لمعرفة محتوى الإتصالات التي تتم عبر شبكات المعلومات داخل نظام المعلوماتية، أو بين أنظمة معلوماتية مختلفة حيث يقوم بالتقاط المعلومات المتضمنة في هذا الإتصال.[23]

الوسيلة الأساسية لإعتراض أنظمة المعلوماتية تتمثل في استخدام الموجات الكهربائية الصادرة عن النظام (Electromagnetic Radiation)[24]، فاعتراض نظام المعلوماتية كما هو معروف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهربائية (Electromagnetic Pikup) هو جمع للمعلومات عن بعد[25].

يختلف الدخول غير المصرح به إلى نظام المعلوماتية عن اعتراض هذا النظام من حيث النشاط الإجرامي في كل منهما، فالدخول إلى النظام لا يتأتى إلا بتشغيله للولوج إلى ما يحتوي عليه من معلومات، أما في حالة التقاط المعلومات عن طريق اعتراض النظام فإن عملية تشغيله تكون قد بدأت بالفعل بواسطة شخص آخر غير الجاني، واقتصر دور الفاعل على اعتراضه للوصول إلى المعلومات التي تتضمنها عملية الإتصال.

أدت هذه الإختلافات بين الدخول إلى نظام المعلوماتية وبين اعتراضه إلى الإتجاه نحو إفراد نص خاص بتجريم كل منهما، وقد أوصى المجلس الأوروبي بضرورة إفراد نص خاص لإعتراض أنظمة المعلوماتية يتم بمقتضاه تجريم كل اعتراض لاتصال يتم من أو إلى أو داخل أنظمة المعلوماتية عبر شبكات الإتصالات.[26]

سارت عدة دول على هذا النهج وجرمت سلوك الإعتراض بنصوص خاصة وواضحة،من ذلك مثلا قانون العقوبات الكندي الذي جاء في مادته 1/430 .[27]

كما عاقبت المادة 342 من القانون ذاته كل شخص يسعى باستخدام وسائط مغناطيسية، صوتية، أو ميكانيكية أو أي أداة أخرى لوقف أو اعتراض أو التسبب باعتراض بصورة مباشرة أو غير مباشر أي وظيفة لنظام المعلوماتية.[28]

جرمت المادة الثامنة من القانون البرتغالي رقم 109 لعام 1991 الخاص بجرائم المعلوماتية اعتراض عمليات الإتصال التي تقوم على نقل المعلومات داخل أنظمة الحاسبات الآلية وشبكات المعلومات باستخدام وسائل تقنية، بينما تجرم المادة السابعة الدخول غير المصرح به إلى أنظمة المعلوماتية، وقد حددت المادة الثانية من هذا القانون المقصود بفعل الإعتراض ووصفته بأنه كل عمل يهدف إلى الوصول إلى المعلومات التي تتضمنها أنظمة المعالجة الآلية للمعطيات باستخدام أجهزة كهرومغناطيسية، سمعية، ميكانيكية أو غير ذلك.[29]

ورغم ذهاب بعض الفقه للقول بأن تجريم فعل الدخول غير المصرح به يشمل فعل الإعتراض دون الحاجة للنص على تجريمه بنصوص خاصة، إلا أننا لا نؤيد هذا الإتجاه للاختلاف الكبير بين الجريمتين والذي يجعلنا ندعو المشرع الجزائري إلى تضمين حماية أنظمة المعالجة الآلية للمعطيات نصوصا تجرم الإعتراض باعتباره سلوكا مهددا لسرية المعلومات.

المطلب الثالث: إشكالات تحديد مجال التلاعب بالمعطيات

إن ارتباط أنظمة المعالجة الآلية للمعطيات بميادين عديدة وتزايد الإعتماد عليهما في مختلف التعاملات جعل الحالات التي يمكن ارتكاب جريمة التلاعب فيها لا حصر لها، وإن كانت تتفاوت فيما بينها من حيث مقدار الخسائر الناجمة عنها وعدد الحالات المرتكبة.

سنتناول تلك الحالات في هذا المطلب من خلال فرعين اثنين، بغية تحديد موقف التشريعات من هذه الجرائم التي تعتبر أبرز ميادين التلاعب بالمعطيات.

الفرع الأول: التلاعب بمعطيات أنظمة التحويل الآلي للأموال.

يتيح استعمال نظام التحويل الآلي للأموال إمكانيات كبيرة في الوصول بشكل أسرع إلى الأموال و الخدمات على نطاق جغرافي واسع، مع خلق نوع من الإستقرار في المعاملات المالية بحكم السرعة الكبيرة التي تتم بها عمليات الإيداع و السحب مما يجعل جميع الأطراف على علم تفصيلي بموقفهم المالي. فضلا عما توفره هذه الأنظمة من زيادة لحجم المبيعات وتقليل للنفقات و حماية للأموال.

رغم ما تتمتع به نظم التحويل الآلي للأموال من مزايا فإن المشاكل الناشئة عنها،والناجمة عن كونها نظاما معلوماتيا يقوم على مجموعة من التحويلات لمعلومات تمثل قيما معنوية في تزايد مستمر لما جذبته من أنماط إجرامية جديدة.

1- مفهوم التلاعب بنظم التحويل الآلي للأموال.

جاء في القانون الفيدرالي الخاص بنظم التحويل الآلي للأموال للولايات المتحدة الأمريكية أن هذه النظم تشمل كل تحويل يبدأ من خلال نهاية طرفية إلكترونية، هاتف، حساب آلي أو شريط مغناطيسي عن طريق إعطاء أمر، تعليمات، أو التصريح لمؤسسة مالية بإجراء عمليات سحب أو إيداع لإحدى الأرصدة، ويعتمد نظام التحويل الآلي للأموال على عمليات تحويل من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر بالبنك الذي يوجد به حسابه.[30]

يتكون نظام التحويل الإلكتروني للأموال من مجموعة أجزاء تعمل داخل إطار واحد تتمثل في الحاسب الآلي المركزي, نقاط البيع, النهايات الطرفية في البنوك,و أجهزة الصرف الآلي.

أشار تقرير صادر عن إدارة العدالة الأمريكية عام 1982 حول نظم التحويل الإلكتروني للأموال إلى خمسة أنماط إجرامية يتصور ارتكابها داخل هذه النظم.

أ- التلاعب في المكونات المادية لنظم تحويل الأموال، ويتضمن ذلك استعمال خطوط الإتصال لخرق، تعديل أو تدمير البيانات أو طلبات التحويل لإستعمال البيانات الخاصة بهذه النظم في الإحتيال على المؤسسات.

ب- استعمال البرامج الخاصة بنظم التحويل الإلكتروني للأموال، والتلاعب بها بغرض إجراء عملية تحويل غير مشروعة أو بغرض إخفاءها.

ج- التلاعب في الإجراءات الداخلية لنظم تحويل الأموال كإصدار بطاقات ائتمانية مزدوجة.

د- الدخول إلى النظام باستخدام بطاقة شخص آخر لسحب مبالغ مالية من رصيده.

ه- الإعتداء على أجهزة الصرف بالكسر مثلا لسرقة ما بها من أموال.[31]

غير أن هذه الجرائم لا تشكل جميعها تلاعبا بالمعطيات باستثناء الحالة الثانية وتتخذ باقي الأشكال تكييفات مختلفة، وقد يرتبط السلوك المجرم بنظام تحويل الأموال دون أن ينطوي على تحويل للأموال بل يحول دون ذلك[32].

2- تجريم التلاعب في نظم التحويل الإلكتروني للأموال.

وضعت بعض التشريعات صياغة عامة لنصوص تجرم كل أشكال الحصول على المال عن طريق التلاعب بالمعطيات بما في ذلك استخدام بطاقة الإئتمان الممغنطة، في حين اتجهت تشريعات أخرى إلى تجريم كل نمط على حدى.

أولا: تجريم التلاعب في نظم تحويل الأموال بنص عام.

أوصى المجلس الأوروبي في توصيته رقم (89) الصادرة في شأن جرائم الحاسب الآلي ضمن القائمة الأساسية لهذه الجرائم بتجريم إدخال، حذف، محو، إعاقة معلومات أو برامج النظام، أو التدخل في عملية المعالجة الآلية للمعلومات بما يؤثر على نتيجة هذه المعالجة مسببا خسارة اقتصادية لشخص آخر بنية تحقيق ربح غير مشروع للفاعل أو لغيره.[33]

وقد جاءت عبارة إدخال المعلومات مجردة لتشمل إدخال معلومات صحيحة وغير صحيحة، بحيث يستوعب النص الحالات التي يتم فيها استخدام البطاقة الإئتمانية من قبل حاملها متجاوزا رصيده أو الحد الأقصى المسموح به.[34]

في الولايات المتحدة الأمريكية تم تجريم هذا الفعل بعد تعديل القانون الفيدرالي لجرائم الحاسبات الآلية عام 1986 بإدراج الفقرة (أ) (4) بالمادة 1030، وعلى مستوى الولايات تناولت كثير من القوانين الحصول غير المشروع على المال باستخدام طرق التلاعب بالمعطيات، من ذلك مثلا المادة 502 (ب) من قانون العقوبات الخاص بولاية كاليفورنيا،والقانون الخاص بجرائم الحاسبات الآلية لولاية كلورادو لعام 1979، وكذلك قانون الحاسبات الآلية لولاية هاواي عام 1992، وقانون ولاية كنساس لعام 1985[35].

في ألمانيا نص قانون العقوبات في المادة 263 (أ) على أن أنه يعد مرتكبا للجريمة كل من يقوم بنية تحقيق ربح غير مشروع له أو للغير وإلحاق ضرر بالغير، بالتأثير في نتيجة المعالجة الآلية للمعطيات عن طريق برمجة غير سليمة، استعمال بيانات غير صحيحة أوغير مكتملة، الإستعمال غير المصرح به للبيانات أو عن طريق التدخل غير المصرح به في عملية المعالجة ذاتها.

وتضمنت الجريمة المادة 386 (أ) من قانون العقوبات اليوناني على نحو يشبه ما أدرجته المادة سالفة الذكر من القانون الألماني.

ثانيا: تجريم التلاعب بنظم تحويل الأموال بنص خاص.

جرمت بعض التشريعات أشكالا محددة من التلاعب بالمعطيات للحصول على الأموال،وقد استدعت التدخل التشريعي هذا كثرة الإعتداءات بهذا المجال وتنوعها.

صدرت بالولايات المتحدة الأمريكية- سواء على المستوى الفيدرالي أو على مستوى الولايات- عدة قوانين تتصل مباشرة بنظم التحويل الإلكتروني للأموال وبتنظيمها، إلا أنها لم تتضمن الإشارة بشكل مباشر إلى التلاعب بهذه النظم، وتعرضت قوانين ولايات أخرى بها للإستعمال غير المشروع لهذه الأنظمة، منها مثلا ولاية كنتاكي التي تجرم التلاعب بالبيانات التي تحتوي عليها نظم التحويل الإلكتروني للأموال.[36]

في بريطانيا تمت إضافة المادة 15 (أ) إلى القانون الخاص بالسرقة عام 1996، وتعاقب هذه المادة كل من يقوم بتحويل إلكتروني غير مشروع للأموال أيا كانت الطريقة التي تم بها التلاعب في البيانات من أجل إجراء عملية التحويل.

الفرع الثاني : التلاعب باستعمال بطاقة الإئتمان الممغنطة.

يقصد ببطاقة الإئتمان[37] تلك البطاقة التي تحتوي على بيانات معالجة آليا، حيث يوجد بها شريط ممغنط يتضمن بيانات تتعلق بحساب العميل لدى البنك وشريط لاصق يدون عليه توقيع صاحب الحساب، وتمكن هذه البطاقة صاحبها من سحب مبلغ من جهاز السحب الآلي الخاص بالبنك أو الحصول على السلع والخدمات في حدود مبلغ معين، لتقتطع المبالغ بعد ذلك من حسابه، وقد لاقى الإستخدام غير المشروع لهذه البطاقة اختلافا كبيرا لدى الفقه والقضاء حول تكييفه لا يتسع المقام لتفصيله.[38]

اختلفت التشريعات في التصدي للجرائم المرتكبة باستخدام بطاقة الإئتمان، ففي سويسرا مثلا يجرم المشرع الإستعمال التعسفي للبطاقة من قبل حاملها في المادة 148 من قانون العقوبات في حين يدرج الإستخدام غير المشروع لهذه البطاقة من قبل الغير ضمن المادة 147 الخاصة بحالات التلاعب بالمعلومات داخل الأنظمة بقصد الإحتيال والتي تشمل أيضا التحويل الإلكتروني غير المشروع للأموال .

ويجمع القانون الفنلندي بين استعمال البطاقة من قبل حاملها أو من قبل الغير بصورة غير مشروعة في نص واحد،[39] وقد اتجهت تشريعات أخرى إلى الجمع بين جميع الأفعال غير المشروعة المتصلة ببطاقة الإئتمان سواء تمثلت في استعمالهامن قبل حاملها أو من قبل الغير أو تزويرها وتقليدها أو مجرد حيازة الأدوات اللازمة لهذا التزوير كما هو الحال في الولايات المتحدة الإمريكية.[40]

أما المشرع الفرنسي فقد اقتصر على تخصيص نصوص تجرم تزوير وتقليد بطاقة الإئتمان دون التطرق لاستعمالها غير المشروع،[41] مما أظهر اختلافا كبيرا لدى القضاء حول تكييف هذه الأفعال.[42]

عمد المشرع الفرنسي في القانون رقم 91/1382 المتعلق بتأمين الشيكات وبطاقات الدفع الإلكتروني إلى تجريم استخدام أو محاولة استخدام البطاقة المزورة في المادة 67 منه، وكان استحداث نصوص تجرم شتى أنواع التلاعب بنظام المعلوماتية في قانون العقوبات الفرنسي إحتواء لهذا النوع من الإجرام.

وسار المشرع الجزائري نهج المشرع الفرنسي بجعل صياغة المادة المجرمة للتلاعب داخل أنظمة المعلوماتية من المرونة بحيث تستوعب شتى أنواع التلاعب بالمعطيات وتساير التطور المتواصل بهذا المجال وإن كان قد خص بعض أنواع البطاقات بنصوص مستقلة، كالقانون 08-01 المتعلق بالتأمينات الإجتماعية الذي يجرم الاعتداء على بطاقة الشفاء الإلكترونية.[43] غير أن هذا القانون يبقى قاصرا عن حماية باقي أنواع البطاقات.

الخاتمة

بات السعي إلى التطور في شتى المجالات مرهونا باتصال الأنظمة المحلية بالشبكات العالمية بحكم ما تجلبه هذه التقنيات من مصالح وما توفره من طاقات أثبتت تجارب الدول المتقدمة استحالة تحقيق النمو في غيابها.

وقد استدعى اعتماد أنظمة تكفل تدفق المعلومات بشكل يمكن من الإستفادة منها وجود سبل ردعية تتولى حمايتها من أي اعتداء قد يؤدي إلى الإخلال بسير وظائفها ويشعر المتعاملين بها بالأمان إثر إيداع أموالهم أو خصوصياتهم بها.

غير أن وضع تشريعات تمكن من مواجهة هذه الجرائم يتطلب بداية تجاوز أهم الإشكالات التي تقف عائقا إما أمام تطبيق نصوصها وإما أمام تجسيد التعاون الدولي لمكافحتها, فحداثتها النسبية أدت إلى ظهور كثير من الاختلافات بشأنها سواء فقهيا , قضائيا ، وحتى تشريعيا، وقد خلصنا بعد الوقوف على أهم ما قد يثار بشأنها إلى النتائج التالية:

1-يثير الركن الشرعي في جرائم المعلوماتية إشكالية استخدام مصطلحات مختلفة ذات دلالات متباينة، وإن كانت بعض التشريعات قد عمدت إلى تحديدها، فإن غالبية المشرعين يوكلون تلك المهمة للفقه والقضاء، وقد اتجه المشرع الجزائري الإتجاه الثاني.

2- اختلفت التشريعات في شكل التدخل لمواجهة جرائم المعلوماتية، فذهبت بعضها إلى إضافة حالات الإعتداء على أنظمة المعلوماتية إلى النصوص القائمة، أو تعديلها على نحو يناسب احتواء جرائم المعلوماتية، واتجهت تشريعات أخرى إلى وضع نصوص جديدة ضمن تشريع مستقل أو ملحق بالتشريع الجزائي، وكثيرا ما اعتمدت الوسيلتين معا، أما المشرع الجزائري فقد ضمن النصوص المجرمة للإعتداء على أنظمة المعلوماتية في قسم خاص ضمن قانون العقوبات.

3- تذهب بعض التشريعات الجزائية إلى النص على تجريم فعل الدخول الذي قد ينصرف إلى الدخول أو البقاء أو اعتراض أنظمة المعلوماتية، في حين تفرق تشريعات أخرى بين هذه الإعتداءات وتفرد لكل منها نصا خاصا استنادا إلى التباين الجوهري بينها، وقد جمع المشرع الجزائري فعلي الدخول والبقاء غير المشروعين داخل أنظمة المعلوماتية في نص تجريمي واحد إلا أنه دل عليهما بمصطلحين مختلفين ولم يشر إلى فعل الإعتراض، مما يفتح الباب واسعا أمام اعتبار اعتراض الأنظمة مجرما بتجريم الدخول باعتباره أحد أشكاله أوعده فعلا مباحا إلى حين تجريمه بنص خاص.

وارتأينا ختاما لهذه الدراسة الإسهام بتوصيات قد تعزز من خطوات مكافحة جرائم المعلوماتية نلخص أهمها فيما يلي:

1- العمل على توافق السياسات الجزائية في مواجهة هذه الظاهرة الإجرامية كخطوة أولى للتعاون بين مختلف الهيئات والدول بوضع اتفاقيات دولية تستمد منها التشريعات الجزائية الداخلية ضوابط نصوصها التجريمية لتحقيق تنظيم جزائي شامل.

2- أهمية توحيد المفاهيم الخاصة بكل عناصر المعلوماتية و الإعتداءات الماسة بها، وتقريب الإتجاهات القانونية المختلفة حول تحديد السلوك المجرم بما يتناسب مع فكرة عالمية أنظمة المعلوماتية وجرائم الإعتداء عليها، وبما يسمح باستيعاب ما قد يجد في هذا المجال من تطور مما يلقى على عاتق أهم المؤسسات العالمية، والمحلية مثل منظمة التعاون الإقتصادي والتنمية، مجلس أوروبا، جامعة الدول العربية، وغيرها.

3- ضرورة تجريم اعتراض أنظمة المعلوماتية غير المصرح به بنصوص خاصة ومنفصلة عن تلك المتعلقة بجريمة الدخول إلى هذه الأنظمة.

4- الحاجة إلى وضع نصوص خاصة تردع إساءة استخدام كافة البطاقات الممغنطة خاصة مع تزايد أنواعها وانتشار استعمالها.

الهوامش:

1- انظر شرح هذه المفاهيم لدى عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006، ص44-80.

[2] - يمكن أن نلمس نهج المشرع الجزائري في شرحه للألفاظ الواردة في بعض القوانين ذات الطبيعة الخاصة في عدة مواضع نذكر منها على سبيل المثال القانون رقم 04-18 المؤرخ في 25-12-2004 المتعلق بمكافحة المخدرات،والقانون رقم 06-01 المؤرخ في 20-02-2006 المتعلق بالوقاية من الفساد ومكافحته(ج.ر 14مؤرخة في 08-03-2006).

[3] - أنظر أهم الإشكالات التي تعترض تضمين النصوص التقليدية عبارات تجعلها تتسع للجرائم المعلوماتية لدى:
عبد الجبار الحنيص، الإستخدام غير المشروع لنظام الحاسوب من وجهة نظر القانون الجزائي (دراسة مقارنة)، مقال منشور بمجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الأول، 2011 ،ص 202.

[4] أنظر تفصيل ذلك لدى : يونس عرب ، الإتجاهات التشريعية للجرائم الإلكترونية، ورقة عمل مقدمة إلى ورشة عمل تطوير التشريعات في مجال مكافحة جرائم المعلوماتية المقامة من قبل هيئة تنظيم الإتصالات، سلطنة عمان 2-4 أبريل 2006.

[5] - تتباين مواقف الدول فيما يتعلق بالوسيلة التي يلجأ إليها المشرع لتجريم جرائم المعلوماتية فبينما تتجه بعض الدول إلى الإضافة إلى نصوص قائمة كالولايات المتحدة الأمريكية (على مستوى الولايات) أو إلى إضافة نصوص قياسا على نصوص تقليدية كالنمسا وكندا والدانمارك والنرويج وسويسرا، تتجه دول أخرى إلى تمييز الجريمة المعلوماتية عن غيرها من الجرائم إما بوضع نص عام يتعامل مع الأوجه المختلفة لها أو بوضع مجموعة من النصوص المستقلة في قسم خاص ملحق بقانون العقوبات أو في تشريع مستقل كالولايات المتحدة الأمريكية (على المستوى الفيدرالي) وبلجيكا وفرنسا، وأخيرا اتجهت دول أخرى إلى الجمع بين أكثر من وسيلة من هذه الوسائل كهولندا والسويد وهو اتجاه بدأ في الإنتشار.

[6] - القانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات المعدل والمتمم (ج ر71 ص 11و12).

[7] - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2005، بيروت ، لبنان، ص317.

[8] - مثال ذلك الحالة التي تمكن فيها أحد الأشخاص من الدخول إلى النظام المعلوماتي الخاص بأحد المصانع المخصصة لتصنيع وتجربة الأسلحة النووية بكاليفورنيا بالولايات المتحدة الأمريكية، وقد تحمل المصنع خسائر مادية قدرت بحوالي مئة ألف دولار أمريكي وهي تكلفة الأبحاث التي أجريت لمحاولة وقف هذا الدخول غير المصرح به.
أنظر The law commission working paper N°110 computer misuse, C.L.S.R, May-June 1989-1990
مشار إليه لدى نائلة عادل محمد فريد قورة، المرجع السابق، ، ص317.

[9] - مثال ذلك إيقاف محاولة الدخول وتسجيلها إذا تعدت الشفرات الخاطئة المستخدمة عددا محددا من المرات.

[10] - يحدث كثيرا أن يترك الفاعل رسالة تشير إليه وذلك لشعوره بالفخر لنجاحه في الدخول إلى النظام المعلوماتي ويطلق على هؤلاء مرضى الحاسبات الآلية.

[11] - أنظر المادة 394 مكرر من قانون العقوبات الجزائري، المادة 1/323 من قانون العقوبات الفرنسي، المادة الأولى من القانون الانجليزي الخاص بإساءة استخدام الحاسبات الآلية لسنة 1990، المادة 1/202 من قانون العقوبات الألماني، المواد 7 و 8 من القانون البرتغالي لجرائم المعلوماتية عام 1991 ، المادة 3/370 من القانون العقوبات اليوناني، المادة 21 من القانون السويدي للمعلوماتية لعام 1973، المادة 1/138 من قانون العقوبات الهولندي، المادة 1030 (أ) من القانون الفيدرالي لإساءة استخدام الحسابات الآلية في الولايات المتحدة الأمريكية، الفقرة الثانية والرابعة من المادة 76 من قانون العقوبات الاسترالي ، المادة 1/342 من قانون العقوبات الكندي، المادة 525 من قانون العقوبات التركي، المادة 8 من الفصل السابع من قانون العقوبات الفنلندي، المادة 1/509 من قانون عقوبات لكسمبورغ، المادة 143 مكرر من قانون العقوبات السويسري، المادة 145 من قانون العقوبات النرويجي.

[12] - نائلة عادل محمد فريد قورة، المرجع السابق ص320.

[13]- تبنى هذا الاتجاه القانون الانجليزي.

[14] - ذهب إلى السير في هذا الاتجاه القانون الفرنسي.

[15]- اعتبر المشرع الأمريكي في قوانين إساءة استخدام الحاسبات الآلية لعامي 1984 و 1986 جريمة الدخول غير المصرح به نقطة البداية لأية جريمة معلوماتية أخرى.

[16] - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص360.

[17] - محمد خليفة، جرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات، دار النهضة العربية، ص 155.

[18] - آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة،الجزائر، الطبعة الأولـــى، 2006، ص 112.

[19] - نائلة عادل محمد فريد قورة، المرجع السابق، ص 349 .

[20]- ذكرت الأعمال التحضيرية لقانون العقوبات الفرنسي لسنة 1988 مثالا لهذه الجريمة تمثلت في حالات تجديد العقود الخاصة بالدخول إذا لم يتم الاتفاق بين الأطراف المعينة على هذا التجديد.

[21] - محمد خليفة، المرجع السابق، ص 157.

[22]- نائلة عادل محمد فريد قورة،المرجع السابق، ص 350.

[23] - أسامة أحمد المناعسة، وآخرون، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشـــر عمان الأردن،2001.، ص 236

[24]تسمى الموجات الكهربائية المنبعثة من النظام المعلومـــاتي باســـم (Elctromagnetic Radiation) أو (Radio Frequency interférence)، و يمكن التقاط هذه الموجات من مسافة مائتي متر تقريبا.

[25]- من الممكن جمع معلومات يتم إرسالها من خلال نظام للمعالجة الآلية للمعلومات داخل مبنى، و ذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، و تقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط بمكونات النظام، و التي تتحول إلى معلومات مقروءة على شاشة الحاسب لدى الجاني كما يمكنه تسجيلها.

[26] -" Unauthorised interception ; the interception made without right by technical means, of comunication to, from and within computer system or network",Russell G.Smith, Peter Grabosky, Gregor Urbas ,Cyber Criminals on Trial, Cambridge University Press,2004, p 100.

[27] -تنص المادة 1/430على معاقبة كل شخص يقترف عن قصد أدى باعتراض سبيل أو مقاطعة أو تدخل مع أي شخص فـــي الإستخدام القانوني للبيانات

Every one commits mischief who willfully
(C) obstructs, interrupts or interferes with the lawful use of data; or
(D) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

أنظر المادة 1/430 من قانون العقوبات الكندي على الموقع:

http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html

[28] - Every one who, fraudulently and without colour of right,
(A) obtains, directly or indirectly, any computer service,
(B) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system.

أنظر المادة 1/342 من قانون العقوبات الكندي على الموقع المشار إليه سابقا.

[29]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 352.

[30]- محمد أمين احمد الشوابكة، جرائم الحاسوب و الانترنت، دار الثقافة للنشر و التوزيع، الطبعة الأولى 2004.

[31] - نائلة عادل محمد فريد قورة، المرجع السابق، ص 501.

[32]- من أمثلة ذلك قيام مبرمج بأحد المتاجر الفرنسية بالتلاعب في النظام الخاص بالمتجر للحيلولة دون سحب قيمة البضائع التي قام بشراءها من المتجر بواسطة البطاقة الائتمانية.

[33] - the Recommendation N° R. (89) 9 on computer related crime, P 38.

34- مشار إليها لدى نائلة عادل محمد فريد قورة، المرجع السابق، ص 594.

سنتناول الاستعمال غير المشروع لبطاقات الائتمان الممغنطة في المطلب الثاني من هذا المبحث.

[35]- أنظر تفصيل تجريم هذا الفعل في قوانين الولايات الأمريكية لدى نائلة عادل محمد فريد قورة، المرجع السابق، ص 595.

[36]- نائلة عادل محمد فريد قورة، المرجع السابق، ص 603.

[37]- أنظر تفصيل أنواع البطاقات المخصصة للتعاملات المالية :

أسامة أحمد المناعسة، المرجع السابق، ص173 ، عبد الفتاح بيومي حجازي،مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص555.

[38]- مشار إلى هذه الإختلافات الفقهية تفصيلا لدى:

فتحية محمد، الحماية الجنائية لبطاقة الإئتمان ، مجلة الحقوق للبحوث القانونية والإقتصادية، ع الأول، كلية الحقوق،2003 ص15،

- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع عمان الأردن، 2004، ص64.

[39]- المادة 8 من الفصل السابع من قانون العقوبات الفنلندي.

[40]-المادة 1029(أ) من الباب الثامن عشر من القانون الفيدرالي للولايات المتحدة الأمريكية.

[41] المادة11 من القانون رقم 91-1382 الصادر في 30 ديسمبر عام 1991 المعدلة للمادة 67 من القانون الصادر في 30 أكتوبر عام 1935

42- أنظر تلك الإختلافات في الأحكام القضائية لدى: فتحية محمد ، المرجع السابق، ص 32.

[43] قانون رقم 08-01 مؤرخ في 23-01-2008 يتمم القانون رقم 83-11 المؤرخ في 02-07-1983 المتعلق بالتأمينات الإجتماعية (ج ر عدد 04 مؤرخة في 2008/01/27).